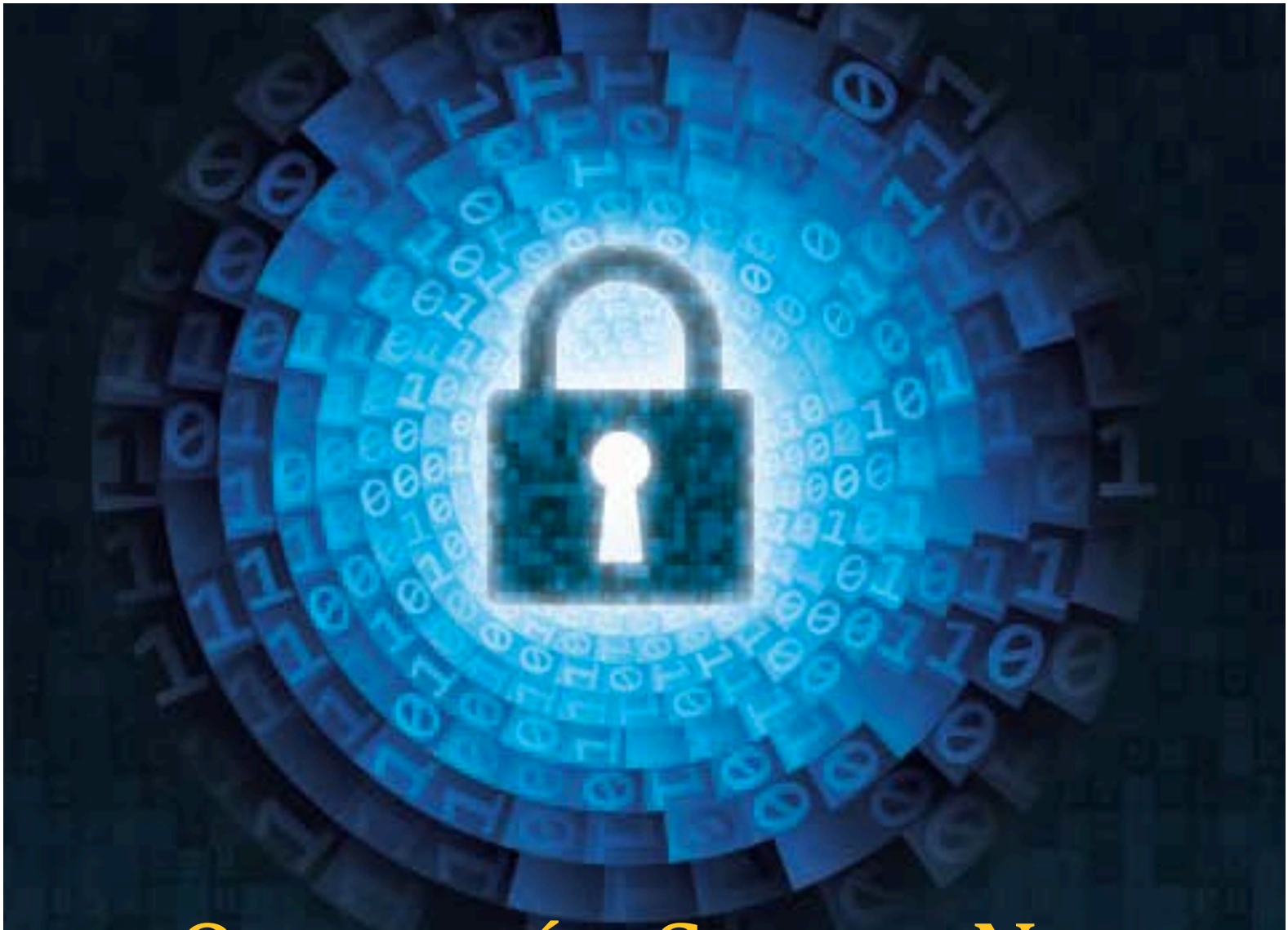


Operación Safety Net

Mejores Prácticas Recomendadas Para Enfrentar Amenazas en Línea, Móviles y Telefónicas

Preparado por

Messaging, Malware and Mobile Anti-Abuse Working Group

y

London Action Plan

1 de junio de 2015

En español

Este documento fue traducido por ICANN al español, a partir de su versión original en inglés, como un servicio a la industria

Este reporte es relativo a algunos productos comerciales como posibles soluciones a diferentes amenazas electrónicas. La mención de estos productos no constituye endoso de las organizaciones que han apoyado o contribuido a este reporte.

Preámbulo

En octubre de 2011, los miembros del London Action Plan (LAP) y el Messaging Malware Mobile Anti-Abuse Working Group (M³AAWG) realizaron una presentación ante el Comité sobre Políticas de Consumidores (CCP) de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre las perspectivas actuales de las recomendaciones antispam de la OCDE con el fin de abordar las amenazas en línea.

Durante el encuentro, un delegado canadiense del LAP advirtió que, mientras que el conjunto existente de recomendaciones sobre spam de la OCDE tenía una alta tasa de éxito en la movilización de industrias y gobiernos para que accionen en el abordaje de la problemática del spam, sería de gran ayuda lograr una mejor comprensión sobre la nueva generación más sofisticada de amenazas en línea. Sobre la base del seguimiento inicial con el delegado canadiense del CCP y el presidente del CCP, el Organismo Nacional de Coordinación Antispam del Ministerio de Industria de Canadá preparó el borrador de un informe que será redactado por miembros voluntarios del M³AAWG y del LAP. Este borrador se presentó y obtuvo el acuerdo de los miembros del M³AAWG y del LAP y fue revisado por la Secretaría del CCP.

El 6 de junio de 2012, los miembros del LAP y del M³AAWG se reunieron en Berlín para dar inicio al desarrollo del informe que se publicó en octubre de ese mismo año. En la actualidad, tres años más tarde, este informe ha sido actualizado para que refleje el cambiante panorama y los nuevos medios que utilizan los ciberdelincuentes para ser exitosos y evitar ser identificados.

El informe original se dividió en cuatro secciones clave:

i) Malware y botnets;
ii) ISP y DNS;
iii) Phishing e ingeniería social; y
iv) Amenazas móviles.

Esta segunda versión del informe ha actualizado las cuatro secciones originales y cubre nuevas áreas, como fraude por telefonía de voz y por voz sobre IP (VoIP), suplantación de identificadores de llamadas, cuestiones de abuso en cuanto a servicios de hosting y en la nube, y acoso en línea.

La actualización del informe sobre las mejores prácticas recomendadas involucró una invitación a los miembros del M³AAWG y del LAP a colaborar con el informe. Se designaron expertos de la industria como guías de cada sección que a su vez buscaron aportes y contribuciones de expertos que no eran miembros del M³AAWG ni del LAP. Al final de este informe, se encuentra una lista de los colaboradores.

El M³AAWG, el LAP y la Coalition Against Unsolicited Commercial Email (CAUCE) le han brindado su respaldo oficial a este informe. Además, los colaboradores agradecerán los comentarios sobre el informe de la OCDE, el CCP, el Grupo de Trabajo sobre Privacidad y Seguridad de la Información (WPISP) y del Comité sobre Información, Comunicaciones y Política Informática (ICCP). Cuando corresponda, los colaboradores también agradecerán el aporte de otros foros sobre esta iniciativa.

ÍNDICE

Operación Safety Net 1
Mejores prácticas recomendadas para enfrentar amenazas en línea, móviles y telefónicas... 1
Resumen ejecutivo 7
Malware y botnets 7
Phishing e ingeniería social 8
Ataques al protocolo de Internet y al Sistema de Nombres de Dominio 8
Amenazas móviles, telefónicas y de voz sobre IP (VoIP) 9
Servicios de hosting y en la nube 10
Conclusión 11
Introducción: La evolución de las amenazas en línea 12
Malware y botnets 14
El Panorama Actual de las Amenazas A Través de Botnets y Malware 15
El Panorama Futuro de las Amenazas A Través de Botnets y Malware 16
Las Mejores Recomendaciones Para Abordar el Malware 16
Las mejores prácticas para educadores y usuarios 17
A) Mejores prácticas: Prevención 17
B) Mejores prácticas recomendadas: Detección 18
C) Mejores prácticas recomendadas: Remediación 19
Las Mejores prácticas recomendadas para el gobierno y la industria 19
Phishing e ingeniería social 26
El daño para los consumidores y la industria 26
El panorama del phishing 27
Los objetivos de los ataques de phishing: Qué buscan 27
Línea de tiempo de una típica campaña de phishing 29
Evolución de los métodos de ataque 30
El aumento en el desarrollo de los ataques de phishing 31
Las mejores prácticas recomendadas contra el phishing y la ingeniería social 33
Referencias 39
Estadísticas 39
Programas a nivel de usuario 40
Presentacón de informes sobre Phishing: 40
Las mejores prácticas recomendadas 42

Nombres de dominio y direcciones IP 43
Descripción general sobre tecnología 43
Direcciones IP 43
El Sistema de Nombres de Dominio 44
Ataques Contra el DNS 44
Envenenamiento de la Memoria Caché 44
Mejores prácticas recomendadas: 45
Malware que Ataca al DNS 46
Mejores prácticas recomendadas: 46
Ataques Contra Los Servicios de Registro de Nombres de Dominio 47
Mejores prácticas recomendadas: 48
Ataques a la web y a otros DNS de servidores 50
Mejores prácticas recomendadas: 50
Ataques a direcciones IP 51
Suplantación de direcciones IP 51
Mejores prácticas recomendadas: 51
Anuncios deshonestos 52
Mejores prácticas recomendadas: 52
Robo de rangos de direcciones 52
Mejores prácticas recomendadas: 52
Referencias 52
Amenazas móviles y de voz 54
El entorno móvil 54
Mercados de aplicaciones 54
Amenazas específicas y las mejores prácticas recomendadas 54
Seguridad de los Mercados de Aplicaciones 54
Las mejores prácticas recomendadas sobre las tiendas de aplicaciones para el gobierno y la industria: 56
El malware móvil 57
Las mejores prácticas recomendadas para la industria y el gobierno para evitar el malware móvil: 58
Amenazas mixtas 59
Modificación de dispositivos móviles 60
Jailbreaking de un dispositivo 60
Rooting de un dispositivo 60
Desbloqueo de un dispositivo 60

Las mejores prácticas recomendadas a un individuo sobre la modificación de dispositivos móviles: 61
Las mejores prácticas recomendadas para la industria y el gobierno en relación con la modificación de dispositivos móviles: 61
Amenazas de banda base 61
Las mejores recomendaciones para la industria y el gobierno para evitar las amenazas de banda base: 62
El modelo comercial de tarifa elevada: 62
Las mejores recomendaciones para a industria y el gobierno para evitar las estafas mediante los servicios de tarifa elevada: 64
Spam móvil 64
Las mejores recomendaciones para la industria y el gobierno para evitar el spam móvil: 65
El aumento de los ataques internacionales 66
Consideraciones internacionales 67
El costo de las investigaciones internacionales 68
Las mejores recomendaciones para el gobierno y la industria de acuerdo con cuestiones de colaboración cruzada: 68
Amenazas telefónicas de voz 69
El entorno de la telefonía de voz 69
Amenazas por VoIP 70
Llamadas automatizadas 70
Las mejores prácticas recomendadas para combatir las llamadas automatizadas: 71
Ataques telefónicos por denegación de servicio (TDoS) 73
Las mejores prácticas recomendadas sobre TDoS: 74
Suplantación de llamadas 74
Las mejores prácticas recomendadas para prevenir la suplantación de llamadas: 75
Servicios de hosting y en la nube 76
Tipos de hosting 76
Formato de la infraestructura de Internet: 76
Categorías de infraestructura de Internet 77
El escenario de las amenazas 79
Principales áreas de interés 80
Las mejores recomendaciones 82
Acoso en línea 86
Conclusión 89
Glosario 90
Referencias 92
End Notes 93
Steering Committee/Contributors/Participants 96

RESUMEN EJECUTIVO

Este informe brinda a sus lectores una descripción en lenguaje simple de las amenazas que enfrentan los negocios, los proveedores de redes y los consumidores en el entorno móvil y en línea. Como muchos de nosotros sabemos, las tecnologías móviles y de Internet han sido el impulso clave de la economía global en los últimos veinte años. Estas tecnologías tienen un impacto sobre casi todos los aspectos de nuestra vida diaria y se han incorporado también en casi todos los modelos comerciales y cadenas de suministro. Debido a la incorporación de los equipos portátiles, los teléfonos inteligentes y las tabletas a nuestra vida personal y laboral, nuestra dependencia de estos dispositivos también se ha incrementado. Utilizamos los dispositivos para conectarnos con la familia y los amigos, para comprar y realizar operaciones bancarias en línea, relacionarnos con colegas y socios comerciales, reestructurar cadenas de suministro y ofrecer productos directamente desde la fábrica a los locales de venta al público.

Con la creciente dependencia del sector comercial y del consumidor, y la rápida migración de las transacciones comerciales a las plataformas móviles y en línea, aparecen las amenazas de los ciberdelincuentes. Los ciberdelincuentes sacan provecho del envío de spam, del phishing, de la introducción de malware en sitios web, de la propagación de botnets, del redireccionamiento de tráfico de Internet hacia sitios web maliciosos, de la apropiación de servicios de hosting y en la nube, y de la inserción de spyware en computadoras y dispositivos móviles.

No es fácil calcular el impacto económico de estos ataques continuos, ya sea por país o en una escala mundial, dado que las pérdidas producidas por la ciberdelincuencia con frecuencia no se informan o se minimizan por parte de las víctimas, las instituciones financieras que cubren los gastos derivados de las pérdidas o las empresas que afrontan los costos, incluyendo costos de defensa y remediación hasta costos por caídas de servicios debido a ataque.

El objetivo principal de este informe no es sólo estudiar las amenazas frente a los entornos en línea, móvil y de VoIP que amenaza a consumidores, empresas y gobiernos todos los días, sino, lo que es más importante, sugerir las mejores prácticas recomendables para que la industria y los gobiernos puedan abordar estas amenazas. El enfoque del informe apunta a cinco áreas principales:

MALWARE Y BOTNETS

El malware y las botnets se incluyen entre las amenazas más graves a la economía de Internet. El software malicioso o "malware" es creado o utilizado por los delincuentes para afectar operaciones informáticas, recolectar información confidencial o acceder a sistemas informáticos privados. Las botnets son grupos de equipos infectados con malware que se comunican y se coordinan entre sí (con frecuencia mediante una red compleja de equipos infectados) y que recojen información sobre cada dispositivo infectado de manera individual. Las botnets maximizan la impactante capacidad del ancho de banda y potencia informática que significa controlar más de un millón de dispositivos.

Los delincuentes continuamente cambian o "transforman" el malware para evitar que sea descubierto y eliminado. En consecuencia, la mayoría de los antivirus (AV) enfrentan la dificultad de tener que identificar amenazas nuevas y recientes. Cada vez son más las formas de malware que tienen la habilidad de detectar que están siendo monitoreados mientras se ejecutan, posiblemente por parte de un investigador que realiza análisis de código malicioso, y alterar sus características para lograr que los expertos en malware no logren detectar o analizar sus funciones. Algunas clases de malware

incluso realizarán un contraataque al intento de vigilancia y análisis mediante un ataque DdoS (denegación distribuida de servicios).

En consecuencia, cada vez se vuelve más difícil para el entorno de seguridad en línea seguirle el ritmo a las amenazas de malware.

PHISHING E INGENIERÍA SOCIAL

El phishing involucra técnicas que utilizan actores maliciosos para hacer que una víctima revele información financiera, comercial o personal que es confidencial.

El phishing ha avanzado ininterrumpidamente en cuanto a frecuencia, sofisticación y perjuicio provocado desde sus inicios como amenaza a mediados de la década de los noventa y no muestra signos de reducción. De hecho, el phishing ha estado en alza desde 2011, y casi el 25 % de los destinatarios abren los correos electrónicos con phishing y más del 10 % hacen clic en archivos adjuntos maliciosos. Asimismo, el tipo de información que busca el phishing aumenta su valor cada vez más: desde un simple acceso a una cuenta de correo electrónico o a una cuenta bancaria que provocan pérdidas individuales en miles de dólares, hasta objetivos de gran valor.

Los objetivos de gran valor, concretamente cuentas comerciales que poseen un secreto comercial o brindan privilegios especiales a cuentas bancarias y financieras, han sido atacados en repetidas ocasiones y con gran frecuencia, situación que produce pérdidas catastróficas, financieras y de propiedad intelectual, en un mismo evento de cientos de millones de dólares; un número incalculable de estos eventos ocurre todos los años.

Aunque el phishing no es una novedad, el aumento en la cantidad, en los objetivos y en la sofisticación de los ataques en los últimos años representa una amenaza más fuerte para las compañías, los gobiernos y los consumidores y también destruye la confianza general en la economía digital. Se deben coordinar defensas para lograr soluciones transparentes y abiertas con varios grupos de interés para maximizar la eficacia, minimizar los costos e incrementar la confianza.

ATAQUES AL PROTOCOLO DE INTERNET Y AL SISTEMA DE NOMBRES DE DOMINIO

Diferentes clases de actividades ilegales atacan las vulnerabilidades asociadas al Sistema de Nombres de Dominio (DNS) y las direcciones de protocolo de Internet (IP). Los ataques más graves al DNS son el ataque de resolutores o el envenenamiento de la memoria caché, en los que los delincuentes introducen datos falsos para redireccionar el tráfico en Internet hacia la versión falsa de un sitio web de popularidad.

Todo equipo con Internet posee una dirección IP, que se utiliza para identificarlo, de la misma manera que se identifica a un aparato telefónico mediante un número de teléfono. Las direcciones IP tradicionales, llamadas direcciones IPv4 (Protocolo de Internet versión 4), son cifras binarias de 32 bits, escritas como cuatro números decimales, por ejemplo, 64.57.183.103. La primera porción de la dirección, en este caso 64 57 183, con frecuencia identifica la red; el resto, en este caso 103, al equipo ("host") en la red. La división entre la red y el host varía según el tamaño de la red, por lo que el ejemplo anterior es simplemente típico. Dado que el hombre difícilmente recuerde la

dirección IP y está atado a una red física, el DNS es una base de datos distribuida de nombres que le permite a los usuarios utilizar nombres como www.google.com en lugar de su dirección IP 173.194.73.105.

A pesar de su enorme tamaño, el DNS posee un rendimiento excelente mediante la delegación y las memorias caché. Las más serias vulnerabilidades en el DNS se encuentran al nivel de los resolutores y se conocen como envenenamiento de la memoria temporal (cache poisoning), en la que los delincuentes alteran la información de resolución de nombres de dominio con el fin de redirigir el tráfico de Internet hacia sitios web falsos -controlados por los delincuentes mismos- que copian sitios web populares.

Cada computador en Internet tiene una dirección IP, que es utilizada para identificar ese dispositivo de una forma similar a como los teléfonos son identificados por los números telefónicos. Las direcciones IP tradicionales, conocidas como IPv4 (Internet Protocol version 4), son números compuestos por 32 bits binarios, representados por cuatro números decimales, como 64.57.183.103. La primera parte de la dirección, en este caso 64.57.183, identifica la red y el resto, en este caso 103, identifica el dispositivo en particular (el host) en la red. Esa división entre red y host varía dependiendo del tamaño de la red, siendo este ejemplo mencionado bastante típico. Puesto que las direcciones IP son difíciles de recordar para los humanos, y puesto que están atadas a redes físicas, el DNS es una base de datos distribuida que incluye nombres y que permite a las personas usar nombres como www.google.com en lugar de la respectiva dirección IP 173.194.73.105.

A pesar de su enorme tamaño, el DNS opera de manera muy eficiente puesto que utiliza delegaciones y memorias temporales. Es decir, diferentes organizaciones son responsables de su parte del DNS y los dispositivos de los usuarios recuerdan los resultados de DNS que han recibido. Puesto que no sería práctico almacenar todos los nombres en el DNS en una única base de datos, el sistema se divide en zonas que son almacenadas en diferentes servidores, lógicamente vinculados entre sí para crear una inmensa base de datos inter-operable y distribuida.

Las vulnerabilidlades en las direcciones IP y en el DNS incrementan el riesgo para los consumidores porque en muchos casos no saben que han sido redirigidos a un sitio falso, no al sitio al que ellos de verdad querían acceder.

AMENAZAS MÓVILES, TELEFÓNICAS Y DE VOZ SOBRE IP (VOIP)

Con el advenimiento de los teléfonos inteligentes y el mercado de aplicaciones para dispositivos que utilizan Android, Apple, Windows y Blackberry, el entorno del comercio electrónico se ha ampliado y ahora incluye a los dispositivos móviles. Dado que los consumidores migran sus actividades de comercio electrónico a las plataformas móviles, los delincuentes que buscan aprovecharse y defraudar rápidamente se adaptan. Además, el entorno móvil crea oportunidades únicas para los nuevos tipos de ataques y amenazas dirigidas tanto a consumidores como a empresas.

Los dispositivos móviles les proporcionan a los consumidores una mayor funcionalidad y facilidad de uso. Los usan con frecuencia usuarios individuales, que por lo general los mantienen en un estado activo, a menudo con el GPS habilitado y son *location aware* (los dispositivos mismos conocen su ubicación). Por lo tanto, los dispositivos móviles poseen un mayor atractivo inherente para un ataque malicioso.
En los últimos años, el entorno móvil ha sufrido un crecimiento en el desarrollo de malware, las primeras botnets móviles, un aumento en estafas por mensaje de texto (SMS) de tarifa elevada y

ataques sofisticados que se han asociado con el jailbreaking (modificación del sistema operativo que permite la descarga de aplicaciones desde cualquier lugar, no sólo la desde la tienda de aplicaciones que ofrece un nivel de seguridad y confianza) de dispositivos móviles.

Con el aumento en las suscripciones a la banda ancha móvil, las amenazas telefónicas de voz y de VoIP también registran un crecimiento. La frecuencia y la gravedad de las estafas por llamadas automatizadas aumentan, y la nueva tecnología que les permite a los delincuentes ocultarse o cambiar sus números de teléfono salientes para engañar a objetivos confiados hace que el fraude sea más efectivo. A medida que una mayor cantidad de servicios de telefonía se transforman en servicios en línea, los ataques por denegación de servicio de telefonía (TDoS) también aumentan en cantidad y frecuencia. Este tipo de ataques puede ser devastador cuando el blanco son servicios esenciales, porque logra que los sistemas telefónicos colapsen y que las llamadas de individuos legítimos que intentan comunicarse, por ejemplo con el Departamento de Bomberos o con una ambulancia, no lleguen a destino.

Los ciberdelincuentes tienen una fuerte preferencia para operar en un entorno internacional, lo que complica aún más la aplicación de la ley. Por ejemplo, un vendedor en línea de medicamentos ilegales que vive en los Estados Unidos podría enviar un spam con publicidad de sus medicamentos desde un equipo afectado en Brasil, que dirige a sus potenciales compradores a un sitio web con un nombre de dominio ruso, mientras que físicamente el servidor de ese sitio web está ubicado en Francia. El pago de la compra con tarjeta de crédito se podría procesar a través de un banco en Azerbaiyán, el pedido podría ser enviado en barco desde un sitio en la India y el ingreso podría ser canalizado hacia un banco en Chipre. Los delincuentes saben que al actuar de esta manera existen muchos factores que complican las investigaciones oficiales de sus delitos en línea y reducen su probabilidad de captura. Estos factores son la falta de colaboración, las diferencias entre jurisdicciones y el costo de las investigaciones internacionales.

SERVICIOS DE HOSTING Y EN LA NUBE

"Hosting" se refiere a proveedores de servicios que brindan acceso comercial a sitios web, archivos e intranet, y acceso a Internet a través de múltiples servidores conectados en lugar de un servidor único o virtual. Los hosts son empresas que proporcionan espacio en un servidor propio o concesionado para que sus clientes lo usen; también pueden proporcionar espacio de centro de datos y conectividad a Internet. Los servicios de hosting más básicos son el hosting web y de archivos de menor tamaño. Muchos proveedores de servicios Internet (ISP) ofrecen este servicio gratis a los suscriptores. Estos hosts controlan los principios básicos que hacen al funcionamiento de Internet y pueden operar como empresas unipersonales o internacionales de Internet.
La computación en la nube comprende el almacenamiento y acceso a datos y programas mediante la Internet en lugar de utilizar un disco duro local. La "nube" es simplemente una metáfora de la Internet. Se remonta a cuando existían los diagramas de flujo y las presentaciones que representarían la gigantesca infraestructura de Internet tipo "granja de servidores" como una nube blanca y pomposa.

Las amenazas móviles y en línea que atacan servicios de hosting y en la nube están en aumento e incluyen el spam, el spamvertising, el phishing, los sitios web pirateados, ataques por DDoS, la exploración de puertos para localizar vulnerabilidades, páginas web desfiguradas, infracción de derechos de autor/marcas registradas y malware. Este documento clasifica los tipos de hosting y

define las áreas de interés. Proporciona un análisis del panorama actual de las amenazas en la nube y en línea, y un breve recorrido por los métodos de corrección que se utilizan para abordar estas cuestiones críticas.

CONCLUSIÓN

Con el fin de proteger la Internet y garantizar su promesa frente a los ciudadanos del mundo, es fundamental que identifiquemos respuestas eficientes y efectivas a todas estas amenazas. Este informe, presentado por un grupo internacional de expertos de la industria y del gobierno, resume las mejores prácticas recomendadas para enfrentar estas nuevas y más sofisticadas amenazas en línea, móviles y telefónicas. Esperamos que este informe facilite la colaboración permanente y efectiva entre este grupo y la comunidad internacional para combatir estas amenazas.

INTRODUCCIÓN:
LA EVOLUCIÓN DE LAS AMENAZAS EN LÍNEA

Desde 2006, la economía mundial móvil y de Internet ha sufrido el desarrollo de las amenazas en línea y la aparición de nuevos ataques. Hoy en día, las herramientas utilizadas para defraudar y robar información en el entorno móvil y en línea son cada vez más sofisticadas, y les ofrecen a los delincuentes y los estafadores una variada caja de herramientas.

En este contexto, como probablemente sus padres le han dicho más de una vez, mejor prevenir que curar. Este informe no sólo describe el entorno de las amenazas en línea, móviles y telefónicas de manera tal que cualquier persona pueda entenderlo, sino que proporciona una lista de herramientas a la industria y los gobiernos para que las adopten como las mejores prácticas recomendadas y eviten que este tipo de amenazas se conviertan en ciberataques exitosos.

Mientras que gran parte de esta ilícita actividad en línea se neutraliza antes de que llegue al usuario final típico gracias a las técnicas de bloqueo y filtrado aplicadas en la actualidad, el spam sigue siendo un vehículo importante, que con frecuencia transporta una carga malintencionada así como correos electrónicos no deseados y a menudo maliciosos. El spam no es sólo un fenómeno asociado al correo electrónico. Se expande a diferentes tipos de nuevos medios. Por ejemplo, el spam por mensajería móvil y VoIP en la actualidad es frecuente, así como también los comentarios no deseados (*spam comments*) en redes sociales, blogs y sitios web, y las entradas no deseadas que contaminan y degradan la calidad de los resultados de la búsqueda en motores de búsqueda en línea.

La industria de los nombres de dominio (que consiste principalmente en ICANN), los registradores y los registros pueden tener un rol crítico en la esfera antiabuso, en particular dado que los nuevos protocolos de Internet (por ejemplo, IPv6) se vuelven más prevalentes, y se lanza un número considerable de nuevos dominios de alto nivel (TLD). Tradicionalmente, existían aproximadamente 24 TLDs, por ejemplo .com, .org, .net, .gov, además de los TLD de dos letras para país, por ejemplo, .ca para Canadá o .jp para Japón. Recientemente, ICANN lanzó más de 500 nuevos TLD genéricos, que incluyen .bike, .city y .clothing y hay cientos más en proceso de ser lanzados.

Recomendamos que los participantes de la OCDE y otras organizaciones internacionales fortalezcan su colaboración en la principal entidad coordinadora en la esfera de los dominios, el Consejo Asesor Gubernamental (GAC) de ICANN, trabajando para alentar a ICANN a redoblar sus esfuerzos en el área de cumplimiento contractual y supervisión de los registros y registradores.

Se han realizado muchos esfuerzos para romper barreras y facilitar acciones colaborativas entre empresas, ONG, gobiernos, entidades reguladoras y organismos del orden público. La OCDE, el LAP, el M^{3}AAWG y otras organizaciones internacionales han tenido éxito en el desarrollo de una coordinación pública-privada existente y mayor colaboración entre los diferentes sectores. Por ejemplo, el Grupo de Trabajo para DNS Changer[i] y el Grupo de Trabajo para Conficker[ii] son amalgamas de expertos en la materia, organismos de orden público y representantes de la industria que han tenido un notable éxito basado en un modelo de confianza mutua que deja de lado las cuestiones competitivas. Esta colaboración ha sido un enorme acierto y seguirá siendo fundamental a la hora de realizar esfuerzos antiabuso.

Sin embargo, sigue existiendo la necesidad de tener una legislación antiabuso y antispam más sólida, más completa e independiente de la tecnología y regímenes regulatorios que faciliten la colaboración entre países. Parte de la solución reside en el ámbito diplomático, en particular, cuando se trata de permitir acciones internacionales de orden público más efectivas. Una mejora considerable en la educación y la concientización del usuario final es una cuestión importante en la toma de medidas eficaces antiabuso.

MALWARE Y BOTNETS

El software malicioso o "malware" es creado o utilizado por los delincuentes para afectar operaciones computacionales, recolectar información confidencial o acceder a sistemas informáticos privados. Se puede presentar en distintos formatos, desde programas compilados hasta secuencias o fragmentos de código insertados en un software por lo demás legítimo. "Malware" es un término general utilizado para definir un conjunto de formatos de software hostil, invasivo o fastidioso. En general, el malware comprende virus, gusanos, troyanos, instaladores, spyware, adware, rootkits, spamware y otros programas maliciosos. El malware está generalmente diseñado para cumplir una o más funciones, desde facilitar la introducción de otro tipo de malware (por ejemplo, instaladores/descargadores de troyanos) hasta la recopilar información (por ejemplo, spyware). Otras formas de malware se pueden especializar en la interrupción de equipos, usuarios y redes.

Las botnets son grupos de equipos infectados con malware que se comunican para coordinar entre sí y recolectar información acerca de los dispositivos comprometidos. Las botnets con mayor frecuencia reciben el nombre del malware específico utilizado para infectar y reclutar dispositivos, por ejemplo, Zeus y SpyEye. Sin embargo, todos los equipos que componen una botnet pueden contener diferentes componentes de un malware. Por ejemplo, un nodo de botnet Zeus puede contener el malware Zeus (que maneja la comunicación del botnet, roba información y descarga otras formas de malware), así como otras amenazas, como el spamware (por ejemplo, Cutwail) o componentes de "ataque" (como el malware Pushdo DDoS).

Las botnets pueden ser de gran tamaño. Se han observado botnets compuestos por más de un millón de equipos bajo el control de un solo botmaster. Sin embargo, no es necesario que una botnet tenga un tamaño similar a este para ser extremadamente perjudicial. Incluso una botnet compuesta por 1000 o 2000 nodos (equipos) puede causar un enorme caos.

En sus comienzos, el malware era desarrollado con frecuencia por "aficionados": entendidos en computación que buscaban desafíos o diversión. Desde ese momento, los delincuentes, y el crimen cada vez más organizado, se han dado cuenta de que pueden ganar mucho dinero con el malware. Un ejemplo es el caso de WinFixer, en el que los delincuentes amedrentaron a sus víctimas haciendo que realizaran pagos por registro de software[iii]. Hoy en día, prácticamente todas las formas de malware se crean y utilizan con fines delictivos. En menor medida, el malware puede también estar financiado por el Estado y ser utilizado por agencias de inteligencia para llevar a cabo acciones encubiertas contra sistemas informáticos de otros estados o para espiar activistas, periodistas y disidentes; asímismo, puede ser utilizado por hacktivistas y extremistas con fines ideológicos, políticos o sociales.

El malware es una de las principales amenazas para la economía de Internet y se utiliza para llevar a cabo las siguientes actividades:

- Recopilar información personal y comercial mediante:
    - la captura de las pulsaciones de teclas;
    - la recopilación de inicios de sesión y contraseñas;
    - la copia de libretas de direcciones;
    - el robo de información, documentación y/o secreto comercial que es confidencial, o incluso la captura de información gubernamental o militar confidencial;
    - la recopilación de información bancaria y transaccional.

- Facilitar grandes ataques de DDoS patrocinados por gobiernos,o como forma de activismo político o como un preludio a la extorsión, entre muchos otros fines.
- Enviar spam por correo electrónico, SMS y otros medios.

Los delincuentes modifican el malware continuamente para evitar la detección y la remediación. La mayoría de las herramientas de software antivirus (AV) tiene poca capacidad de identificar amenazas actuales y recientes. Cada vez son más las formas de malware que tienen la habilidad de detectar que están siendo monitoreados "vigilando" (posiblemente por parte de un analista de malware) y alterar su comportamiento para lograr que los analistas no puedan determinar su funcionamiento. Algunas clases de malware incluso intentan desalentar esas labores de monitoreo mediante la realización de ataques de DdoS dirigidos contra los analistas de seguridad. Por todo esto, cada vez es más difícil para la comunidad de seguridad en línea seguir el ritmo con el que evoluciona el entorno de las amenazas por malware.

EL PANORAMA ACTUAL DE LAS AMENAZAS A TRAVÉS DE BOTNETS Y MALWARE

El panorama no ha cambiado y es poco probable que lo haga. La reticencia general de los gobiernos, los bancos y las corporaciones a compartir datos privados o confidenciales, obstaculizada por barreras legales y regulatorias reales o percibidas o un miedo a la responsabilidad, significa que los creadores de malware aún conservan el control cuando se trata de la capacidad de brindar con precisión su producto. No es posible calcular exactamente la magnitud de la cuestión, dado que no existen indicadores generalmente aceptados para las infecciones por malware, bots o botnets.

En el malware transmitido por correo electrónico, el correo electrónico poco convincente con errores de ortografía ha sido sustituido por nuevas técnicas de phishing, que se discuten más adelante en este informe. Aunque el volumen global de spam ha disminuido en los últimos años, en la actualidad las redes sociales utilizan cada vez más técnicas como "clickjacking" o "likejacking" en las que el usuario hace clic en un enlace a un sitio web para ver un video tentador y el atacante utiliza ese clic para publicar un comentario visible a todos los amigos de Facebook del usuario, que los tienta a hacer clic en el mismo enlace malicioso. Facebook ha contrarrestado en gran parte este ataque mediante una solicitud al usuario para que confirme un "Me gusta" antes de su publicación si el usuario está haciendo clic en un dominio que no es confiable.

En términos de malware transmitido por la Web, Symantec descubrió que en 2013 los ataques a través de la Web habían aumentado un 23 % más que en 2012 y que 1 de 8 sitios web mostraba una vulnerabilidad crítica.[iv] Esto indica que los atacantes intentan evadir las operaciones a favor de la seguridad haciendo que los sitios web dispersen el malware, en lugar de adjuntarlo a los correos electrónicos como forma de infección.

Las amenazas contra los sistemas operativos iOS y Apple OSX, aunque sean relativamente pocas en cantidad, representan la propagación del malware hacia plataformas que hasta ahora casi no habían sufrido ataques de malware. Los medios de ataque son similares a los observados en las

plataformas Windows y Android. El hecho de que muchas herramientas de ataque han cruzado entre diferentes plataformas, haciendo uso de los ataques de Java, por ejemplo, es en sí mismo un nuevo método de propagación de malware.

EL PANORAMA FUTURO DE LAS AMENAZAS A TRAVÉS DE BOTNETS Y MALWARE

De acuerdo con el informe "Predicciones sobre Amenazas" de McAfee[v], el malware móvil será el motor de crecimiento de la innovación técnica y del volumen de ataques en el "mercado" mundial del malware en 2015. Los ataques con ransomware malicioso ocurren cada vez más, impulsados por el aumento de la moneda virtual. Asímismo, se espera el despliegue de un número creciente de aplicaciones corporativas basadas en la nube, que tendrán como consecuencia la expansión de las superficies de ataque frente a las que los delincuentes dirigirán sus actividades.

Por último, es difícil concebir la gran cantidad de otras amenazas de mayor importancia en los próximos años que la que plantea la Internet de las cosas. Como miles de millones de dispositivos se conectan a Internet, habrá un número creciente de amenazas a la infraestructura fundamental que representan los dispositivos sin parches o con una vulnerabilidad inherente. Es probable que muchos dispositivos conectados no reciban los parches de seguridad regulares; algunos proveedores no considerarán la seguridad como parte de su responsabilidad, ya que priorizan la próxima versión del producto y se enfocan más en las características estéticas o prácticas.

Es posible que los consumidores no ejerzan presión sobre los proveedores de equipos para obtener los parches de seguridad. Si, por ejemplo, un dispositivo funciona satisfactoriamente como una nevera, una bombilla eléctrica o u termostato, pero tiene un problema de seguridad con su ciberfuncionalidad, los consumidores pueden no demostrar una motivación para reemplazarlo sólo por motivos de seguridad. En consecuencia, la larga cola de dispositivos inseguros seguirá creciendo.

LAS MEJORES RECOMENDACIONES PARA ABORDAR EL MALWARE

Aunque gran parte de lo que trata esta sección hace hincapié en educar a los individuos y a los ISPs, se debe reconocer que el abordaje del malware es un problema de todo un ecosistema que requerirá un enfoque multifacético y acciones de diferentes grupos, que no se limita a los ISPs o a educar a los usuarios finales.

Para gobiernos y educadores, esta sección se centra en la prevención, detección y remediación de malware. Para los ISPs, esta sección se centra en brindar asesoramiento en relación con lo que un ISP puede hacer para colaborar con un individuo en la detección de malware. La sección concluye con un análisis forense sobre el malware en las áreas legales y regulatorias de los gobiernos, así como prácticas usuales de la industria.

LAS MEJORES PRÁCTICAS PARA EDUCADORES Y USUARIOS

A) Mejores prácticas: Prevención

Estas recomendaciones apuntan a cómo un individuo puede prevenir una infección con malware.

1. **Elegir un sistema operativo seguro y actual**: Al elegir un sistema operativo (SO), busque uno que haya demostrado ser capaz de reducir su exposición al malware. Independientemente del sistema operativo que elija, asegúrese de ejecutar la versión más reciente. Los sistemas operativos modernos tienen defensas integradas que ayudan a combatir ataques de malware que comprometen el sistema.
2. **Mantener al día los parches y las actualizaciones**: Asegúrese de que los sistemas operativos y todas las aplicaciones, por ejemplo las aplicaciones de asistencia (Acrobat Reader, Flash Player, Java y QuickTime), contengan los últimos parches disponibles (es decir, que se hayan descargado todas las actualizaciones a medida que estuvieran disponibles). En la mayoría de los ataques causados por malware, los parches disponibles tenían más de un año. En los sistemas que ejecutan Microsoft Windows, Microsoft pone a su disposición una serie de descargas recomendadas.[vi] Secunia PSI[vii] es también una popular herramienta que puede ayudarlo a mantener actualizadas las aplicaciones de terceros.
3. **Utilizar sólo lo necesario**: En general, lo mejor es descargar o utilizar solamente el software necesario para realizar sus tareas. Evite descargar software o archivos que no aportan características o funciones útiles o necesarias, y elimine el software sin uso.
4. **Buscar ayuda de expertos**: Consúlteles a los expertos cuál es la mejor opción para sus necesidades. (Los "expertos" pueden responder de diferentes maneras, pero si usted confía en ellos a la hora de obtener asistencia, hacer lo que ellos le digan será casi siempre mejor en sus circunstancias).
5. **Ejecutar un programa antivirus**: Aunque los productos antivirus no son perfectos, lo pueden ayudar de todas formas, por lo que seleccione uno, utilícelo y manténgalo al día mediante la descarga de actualizaciones cuando así le sea indicado. Programe un análisis completo del sistema una vez por semana como mínimo. Asegúrese de seleccionar un antivirus real y evite ser engañado a instalar un antivirus falso que es ¡el mismísimo malware! (Y si su antivirus no protege también contra el spyware, también deberá instalar un antispyware).
6. **Utilizar un firewall**: Aunque no son infalibles, los firewall para hardware o software al menos añadirán potencialmente otra capa de protección.
7. **Utilizar contraseñas seguras**: Las contraseñas deben tener la suficiente complejidad para resistir ser descifradas o violadas. Algunas personas eligen contraseñas que tienen como mínimo ocho caracteres de longitud y mezclan mayúsculas, minúsculas, números y símbolos especiales. Otros prefieren seleccionar entre tres y cinco palabras no relacionadas que son más fáciles de recordar, pero que a su vez dificultan el trabajo de las herramientas de software que las descifran. De cualquier manera, nunca utilice la misma contraseña en diferentes sitios. Las aplicaciones de contraseñas facilitan este proceso.[viii]
8. **Realizar copias de seguridad de forma regular**: Si el sistema se infecta, tener una copia de seguridad limpia puede ser de gran utilidad a la hora de desinfectarse y volver a estar en línea.

9. **Eliminar archivos temporales innecesarios**: Algunas clases de malware pueden ocultar copias propias entre los archivos temporales, e incluso si no hay archivos temporales infectados, la eliminación de los archivos temporales acelerará los análisis del sistema y reducirá el tamaño de las copias de seguridad. Una herramienta muy utilizada para la limpieza de archivos temporales en las plataformas Windows es CCleaner.
10. **No ejecutar como administrador de forma rutinaria**: Las cuentas "Administrador", "raíz" y otras que tienen funciones especiales sólo se deben utilizar cuando esté haciendo algo que requiera los privilegios especiales asociados a las cuentas de gran capacidad (por ejemplo, la instalación intencional de un nuevo software). Cuando esté haciendo tareas habituales, ejecute el sistema como un usuario normal.
11. **Desactivar JavaScript (o utilizar NoScript)**: JavaScript (un lenguaje de programación que no está relacionado con Java, a pesar del nombre) habilita muchas aplicaciones interactivas llamativas. Sin embargo, también sufre muchos ataques y se utiliza para introducir malware en sistemas vulnerables. Si no se necesita Javascript, no lo habilite en el navegador web.
12. **Bloquear los nombres de dominio maliciosos conocidos en el DNS**: Algunas clases de malware cuentan con la capacidad de traducir con éxito nombres de dominio a números. Si usted bloquea la resolución de esos dominios a través de su servidor de DNS, es posible que el malware no se logre ejecutar. Como ejemplo, OpenDNS es una empresa que ofrece DNS con filtros para el tráfico malicioso.
13. **Filtrar/remover el contenido malicios de los correos electrónicos potencialmente peligrosos**: Su administrador de correo electrónico debe ejecutar un examen para detectar adjuntos, enlaces o contenidos potencialmente peligrosos que usted puede recibir por correo electrónico. Un programa que puede ayudar con esto es MIMEDefang.
14. **Los archivos descargados mediante aplicaciones P2P con frecuencia están infectados**: Sepa que muchos de los archivos compartidos en redes de punto a punto (P2P) para compartir archivos pueden estar infectados con malware de manera intencional o accidental.
15. **Asuma que todas las unidades USB esconden "trampas cazabobos"**: Si recibe una unidad USB, o encuentra una unidad USB "perdida", **nunca** la conecte en su equipo. Puede haber sido infectada en forma intencional con malware, y luego colocada en un lugar donde la encuentre con el fin de introducir malware en su sistema.
16. **Evite el uso de puntos de acceso de Wi-Fi desconocidos:** Algunos puntos de acceso Wi-Fi abiertos pueden interceptar tráfico no cifrado y, de este modo, pueden violar su privacidad. El uso de una red privada virtual (VPN) le puede brindar cierta protección. Asegúrese de que cualquier punto de acceso inalámbrico que utilice esté protegido con WPA2 (un programa de protocolo y certificación de seguridad desarrollado por Wi-Fi Alliance para proteger las redes informáticas inalámbricas) para restringir el acceso.

B) MEJORES PRÁCTICAS RECOMENDADAS: DETECCIÓN

Estas recomendaciones ponen el acento en cómo se detecta el malware cuando falla la prevención.

1. **Tomar consciencia cuando una exploración local detecta algo**: Una de las formas más comunes de detectar un malware es mediante el análisis de un antivirus. Otra opción similar sería realizar un análisis mediante una exclusiva herramienta antimalware especialmente diseñada como "sólo limpieza"[ix].
2. **Advertir cuando el sistema comienza a funcionar de forma extraña**: Otro indicador importante de que algo no anda bien es cuando el sistema comienza a funcionar "de manera

extraña". El funcionamiento extraño puede incluir: ejecución lenta o bloqueos, ventanas emergentes no deseadas (por ejemplo, notificaciones falsas del antivirus), solicitar una página web y terminar en otra, no lograr ir a determinados sitios (sobre todo si son sitios de actualización o sitios relacionados con la seguridad), etc.

3. **Tomar medidas si su ISP le indica que su sistema no funciona correctamente:** Por ejemplo, su ISP le notifica que se ha observado que su sistema ha enviado spam o atacado a otro sistema en Internet.

C) MEJORES PRÁCTICAS RECOMENDADAS: REMEDIACIÓN

Estas recomendaciones apuntan a cómo tratar sistemas infectados con malware.

1. **Limpieza en el lugar**: Este enfoque se basa en que el usuario (o alguien en nombre del usuario) ejecute uno o más antivirus en el sistema infectado, con el fin de limpiarlo (en algunos casos, los expertos también pueden eliminar archivos infectados de forma manual). Este proceso puede llevar mucho tiempo y básicamente puede funcionar o no. Incluso después de haber realizado un gran esfuerzo para limpiar un sistema infectado, es posible que la infección continúe o que el sistema sea inestable o inutilizable.
2. **Reversión**: Si el usuario tiene una copia de seguridad limpia, otra opción es revertir el estado de ese equipo a esa copia de seguridad limpia. Esta opción puede provocar la pérdida de trabajo desde que realizó la última copia de seguridad, a menos que esos archivos recientes se conserven por separado y se puedan restaurar (si hace esto, es necesario hacerlo con mucho cuidado para garantizar que la restauración de los archivos no provoque una nueva infección). En términos generales, una estrategia de reversión funciona mejor cuando las copias de seguridad son frecuentes y es posible seleccionar de todas las generaciones de copias de seguridad disponibles.
3. **Completar la nueva instalación**: En esta opción, el sistema se vuelve a formatear, y el sistema operativo y las aplicaciones se reinstalan desde cero. Esto puede llevar mucho tiempo, y con frecuencia será frustrante por la falta de medios originales (muchos proveedores ya no incluyen una copia del sistema operativo en un medio físico cuando venden un hardware nuevo).
4. **Reemplazar el sistema**: Por último, al menos una fracción de los usuarios puede decidir que simplemente desean reemplazar su sistema infectado, en lugar de intentar limpiarlo. O también, esta puede ser la única manera de desinfectar de forma segura un equipo. Esta opción puede ser más aceptable si el sistema infectado es viejo o no era muy potente, en principio, o si el usuario desea cambiar el sistema operativo o el equipo de escritorio a uno portátil, por ejemplo. La jerga de la industria para este tipo de acción es "dinamitar y pavimentar" (*nuke and pave*).

LAS MEJORES PRÁCTICAS RECOMENDADAS PARA EL GOBIERNO Y LA INDUSTRIA

A) Las mejores prácticas recomendadas para la detección y notificación (ISP a usuario)

En la actualidad, muchos ISP les notifican a sus clientes si están infectados con malware. Los ISP pueden utilizar diferentes técnicas para notificar la infección a los individuos. Esta sección enumera diferentes acciones que los ISP deben realizar para notificar a los usuarios finales; sin embargo, no se

debe entender que cualquier técnica haya sido identificada como la mejor práctica. Existen diferentes ventajas y desventajas asociadas a cada tipo de notificación. Algunos ejemplos incluyen los siguientes:

1. **Correo electrónico**: Cuando se detecta un sistema infectado, el ISP puede notificar al usuario por correo electrónico. Lamentablemente, muchas veces los usuarios nunca leen la dirección de correo que el ISP proporciona para su uso, y es posible que el usuario nunca le brinde al ISP la dirección de correo electrónico que utiliza habitualmente. También es posible que los usuarios también sean más cautelosos al confiar en las notificaciones de correo electrónico como resultado de la cantidad de ataques de phishing y estafas por soporte técnico que confunden a los consumidores ante la presencia de malware en sus computadoras.
2. **Teléfono**: El ISP también puede notificar al usuario por teléfono. Al contactar a los clientes, es importante considerar que, si bien la llamada automatizada puede ser eficiente, los usuarios pueden sospechar de las notificaciones por teléfono, como resultado de los ataques de phishing por voz. Por otro lado, la notificación telefónica realizada por una persona puede ser tediosa y llevar mucho tiempo si es necesario notificar a una gran cantidad de usuarios infectados.
3. **Mensaje de texto**: En los casos en los que el ISP conoce el número de teléfono móvil del cliente, otra opción sería enviarle al usuario la notificación por mensaje de texto.
4. **Correo tradicional (en papel)**: Un ISP puede considerar la notificación de los usuarios mediante correo postal tradicional, posiblemente adjuntándola a la factura mensual. Sin embargo, si el ISP no aprovecha un correo que ya le está enviando al cliente, el envío de notificaciones de correo *ad hoc* puede resultar costoso y bastante inefectivo, sobre todo si el usuario descarta comunicaciones de correo sin abrir creyendo que son probablemente publicidad.
5. **Servicio de soporte a domicilio**: En situaciones en las que el usuario ha comprado un contrato de soporte en el lugar, es posible utilizar otro tipo de notificación mediante una "visita al domicilio" del cliente. Por supuesto, el técnico del ISP deberá mostrarle al cliente su credencial y también se debe considerar que esta puede ser una opción de notificación muy costosa.
6. **Notificación en banda (web)**: En este enfoque, un ISP notifica al usuario mediante la interposición de un mensaje intersticial cuando el usuario intente visitar un sitio web normal. Este enfoque puede ser algo desconcertante para los usuarios, pero es menos perjudicial que otros enfoques, tales como el "jardín amurallado" (ver más adelante).
7. **Jardín amurallado**: Si un ISP necesita restringir de inmediato el daño que un usuario infectado puede causar, una opción es colocarlo en lo que se conoce como un "jardín amurallado". Cuando esto ocurre, se le permite al usuario acceder a sitios seleccionados con fines de remediación y protección, y posiblemente se le permita continuar con el acceso a servicios de VoIP, por ejemplo, para el acceso a servicios de emergencia, pero por lo general no podrá acceder a la mayoría de los recursos de Internet. Se debe hacer hincapié en que esta estrategia no será una penalidad. Los jardines amurallados han tenido una gran eficacia en la disminución de la cantidad de infecciones a nivel del ISP, del consumidor y, de hecho, impulsen un movimiento de malware y botnets hacia servicios de hosting.

Para obtener mayor información, consulte también las recomendaciones para la corrección de bots en redes de ISP del Grupo de Trabajo en Ingeniería de Internet RFC6561.[x]

La notificación a los usuarios finales no se limita a los ISP. Otras porciones del ecosistema de Internet que tienen una relación con los usuarios finales pueden, y deben, realizar las notificaciones. Por ejemplo, se ha difundido ampliamente que tanto Google como Facebook intentaron alertar a los usuarios finales sobre las posibles infecciones asociadas con el malware DNS Changer.

B) Las mejores prácticas recomendadas para la concientización

1. **Momentos adecuados para la enseñanza cara a cara**: En el desafortunado caso en el que el sistema de un cliente se infecte, ese puede ser un excelente "momento de enseñanza" cuando las técnicas seleccionadas para evitar una nueva infección pueden ser particularmente destacadas.
2. **Sitio web para la seguridad del cliente**: El ejemplo más básico para ofrecer educación y concientización al cliente es, probablemente, la creación de un sitio web sobre seguridad que le ofrece al cliente asesoramiento y acceso a herramientas.
3. **Adjuntos con la facturación**: Si los ISP, en forma rutinaria, envían información a los clientes mediante correo tradicional, esta puede ser otra oportunidad más para compartir recomendaciones con el fin de proteger el sistema del cliente, y es algo que se puede distribuir a todos los clientes, incluso a aquellos que no han mostrado hasta ese momento signo alguno de infección.
4. **Anuncios de servicio público (PSA)**: Otra oportunidad para educar a los usuarios finales sobre el malware sería a través de anuncios de servicio público a través de la televisión y la radio. Por ejemplo, en los Estados Unidos, la Campaña Nacional de Concientización sobre Ciberseguridad *"PARA. PIENSA. CONÉCTATE"* ha desarrollado numerosos anuncios de servicio público que comenzaron a circular en forma anual desde 2010.
5. **Material promocional**: También hay una variedad de materiales promocionales como mouse pads, tazas, camisetas, destapadores de botellas, bolígrafos o lápices, u otros obsequios que pueden ayudar a crear conciencia sobre las amenazas relacionadas con malware y botnets.
6. **Concursos**: Otra oportunidad para compartir un mensaje de ciberseguridad puede estar asociada con concursos, en especial, concursos de ensayos destinados a usuarios en edad escolar.
7. **Educación formal**: Otra parte fundamental de la educación y la concientización es incorporar en las escuelas un plan de estudios que trate temas de ciberseguridad o ciudadanía digital. Apuntar a la ciberseguridad en general, y al malware y las botnets en particular, es una cuestión de seguridad pública a largo plazo; y al igual que otras cuestiones de seguridad pública, es posible un mejor abordaje mediante el establecimiento de normas sociales que en muchos casos se pueden inculcar mejor si es parte de la educación formal de un individuo.

Debido al rápido cambio en el panorama y en la complejidad de las amenazas con malware y botnets, educar y concientizar sólo puede ser efectivo en parte a la hora de proteger a los usuarios finales. Los esfuerzos del ámbito legal, regulador, técnico e industrial se mantendrán a la vanguardia en cuanto al abordaje del problema con malware y botnets. Sin embargo, la educación básica y la concientización sobre las amenazas en línea siguen siendo ingredientes necesarios para proteger a los usuarios finales.

Las industrias, las asociaciones y los gobiernos deben desarrollar y promover programas de comunicación que brinden al usuario final un conocimiento básico sobre las amenazas y las técnicas fáciles de entender con el fin de aprender a protegerse.

Muchas de estas iniciativas ya existen y pueden ser utilizadas como modelo o simplemente como una fuente de material educativo (véase más adelante). Varios de estos recursos se basan en las cuestiones generales relacionadas con malware y botnets en lugar de hacer un estricto hincapié en ellos. Sin embargo, por lo general, es mejor proporcionar al usuario final un mensaje combinado sobre seguridad en Internet en lugar de realizar numerosas sugerencias sin coordinación. En otras palabras, la información debe ser breve y coherente siempre que sea posible.

- Alianza Nacional para la Ciberseguridad - Mantenga limpia su computadora - http://www.stopthinkconnect.org/campaigns/keep-a-clean-machine (parte de la Campaña Nacional de Concientización en Ciberseguridad *PARA. PIENSA. CONÉCTATE.* que apunta a botnets y malware)
- Oficina Federal de Investigación (FBI): http://www.fbi.gov/scams-safety
- Real Policía Montada de Canadá (RCMP): http://www.rcmp-grc.gc.ca/is-si/index-eng.htm
- Iniciativa Nacional de los Estados Unidos para la Educación en Ciberseguridad: http://csrc.nist.gov/nice/
- Comisión Federal de Comercio de los Estados Unidos (FTC): https://www.onguardonline.gov and http://www.consumer.ftc.gov/media/video-0103-hijacked-computer-what-do http://csrc.nist.gov/nice/

C) Las mejores prácticas recomendadas en el ámbito legal y regulatorio

En el contexto del análisis forense sobre el malware, *Malware Forensics*: *Investigating and Analyzing Malicious Code*[xi] sugiere algunas prácticas recomendadas para la investigación sobre malware, que incluyen:

- Enmarcar y reenmarcar objetivos y metas de investigación en forma temprana y frecuente.
- Desde el principio, comprender la importancia de identificar pruebas inculpatorias, pruebas exculpatorias y la falta de prueba.
- Diseñar una metodología que asegure que las fases de la investigación no alterarán, eliminarán o crearán pruebas, ni alerten a los sospechosos o comprometan de otra manera la investigación.
- Crear y mantener un meticuloso análisis paso a paso y una cadena de documentación en custodia.
- Nunca perder el control sobre las pruebas.
- Definir, redefinir y adaptar estos principios durante el curso de una investigación con el fin de clarificar y lograr objetivos de investigación más alcanzables.

- Considerar las siguientes cuestiones de importancia desde el principio:
    - ¿La jurisdicción de una investigación requiere una certificación o licencia especial para llevar a cabo el análisis forense digital?
    - ¿Qué autoridad investiga y qué límites posee dicha autoridad?
    - ¿Cuál es el alcance de la investigación autorizada?
    - ¿Cómo se evitará la intromisión en los derechos de privacidad de los custodios de datos relevantes?

D) Las mejores prácticas recomendadas para obtener colaboración de los gobiernos y la industria

Las prácticas recomendadas para el desarrollo de software seguro representan la mejor práctica recomendada para restringir la propagación de malware. El Foro de Garantía de Software para la Excelencia en el Código[xii] (SAFECode) es una iniciativa mundial liderada por la industria para identificar y promover las mejores prácticas recomendadas en el desarrollo y la provisión de software, hardware y servicios más seguros y confiables.

El Grupo de Trabajo n.° 7 del Consejo de Seguridad, Confiabilidad e Interoperabilidad en las Comunicaciones (CSRIC) de la Comisión Federal de Comunicaciones de los Estados Unidos (FCC) presentó de forma voluntaria un Código de Conducta Antibot para ISP y operadores de red el 22 de marzo de 2012, como una iniciativa de colaboración entre la industria y el gobierno[xiii]. El Código pone el acento en los usuarios de Internet residenciales e incluye cinco áreas de interés para los ISP: educación, detección, notificación, corrección y colaboración. Para participar en este Código, se requiere que los ISPs participen en al menos una actividad (es decir, adoptar una medida significativa) en cada una de las siguientes áreas generales:

- Educación: ayudar a maximizar la educación y la concientización del usuario final sobre problemas con botnets y sobre cómo ayudar a prevenir las infecciones de por bots;
- Detección: identificar la actividad del botnet en la red del ISP, obtener información sobre la actividad del botnet en la red del ISP o permitir que los usuarios finales puedan determinar por sí mismos posibles infecciones por bots en los dispositivos que utilizan como usuario final;
- Notificación: dar aviso a los clientes de la sospecha de infecciones por bots o habilitar que los clientes determinen si tienen una infección por bot;
- Corrección: proporcionar información al usuario final sobre cómo puede corregir infecciones por bots o ayudar al usuario final en la corrección de las infecciones por bot;
- Colaboración: compartir la experiencia adquirida y comentarios con otros ISP a partir de la participación del ISP en las actividades de SAFECode.

Los sistemas operativos y las aplicaciones con una correcta configuración (protegida) también pueden reducir la tasa de infección por malware. La Agencia Nacional de Seguridad de los Estados Unidos (NSA) proporciona pautas sobre la protección de equipos contra todas las amenazas, incluso el malware[xiv]. Existe información adicional para routers, conmutadores inalámbricos, VoIP, servidores de bases de datos y aplicaciones en el mismo lugar. Además, es posible encontrar recursos para proteger el sistema operativo y las aplicaciones contra malware en las listas de verificación del Instituto Nacional de Estándares y Tecnología (NIST)[xv] (se incluyen los dispositivos Android).

La Agencia de Seguridad e Internet y Corea (KISA) ofrece un servicio de "Refugio Contra DDoS" de forma gratuita a las pequeñas empresas que no cuentan con las herramientas adecuadas para protegerse contra un ataque DDoS. El "Refugio Contra DDoS" filtra el tráfico malicioso del ataque DDoS y deja pasar el tráfico normal. Asimismo, la KISA detecta la presunta IP zombi en una trampa de spam y le solicita a los ISP nacionales que tomen las medidas necesarias contra estas direcciones IP en sus redes.

Es posible encontrar otros esfuerzos específicos por país en los siguientes sitios web:

- Internacional: https://code.google.com/p/evidenceontology
- Botfrei: https://www.botfrei.de/
- Melani (Suiza): http://www.melani.admin.ch
- Ficora (Finlandia): http://www.ficora.fi/en
- Proyecto ACDC de la UE: http://www.acdc-project.eu/
- Canadá: http://fightspam.gc.ca
- Australia: http://www.acma.gov.au/Citizen/Stay-protected/My-mobile-world/Dealing-with-mobile-spam/dealing-with-spam-i-acma

E) Las mejores prácticas recomendadas para los ISP

Es posible minimizar la amenaza de malware reduciendo o eliminando los vectores de infección. El correo electrónico es todavía un método muy eficaz para propagar un malware. Para mitigar este vector, la mayoría de los ISP, los hoteles y los puntos de acceso gratuitos siguen las mejores prácticas recomendadas de bloqueo de correo saliente (puerto 25) desde cualquier equipo de la red excepto desde sus propios servidores de correo. Esto impide que los equipos infectados propaguen el malware a través de un correo directo.

En Europa, algunos proveedores de Internet dieron un paso más allá. Los usuarios de estas redes, en forma predeterminada, sólo tienen acceso a Internet. El tráfico para el resto de los puertos es denegado. Para ofrecerles a los usuarios sofisticados una mayor flexibilidad, estos ISP proporcionan herramientas que autorizan a ciertos usuarios a utilizar otros puertos/protocolos y servicios.

En ambos casos, la supervisión de los intentos de conexión bloqueados se puede utilizar como un indicador de alerta temprana de equipos infectados con malware, así como también un obstáculo para la propagación de malware y las comunicaciones de controles y comandos.

F) Las mejores recomendaciones para servidores y proveedores de hosting

En la actualidad, uno de los reservorios más prevalentes de malware son los servidores web afectados. Estos servidores se infectan cuando no se aplican los parches de seguridad actuales para el sistema operativo y para las aplicaciones de soporte e infraestructura web, o debido a contraseñas de usuario inseguras. Las infecciones se exacerban en la mediana y pequeña empresa y en muchos proveedores de hosting debido a ataque menores de empleados/personal. Algunos

utilizan la automatización para aliviar estas cuestiones; esta práctica debería ser una práctica recomendada a nivel mundial.

1. **Requisitos de las condiciones de servicio para actualizaciones oportunas de seguridad**: Todos los clientes deberían acordar actualizar los parches de seguridad actuales o permitir que el proveedor de hosting actualice la infraestructura en sus directorios.
2. **Mantener los parches de seguridad actualizados**: Todos los parches de seguridad deben estar actualizados. Este proceso puede ser manual, en el caso de sistemas muy pequeños, o programado, en el caso de los proveedores de hosting más importantes.
3. **Utilizar herramientas de auditoría para identificar un host**: Las herramientas para realizar una auditoría a nivel de servidor en el caso de versiones de software inseguras se deberían ejecutar como mínimo semana por medio, y el software identificado se debería ser parchear.
4. **Utilizar software de seguridad de IT:** Las herramientas (como Tripwire) se deberían utilizar para supervisar la integridad de cada servidor.
5. **Ejecutar un antivirus**: Ejecute un antivirus con frecuencia (si es posible dos antivirus diferentes) para supervisar archivos variables del host para contagio.
6. **Considerar el uso de servidores en la nube:** Puesto que los servidores en la nube son mantenidos y utilizados por motivos profesionales por muchos clientes, tienden a ser más seguros; por otra parte, pueden ser un objetivo más interesante para el ataque (por ejemplo, un DDoS). Sin embargo, los servidores en la nube se deberían considerar una alternativa posible para una mejor seguridad, teniendo en cuenta la reputación del proveedor en la nube, las medidas de seguridad definidas, y si los servidores han sido atacados alguna vez. Más adelante en este informe, encontrará más información sobre amenazas al servicio de hosting y a la Nube y las mejores prácticas recomendadas.

PHISHING E INGENIERÍA SOCIAL

El phishing se refiere a técnicas utilizadas por actores maliciosos para engañar a una víctima para que realice una acción que de lo contrario no tomaría en línea, con frecuencia revelando información confidencial, como datos personales o financieros. Los estafadores se presentan como entidades conocidas (amigos o empresas) y aprovechan relaciones de confianza existentes para afectar a su víctima.

El phishing ha avanzado ininterrumpidamente en cuanto a frecuencia, sofisticación y perjuicio provocado desde sus inicios como amenaza a mediados de la década de los noventa y no muestra signos de agonía. El tipo de datos que se busca mediante el phishing también se ha vuelto cada vez más valioso, desde el simple acceso a un correo electrónico y cuentas bancarias de un consumidor que ocasionaban pérdidas individuales de miles de dólares hasta los objetivos actuales como cuentas corporativas con privilegios especiales ("súperusuario") e información bancaria de empresas.

Estos ataques pueden conducir a una violación masiva de datos mediante la que se roban en masa datos personales de los clientes, se exfiltra la propiedad intelectual de una empresa o se destruyen datos e incluso sistemas físicos. Un evento puede involucrar propiedad intelectual de una empresa y producir pérdidas financieras de hasta decenas o incluso cientos de millones de dólares, y existe una cantidad incalculable de eventos que se producen todos los años.

> ***¿Por qué la "ph"?***
>
> *El término "phishing" proviene de la palabra "fish" ("pescar"), dado que los estafadores de Internet usan "señuelos" para "pescar" la información financiera de un usuario y los datos de la contraseña. Los piratas informáticos tienen una adorable tendencia a cambiar la letra efe por "ph", y "phishing" es uno de estos ejemplos. La transformación de la efe a la "ph" no es una estrategia nueva entre los piratas informáticos; este fenómeno apareció por primera vez a finales de la década de los sesenta entre los piratas telefónicos, que se autodenominaban "phone phreaks".*

En la actualidad, el suplantador de identidad falsifica mensajes y sitios web que difíciles de distinguir de los auténticos, mediante ejércitos de equipos legítimos afectados (botnets) y software infectado (malware) con el mismo fin que previamente requería una interacción más pública con el usuario final. El suplantador de identidad también ha desarrollado un malware móvil que puede inutilizar algunas medidas de protección.

EL DAÑO PARA LOS CONSUMIDORES Y LA INDUSTRIA

Es difícil calcular el impacto del phishing en los consumidores y la economía, y los resultados son muy diferentes. Un punto en el que se ha llegado a un acuerdo general es que los ataques de phishing están aumentando. El informe anual de Investigaciones sobre Violación de Datos de Verizon muestra que después de una breve caída en 2010, el phishing ha aumentado durante varios años consecutivos. En 2014, se informó que el phishing era la tercera causa de violación de datos[xvi] y que había aumentado en un 23 %, de 253 a 312, en 2013. También en 2014, los atacantes continuaron con la violación de redes, con ataques puntuales a objetivos importantes, que aumentaron s un 8 % de los ataques en general. Estos ataques eran más sofisticados y específicos, con un 14 % menos de correo electrónico enviado hacia un 20 % menos de objetivos.[xvii]

El Grupo de Trabajo Antiphishing (APWG) presenta informes trimestrales sobre las tendencias del phishing. El informe presentado en 2014 observó el mayor número de ataques de phishing desde 2009. El mismo informe documentó el mayor número de marcas utilizadas con fines de phishing en la historia, con 756 durante la primera mitad de 2014.[xviii, xix] El Informe Mensual sobre Fraude de la RSA publicado en diciembre de 2014 informó pérdidas por phishing de USD 453 millones en un único mes a nivel mundial o pérdidas anuales por aproximadamente USD 5000 millones, con un 75 % de los ataques apuntando a los Estados Unidos y Canadá.[xx] Sin embargo, mientras que el phishing es una pequeña parte de las pérdidas mundiales estimadas por ciberdelincuencia, que se estiman en USD 445 000 millones[xxi], USD 5000 millones representan una pérdida importante y evitable.

Asimismo, la prevención se ha convertido en una tarea importante, con un tiempo para hacer clic promedio de un minuto y veintidós segundos, y los datos del APWG que sugieren que la infraestructura utilizada para realizar estas campañas es bastante extensa con más de 9000 dominios y casi 50 000 URL suplantadas que se descubren por mes entre los miembros del Grupo.

EL PANORAMA DEL PHISHING

El phishing se clasifica según los tipos de información buscados, los tipos de blanco atacados y los canales mediantes los que se llevan a cabo los ataques. El phishing se identifica generalmente mediante correo electrónico, SMS u otro mensaje que contiene un enlace que redirige al destinatario a un sitio web falso que solicita la información de la cuenta del usuario, por ejemplo nombre de usuario y contraseña, número de tarjeta de crédito u otra información personal.

LOS OBJETIVOS DE LOS ATAQUES DE PHISHING: QUÉ BUSCAN

La información obtenida por el phishing se utiliza generalmente para algún tipo de robo financiero, directamente contra la víctima, o contra otro destino como el empleador de la víctima. Dado que monetizar la información de una tarjeta de crédito y el número del Seguro Social es cada vez más difícil, "los piratas informáticos irán detrás de cualquier persona que posea información para la atención de la salud", dijo John Pescatore, director de nuevas tendencias de seguridad del Instituto SANS, y agregó que en los últimos años los piratas informáticos han fijado su objetivo cada vez más en los registros electrónicos de la salud (EHR) que fácilmente se convierten en dinero en efectivo.[xxii] Además, el phishing ha sido empleado como primer paso en la violación de redes corporativas y gubernamentales mediante la obtención de credenciales que permiten el acceso a los sistemas.

Las estafas del 419: Se trató de las formas tempranas y poco sofisticadas de phishing, que recibe el nombre por el Capítulo 38, Sección 419 del Código Penal nigeriano que penaliza este tipo de fraude. *"Cualquier persona que mediante un pretexto falso, y con intención de defraudar, obtenga de otra persona cualquier cosa pasible de ser robado, o induzca a otra persona a entregar a un tercero cualquier cosa pasible de ser robado, es culpable de delito y será castigado con prisión de tres años".* Estas fueron los famosos correos electrónicos o esquemas de pago por adelantado del príncipe nigeriano en los que la víctima es engañada para gastar dinero a cambio de obtener riquezas incalculables a final del

El phishing, en sí mismo, es generalmente sólo un primer paso y no necesariamente resulta de inmediato en un robo financiero directo. La creciente tendencia a robar registros de salud generalmente comienza con ataques de phishing para obtener acceso a los sistemas. Una vez obtenido el acceso, los ladrones utilizan otras herramientas, como malware y spyware, para robar información confidencial: en el primer trimestre

de 2015, más de 120 millones pacientes en los Estados Unidos han sufrido el robo de sus registros.[xxiii] Además, el spear phishing para el robo de credenciales de empleados corporativos suele ser uno de los primeros pasos en la violación de datos a gran escala y, por lo tanto, es el primer paso de una parte significativa de pérdidas impactantes atribuidas a la violación de datos.

- Las técnicas en línea y fuera de línea que engañan a los usuarios para que divulguen información con frecuencia se denominan "ingeniería social" y preceden a la Internet. Cuando se inició el phishing por correo electrónico, los atacantes no eran muy exigentes. Enviaban correos electrónicos generales a todas las personas posibles y esperaban que un porcentaje fuera engañado. A medida que las defensas contra estos ataques se fortalecieron, los atacantes refinaron sus estrategias. Existen cuatro tipos reconocidos de phishing:

  *i) una **redirección** mediante un enlace contenido en un mensaje hacia una ubicación en Internet que puede contener un sitio falso de un banco, comercio o sitio de correo electrónico;*

  *ii) correos electrónicos con un **adjunto html** que contiene la forma de phishing;*

  *iii) **un enlace/una enumeración** de un número telefónico sobre el que una víctima debe hacer clic o llamar; o*

  *iv) un phishing simple con una **respuesta**, donde el mensaje contiene una solicitud de las credenciales deseadas y se le solicita al usuario que responda con la información.*

En las dos primeras formas, el destinatario del mensaje proporciona información personal con frecuencia mediante el envío de un correo electrónico al delincuente que contiene las credenciales robadas. El phishing basado en un número telefónico puede involucrar un sistema automatizado de contestador telefónico le solicita a la víctima sus credenciales o una persona que intenta aplicar la ingeniería social. Las estafas del 419, con la promesa de obtención de riquezas incalculables, y otros fraudes por pago adelantado eran las formas tempranas de ingeniería social mediante correo electrónico. A pesar de los avances en las técnicas de phishing, estas estafas aún persisten.

- **Spear phishing/Phishing dirigido:** Mientras que los intentos de phishing tradicional con frecuencia se envían en forma indiscriminada a casi todos los usuarios, los ataques de phishing dirigido se realizan contra ciertas personas u organizaciones. Este tipo de phishing generalmente implica una extensa investigación por parte de los estafadores, por ejemplo, conocer pasatiempos, donaciones de caridad, exempleadores y redes sociales favoritas, con el fin de que el ataque sea mucho más verosímil y creíble. Es posible personalizar el ataque para engañar a las víctimas que son tradicionalmente más valiosas (y sospechosas) que el usuario promedio. Se podría tratar de empleados de una compañía blanco que un atacante intenta penetrar. Una variante del spear phishing que es particularmente efectiva implica enviar a la víctima un mensaje falso que parece ser de un proveedor, acreedor u organización conocidos con instrucciones de pago fraudulentas para transacciones que la víctima espera o reconoce como normales.
- **VoIP/Vishing:** A medida que las actividades telefónicas y similares migran a mecanismos basados en la Internet, que se conocen ampliamente como "Voz sobre IP" o VoIP, los fraudes también se adaptan a la migración. La integración de equipos con sistemas de teléfono hace posible engañar a las víctimas para que hagan clic en enlaces fraudulentos que automáticamente realizan una llamada telefónica, en lugar de ir a un sitio web. La llamada en

sí misma puede generar directamente un ingreso para el atacante, o puede dirigir a la víctima a un ingeniero social que la convence para revelar información. Los teléfonos inteligentes maximizan la amenaza al simplificar esta integración telefonía/Internet para el usuario. Para obtener mayor información, véase la sección Amenazas telefónicas y móviles de este informe.

- **Fax:** El fax fue uno de los primeros métodos de phishing electrónico y ha sido reemplazado principalmente por los otros métodos de ataque que aquí se analizan. Sin embargo, con el advenimiento del fax basado en Internet que disminuía los costos, este método experimenta un resurgimiento. Dado que su uso no es frecuente, no siempre se detecta.
- **Redes sociales:** Crean una experiencia de grupo que conduce a un sentido de confianza que, a su vez, es beneficioso para la ingeniería social que ataca las relaciones en línea de la víctima. Esto puede funcionar muy bien cuando el atacante imita el mensaje de un amigo en línea de confianza o ha afectado la cuenta de un amigo.

LÍNEA DE TIEMPO DE UNA TÍPICA CAMPAÑA DE PHISHING

Una campaña de phishing posee cuatro elementos:

1. **Mensaje inicial (spam)**: El usuario final recibe y lee el mensaje. Parece ser genuino y, por lo tanto, tiene un alto grado de credibilidad; por lo general, contiene componentes de un mensaje legítimo pero falsificado, y parece proceder de una fuente legítima, como el banco de la víctima.
2. **Llamado a la acción (clic del usuario):** Se alienta a la víctima a hacer clic en un enlace o responder el mensaje con información confidencial. Las llamadas a la acción más eficaces se aprovechan del miedo y de la codicia, ya sea personalmente o en relación con la organización para la que trabaja el destinatario. Un mensaje basado en el miedo puede indicar que la víctima ya se ha visto afectada o puede perder acceso a un recurso si no adopta una medida, o que la empresa está sujeta a una demanda o sanción económica. Un mensaje basado en la codicia puede prometer un descuento o una recompensa financiera con la participación en una encuesta o el envío de información.
3. **Contenido malicioso:** Este contenido hace que la víctima divulgue su información confidencial. Puede estar en el mensaje inicial o en un sitio web blanco, denominado "página de llegada". El sitio web puede estar afectado, o puede tener un nombre de dominio de aspecto similar para confundir al usuario final. La carga, por lo general, posee una forma que requiere que la víctima introduzca información confidencial. Algunos sitios de phishing también contienen un mecanismo de "descarga oculta" en el que la visita del destinatario al sitio web inicia un proceso automatizado de ataque e inventario del sistema que se traduce en la introducción silenciosa de un malware en el equipo de la víctima, que le permite a los delincuentes obtener datos confidenciales, para posteriormente redirigir a la víctima al sitio legítimo.
4. **Ataque/Exfiltración/Obtener información:** El juego final de cualquier campaña de phishing es convertir las credenciales recolectadas en valor para los delincuentes. Se ha observado una amplia gama de esquemas: el más simple es iniciar sesión en la cuenta y utilizarla para transferir fondos o hacer compras, mientras que otros ataques mucho más

sofisticados utilizan en primer lugar el phishing para obtener acceso a una cuenta de correo electrónico y luego la utilizan como base para la ingeniería social adicional y/o propagación de malware con la posibilidad de infiltrarse a fondo en la organización del destinatario. También se han observado intentos de extorsión.

Existe una serie de puntos en los que es posible prevenir o interrumpir el flujo de trabajo de una campaña de phishing, como se indica en el diagrama a continuación:

EVOLUCIÓN DE LOS MÉTODOS DE ATAQUE

La forma más conocida y original de phishing involucró a delincuentes que iniciaban sesión directamente en una institución financiera e intentaban transferir fondos de la cuenta de la víctima a otra cuenta controlada por los delincuentes. Cuando las instituciones financieras comenzaron a detectar y bloquear las transferencias de dinero internacionales y fraudulentas con mayor facilidad, los delincuentes se adaptaron a las circunstancias. Transferían el dinero a una cuenta nacional o del mismo banco, y el fraude con frecuencia no se detectaba tan fácilmente. A veces esto se lograba mediante el pago de facturas en línea o simples transferencias cuenta a cuenta. En estas situaciones, el delincuente, que con frecuencia estaba en el extranjero, necesitaba los servicios de delincuentes nacionales que actuaban como mulas de dinero.

En otros casos, la llamada a la acción contenida en el correo electrónico de phishing pretende obtener la divulgación de datos de una tarjeta de crédito. Con el número de una tarjeta de crédito, la fecha de vencimiento y el código CVV, la tarjeta se puede vender en el mercado negro o se utiliza para todos los tipos de fraude con tarjeta no presente. Con el número de la tarjeta de crédito, la fecha de vencimiento y el CVV, el suplantador de identidad visita casi a cualquier minorista en línea y hace compras. Para evitar su detección, se utilizan mercados ilegales secundarios para el reenvío y servicios de terminales remotos. Para derrotar a los sistemas de detección de fraude minorista, los suplantadores de identidad comprarán el uso de una dirección IP de servicios de terminales remotos en un área geográfica que coincida con la geografía del dueño de la tarjeta de crédito. Asimismo, si se

deben realizar envíos, también se utilizará un lugar para recibir los paquetes que coincida con la geografía de la víctima.

Asimismo, el ataque por reutilización de contraseñas es otra amenaza al consumidor en línea que puede ser resultado de un ataque de phishing. Debido a que las personas con frecuencia utilizan la misma contraseña en muchos sistemas, los delincuentes son capaces de utilizar la misma identificación de usuario y contraseña en diferentes lugares, por ejemplo una institución financiera, minoristas en línea, e incluso sistemas con un VPN corporativo (véase la sección Malware y botnets para obtener mayor información sobre la creación y el almacenamiento de contraseñas seguras).

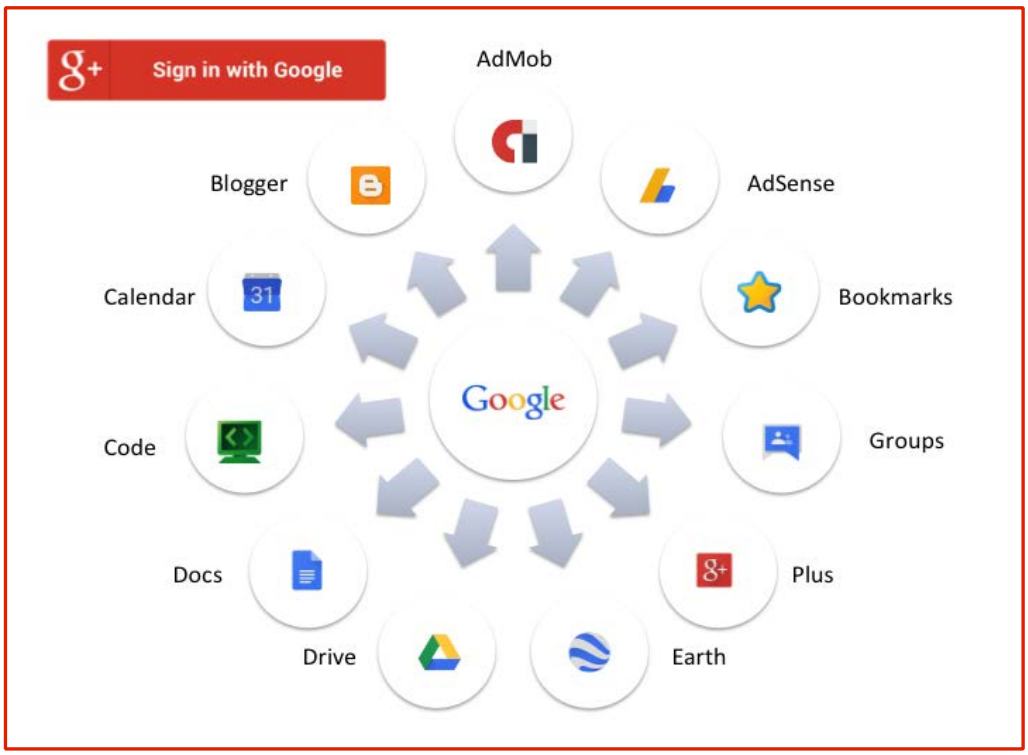
La violación de datos a gran escala que ha sido noticia en los últimos años con frecuencia comienza con algún tipo de phishing dirigido o spear phishing que tiene por víctima a ejecutivos o personas con acceso a los controles de una red corporativa. Este tipo de ataques han llevado a dirigir los delitos financieros, como el robo de información personal y credenciales de usuario, y su reventa en el submundo del delito. Un número grande y creciente de las campañas de spear phishing también promueven el espionaje industrial, los esquemas de extorsión, la infiltración patrocinada por el estado y otros delitos no financieros.

EL AUMENTO EN EL DESARROLLO DE LOS ATAQUES DE PHISHING

A medida que más organizaciones migran a sistemas de correo electrónicos basados en la Web, los ataques de phishing se han vuelto más frecuentes por dos razones principales. En primer lugar, y lamentablemente, muchas organizaciones utilizan entornos de inicio de sesión único, con la misma contraseña tanto para cuentas de correo electrónico como para las tareas de recursos humanos, como la cuenta bancaria donde se transfiere el dinero en el día de pago. En segundo lugar, una vez que se accede a una cuenta de correo electrónico corporativo, el delincuente tiene una plataforma desde la que pueden estudiar la organización, saber quién puede tener acceso a los más valiosos activos digitales de la compañía, por ejemplo las cuentas financieras y la propiedad intelectual, y apuntar a esos empleados. Este tipo de ataques se pondrán en marcha a partir de una cuenta de correo electrónico de un empleado que la empresa conoce y en quién confía, ya sea mediante ingeniería social o la transferencia de malware mediante adjuntos de correo electrónico que imitan el modelo de los documentos comerciales normales que se encuentran en la cuenta afectada.

Incluso para el correo electrónico no corporativo, el ataque de phishing contra los proveedores de correo electrónico, como Gmail, Yahoo, Outlook y AOL es cada vez más frecuente por muchas de las mismas razones. Estas cuentas pueden parecer "objetivos de poco valor" y no están vigilados con tanto esmero como el resto; sin embargo, controlan la capacidad de restablecer contraseñas o dirigir el acceso a otras cuentas para realizar una amplia variedad de ataques. Estas cuentas de correo electrónico afectadas han dado lugar a un volumen importante de delitos financieros (por ejemplo, la cuenta de adquisición, transferencias electrónicas fraudulentas) que están bien documentadas por las entidades financieras.

Otros servicios, como las redes sociales brindan un "inicio de sesión único" para una amplia gama de servicios al consumidor. Esto hace que este tipo de cuentas sean blancos para los suplantadores de identidad, ya que pueden monetizar directamente dichos servicios, redirigir envíos de productos o, en general, tomar el control de muchos aspectos de la identidad en línea de una persona. El siguiente diagrama muestra que si los piratas informáticos pueden ingresar en una cuenta de Google, con frecuencia tienen acceso a una enorme cantidad de otros datos. Se puede decir lo mismo de cuentas de Apple y iTunes.



La creciente sofisticación de los delincuentes los ha llevado orientarse a elementos de la infraestructura que les proporcionan un mayor potencial. Por ejemplo, los suplantadores de identidad ahora tienen acceso a los proveedores de servicios de correo electrónico (ESP) de terceros, que envían correo electrónico masivo en nombre de las marcas más importantes del mundo. Los delincuentes acceden a la infraestructura de un ESP mediante cuentas afectadas, roban listas de clientes y envían spam o malware de phishing a los destinatarios inconscientes, que creen que el mensaje pertenece a una lista de correo de una empresa legítima.

Otra tendencia reciente es el aumento de los ataques de elementos de infraestructura de Internet, como cuentas de hosting o credenciales de registro de dominios. Una vez que los suplantadores de identidad obtienen acceso a los controles fundamentales de la infraestructura como estos, pueden establecer sitios web, lanzar nuevos ataques y crear nuevos elementos de infraestructura, como nombres de dominio para rotar sus esquemas (véase la sección Servicios de hosting y en la nube).

Una táctica en particular perjudicial es añadir nombres de host maliciosos a un nombre de dominio sólido con una buena reputación, sin modificar el dominio original. Esto permite a los delincuentes atacar la buena reputación de un dominio mediante sus campañas para evitar filtros y bloqueos o cierres (véase la sección Nombre de dominio y direcciones IP).

LAS MEJORES PRÁCTICAS RECOMENDADAS CONTRA EL PHISHING Y LA INGENIERÍA SOCIAL

Existe una amplia gama de mejores prácticas recomendadas antiphishing a disposición de las organizaciones para proteger su marca y sus clientes. Dicho esto, no hay un "santo remedio" para los desafíos que plantea el phishing, y es necesario abordarlo en todo el ciclo del proceso: cualquier fase que se pueda impedir puede proteger a docenas de millones de víctimas en función de la escala del ataque y el alcance de varias soluciones. Las empresas deben abordar este problema con un enfoque de "defensa en profundidad", asumiendo que algunas medidas serán efectivas para evitar que lleguen los primeros correos electrónicos, pero que algunas no servirán y será preciso definir otras defensas. En esta sección se resaltarán algunas de las principales técnicas y mejores prácticas recomendadas, pero se obtendrá mucho más detalle y asesoramiento específico a partir de diversas organizaciones de la industria, publicaciones gubernamentales y proveedores de soluciones antiphishing.

1. Prevenir el ataque de phishing de manera exitosa

El primer punto para abordar los ataques de phishing es impedir que alcancen a las víctimas y/o mantener a las víctimas alejadas de los sitios de phishing en primer lugar. Hay tres puntos de contacto primario para lograr este objetivo: detener el flujo de correos electrónicos de señuelo, evitar que los señuelos lleguen a los usuarios y bloquear el acceso a los sitios web de phishing y a otros activos.

a. Prevenir el envío de email como señuelo

Los mecanismos de autenticación basados en correo electrónico que son relativamente recientes facilitan algunas protecciones utilizadas con facilidad contra algunas formas de phishing y suplantación. Estas técnicas se basan en la creación de una infraestructura de autenticación de correo electrónico. Los mecanismos de autenticación de correo electrónico más frecuentes son el convenio de remitentes (SPF)[xxiv] y el correo electrónico identificado por clave de dominio (DKIM)[xxv], que emplean nombres de dominio[xxvi] como identificadores validados. Estos le permiten al propietario de un nombre de dominio controlar el uso de su dominio en el correo electrónico y reducir los casos de suplantación de identidad.

Con el fin de abordar de forma exitosa los problemas de phishing y suplantación de dominios, los propietarios de marcas e ISP necesitan compartir información entre sí sobre su actividad de correo electrónico, por ejemplo, las políticas de autenticación y los informes sobre problemas. Históricamente, estos arreglos fueron bilaterales y privados, entre los propietarios de marcas y los ISP individuales. Sin embargo, un consorcio de la industria *ad hoc* desarrolló una especificación técnica llamada Autenticación, Informe y Conformidad de Mensajes Basados en Dominios (DMARC)[xxvii].

La DMARC, introducida a principios de 2012, hace uso de SPF y DKIM para proporcionar los propietarios de marcas con un medio para comunicar fácilmente a los ISP cómo desean manejar los mensajes autenticados de manera incorrecta. Asimismo, la DMARC les proporciona a los ISP y a otros destinatarios de correo electrónico un mecanismo para el envío a los propietarios de las marca de comentarios acerca del funcionamiento de la herramienta de autenticación de correo electrónico, así como también de la inteligencia a nivel forense.

Para las operaciones de envío de correo electrónico, el abordaje recomendado es el siguiente:

- *Auditar:* mediante el inventario de todos los equipos y sistemas que envían correo electrónico en nombre de la organización, incluso sistemas externos, como ESP, u otros terceros autorizados
- *Publicar:* los registros de políticas y autenticación en el DNS
- *Modificar:* software para el envío de correo electrónico con el fin de utilizar la autenticación y cumplir la política
- *Establecer:* relaciones de informe sobre actividad que utiliza el nombre de dominio
- *Supervisar:* todos los informes disponibles para los patrones que requieren atención
- *Mantener:* las operaciones para la conformidad en curso

Para las operaciones de recepción de correo electrónico, el respaldo de estos nuevos mecanismos implica principalmente añadir módulos a los sistemas de filtrado de correo electrónico existentes.

b. Filtro de spam entrante

Uno de los métodos más importantes para detener el daño de un ataque de phishing es lograr un filtrado efectivo de spam. Habilitar el filtrado de spam es importante, pero el filtrado efectivo implica algo más que tener un producto comercial instalado en la puerta de enlace de correo electrónico. Las empresas y agencias gubernamentales también deben mejorar su filtro de spam mediante la incorporación de datos sobre amenazas que ayudan a mejorar el filtro de spam.

Esta información se puede obtener a partir de listas negras generadas por organizaciones especializadas, como Spamhaus, SURBL y otras (véase las referencias al final de esta sección). El filtrado de spam está estrechamente asociado a la presentación de informes, ya que los correos electrónicos de phishing que traspasan con éxito un filtro de spam son los que hay que informar con mayor urgencia. Muchos servicios de correo electrónico ofrecen un botón "Marcar como spam" o "Marcar como phishing", que los usuarios deben utilizar.

Las técnicas para el filtrado de spam incluyen:

- *Autenticación:* los remitentes de correo electrónico tienen la posibilidad de inscribirse en los métodos de autenticación, por ejemplo DKIM, SPF y DMARC. Cuando se recibe el correo electrónico, se comprueba la presencia de un token de autenticación. Según DMARC, el dominio de envío se comprueba para ver si se requiere autenticación. Si el token no es válido o no está presente, el correo electrónico puede ser fraudulento.
- *Reputación de direcciones IP:* la dirección IP que envía el correo electrónico puede ya estar asociada con el envío de spam. Al rechazar correos electrónicos de direcciones IP con una mala reputación, es posible bloquear una gran cantidad de spam.
- *Filtro de contenido:* el filtrado basado en reglas, la comprobación de correo electrónico para detectar la presencia de palabras o frases prohibidas o el análisis estadístico de la dirección de correo electrónico (filtro de spam bayesiano) puede identificar los correos electrónicos que posiblemente sean spam. Informar al contenido de los filtros

los datos de los servicios de reputación para los nombres de host y/o URL (por ejemplo, Spamhaus como DNSBL/SURBL) mejora en gran medida esta técnica.

- *Trampas de spam:* mediante la recopilación de correo electrónico enviado a las direcciones que no deben recibir ningún correo electrónico (usuarios que no existen), es posible identificar patrones y aplicarlos para bloquear el correo electrónico enviado a direcciones legítimas.

c. Bloqueo del navegador y otros

La protección contra ataques de phishing está integrada en muchos productos y servicios que los consumidores, las empresas y otras organizaciones pueden aprovechar. Con la información generalizada de los ataques de phishing realizada por marcas y el público en general, estos datos ingresan a los productos que se exponen al phishing, como navegadores web, servidores de correo electrónico y clientes, dispositivos de seguridad (firewalls, sistemas IDS/IPS, proxy de tráfico web, DNS de firewalls), y proveedores de servicios de correo electrónico en línea. Estas herramientas/Estos dispositivos pueden proporcionar una protección aún mejor si se añaden datos de inteligencia sobre amenazas. Por ejemplo, datos sobre reputación de direcciones IP, nombres de host/dominio, URL, direcciones de correo electrónico y otros "indicadores" de comportamiento poco fiable.

Estos se envían en varias formas, por ejemplo, DNSBL, RBL, listas de bloqueo de URL y una tecnología relativamente nueva llamada Zonas de Política de Respuesta de DNS (RPZ). Dichas tecnologías y sus datos se pueden implementar para cortar toda comunicación a ubicaciones de Internet bloqueadas. Las empresas deben elaborar normas operativas y políticas para garantizar que habilitan este tipo de servicios en sus entornos. Esto tiene particular importancia para los productos de puerta de enlace de correo electrónico y herramientas generales de seguridad de red para crear una defensa "en capas". Esta postura de seguridad debe estar bien planificada y actualizada de forma regular.

Los usuarios individuales también se pueden proteger de muchos ataques simplemente habilitando este tipo de servicios en sus navegadores (por ejemplo, navegación segura de Google, filtro de phishing de Microsoft), la incorporación de una "barra de herramientas" a su navegador, que permite la configuración antiphishing y antispam en la cuenta de correo web cuenta de correo y la activación de las protecciones antiphishing en el antivirus.

2. Detección

La detección de ataques de phishing evita el ataque en sí, pero también ayuda a detectar ataques futuros. Además, si no se detecta, los sitios no pueden ser buscados para el análisis forense, bloqueados en los navegadores y filtros de spam, cerrados o investigados. La detección toma varias formas, según el punto de observación desde el que se está produciendo la detección. Cuando hablamos de detección, el objetivo principal es detectar la nueva campaña de sitio de phishing o correo electrónico, pero con frecuencia los medios para la detección estarán en el análisis del flujo de mensajes entre los delincuentes y las posibles víctimas.

- Consumidor/Empleado: dado que los consumidores son los destinatarios más probables del mensaje, es importante que las marcas que son posibles blanco se comunique de manera efectiva con sus clientes sobre cómo proceder si observan un correo electrónico sospechoso. Los ataques de spear phishing estarán dirigidos a los empleados. La detección se realizará con frecuencia mediante un correo electrónico visto por un cliente o empleado de la marca blanco, por lo que proporcionar educación

del usuario y la posibilidad de presentar informes son pasos importantes para la detección de ataques (véase más adelante).

- Correo electrónico rechazado: durante muchos años, uno de los métodos más efectivos para convencer a una posible víctima de que un mensaje de phishing es legítimo ha sido utilizar el dominio de envío de la marca imitada. Los correos electrónicos desde "@paypal.com" o "@bankofamerica.com" probablemente sean tomados al pie de la letra por las posibles víctimas que no son conscientes de cómo es posible imitar fácilmente el campo "De:". Afortunadamente, cuando dichos mensajes no se entregan, con frecuencia porque el spammer se los envía a una cuenta que está desactivada, cerrada, o que ya no recibe mensajes, el servidor de correo en el extremo receptor "rebotará" estos mensajes. Como se describió anteriormente, en el caso de la autenticación de correo electrónico, la DMARC proporciona un protocolo para dirigir dónde enviar estos mensajes rechazados. El análisis de estos mensajes rechazados a menudo puede conducir a la detección de nuevas fuentes y sitios web de phishing.
- URL de referencia: cuando un kit de phishing utiliza un gráfico, un archivo de JavaScript, hojas de estilo u otra característica de la marca imitada, los archivos de registro de la marca imitada mostrarán que el archivo ha sido mencionado por un sitio web de terceros. Si "hackedsite.com/yourbank/verify.php" es una página de phishing y utiliza un gráfico de "yourbank.com/graphics/logo.gif" el registro mostrará que se ha hecho referencia a "logo.gif" desde "hackedsite .com". El análisis de estas direcciones URL de referencia es una excelente manera de detectar nuevos sitios web de phishing. Esto se puede lograr en la empresa con un personal bien capacitado o tercerizado a uno de los tantos proveedores.
- Spam de salida: desde el punto de vista de una empresa, un proveedor de hosting o un ISP, existen varias maneras de detectar correos electrónicos de phishing salientes que se están generando desde la red. Según las Condiciones de servicio para el servicio que se presta, la red puede ser capaz de observar el correo electrónico saliente a partir de la presencia de características sospechosas, como picos inusuales en el volumen, desajustes en el dominio del remitente, intentos de utilizar puertos de correo electrónico de espacio de red no permitido o la inclusión de direcciones IP pertenecientes a la red en varias listas de reputación.
- Reutilización de credenciales: una técnica reciente para la detección de sitios de phishing ha sido exigir a los consumidores utilizar un par único identificador de usuario-contraseña para acceder a una marca de destino. Un plug-in en el navegador del consumidor detecta cualquier intento de utilizar ese par identificador de usuario-contraseña en otra ubicación, e informa la dirección URL a la marca de destino como una URL sospechosa que debe ser investigada.
- Productos de seguridad y software de fuente abierta calibrados para phishing: los servidores de correo electrónico, dispositivos modernos de seguridad y servicios en la nube emplean ingresos a sitios conocidos de phishing, direcciones IP, nombres de dominio y patrones de ataques de phishing. Según las coincidencias directas y el análisis heurístico de las URL incluidas en el correo electrónico o que transitan por la red corporativa, es posible detectar los señuelos de phishing y los "clics" mediante bloqueos, alertas y acciones.

3. Presentación de informes

La presentación de informes de ataques de phishing tiene dos objetivos. Colabora con las marcas que están siendo imitadas a responder a la amenaza y proporcionar un rastro, que le puede ser útil a las fuerzas de orden público. Una vez que se detecta un ataque de phishing, existen varios caminos para informarlo con el fin de evitar que la comunidad en general reciba señuelos o visite sitios de phishing. Las marcas y organizaciones que sufren suplantación en los sitios web y señuelos de phishing pueden alertar a sus clientes, empleados y componentes, que son las víctimas más posibles. Las personas que se topan con sitios de phishing también pueden informarlos, y las marcas victimizadas pueden proporcionar y promover una metodología fácil para que sus clientes y terceros involucrados informen los actos de phishing.

Una vez que una organización sabe que es blanco de una campaña de phishing es importante alertar al ecosistema antiphishing que comprende organizaciones de la industria, proveedores y personal de respuesta de incidentes. Esto se puede hacer para el ataque de phishing ocasional con el informe del ataque a través de uno de los sitios que se enumeran al final de esta sección.

La mayoría de los objetivos principales del phishing emplean servicios de terceros que se especializan en el tratamiento de contenidos en línea ilegales/no deseados como una competencia básica, ya que tienen procesos y relaciones establecidos con los principales proveedores, la capacidad de traducir idiomas e investigadores de inteligencia sobre amenazas entre el personal. Independientemente del método de envío utilizado, reconocer y reportar los ataques de phishing rápidamente puede conducir a la identificación del delincuente.

Para facilitar aún más la acción de informar, muchas marcas han creado direcciones de correo electrónico fáciles de recordar, como "reportphishing@targetedbrand.tld". Para fomentar el informe, las marcas deben redactar pautas sobre cómo informar un ataque de phishing observado en su sitio web y distribuir dicha información en las interacciones que incluyen al cliente.

Muchos servidores afectados contendrán las entradas del registro que dejan un rastro que muestra cómo se pirateó y se colocó el contenido ilegal en el servidor. Además, cada sitio web de phishing debe brindar una manera para que el delincuente reciba las credenciales robadas. En general, esto se realiza mediante correo electrónico, pero también es posible involucrar archivos secretos en el servidor web de donde se roban las credenciales. El análisis de los sitios de phishing identificados puede ayudar a identificar, desactivar o supervisar estos puntos de exfiltración de datos y conducir a la identificación de los delincuentes.

4. Investigaciones corporativas y de orden público

La mayoría de las investigaciones sobre phishing las realiza la empresa cuya marca está siendo suplantada, o los proveedores de inteligencia sobre amenazas u organismos de orden público en representación de esta.[xxviii] Mediante el uso de muchas de las técnicas descritas en el punto "Análisis e Inteligencia" mencionado anteriormente, los investigadores pueden identificar y calcular las víctimas y sus pérdidas, como así también relacionar los tantos sitios de phishing creados o que benefician económicamente al mismo delincuente.

En lugar de resolver cada caso por separado, se fomenta que las empresas desarrollen relaciones con las agencias de investigación con el fin de comprender los mejores métodos para intercambiar dicha información. En los Estados Unidos, el programa InfraGard del FBI y los Grupos de Trabajo sobre Delitos Electrónicos del Servicio Secreto de los Estados Unidos son programas que ayudan a desarrollar este tipo de relaciones. Los centros nacionales como la National Cyber Forensics and

Training Alliance (NCFTA) también ofrecen oportunidades para la alianzas público-privadas con enfoque en la investigación de delitos informáticos. El trabajo con estas organizaciones puede ayudar a las compañias dueñas de marcas a ser participantes activas en el proceso de aplicación de la ley. A menudo tener múltiples marcas como víctimas en un solo caso conduce a una respuesta de aplicación de la ley más activo, al tiempo que provee la llamada "seguridad de los números" para las marcas de las víctimas, que pueden sentirse incómodas al ser nombradas como víctimas.

5. Educación del usuario/de la víctima

McAfee Labs informó a finales de 2014 que el phishing sigue siendo una táctica eficaz para infiltrarse en las redes empresariales. Su estudio encontró que el 80 % de los usuarios corporativos no son capaces de detectar fraudes: los empleados del Departamento de Finanzas y de Recursos Humanos tienen peor estadística que el empleado promedio. Sus empleados pueden realizar la encuesta sobre phishing aquí: https://phishingquiz.mcafee.com.[xxix] Cifras como estas demuestran lo importancia para las empresas y los programas de gobierno de continuar capacitando en forma permanente a sus empleados. Esta fue una de las recomendaciones del Consejo Federal de Examinación de Instituciones Financieras (FFIEC). SANS (www.sans.org) también posee información sobre cómo ejecutar un programa de phishing en su página web SecuringTheHuman.[xxx]

Si bien es más difícil proporcionar una capacitación a los consumidores, las empresas que experimentan altas tasas de phishing reciben la recomendación de realizar la capacitación cuando tengan la oportunidad de interactuar con sus clientes, ya sea mediante un adjunto que acompañe a la facturación, una advertencia especial cuando el cliente inicia sesión en el sistema en línea, o mediante un mensaje grabado mientras exista una interacción telefónica con el consumidor. Las empresas que se preocupan por la asociación se su marca con delitos cibernéticos pueden incorporar un mensaje proactivo, como la campaña "Para. Piensa. Conéctate" o declarar que respaldan campañas de ciberconcientización lanzadas por el gobierno, como la semana o el mes de concientización sobre ciberseguridad que se realiza todos los años en los países más desarrollados.[xxxi, xxxii] Existen muchos recursos disponibles en el marco de estas campañas de divulgación pública que pueden adoptar las empresas.

El APWG fomenta que las empresas colaboren en brindar una capacitación "justo a tiempo" mediante la adopción de la página de inicio de Educación sobre Phishing del APWG como su página de inicio. También se fomenta a que los administradores web que dan de baja un sitio web de phishing por haber sido pirateado sustituyan la página con la página de inicio del APWG.[xxxiii]Varias organizaciones han desarrollado sus propias páginas de capacitación excelentes para colaborar en la capacitación de los usuarios. Se incluyen Visa y Stay Safe Online:

http://www.visasecuritysense.com/en_US/phishing-attack.jsp
https://www.staysafeonline.org/

La Comisión Federal de Comercio (FTC) de los Estados Unidos utiliza una generosidad un poco liviana para alertar a los consumidores sobre los riesgos asociados con el phishing representando estratagemas de phishing estándar para alertar a los consumidores sobre este problema a través de los juegos en línea y videos de YouTube

- Juegos en línea: http://www.onguardonline.gov/media/game-0011-phishing-scams, and
- Videos de YouTube: https://www.consumer.ftc.gov/media/video-0006-phishy-home.

6. Participación de la industria

Las organizaciones para compartir información, como el Centro de Análisis e Intercambio de Información de los Servicios Financieros (FS-ISAC) y el Equipo de Respuesta ante Incidentes Cibernéticos de las Instituciones Financieras de Canadá (TPI-CIRT) también son organizaciones muy importantes que ayudan a abordar delitos de phishing "entre marcas".

La participación en grupos de defensa de la industria, como el APWG[xxxiv], el M[3]AAWG[xxxv], la Asociación de Confianza en Línea (OTA)[xxxvi], el Consejo de comerciante de Riesgos (MRC)[xxxvii], y los Equipos del Foro de Seguridad y Respuesta ante Incidentes (FIRST)[xxxviii] son algunas de las tantas organizaciones con membresía para abordar los fraudes en línea y los delitos informáticos. Las reuniones de los miembros, las publicaciones y los grupos de interés especial ofrecen muchos beneficios a las marcas que están sufriendo ataques de phishing. El APWG, por ejemplo, ofrece amplias capacidades de intercambio de información y presentación de informes de gran escala sobre los sitios de phishing a las organizaciones miembros, convirtiéndose en un recurso primordial para las instituciones afectadas por ataques de phishing.

REFERENCIAS

ESTADÍSTICAS

- Informe de tendencias sobre actividades de phishing/Informe sobre uso de dominios del Grupo de Trabajo Antiphishing
  http://www.antiphishing.org/resources/apwg-reports/

  [N.B.: El APWG puede brindar hojas de cálculo con datos de origen sobre los informes presentados en 2006, según solicitud por escrito. Contacto: secretarygeneral@apwg.org]http://www.apwg.org/reports/APWG_CrimewareReport.pdf
- Encuesta global sobre phishing del Grupo de Trabajo Anti-Phishing:
  http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf
- Encuesta sobre vulnerabilidad en la Web del Grupo de Trabajo Anti-Phishing
  http://www.apwg.org/reports/apwg_web_vulberabilities_survey_june_2011.pdf
- Phishing: ¿Cuántos muerden el anzuelo? Gobierno de Canadá
  http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspx

PROGRAMAS A NIVEL DE USUARIO

- El Código de Conducta Anti-Bot para Proveedores de Servicios de Internet: http://www.m3aawg.org/abcs-for-ISP-code
- iCode.org - Asociación de la Industria de Internet: https://icode.org
- Centro de Asesoramiento Antibotnet - ECO (Alemania): https://www.botfrei.de/en/
- PARA. PIENSA. CONÉCTATE.: http://www.stopthinkconnect.org
- Consejo al consumidor del APWG: http://www.antiphishing.org/resources/overview/
- Educación para el consumidor del APWG: http://www.antiphishing.org/resources/Educate-Your-Customers/

PRESENTACÓN DE INFORMES SOBRE PHISHING:

Grupo de Trabajo Anti-Phishing:
http://www.antiphishing.org/report-phishing/
Correo electrónico: reportphishing@apwg.org

Principales proveedores de webmail/navegadores:
Google:
https://www.google.com/safebrowsing/report_phish/
Microsoft:
www.microsoft.com/security/online-privacy/phishing-scams.aspx#Report
Yahoo:
https://safety.yahoo.com/Security/IVE-BEEN-PHISHED.html

Recursos en línea para proveedores de seguridad:
http://www.phishtank.orghttp://www.phishtank.org
https://submit.symantec.com/antifraud/phish.cgi
http://phishing.eset.com/report
http://toolbar.netcraft.com/report_url

Estados Unidos:
El Centro de Reclamos sobre Delitos en Internet brinda un servicio centralizado de informe sobre casos de cyberdelincuencia que hayan causado pérdidas:
www.ic3.gov/default.aspx
El Equipo de Respuesta ante Emergencias Informáticas (US-CERT, en inglés) también tiene dónde enviar informes sobre phishing:
https://www.us-cert.gov/report-phishing
Correo electrónico: phishing-report@us-cert.gov
El sistema de informe sobre spam de la Comisión Federal de Comercio envía información a la Base de Datos Centinela del Consumidor, una herramienta de orden público para contactos investigativos:
UCE@ftc.gov

Canadá:
Centro de informe sobre spam: fightspam.gc.ca
Correo electrónico: spam@fightspam.gc.ca
Centro Canadiense Anti-Fraude:
www.antifraudcentre.ca/english/reportit-howtoreportfraud.html
Asociación Bancaria de Canadá enumera la lista de "Informe sobre Phishing" para la mayoría de los bancos canadienses: www.cba.ca/en/consumer-information/42-safeguarding-your-money/91-email-fraud-phishing

Reino Unido:
El Centro Nacional de Informe sobre Ciberdelincuencia y Fraude maneja los reclamos sobre fraude, intento de fraude y virus o estafas en línea Para informe un caso de fraude, los consumidores deben utilizar el siguiente enlace.
www.actionfraud.police.uk/report_fraud
La Herramienta para Informar Acciones de Fraude Comercial está dirigida a expertos en seguridad que necesitan informar muchas acciones de fraude por día:
https://app03.actionfraud.police.uk/report/Account

Irlanda:
https://www.botfrei.de/ie/ueber.html

Australia:
http://www.acma.gov.au/Citizen/Stay-protected/My-online-world/Spam/reporting-spam-i-acma
https://www.scamwatch.gov.au/content/index.phtml/tag/reportascam
https://report.acorn.gov.au/
Correo electrónico: report@submit.spam.acma.gov.au

Nueva Zelanda:
http://complaints.antispam.govt.nz/

Francia:
https://www.signal-spam.fr
EL CERT-LEXSI francés, Europol y los gobiernos de los Países Bajos y Luxemburgo también ofrecen un sitio para informar casos de phishing:
https://phishing-initiative.eu

LAS MEJORES PRÁCTICAS RECOMENDADAS

- Qué hacer si su sitio web ha sido pirateado
  http://www.apwg.org/reports/APWG_WTD_HackedWebsite.pdf
- Advertencia sobre registros de subdominios
  http://www.apwg.org/reports/APWG_Advisory_on_Subdomain_Registries.pdf
- Las mejores recomendaciones sobre prácticas antiphishing para registradores
  http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf
- Medidas para proteger los servicios de registro de dominio contra el abuso o el mal uso
  http://www.icann.org/committees/security/sac040.pdf
- Las mejores prácticas de comunicación para remitentes del M³AAWG
  https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf
- La confianza en un correo electrónico comienza con la autenticación (Papel blanco de autenticación de correo electrónico del M³AAWG)
  https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Email_Authentication_Update-2015.pdf
- Las mejores prácticas antiphishing del M³AAWG/APWG para ISP y proveedores de casillas de correo electrónico
  https://www.m3aawg.org/sites/default/files/M3AAWG_AWPG_Anti_Phishing_Best_Practices-2015-06.pdf

NOMBRES DE DOMINIO Y DIRECCIONES IP

Una variedad de actividades ilegales y malintencionadas se aprovechan de vulnerabilidades en el DNS como resultado de malas prácticas comerciales y de seguridad entre operadores de Internet para manejar la infraestructura y los registros de nombres de dominio, registradores, revendedores y proveedores de servicios proxy y de privacidad. Es posible mitigar estas amenazas mediante un mejor manejo por parte de los operadores de red y mejores prácticas desarrolladas por las organizaciones que gestionan direcciones IP y nombres de dominio, u organizaciones que proveen servicios de registro de nombres de dominio.

DESCRIPCIÓN GENERAL SOBRE TECNOLOGÍA

DIRECCIONES IP

Cada equipo de Internet tiene una dirección IP, que se utiliza para dirigir el tráfico desde y hacia ese equipo. Las direcciones IP tradicionales, conocidas como IPv4, son números binarios de 32 bits, invariablemente, por escrito como cuatro números decimales, tales como 64.57.183.103. La primera parte de la dirección, que en este ejemplo podría ser 64.57.183, identifica la red, y el resto de la dirección, 103 en este ejemplo, el equipo en particular ("host") en la red. La división entre la red y el host varía según el tamaño de la red, por lo que el ejemplo anterior es simplemente típico. Una versión más reciente, IPv6, utiliza números de 128 bits mucho más grandes, escritos como bloques de dígitos separados por dos puntos, por ejemplo 2001:500:2f::f. Casi todas las direcciones IPv4 ya han sido asignadas, por lo que ahora se encuentran en medio de una transición gradual a IPv6.

Para que el tráfico de red fluya desde un equipo a otro, por ejemplo, desde el equipo de un usuario a los servidores web de Google o viceversa, el tráfico desde el equipo emisor fluye a través de equipos intermedios, llamados enrutadores, hacia su destino.

Existen alrededor de 500.000 rutas de red visibles a los enrutadores más grandes de Internet, conocidos como enrutadores troncales. (El número total de redes es mucho mayor, ya que una única ruta troncal normalmente cubre docenas de miles de redes de clientes). Para mantener las tablas de 500.000 rutas, los enrutadores troncales utilizan un sistema llamado protocolo de puerta de enlace de borde (BGP) para intercambiar información, por lo que los enrutadores pueden ajustar automáticamente las tablas cuando llegan nuevas redes en línea o un enlace entre redes falla o se repara.

Como un número de teléfono, cada dirección IP visible al mundo debe ser única. Los proveedores de Internet y las grandes empresas obtienen bloques de direcciones directamente de los Registros Regionales de Internet, como ARIN, que asigna espacio IP para los Estados Unidos, Canadá y partes del Caribe, mientras que las empresas más pequeñas y los individuos utilizan partes de bloques asignados a sus proveedores de Internet. Algunas direcciones IP no son visibles al mundo, por ejemplo 192.168.1.1 o 10.0.0.51; estas son análogas a las extensiones de la central de conmutación (PBX) del sistema telefónico de una empresa, que sólo se pueden acceder desde dentro de la propia red de la organización.

EL SISTEMA DE NOMBRES DE DOMINIO

Dado que a los seres humanos les resulta difícil recordar las direcciones IP y estas se atan a redes físicas, el DNS es una base de datos distribuida de nombres que les permite a las personas usar nombres como www.google.com en lugar de la dirección IP correspondiente 173.194.73.105 (para IPv4) o 2607:f8b0:4000:807::1012 (para IPv6). A pesar de su enorme tamaño, el DNS posee un rendimiento excelente mediante la delegación y las memorias caché. Dado que no sería práctico almacenar todos los nombres del DNS en una sola base de datos, que se divide en zonas que están almacenados en diferentes servidores, pero lógicamente unidas entre sí.

En principio, para encontrar la dirección de www.google.com de Google, el software de consultas al DNS en el equipo del usuario, llamado resolutor, contacta primero a uno de los servidores "raíz", que responde enviando la información de los servidores de resolución del TLD .com. Luego el resolutor envía la consulta a los servidores de resolución de .com, que responde enviando la información de los servidores de resolución de google.com. En el siguiente paso, el resolutor del usuario envía la consulta a esos servidores de google.com, que responden finalmente con la dirección IP asociada al dominio www.google.com.

Dado que los usuarios de Internet tienden a buscar los mismos nombres en varias ocasiones, los dispositivos de los usuarios individuales, junto con los servidores de resolución de DNS, tienen una memoria caché que recuerda las últimas consultas y respuestas del DNS, permitiendo que las consultas posteriores pueden ser respondidas desde esa memoria temporal en lugar de viajar de nuevo a través de todo el DNS, reduciendo la cantidad de consultas que llega hasta los servidores raíz y acelerando los tiempos de respuesta para los usuarios.

Dado que existen diferentes maneras en las que actores hostiles pueden inyectar datos del DNS falsificados en la memoria temporal de los servidores de resolución y de los dispositivos de los usuarios (algunas se discuten a continuación), DNSSEC añade firmas criptográficas seguras a los datos devueltos por los servidores del DNS, por lo que el equipo del usuario puede comprobar la validez de las firmas y asegurar que los datos del DNS que utiliza son legítimos y que en realidad proceden de un actor igualmente legítimo. DNSSEC ha estado en desarrollo durante 17 años, pero sólo se ha utilizado de manera significativa en los últimos años. La administración de las llaves de cifrado de DNSSEC es compleja y puede presentar un desafío para los administradores de los servidores de resolución.

ATAQUES CONTRA EL DNS

Los ataques más graves al DNS son ataques que afectan a los servidores de resolución, en los que los ciberdelincuentes introducen datos falsos para redirigir el tráfico web y otro tráfico a versiones falsas de los sitios web más populares.

ENVENENAMIENTO DE LA MEMORIA CACHÉ

Una categoría de tales ataques es el envenenamiento de la memoria caché, es decir, la utilización de los agujeros de seguridad para introducir datos falsos en la memoria caché de los servidores de DNS, que luego son enviados a los equipos de las víctimas. Pocos usuarios tendrán alguna capacidad para detectar la información falsa del DNS al utilizar sus equipos. Mediante la combinación de múltiples ataques en conjunto, un delincuente puede presentar una réplica perfecta de un sitio web,

un sello de confianza, un logotipo y mostrar el nombre de dominio correcto en la barra de direcciones del navegador. El resultado puede ser el robo de credenciales, el acceso a los recursos financieros, la afectación de la inteligencia corporativa o del Estado o la Nación, o el redireccionamiento de ingresos por publicidad.

Los ataques en contra de los servidores de resolución se producen completamente dentro del proveedor de servicios de resolución de dominios (NSP, por ejemplo, un servidor de resolución corporativo o un servicio público de DNS como OpenDNS o Google DNS) y los sistemas de los operadores de red, sin que sea necesario comprometer los dispositivos de los usuarios.

Cuando todos los involucrados han implementado DNSSEC correctamente, incluyendo al registrante del dominio, el registrador, el registro y el proveedor de servicios de resolución, se evita el envenenamiento de la memoria caché y otras usos incorrectos del DNS. En este momento, DNSSEC no está ampliamente implementado y por esta razón aún no se considera una defensa contundente contra los ataques de envenenamiento de la memoria caché. La defensa implementada actualmente contra el envenenamiento de la memoria caché se llama Source Port Randomization (UDP), pero esta defensa requería, en 2008, que todas las herramientas de software del DNS se actualizaran a la última versión.

El software del DNS, al igual que todo el software de infraestructura de Internet, se debe actualizar periódicamente para corregir los defectos conocidos a medida que el proveedor de software los descubre y corrige. Se recomienda realizar una supervisión cuidadosa en todo momento para detectar condiciones anómalas en la infraestructura en línea. Esta supervisión es de suma importancia después de la actualización de un software, ya que una actualización podría corregir algunos defectos, e introducir otros.

La seguridad contextual también requiere una mención. Aún si el software del DNS estuviera completamente libre de errores, sería necesario actualizar, proteger y supervisar el sistema operativo y los sistemas de virtualización, además de los como enrutadores, conmutadores, firewalls y los sistemas de detección y prevención de intrusiones. El documento RFC 2196, Manual de Seguridad del Sitio, ofrece una visión general de estas cuestiones.

MEJORES PRÁCTICAS RECOMENDADAS:

1. Respalde la implementación mundial de DNSSEC para garantizar la distribución de datos del DNS. Esto incluye la firma de todas las zonas de autoridad con DNSSEC y la habilitación de la validación de DNSSEC en todos los servidores recursivos del DNS.
2. Utilice TSIG para todas las actualizaciones de DNS en línea y para las operaciones de "transferencia de zona" entre servidores, para garantizar la autenticidad y que provengan de servidores con autoridad (*authoritative*).
3. Instale los parches de la últimas versiones recomendadas por los proveedores en el software del DNS y supervise la infraestructura de DNS en busca de anomalías en todo momento, pero en especial después de instalar un parche del proveedor.
4. Elabore un documento sobre mejores prácticas recomendadas respect de una política de seguridad para los resolutores del DNS, con el fin de educar a los administradores de sistema y de red.

MALWARE QUE ATACA AL DNS

El método "DNS Changer" es otra manera de falsificar respuestas del DNS. Este malware modifica el equipo de la víctima para cambiar los resolutores que utiliza el DNS, sustituyendo los resolutores del DNS del ISP del usuario por servidores controlados por delincuentes. De esta forma, el delincuente proporciona respuestas falsificadas en forma selectiva cada vez que hacerlo le brinde un ingreso adicional.

El malware DNS Changer funciona no sólo en el equipo de los usuarios, sino también en los enrutadores de hogar o de pequeñas empresas. La ventaja del delincuente al alterar la configuración del enrutador es que el cambio es probablemente más duradero y cubre todos los equipos, teléfonos, iPads y otros dispositivos del hogar o de la oficina, que incluyen posiblemente dispositivos de control del hogar habilitados para Internet, como termostatos, cámaras, marcos de fotos, redes conectadas o inalámbricas, etc. El enrutador puede estar dentro del módem proporcionado por el servicio de banda ancha o puede ser un dispositivo adicional adquirido e instalado por el usuario.

El FBI trabajó con la industria privada para quitar a los ciberdelincuentes responsables del DNS Changer sus recursos (y su libertad).[xxxix] Las direcciones IP utilizadas por los resolutores comprometidos fueron re-enrutadas hacia servidores específicos que estuvieron en operación durante unos meses mientras grupos de voluntarios notificaban a los ISPs y a los usuarios afectados. Nota: la estrategia básica utilizada por los delincuentes responsables del DNS Changer funcionaría de igual manera ante un nuevo intento: todas las vulnerabilidades subyacentes necesarias están aún presentes en equipos muy populares que los proveedores no pueden actualizar.

La detección de tráfico DNS mal dirigido se puede realizar a nivel del ISP mediante la supervisión del tráfico del DNS saliente del cliente que se dirige hacia un resolutor diferente al proporcionado por el mismo ISP. Tenga en cuenta que es muy común que los usuarios que poseen conocimientos técnicos avanzados, o quienes se suscriben intencionadamente a un servicio de DNS diferente, envíen su tráfico de DNS hacia otro lugar. El diseño cuidadoso de los sistemas de detección es necesario para evitar falsos positivos.

En el futuro, los usuarios pueden ser engañados para cambiar a un resolutor de DNS de un delincuente mediante ingeniería social o algún incentivo. Por ejemplo, si se requieren resolutores del ISP para denegar el acceso a algunos nombres del DNS (como contenido pirata o ilegal), los usuarios pueden responder a las ofertas de acceso a servidores de DNS no censurados. Existen muchas razones legítimas para permitir a los usuarios elegir su servicio de resolución de DNS sin censura o interferencia.

MEJORES PRÁCTICAS RECOMENDADAS:

1. Eduque al público sobre los peligros de los cambios de resolutores de DNS, para limitar los ataques de ingeniería social.
2. Fomente el que los operadores de redes compartan información anonimizada a través de *feeds* de las memorias locales (*cache*) de alto nivel de sus servidores de DNS, relativa a consultas enviadas a través de sus redes, con el fin de detecar posibles servidores de DNS maliciosos.

3. Permita acceso a esos feeds a investigadores anti-abuso para ayudar en la detección de servicios que engañan a los usuarios o falsifican respuestas de DNS, adicionalmente con el fin de diferenciarlos de los servicios legítimos de resolución de DNS.
4. Desarrolle estadísticas basadas en los datos agregados para ayudar a identificar a los delincuentes con el fin de tomar acciones legales, actualizar listas negras de resolutores ilegítimos y crear operaciones coordinadas de mitigación, como ocurrió en el caso de DNS Changer.
5. Establezca las mejores prácticas recomendadas para lograr un adecuado nivel de anonimidad, con el find de evitar que se asocie a cada usuario, su ISP y la actividad que desarrolla en el DNS. Así se pueden evitar represalias contra los usuarios que eluden formas de censura y se evita también que estos usuarios decidan utilizar servidores de DNS de más difícil detección, que posiblemente están comprometidos.

ATAQUES CONTRA LOS SERVICIOS DE REGISTRO DE NOMBRES DE DOMINIO

La facilidad con la que los ciberdelincuentes pueden registrar y utilizar nuevos dominios les ayuda a llevar a cabo sus fraudes. El uso de información de identidad falsa y, a menudo, de credenciales financieras robadas dificulta la detección de los verdaderos propietarios de los dominios que se utilizan para cometer fraude. La carga de detectar el uso malicioso de los nombres de dominio descansa sobre los hombros de los investigadores anti-abuso, con frecuencia mucho después de que la actividad malintencionada haya comenzado o, en ocasiones, finalizado. La carga de reducir la cantidad de dominios maliciosos está en las empresas que proporcionan acceso a Internet a los usuarios, ya sea mediante solicitudes de suspensión o cancelación de actividad maliciosa o a través de la frecuentemente lenta propagación de las listas de bloqueo de dominios. Las listas de bloqueo son necesarias ya que las solicitudes para redirigir, suspender o eliminar nombres de dominio a menudo se ignoran.

Los ciberdelincuentes explotan los servicios de registro de nombres de dominio mediante el uso de tarjetas de crédito robadas, mediante el registro automatizado de muchos dominios a alta velocidad, mediante el registro de dominios a través de distribuidores o proveedores de servicios de privacidad o de proxies que frecuentemente no responden o parecen permitir la actividad maliciosa, y mediante el uso de dominios que pueden utilizar en cuestión de minutos o incluso segundos después del registro. Los investigadores de ataques por lo general sólo pueden monitorear la información de registro en el DNS cada 24 horas. Los operadores de listas de bloqueo se tardan en reconocer los dominios maliciosos y propagar la información sobre reputación, una vez los delincuentes han llevado han desarrollado su actividad maliciosa.

Los ciberdelincuentes pueden crear cualquier subdominio bajo los dominios que hayan registrado, por ejemplo nombredebacno.ssl-cgi.delincuente.com. No existen restricciones en cuanto a la cantidad de este tipo de nombres que se pueden crear sin costo. El engaño a los usuarios no requiere un nombre de marca; simplemente cualquier cosa que parezca legítima. Los nombres como secure-order.verified. example.com son aceptados por la mayoría de los usuarios ya que se parecen a otros que ven a menudo.

Algunas entidades y personas incluso ayudan a abusar de marcas al crear dominios que pueden crear confusión en los usuarios. Estos servicios crean nombres de dominio que voluntariamente imitan

marcas mediante el uso de errores tipográficos, como SEARZ con la letra "Z" en lugar de la letra "S", o PAYPA1 con un dígito "1" en lugar de una letra "L". Mientras que estos dominios no se pueden utilizar en una campaña de phishing, hay millones de este tipo de dominios que dificultan la tarea de los investigadores de ataques para distinguir typosquatters relativamente inofensivos, frente a la actividad maliciosa como tal, antes de que ésta suceda.

Además, los atacantes se roban los nombres de dominio a través de otras técnicas, por ejemplo:

- Comprometer las credenciales de acceso del registrante al panel de control del registrador (robar la contraseña que los clientes utilizan para iniciar sesión en su sitio de administración del dominio);
- Comprometer los sistemas propios del registrador con el fin de robar todas o algunas de las contraseñas (conocidos como códigos EPP o códigos de autenticación) que se requieren para transferir los nombres de dominio de un registrador a otro; y
- Comprometer los servidores de DNS del mismo registrante o su base de datos de DNS con el fin de alterar los datos del dominio de la víctima *in situ*, sin ningún cambio de redireccionamiento ascendente (*no upstream redirection*).

MEJORES PRÁCTICAS RECOMENDADAS:

1. Los registros de nombres de dominio, tanto de dominios genéricos de alto nivel (gTLD) como de código de país (ccTLD), así como a los registradores con quienes hacen negocios, deben implementar y supervisar de cerca los programas "Conozca a su cliente" (*Know Your Client* o *KYC*) para prevenir el abuso en el registro de los dominios. Esto les permitirá determinar si deben evitar hacer negocios con un registro, un registrador, un distribuidor o un proveedor de servicios de privacidad/proxy y cuándo deben hacerlo.
2. Todos los registros de nombres de dominio, los registradores, revendedores y proveedores de privacidad/proxy deberían implementar autenticación de múltiple factor vía HTTPS obligatoria, para reducir el riesgo de robo de credenciales de acceso a las cuentas de sus clientes y para proteger de una manera más apropiada las sesiones transaccionales de sus clientes.
3. Los registros de nombres de dominio y los registradores deberían considerar acuerdos de cooperación o memorandos de entendimiento con las organizaciones que ayudan a proteger a los consumidores, por ejemplo LegitScript y APWG. Mediante el establecimiento de niveles predefinidos de confianza, los reportes de abuso que son enviados por estas entidades pueden ser abordados de una manera mucho más rápida y efectiva, siendo una de estas vías el Programa de Suspensión de Dominios Maliciosos del APWG (*Malicious Domain Suspension Program* o *AMDoS*).
4. Los registros y los registradores de nombres de dominio deberían verificar el uso de tarjetas de crédito robadas, para evitar el registro de dominios maliciosos.
5. Hacer cumplir las obligaciones legales (en sus propias jurisdicciones) y contractuales que los proveedores de servicios de registro de dominio, incluyendo los registros, registradores, revendedores y proveedores de servicios de privacidad/proxy deben cumplir, en lo que respecta a la respuesta frente a reportes de abuso.

6. Respecto de los servicios de privacidad y proxy, hay una necesidad urgente de implementar y hacer cumplir programas de acreditación. Estos aclararán las normas y procedimientos respecto de las solicitudes de *retransmisión* (*relay*), es decir, cuando deben reenviar comunicaciones a sus clientes, y *revelar* (reveal), es decir, cuando deben revelar la identidad de su cliente. Esto aplica para todos los servicios de proxy y privacidad, independientemente de si operan en el espacio de los gTLDs o los ccTLDs, e independientemente de si un registro o un registrador es propietario, administrador u operador de estos servicios.
7. Los registros y registradores para los espacios gTLD y ccTLD deberían evitar hacer negocios con proveedores de servicios de proxy/privacidad que no están cubiertos por un programa de acreditación.
8. Antes de procesar las solicitudes de registro de nuevos nombres de dominio o aceptar transferencias entrantes de dominios, los registradores y los operadores de ccTLDs que ofrecen servicios de registro directamente al público deberían validar la reputación de ciertos elementos de datos de registro, como:
    a. direcciones de correo electrónico utilizadas por los solicitantes, el titular de la cuenta o cualquiera de los otros contactos de Whois;
    b. la dirección IP desde la que se solicitan las transacciones;
    c. los servidores de nombres que los clientes desean asociar a sus nombres de dominio;
    d. la dirección postal del titular; y
    e. una muestra estadísticamente válida de nombres de dominio ya registrados por el mismo cliente.

    A modo de ejemplo, un servicio de validación de reputación lo proporciona sin costo alguno la *Secure Domain Foundation*, que le permite a los registradores y a los registros decidir si desean negar la creación de un nuevo nombre de dominio, o aceptar transferencias entrantes, si alguno de estos datos tiene mala reputación, que indica actividad malintencionada reciente e importante.
9. Mejorar los algoritmos usados para definir la reputación de dominios y direcciones IP, con el fin de incluir en ellos la antigüedad de cada dominio como factor reputacional: los dominios que tienen más de un año son menos propensos a ser dominios desechables; algunos organismos de acreditación de correo evitan que los clientes utilicen dominios de menos de un mes y, usualmente, examinardominios de menos de un día es una manera eficaz de detectar actividad maliciosa.
10. Puesto que los delincuentes que roban dominios utilizan direcciones IP que son generalmente diferentes de las utilizadas por los solicitantes, los registradores y los revendedores deberían habilitar la verificación de las direcciones IP desde la que se origina la actividad de las cuentas de sus clientes. Si la cuenta de un cliente es accedida desde una nueva dirección IP, el registrador o el revendedor deberìan informar al registrante y al contacto administrativo del nombre de dominio en cuestión.
11. Continuar las mejoras a los navegadores de Internet y a la educación de los usuarios con el fin de que éstos puedan reconocer las señales del navegador de los certificados de validación extendida ("barra verde"), y para evitar la confusión en los sitios que utilizan términos como "seguro" o "ssl".
12. Capacitación a las empresas para que envíen notificaciones a los usuarios que sean difíciles de imitar, para disminuir el phishing y la ingeniería social.

13. Para el software y los sitios que utilizan listas de bloqueo de dominios, fomente un enfoque *multi-layer* con diversos tipos de listas de bloqueo que incluyan métodos de bloqueo preventivo y listas de naturaleza reactiva, con el fin de mejorar la eficacia del bloqueo.
14. Respalde proyectos de DNS pasivo, como el *Secure Information Exchange* (SIE) de Farsight Security Inc (FSI) que proporcionan alertas tempranas a los investigadores académicos y comerciales sobre los subdominios maliciosos activamente en uso.
15. Considere tecnologías de firewall de DNS como las *Response Policy Zones* o *RPZ*s, que son un mercado abierto con múltiples proveedores y consumidores que ofrecen políticas sobre recomendaciones de resolución a servidores de DNS recursivos. (Véase http://dnsrpz.info/).

ATAQUES A LA WEB Y A OTROS DNS DE SERVIDORES

Los ciberdelincuentes atacan la reputación de dominios legítimos mediante el ingreso en sus servidores web y la inyección de archivos maliciosos que luego infectan al dominio legítimo en la dirección URL. (Esta técnica es inmune a las listas de bloqueo de dominio a menos que las listas estén dispuestas a incluir dominios legítimos que distribuyen contenido malicioso, también bloqueando de esta manera algún contenido legítimo).

Los ciberdelincuentes utilizan redireccionamientos web para presentar inicilalmente dominios con buena reputación y luego redirigir al usuario al sitio malicioso. Estos individuos utilizan múltiples niveles de redireccionamiento y recientemente incluso han redireccionado tráfico hacia direcciones URL con direcciones IP numérica sen lugar de nombres de dominio.

El éxito de estas técnicas depende de métodos inadecuados de detección que sólo son capaces de reconocer este tipo de ataques si los usuarios no "actúan como una víctima" siguiendo los redireccionamientos. Lamentablemente, algunos actores complican aún más las cosas al usar múltiples niveles de redireccionamiento para rastrear la reacción de los consumidores frente a los correos electrónicos de marketing. Los servicios de acortamiento de URL son a menudo atacados y utilizados para redirigir tráfico desde dominios conocidos como bit.ly hacia los sitio web de los ciberdelincuentes. Es difícil para los usuarios distinguir entre millones de URLs legítimas de bit.ly, que son utilizadas para acortar una dirección web extensa para una publicación de Twitter, de las que se utilizan para insertar un malware o, por ejemplo, un anuncio para la venta ilegal de productos farmacéuticos.

Hace un tiempo la misma ICANN fue víctima de un grupo de atacantes que logró acceder a la cuenta de administración de los dominios de ICANN en register.com. En este caso, los atacantes alteraron la configuración del DNS de varios dominios (icann.net iana-servers.com, icann.com y iana.com) y redireccionaron el tráfico de los visitantes a un sitio web modificado.

MEJORES PRÁCTICAS RECOMENDADAS:

1. Establezca y mantenga un sistema de bloqueo de dominios legítimos comprometidos con contenido malicioso, junto con prácticas de notificación rápida, un segundo nivel de testeo que permita desbloquear dominios no maliciosos y asistencia para mejorar la seguridad en todos los servidores web asociados al dominio comprometido.
2. Fomente que los servicios de acortamiento de URL verifiquen y reverifiquen todos los redireccionamientos de la cadena para toda redirección que brinden y que trabajen con varios proveedores de servicios de protección contra abuso para identificar nuevos atacantes.

3. Educar a la industria y a los usuarios finales y darles recursos que les permitan identificar y evitar URLs acortadas que no cuenten con suficientes medidas anti-abuso.
4. Mejorar la eficacia de las pruebas relativas a la verificación de la reputación de las URLs mediante, entre otros, la realización de pruebas a las redirecciones, el uso de pruebas que simulen usuarios reales que siguen los redireccionamientos y mediante el desarrollo de políticas relacionadas con la cantidad máxima de redireccionamientos , todo con el fin de reducir el abuso de los servicios de acortamiento de URLs.

ATAQUES A DIRECCIONES IP

Los ataques a direcciones IP se clasifican en dos categorías generales: correos electrónicos cuya dirección IP no es real (*spoofing*) y redes que utilizan rangos de direcciones IP que no están autorizados (*rogue announcements*).

SUPLANTACIÓN DE DIRECCIONES IP

Cada paquete de datos enviado a través de Internet incluye las direcciones IP "fuente" del equipo desde donde fue enviado y del equipo hacia dónde está destinado. Es posible que un equipo hostil ponga una dirección de origen (suplantada) falsa en el tráfico saliente. Para las transacciones en las que el destino envía un paquete de retorno a la dirección de origen, en particular el DNS, esto puede crear tráfico no deseado a la dirección de origen falsificada. Es fácil enviar solicitudes al DNS de tamaños pequeños que generan respuestas de gran tamaño, causando denegaciones de servicio en contra de la dirección que haya sido falsificada.

MEJORES PRÁCTICAS RECOMENDADAS:

1. Los ISP y las redes de tráfico deberían filtrar el correo electrónico entrante, realizar el seguimiento del rango de direcciones asignado a cada cliente de red y descartar el tráfico con direcciones de origen fuera del rango asignado, para evitar que sus clientes envíen tráfico con direcciones de origen falsificadas. Esto se conoce generalmente como BCP 38[xl], un documento de la IETF con las mejores prácticas actuales. El BCP 84, otro documento de la IETF con las mejores prácticas actuales, recomienda que los proveedores de conectividad de IP que preceden en la cadena filtren los paquetes que ingresan en sus redes de clientes que siguen en la cadena y desechen los paquetes que tienen una dirección de origen que no está asignada a esos clientes.[xli]
2. Fomente una práctica universal de *ingress filtering* para todos los clientes conectados a redes vecinas (*peer networks*).

ANUNCIOS DESHONESTOS

Toda red puede anunciar vía BGP sus propios rangos de direcciones IP. Las redes hostiles pueden anunciar rangos de red que no están autorizados a utilizar. Esto puede resultar en un redireccionamiento y desvío de tráfico destinado a la red real, o puede permitir un tráfico "sigiloso" que anuncia un rango de direcciones específico; el ataque se produce y luego el anuncio se retira. A menos de que las víctimas sean conscientes del *rogue announcement*, se culpará al propietario legítimo de las direcciones.

MEJORES PRÁCTICAS RECOMENDADAS:

1. Los operadores de red deberían implementar un filtro de *ingress filtering* BCP 84[xlii] (se discute más arriba), en el que los anuncios de BCP entrantes desde los clientes y usuarios del mismo nivel se limitan a una lista explícita de redes conocidas y asignadas a ese cliente o usuario del mismo nivel.
2. Los ISP deben procurar, en la medida de lo posible, aplicar BGPSEC (seguridad BGP) para proteger criptográficamente los anuncios de ruta y evitar la publicación de datos deshonestos.

ROBO DE RANGOS DE DIRECCIONES

En los primeros días de Internet, la asignación de direcciones a menudo se hacía con bastante informalidad, con registros incompletos. Como resultado de ello, se ha *heredado* un espacio considerable de direcciones asignadas que puede ser obsoleto, ya sea porque las empresas ya no recuerdan los rangos de direcciones que les fueron asignados o porque las empresas que los recibieron ya no existen. Los ciberdelincuentes han aprovechado estas direcciones abandonadas mediante la falsificación de documentos o el nuevo registro de dominios abandonados usados en correo electrónico para obtener el control del espacio obsoleto de direcciones IP.

MEJORES PRÁCTICAS RECOMENDADAS:

1. Los registros regionales de Internet deberían implementar y cumplir con los procedimientos para verificar la identidad de los supuestos dueños del espacio heredado, para evitar que los ciberdelincuentes obtengan el control del espacio de direcciones. ARIN, el RIR de América del Norte, ha detallado los procedimientos para ello.[xliii]

REFERENCIAS

- Wikipedia, Discusión del DNSSEC: http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- RFC 2196, *Site Security Handbook*, B. Fraser, Ed., September 1997, http://www.rfc-editor.org/info/rfc2196
- RFC 4034 *Resource Records for the DNS Security Extensions*. R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. March 2005, http://www.rfc-editor.org/info/rfc4034
- RFC 4035 Protocol Modifications for the DNS Security Extensions. R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. March 2005, http://www.rfc-editor.org/info/rfc4035
- Advertencia de vulnerabilidad VU#800113 del CERT de los Estados Unidos, “Múltiples implementaciones de DNS vulnerables al envenenamiento de la caché”, http://www.kb.cert.org/vuls/id/800113/
- Grupo de Trabajo para DNS Changer, http://www.dcwg.org/

- Brian Krebs, “A Case of Network Identity Theft”, http://voices.washingtonpost.com/securityfix/2008/04/a_case_of_network_identity_the_1.html
- Proyecto de resolutores abiertos, http://openresolverproject.org/
- Las mejores prácticas recomendadas de enviados del M³AAWG, https://m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf
- FCC Cuatro informes del III Grupo de Trabajo de la FCC CSRIC sobre las mejores prácticas recomendadas sobre seguridad del BGP: http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

AMENAZAS MÓVILES Y DE VOZ

EL ENTORNO MÓVIL

Con la llegada de los teléfonos inteligentes y los mercados de aplicaciones para dispositivos Android, Apple, Windows y Blackberry, los consumidores utilizan cada vez más sus dispositivos móviles para acceder a las cuentas en línea, realizar compras y realizar otras transacciones financieras. Los teléfonos inteligentes representan el 70 % de los casi 1850 millones de teléfonos móviles vendidos en todo el mundo en 2014[xliv], con Android y iPhone dominando la esfera de los dispositivos que actualmente se utilizan. Las tabletas, que confunden el límite entre el teléfono y computadora tradicional, se han convertido también en un actor significativo en este ámbito. Las ventas minoristas de dispositivos móviles, que incluyen las tabletas, aumentó del 11 % del mercado electrónico mundial en 2011[xlv] al 13 % en 2014[xlvi]

En el mundo, existen aproximadamente 3700 millones de usuarios activos de telefonía móvil[xlvii], que supera el 50 % de la población mundial de 7300 millones de habitantes,[xlviii] y los teléfonos móviles son el principal punto de acceso a Internet para muchas partes del mundo. En el último trimestre de 2014, los proveedores enviaron más de 500 millones de unidades móviles a todo el mundo.[xlix]

MERCADOS DE APLICACIONES

A diferencia del mercado del software, donde las principales aplicaciones son desarrolladas por proveedores conocidos y confiables y los usuarios son menos propensos a instalar aplicaciones de fuentes menos confiables, el ecosistema de las aplicaciones móviles fomenta que los usuarios finales descarguen una gran cantidad de aplicaciones de bajo costo desde pequeños proveedores que con frecuencia son menos confiables como, en algunos casos, empresas unipersonales. En muchos países, la mayoría de las aplicaciones se obtiene de los mercados de aplicaciones que poseen un nivel de seguridad inadecuada, y que brindan aplicaciones con malware incluido. En otros países, los usuarios se pueden limitar inicialmente a la carga de aplicaciones que provienen sólo de proveedores del OS del teléfono o de mercados de aplicación aprobados por el operador; sin embargo, los usuarios pueden omitir configuraciones, permitiendo así el acceso a cualquier aplicación del mercado. Los principales proveedores de OS para teléfonos, por ejemplo Google, Apple, Microsoft y RIM operan mercados de aplicaciones de alto volumen con mayor seguridad. Apple, por ejemplo, tiene 1,4 millones de aplicaciones en su tienda de aplicaciones y genera un total acumulado de USD 25 000 millones en ventas de aplicaciones y desarrolladores de juegos hasta la fecha. Sin embargo, la escala de incluso los mercados más seguros de aplicaciones dificulta la prevención de la oferta ocasional de malware. Como el comercio electrónico ha migrado al entorno móvil, los actores maliciosos y estafadores se han adaptado rápidamente.

AMENAZAS ESPECÍFICAS Y LAS MEJORES PRÁCTICAS RECOMENDADAS

SEGURIDAD DE LOS MERCADOS DE APLICACIONES

Los teléfonos inteligentes pueden ser afectados por la instalación de nuevo software, a menudo obtenido de mercados controlados por el fabricante del OS del teléfono. En 2014, Symantec halló que el 17 % (más de 160 000) de todas las aplicaciones Android eran realmente malware oculto[l]. En una revisión de las 100 aplicaciones de salud disponibles en la tienda de aplicaciones, el 20 % transmitían las credenciales del usuario sin cifrarlas, más de la mitad (el 52 %) no tenía ninguna política de privacidad visible y, en promedio, cada aplicación contactó cinco de dominios de Internet (típicamente una mezcla de publicidad y servicios de seguridad)[li].

Algunos proveedores de sistemas operativos y mercados de aplicaciones tienen la capacidad de eliminar aplicaciones maliciosas de los teléfonos si las aplicaciones fueron originalmente descargadas desde los mercados de aplicaciones. Antes de entrar en esos mercados, las aplicaciones son rechazadas si violan las políticas de seguridad correspondientes.

Apple ha colocado más restricciones en las aplicaciones antes de permitirles ingresar en el mercado (el llamado *App Store*). La tienda Google Play tiene una política de aceptación más abierta y depende más de la eliminación de aplicaciones aceptadas que son malintencionadas o violan las políticas de la tienda de aplicaciones.

Cuando un consumidor compra un teléfono inteligente, el acceso a la tienda de aplicaciones no oficiales por lo general está desactivado; el teléfono sólo puede ingresar en un pequeño grupo de tiendas de aplicaciones "oficiales" (por ejemplo, el fabricante del OS y el operador de telefonía móvil). Los dispositivos móviles que utilizan el sistema operativo Android tienen una configuración denominada "orígenes desconocidos" con una casilla de verificación para autorizar la instalación de aplicaciones fuera del mercado. El usuario puede configurar los teléfonos Android para permitir la conexión a tiendas de aplicaciones no oficiales o alternativas. Los dispositivos de Apple requieren un proceso técnicamente más difícil de "jailbreaking"; sin embargo, para los usuarios menos experimentados, el jailbreaking se ofrece como un servicio de bajo costo en muchos quioscos y puntos de venta. Incluso para acceder a las tiendas de aplicaciones alternativas y legítimas, como la tienda de aplicaciones de Amazon, esta casilla de verificación puede ser necesaria. Lamentablemente, luego el teléfono queda abierto a la instalación de fuentes desconocidas. Entonces, es más fácil que los usuarios instalen malware. El creador del malware consigue un pase libre sin supervisión por parte de cualquier tienda de aplicaciones móviles y oficial una vez habilitado el acceso a tiendas de aplicaciones no oficiales.

También existen nuevas formas de que los estafadores evadan las restricciones de la tienda de aplicaciones incluso si el teléfono está configurado para utilizar sólo la tienda de aplicaciones oficial. Los navegadores de dispositivos móviles pueden utilizarse para instalar aplicaciones HTML5, que coloca un ícono en la pantalla principal del dispositivo que se asemeja a una aplicación instalada en una tienda de aplicaciones. Los delincuentes luego pueden atacar vulnerabilidades en el navegador de stock que viene con el dispositivo móvil o los navegadores alternativos que el usuario puede elegir para instalar. Los vínculos desde el navegador con las funciones nativas del dispositivo como cámara, micrófono, marcadores de teléfono y ubicación geográfica pueden ser utilizados por un delincuente para obtener datos de carácter personal y las actividades actuales del usuario del dispositivo móvil.

El inicio de sesión de usuario y la contraseña que utiliza cada dispositivo móvil para acceder a la tienda de aplicaciones y autorizar las compras es un punto importante de vulnerabilidad. Una vez que obtienen estas credenciales, los delincuentes pueden causar pérdidas financieras e instalar spyware. Los sistemas operativos para móviles de Apple y Google en la actualidad requieren el mismo usuario y la misma contraseña como clave para ingresar a la tienda de aplicaciones y al resto de los servicios que incluyen equipos portátiles, almacenamiento de archivos en la nube, contactos, calendario y correo electrónico. Mientras sólo un nombre de usuario y una contraseña en el pasado le permitirían a un delincuente acceder a la cuenta de correo electrónico del suscriptor, las mismas credenciales ahora brindan el acceso a la tienda de aplicaciones. En varios casos, los usuarios han sufrido la eliminación de datos de equipos portátiles y teléfonos después de que los delincuentes obtienen esta información clave. Diferentes proveedores ofrecen una protección antivirus para algunos teléfonos e intentan probar todas las aplicaciones nuevas en las tiendas de aplicaciones para descartar actividad o intentos maliciosos.

LAS MEJORES PRÁCTICAS RECOMENDADAS SOBRE LAS TIENDAS DE APLICACIONES PARA EL GOBIERNO Y LA INDUSTRIA:

1. "Neutralidad de la aplicación": Le permite a los usuarios, a los operadores de redes o terceros confiados para especificar de manera explícita otras tiendas de aplicaciones "confiables", y tal vez el nivel de confianza asociado a cada uno. Esto le permite a los consumidores elegir otras tiendas de aplicaciones de confianza sin exponerlos a un riesgo de descargas desde fuentes desconocidas.
2. Identifique aplicaciones con potencial malicioso mediante exámenes de seguridad rigurosos antes de permitirles el acceso a las tiendas de aplicaciones para evitar reclamos futuros.
3. Proporcione advertencias, controles y educación a los usuarios para reducir los incidentes de usuarios que son engañados mediante instrucciones malintencionadas para evadir las medidas de seguridad.
4. Mejore las políticas de seguridad para el restablecimiento de contraseñas para las tiendas de aplicaciones y evitar que los delincuentes obtengan credenciales que no les pertenecen.
5. Es posible bloquear auriculares para acceder únicamente a las tiendas de aplicaciones oficiales, como una medida anticompetitiva. Mientras que los consumidores pueden estar bien protegidos por este modelo, invita a los consumidores a emplear soluciones que presentan vulnerabilidades en la seguridad (por ejemplo, dispositivos para jailbreaking, rooting o desbloqueo). Las políticas que permiten o asisten en el bloqueo de la tienda de aplicaciones se deben comparar con el impacto de las vulnerabilidades de seguridad creadas por el desbloqueo.
6. Fomente la membresía de las tiendas de aplicaciones en centros de análisis de amenazas en línea/de botnet, de modo que se pueden beneficiar de análisis, alertas e informes procedentes de estos centros. Es posible detectar, marcar y eliminar las aplicaciones malintencionadas de la manera más rápida posible.
7. Proporcione mecanismos que le permitan a los usuarios realizar un informe sobre aplicaciones potencialmente malintencionadas.

EL MALWARE MÓVIL

Existen aplicaciones maliciosas, llamadas malware móvil, para dispositivos Android, iOS, Windows Phone, Symbian (Nokia) y Blackberry. Actualmente la mayoría de malware móvil apunta a la plataforma Android en áreas con abundante uso de los mercados no oficiales de la aplicación.

La mayoría del malware es o parece ser una aplicación útil y se distribuye en sitios web o a través de tiendas de aplicaciones no oficiales. Con frecuencia, los promotores de malware corromperán aplicaciones legítimas mediante la inserción del código "troyano". Así, los usuarios pueden instalar estas aplicaciones modificadas, sin saber que contienen código malicioso. Los delincuentes utilizan cada vez más la publicidad digital como vehículo para propagar malware; esto se conoce como malvertising. También, el año 2014 vio la aparición de "SMS Worm"[lii] que se propaga a través de SMS entre las listas de contactos de teléfonos móviles infectados. Los destinatarios son engañados para hacer clic en el enlace malicioso que viene en el SMS y que conduce al ataque en sí. Si instalan el ataque entonces sus contactos recibirán el mismo SMS malicioso que hace que este vector de ataque sea muy viral.

En general, el malware realiza acciones que generan ingresos para los atacantes. Los esquemas de monetización directa causan pérdidas financieras directas a la víctima e incluyen aplicaciones malintencionadas que pueden realizar una gran variedad de funciones, por ejemplo el envío de mensajes SMS premium a un código corto registrado por los atacantes, la descarga de contenidos pagos por descarga; clic en vínculos de pago por clic; la realización de llamadas salientes a números de teléfono; interceptación de credenciales de homebanking; la solicitud de un pago por rescate para desbloquear dispositivos de las víctimas. Los atacantes también pueden generar ingresos indirectamente por la recolección de números de teléfono para envío de spam por SMS, recolección de dispositivos y datos de usuario para marketing, despliegue de anuncios, venta de aplicaciones comerciales de spyware y uso del dispositivo infectado para atacar moneda encriptada. Además, las aplicaciones comerciales de spyware le permiten a un tercero supervisar a una persona y recopilar datos de dispositivo y usuario como mensajes SMS, correos electrónicos, ubicación y registros de llamadas.

A continuación se muestran ejemplos destacados de malware para Android, Blackberry e iOS.

Ataque de Oleg Pliss (2014): El ataque de Oleg Pliss utiliza un ataque que afecta a iCloud para bloquear el iPhone de usuarios.

Slocker.A (2014): Aparentemente, Slocker.a es la primera instancia de ransomware móvil de cifrado de archivos. Encripta archivos de datos del usuario en dispositivos Android y luego exige un pago para obtener la clave.

SMScapers (2013 – actualidad): Este malware parece una aplicación para adultos y se difunde a través de la publicidad móvil. Realiza cargos ocultos mediante el envío de un SMS a un código corto de tipo premium y suprime la notificación de SMS entrante de importancia. La campaña se dirigía principalmente al Reino Unido; sin embargo la aplicación de la reglamentación ha contribuido a una brusca disminución de dicha actividad. La campaña se dividió en más de veinte entidades jurídicas diferentes por lo añadió complejidad al proceso de ejecución. La campaña todavía existe en otros 15 países[liii, liv].

Worm.Koler (2014 – actualidad): El año 2014 sufrió el ataque de Android Ransomware donde surgieron numerosas muestras, como ScareMeNot, ScarePackage y ColdBrother. Los Estados Unidos observaron que Worm.Koler se extendía a través de SMS a los contactos almacenados en los teléfonos infectados. El taque también bloquea el dispositivo de las víctimas con una advertencia del FBI falsa que indica el contenido ilegal encontrado en el auricular. Luego se les solicita a las víctimas luego pagar una multa para evitar cargos delictivos y para liberar sus teléfonos.

DeathRing (2014 – actualidad): DeathRing apunta principalmente a Asia y se trata de un malware que intenta suplantar datos confidenciales de las víctimas mediante el envío de SMS falsos. El vector de ataque es único dado que el malware parece sugerir que los delincuentes se infiltraban en la cadena de suministro en algún momento.

LAS MEJORES PRÁCTICAS RECOMENDADAS PARA LA INDUSTRIA Y EL GOBIERNO PARA EVITAR EL MALWARE MÓVIL:

1) Eduque a los consumidores, mediante anuncios de servicio público, páginas web, folletos y otros medios para hacer lo siguiente:
   a) Obtener aplicaciones sólo en mercados de aplicaciones de proveedores con buena reputación que verifican las aplicaciones o los desarrolladores o directamente de los proveedores de aplicaciones reconocidos.
   b) Revisar y entender las pantallas de autorización, los acuerdos de licencia de usuario final, las políticas de privacidad y los términos del acuerdo al instalar las nuevas aplicaciones.
   c) Mantener las restricciones de seguridad predeterminadas en el dispositivo y no hacer jailbreak en el dispositivo (el jailbreak se discute a continuación).
   d) Instalar localizador remoto y sistema de bloqueo de software para asistir en la recuperación y protección de datos en teléfonos robados y perdidos. Por ejemplo, la identidad internacional del equipo móvil (IMEI) es un código de 15 o 17 dígitos que identifica de forma exclusiva un teléfono móvil. El código IMEI le permite a una red GSM o UMTS (Servicio Universal de Telecomunicaciones Móviles) bloquear un teléfono extraviado o robado para que no pueda realizar llamadas.
   e) Instalar y ejecutar software de seguridad móvil en todos los dispositivos.
2) Desarrollar instalaciones y animar a los consumidores a realizar la notificación de aplicaciones sospechosas.
3) Alentar, automatizar y facilitar la realización de la copia de seguridad de datos del teléfono a una nube o a medio de almacenamiento personal (por ejemplo, un equipo).
4) Evaluar el uso de soluciones de seguridad móvil, como un navegador seguro, soluciones de gestión del dispositivo móvil (MDM), espacios aislados móviles y aplicaciones que previenen la pérdida de datos con el fin de minimizar el riesgo de infección y el impacto resultante.

   Un excelente ejemplo de la educación del consumidor con las mejores prácticas recomendadas fue creado por Ofcom y puede encontrarse aquí: http://consumers.ofcom.org.uk/files/2014/1394750/using-apps-safely-and-securely.pdf

AMENAZAS MIXTAS

Los dispositivos móviles ahora se utilizan en el proceso de autenticación de múltiples factores para inicios de sesión de cuenta de alto valor. Un ejemplo de la amenaza mixta de autenticación bifactorial es un usuario que visita un sitio web financiero en su equipo de escritorio e inicia sesión con un nombre de usuario y una contraseña como en el pasado. Pero ahora, el banco exige un paso más para que el usuario acceda a su cuenta: recibir una llamada o un mensaje de texto en su teléfono móvil con un código que el usuario luego escribe en el navegador web del equipo de escritorio. Este paso adicional se añadió debido a existen muchos equipos de escritorio infectados con malware que han enviado la contraseña del banco a los delincuentes. Los delincuentes han demostrado ser persistentes en el ataque a cada nuevo método de protección. Ahora deben obtener ambas contraseñas financieras del usuario y luego llamar su teléfono móvil, y ser capaces de relacionarlas.

Esto hace que los teléfonos sean un blanco aún más valioso para que los delincuentes los ataquen y tomen el control. Este control puede ser físico en el caso del robo del teléfono del usuario o realizado remotamente con un software espía que ataca el dispositivo móvil. De cualquier manera, las amenazas mixtas requieren más esfuerzo de parte de los delincuentes y probablemente apunten a cuentas o sistemas de mayor valor.

Las aplicaciones de un dispositivo móvil también se utilizan como generadores de token, como los códigos de seis dígitos que solíamos ver solamente en los dispositivos de autenticación físicos bifactoriales, como Google Authenticator y Amazon AWS Virtual MFA.

Según el punto de ventaja de los delincuentes, pueden ser capaces de observar el contenido del tráfico entrante y saliente de algunos dispositivos móviles y recopilar los códigos de autenticación. Este es el caso con los códigos enviados por correo electrónico, que algunos bancos ofrecen como opción. El tráfico de SMS (mensajes de texto móvil) no está cifrado.

La falta de una infraestructura para compartir información sobre amenazas mixtas se puede convertir en una amenaza; permite una gran cantidad de ataques que de lo contrario no existirían. Lo que se necesita es diseñar e implementar estrategias de defensa e infraestructuras que involucren entidades técnicas, políticas, policiales y jurídicas en varios países.

MODIFICACIÓN DE DISPOSITIVOS MÓVILES

Muchos fabricantes de equipos originales (OEM) y los operadores de red móvil (MNO) establecen entornos móviles y seguros para mantener la estabilidad y seguridad del dispositivo, y lograr una experiencia de usuario positiva. En muchos casos, la modificación de estos entornos crea vulnerabilidades de seguridad que pueden exponer la información de usuario, habilita el robo de servicio en la forma de llamadas telefónicas o mensajes de texto sin autorización, habilita el control remoto de los recursos del dispositivo, como micrófonos o cámaras que permiten escuchar o ver sin consentimiento del usuario o habilita a un enemigo para realizar una larga lista de otras actividades no autorizadas.

Existen numerosas técnicas para modificar el hardware y software de un dispositivo, pero tres de las modificaciones más conocidas son el "jailbreaking", el "rooting" y el "desbloqueo".

JAILBREAKING DE UN DISPOSITIVO

"Jailbreak" es cuando una persona reemplaza los controles incrustados en un dispositivo. El fabricante puede utilizar controles OEM para aplicar permisos de la aplicación, proteger áreas críticas del sistema de archivos en un dispositivo, forzar la autenticación de aplicaciones en el dispositivo, hacer cumplir la complejidad de la contraseña, entre muchas otras funciones administrativas.

¿Por qué se hace jailbreaking en un dispositivo? Una razón es que, incluso con cientos de miles de aplicaciones disponibles, algunas personas quieren una versión personalizada o modificada de las aplicaciones móviles. En algunos casos, una aplicación modificada puede costar menos que la aplicación oficial (pero puede violar los derechos de autor); sin embargo, la aplicación menos costosa puede también contener contenido malicioso.

ROOTING DE UN DISPOSITIVO

El jailbreaking le permite a un usuario suplantar controles y elevar el acceso del usuario para obtener los privilegios de raíz de un dispositivo, que en última instancia concede al usuario todos los privilegios del sistema operativo. El "rooting" de un dispositivo le permite al usuario los más altos privilegios de un sistema operativo.

¿Por qué se hace rooting a un dispositivo? Además de cargar aplicaciones personalizadas o no autorizadas y evitando controles, el acceso a la raíz habilita que un usuario modifique los componentes y la funcionalidad del OS, o lo reemplace por completo, en un dispositivo. Algunos sistemas operativos instalados en dispositivos móviles se basan en una forma UNIX con un grupo limitado de comandos; mediante la modificación del sistema operativo, los usuarios pueden liberar almacenamiento eliminando funciones innecesarias para la mayoría de los usuarios de dispositivos móviles. El rooting de un dispositivo también le puede permitir a un usuario cargar comandos adicionales según lo desee.

DESBLOQUEO DE UN DISPOSITIVO

Los operadores de redes móviles (MNO) pueden subvencionar las ventas de teléfonos móviles bajo un contrato que requiere el uso de la red del MNO durante un período de tiempo. Para ayudar a prevenir el fraude y el robo, los MNO utilizan con frecuencia un medio técnico conocido como "bloqueo" que restringe el uso del teléfono en su propia red. Un dispositivo se puede desbloquear normalmente introduciendo un único "código de desbloqueo" proporcionado por un MNO según sea solicitado o por cumplimiento de un compromiso contractual. Los consumidores también pueden

encontrar o comprar un código de desbloqueo en línea. Asimismo, si se obtiene el código de fuentes de terceros, los usuarios corren el riesgo de perder datos o tener malware instalado por un vendedor de confianza.

LAS MEJORES PRÁCTICAS RECOMENDADAS A UN INDIVIDUO SOBRE LA MODIFICACIÓN DE DISPOSITIVOS MÓVILES:

1. El jailbreaking, el rooting y el desbloqueo de dispositivos no se recomienda a cualquier persona que busca un dispositivo estándar, estable con el soporte del OEM a largo plazo, ya que pueden introducir vulnerabilidades desconocidas para el usuario.
2. No utilice servicios no oficiales de desbloqueo ofrecidos por "terceros".

LAS MEJORES PRÁCTICAS RECOMENDADAS PARA LA INDUSTRIA Y EL GOBIERNO EN RELACIÓN CON LA MODIFICACIÓN DE DISPOSITIVOS MÓVILES:

1. Desarrolle y promueva la educación y concientización del consumidor sobre los riesgos de la modificación de dispositivos móviles.
2. Cree fuertes protecciones contra la modificación de los OEM.
3. Haga cumplir la ley contra aquellos que promueven ataques a las plataformas móviles.

AMENAZAS DE BANDA BASE

Existen varios tipos de amenazas de banda base. Algunas pueden implicar la creación de una red GSM (sistema Global para comunicaciones móviles) ilícita que atrae a los dispositivos conectarse a ella. Otros pueden implicar ataques que involucran mensajes especialmente diseñados para atacar vulnerabilidades de seguridad en dispositivos móviles. Con el crecimiento de la investigación de bajo costo y las instalaciones GSM delictivas, estas amenazas han proliferado.

Operación Safety Net

Ejemplo: Zeus Mitmo (Hombre en el medio/móvil)

Zeus es un troyano que se ataca a equipos que utilizan Windows e intenta robar información bancaria mediante la pulsación del inicio de sesión en el navegador junto con la recuperación de formularios. Los mecanismos típicos de la proliferación de Zeus eran mediante actividades de descarga oculta e intentos de phishing que engañan al usuario a navegar hacia un sitio malicioso. Se identificó por primera vez allá por 2007 y ha recibido muchas actualizaciones que han incrementado su sofisticación; más recientemente, se observó el ataque en la esfera móvil. Esta actualización beneficia al malware Zeus ya que muchas empresas, incluso las instituciones financieras, están usando SMS como un segundo vector de autenticación, por lo que tener el nombre de usuario en línea y la contraseña ya no es suficiente para el robo de identidad. La evolución de este vector de amenaza establece una alternativa planeada por una pandilla de Zeus: infectar el dispositivo móvil y "olfatear" todos los mensajes SMS que se entregan. El escenario se describe a continuación.

- El atacante roba el nombre de usuario en línea y la contraseña mediante un malware (ZeuS 2.x).
- El atacante infecta el dispositivo móvil del usuario porque lo obliga a instalar una aplicación malintencionada mediante un SMS o un malware que imita una aplicación productiva o bancaria legítima.
- El atacante inicia sesión con las credenciales robadas mediante el equipo del usuario como proxy/socks y realiza una operación específica que requiere autenticación mediante SMS.
- Se envía un SMS al dispositivo móvil del usuario con el código de autenticación. El malware instalado en el dispositivo reenvía el SMS a otra terminal controlada por el atacante.
- El atacante escribe el código de autenticación y completa la operación.

Los piratas informáticos luego utilizan esta información para controlar cuentas bancarias de las víctimas y realizar transferencias no autorizadas a otras cuentas, típicamente dirigidas a cuentas controladas por redes de mulas de dinero.

Tradicionalmente, la operación de una red GSM requiere una inversión considerable, que prácticamente no permitió la investigación fuera de las grandes instituciones, y restringió el descubrimiento y la explotación de los ataques basados en la red. Por ejemplo, para suplantar a una red GSM, un atacante tendría que operar una BTS. Cuando se implementó la tecnología GSM, los ataques basados en la red contra dispositivos finales no ocasionaban mayor preocupación, por lo que los teléfonos no solicitaban autenticación de las redes a la que conectaban. Sin embargo, recientemente el software libre de código abierto, como OpenBTS, ha permitido que cualquier persona cree su propia red GSM a una fracción del costo de los equipos a nivel del operador, y se iniciaron estudios de seguridad GSM al alcance de los investigadores de seguridad y delincuentes.

LAS MEJORES RECOMENDACIONES PARA LA INDUSTRIA Y EL GOBIERNO PARA EVITAR LAS AMENAZAS DE BANDA BASE:

Como portadores de adoptan nuevas tecnologías (por ejemplo, 3G y 4G/LTE), los teléfonos móviles deberían solicitar la autenticación de la infraestructura del operador a la que se conecta.

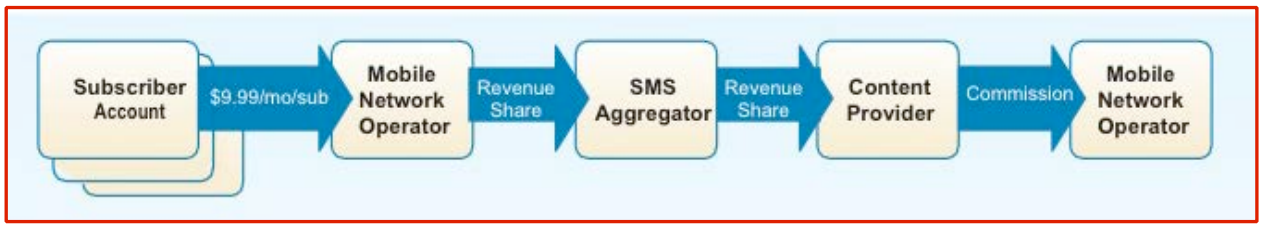
1. Los proveedores de servicios pueden trabajar con fabricantes de teléfonos para notificar a los usuarios cuando el auricular abre una sesión que no utiliza autenticación mutua. Esto alertaría al usuario de este posible vector de amenaza.

ATAQUE MEDIANTE EL SERVICIO DE TARIFA ELEVADA

Normalmente, estos servicios se ofrecen como servicios para aplicaciones de voz y texto facturadas a la cuenta móvil prepaga o postpaga de un suscriptor; los servicios de tarifa elevada comprenden horóscopos pagos por única vez y recurrentes, donaciones de dinero ante desastres, créditos para juegos, asesoramiento y servicios de chat, consejos amorosos mensuales por SMS y una amplia gama de otros esquemas.

EL MODELO COMERCIAL DE TARIFA ELEVADA:

El deseo de crear un ecosistema de aplicación amigable y ampliamente utilizado ha conducido a desarrollar entornos de facturación complejos y largos con varios modelos de participación en los ingresos, como la típica suscripción mensual a SMS por USD 9,99/mes, que son ampliamente atacable (se representa más abajo).



En este ejemplo, un operador de red móvil permite que "agregadores de SMS" independientes obtengan la ruta de un bloque de "códigos breves" (normalmente, se trata de números telefónicos de 4-7 dígitos enrutables dentro de alguna porción de la red de telefonía mundial). El agregador de SMS luego vende conectividad bidireccional y móvil de SMS a un propietario conocido de aplicación de horóscopo, llamado proveedor de contenidos. El proveedor de contenidos paga una comisión por cada suscripción de un afiliado a la publicidad. Las partes adyacentes sólo pueden estar relacionadas en forma libre.

Las partes y las relaciones se vuelven cada vez más problemáticas hacia la derecha de este diagrama. En algunos casos, los proveedores de contenido permiten relaciones sólo por Internet con una autenticación deficiente y con afiliados a la publicidad que facilitan una posible denegación del spam y/o fraude propio o de sus afiliados. Los mecanismos de pago casi anónimos, como transferencias a bancos extranjeros, las transacciones en efectivo virtual no reglamentada en Internet o los mecanismos de pago en línea reducen las barreras y facilitan el fraude al spam.

Las estafas mediante el servicio de tarifa elevada han estado ocurriendo durante muchos años, pero la mayor penetración de los servicios móviles, la evolución de datos móviles y el establecimiento de un ecosistema de ciberdelincuencia mundial han llevado un aumento en la cantidad y variedad de los ataques. El fraude puede ocurrir en casi cualquier paso del proceso del servicio o del pago, desde engañar al usuario para que de forma involuntaria use o se subscriba a un servicio, un afiliado que reclama una subscripción falsa, hasta un malware móvil que sigilosamente envía mensajes a los servicios de tarifa elevada sin el conocimiento del abonado.

Malware de tarifa elevada

Phonepay Plus, el regulador de servicios de tarifa elevada del Reino Unido emitió multas por £330 000 en tres empresas diferentes en diciembre de 2014 tras descubrir que estaban usando malware móvil para generar cargos a propietarios de teléfonos Android. El malware residía en aplicaciones que se descargaban automáticamente sin el consentimiento del usuario cuando visitaban ciertos sitios web para adultos. Una vez instaladas, los consumidores iniciaban de manera involuntaria una suscripción mediante un clic en cualquier lugar en la pantalla. La aplicación entonces enviaba mensajes de texto

Un ataque frecuente involucra a estafador que establece un número de servicio de tarifa elevada y realiza una llamada de voz de "un ring" o envía un mensaje de texto a una víctima, con la esperanza de que respondan. Esto conduce a que la persona que llama lo hace a un servicio de pago por llamada sin su conocimiento o consentimiento. También se ha observado la suscripción no autorizada, "forzada" a los "consejos amorosos" de tarifa elevada o a otros servicios de mensajes de texto de afiliados y/o proveedores de contenidos.

Esto ha causado que muchos agregadores de SMS implementen una verificación secundaria, normalmente mediante un mensaje de confirmación o un intercambio de pines entre los suscriptores al SMS y el agregador de SMS. Pero incluso estos han sido atacados; por ejemplo, el malware para Android GGTracker envía un mensaje SMS de suscripción y confirmación sin conocimiento de los suscriptores.[lv]

La suplantación de identidad del suscriptor, a través del acceso no autorizado a redes o ataques criptográficos es otro método para cometer fraude con tarifa elevada.

LAS MEJORES RECOMENDACIONES PARA A INDUSTRIA Y EL GOBIERNO PARA EVITAR LAS ESTAFAS MEDIANTE LOS SERVICIOS DE TARIFA ELEVADA:

El fraude mediante servicios de tarifa elevada es similar a muchos otros tipos de delitos cibernéticos; se aborda, por lo tanto, de manera apropiada por una serie de técnicas frecuentes, como la autoprotección, la capacitación del consumidor y la protección del consumidor y medidas antimalware.

Muchos operadores móviles han establecido un servicio de notificación para permitir que los suscriptores informen spam por SMS mediante el reenvío de mensajes a un código breve (por ejemplo, 7726 que deletrea la palabra "spam"). Muchos gobiernos y agencias de orden público responsables del spam por SMS spam en algunos países han definido sus propios números para enviar informes, como 1909 en India, 33700 en Francia, y 0429999888 en Australia.

Las medidas específicas para evitar los fraudes de tarifa elevada son la defensa temprana, las acciones sociales y la confirmación adicional.

1. **Reclamos a TSP o reguladores:** Fomente la presentación de reclamos de consumidores. Estos reclamos permiten que los TSP identifiquen la fuente de la amenaza e implementar los mecanismos de defensa que permitan la detección temprana, antes de que se haya transferido dinero. La inclusión y el cumplimiento de las cláusulas sobre la lucha contra ataques en sus términos y condiciones, los TSP y las plataformas de servicio de tarifa elevada puede bloquear los pagos realizados a los delincuentes antes de que ocurran. Se advierte al TSP en una etapa temprana a través de denuncias hace cumplir sus términos y condiciones, desautorizando el caso del delincuente. De manera similar, los reclamos ante los reguladores y las agencias de orden público proporcionan una inteligencia abundante que puede llevar a la aplicación de la ley contra los estafadores.
2. **Acciones de los socios respecto de las relaciones y los pagos:** El fraude depende de la extracción de dinero hacia una ubicación oculta o irrecuperable. Las partes se pueden proteger a sí mismos al exigir una identificación, calificaciones y autenticación válidas de terceros, mediante el uso de mecanismos de pago de buena reputación o por demorar el pago durante un período suficiente.
3. **Otras confirmaciones:** Como muchos de los ataques implican una comunicación falsificada o forzada entre partes adyacentes de la cadena de pago, las notificaciones y confirmaciones entre partes más respetadas pueden prevenir o identificar rápidamente el fraude. Ejemplos de esto comprenden un MNO o un agregador de SMS que confirma la suscripción con el suscriptor en lugar de confiar exclusivamente en las afirmaciones del elemento que precede en el flujo de pago.

SPAM MÓVIL

El siguiente escenario describe la reciente actividad spam internacional y demuestra el papel fundamental que juega la colaboración internacional, en particular entre empresas, como fundamental para la defensa redes y suscriptores.

El operador A y el operador B están en diferentes países; ambos países tienen muchos hablantes del mismo idioma. El spam que se origina en la red del operador A representa la mayoría del spam que ingresa en la red del operador B. El operador A rastrea el spam en su red mediante el informe del spam basado en código breve y el análisis de los registros del servidor de mensajería. El operador B

también tiene informes de spam basado en el código, pero no recopila los números de origen de los mensajes que son reportados como spam. Sin embargo, el operador B realiza una exploración antispam automatizada en el tráfico de mensajería. Como resultado, la red del operador B recopila información acerca de fuentes y el contenido de spam.

El operador A y el operador B descubrieron por separado el spam procedente de la red del operador A y destinado al operador B. El operador A elimina a los spammers que identifica en su red, pero sólo si ha recibido un cierto volumen de los informes de spam contra un número dado de origen. Por lo tanto, siempre que un spammer en la red del operador A envíe spam solamente a números eternos de la red del operador A, este puede enviar spam sin límites a los suscriptores del operador B, porque:

a) El operador A nunca recibirá informes de spam de sus propios abonados, su requisito para la activación de una interrupción; y

b) No existe información alguna sobre compartir prácticas para frustrar a los spammers internacionales.

En ausencia de datos compartidos entre los operadores, los spammers pueden funcionar libremente dentro de un determinado país si ellos envían su spam sólo para los suscriptores de los operadores *que no pertenezcan a la red en la que tienen sus cuentas*.

LAS MEJORES RECOMENDACIONES PARA LA INDUSTRIA Y EL GOBIERNO PARA EVITAR EL SPAM MÓVIL:

Diálogo e intercambio de información: Los spammers aprovechan las vulnerabilidades entre proveedores de servicios en las políticas contra el abuso, las defensas y el conocimiento. Una de las lecciones centrales aprendidas a partir de la proliferación del spam de Internet desde sus inicios en 1993 hasta la actualidad, cuando el spam ya representa aproximadamente el 90 % del tráfico de correo electrónico de Internet, es que cuando los participantes del ecosistema comparten información, cambia el juego para los spammers. El diálogo entre empresas y el intercambio de datos con terceros facilitadores, como desarrolladores de tecnología y organismos industriales es vital para proteger el ecosistema móvil de la migración de herramientas y las técnicas perfeccionadas de spam y de los spammers en Internet durante más de una década o más hacia el mundo móvil interconectado mundialmente cada vez más basado en IP.

Mientras que los siguientes puntos de datos no son críticos para la colaboración entre los proveedores de servicios, son útiles para frustrar a los spammers, y pueden ser capturados a través de informes de spam:

Elementos de datos	Notas
Número móvil del originador spam	MSISDN (el número único asociado con el microteléfono de un abonado) o IMSI (el número único de una tarjeta SIM)
Cantidad recibida de informes sobre spam	Requiere la recopilación y la correlación de informes
Cantidad de informantes únicos de spam	Útil pero no crítico
Red del originador de spam	Derivado de operaciones de búsqueda

Tenga en cuenta que ninguno de los elementos de datos identificados anteriormente brindan información de identificación personal del informante de spam. La información sólo se recoge en el número que se informó como spam de origen.

Como en el ejemplo anterior del operador A y el operador B, el intercambio de datos de los elementos anteriormente ayuda a combatir el correo no deseado dentro de un país determinado, tanto como lo hace a través de las fronteras del país.

Hay beneficios y riesgos para el intercambio internacional entre operadores de los datos seleccionados a partir de informes de spam. Los beneficios incluyen activando soluciones de quejas de suscriptores voluntarios. El intercambio de datos y el diálogo antispam entre operadores también facilita las acciones de vigilancia, refinamiento y cumplimiento de sus propias políticas de uso aceptable. Por último, el intercambio de datos puede proporcionar evidencia que corrobora las decisiones de interrupción del operador, así como para la aplicación de la ley, y los agentes reguladores. La colaboración internacional, entre operadores hacia estas metas hará que sea más difícil para los spammers móviles para ocultar.

Por otro lado, se deben estudiar cuestiones legales, de privacidad y de seguridad durante la implementación de toda colaboración internacional en esta esfera. En la actualidad, estas cuestiones actúan como un impedimento para la colaboración entre países. Algunos han señalado, sin embargo, que estos problemas de privacidad son injustificados porque 1) los informes sobre spam son enviados voluntariamente por los suscriptores; 2) no es necesario incluir ninguna información de identificación personal (PII) cuando se intercambian datos del reclamo; y 3) no es crítico incluir el contenido del mensaje en el intercambio de datos del reclamo. (Compartir el contenido del mensaje puede aumentar el riesgo de intercambio accidental de PII de los informantes o las personas que no sean el spammer. Sin embargo, el contenido de los mensajes informados como spam también puede ser útil para identificar y bloquear el spam).

En resumen, el intercambio internacional de ciertos elementos de datos entre operadores cambia el juego para los spammers, ya que les deja menos lugares donde esconderse. El intercambio de datos requerirá el diálogo y el consenso sobre los datos que se pueden compartir, así como los formatos de intercambio de datos entre los participantes del ecosistema.

La industria también se debe esforzar para informar a las agencias de orden público cuando se adviertan un comportamiento ilegal de sus redes y sistemas. La coordinación con las agencias de orden público, en la esfera penal y regulatoria, a menudo, puede llegar al origen de la amenaza, y elimina las ganas de terceros de participar en dicha conducta.

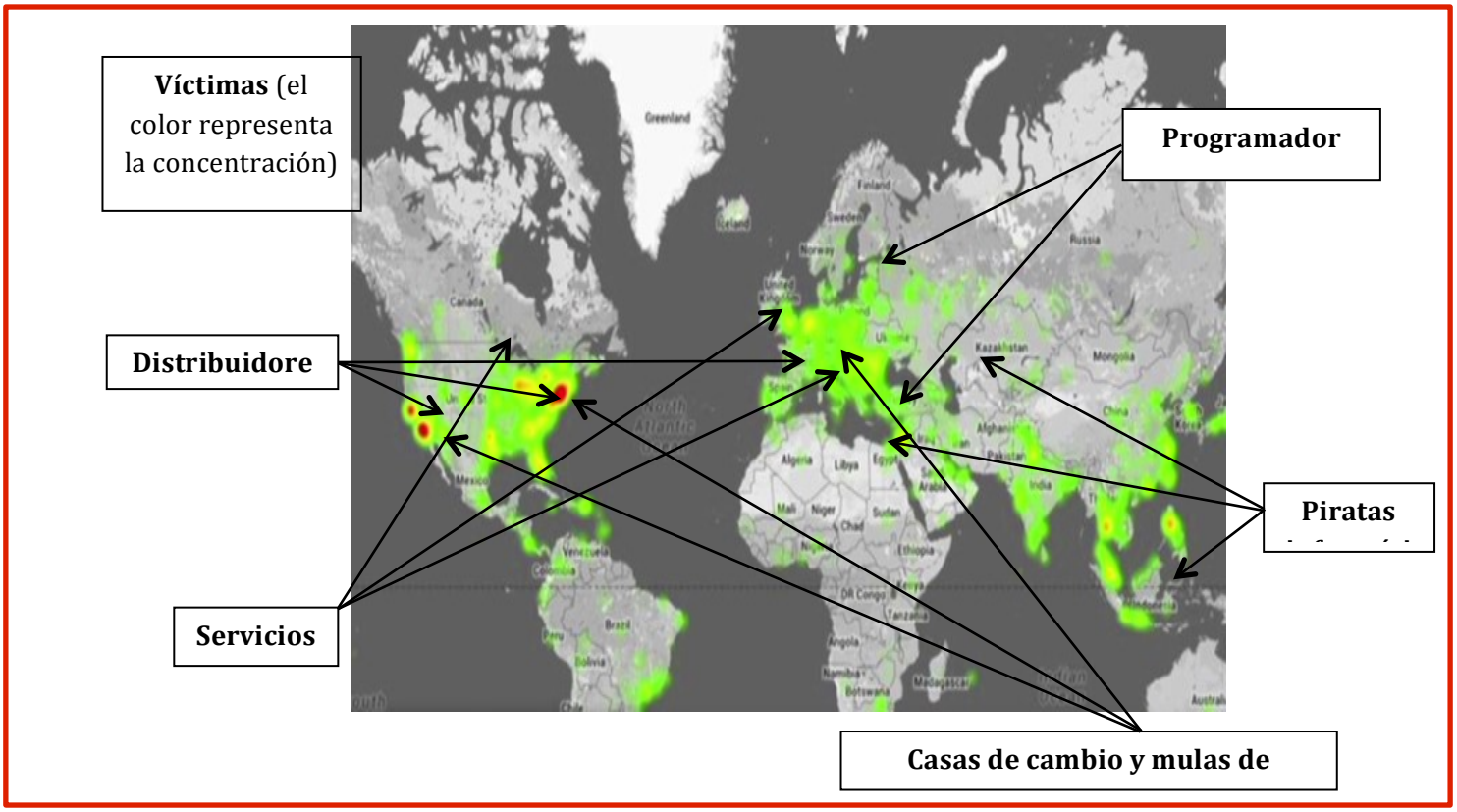
EL AUMENTO DE LOS ATAQUES INTERNACIONALES

A medida que las naciones combaten ataques y amenazas internos, los atacantes dirigen su atención a otra parte para identificar y atacar vulnerabilidades internacionales. Por ejemplo, la campaña de lucha contra el spam "Liberen a iPad/iPhone" realizada en América del Norte estaba dirigida inicialmente a los Estados Unidos. Los operadores de Canadá y los EE.UU. implementaron defensas técnicas para bloquear el spam enviado a sus suscriptores. Los atacantes rápidamente identificaron esto y comenzaron a enviar el spam de SMS a los abonados canadienses de teléfonos basados en los Estados Unidos, evitando así las defensas. Existen casos similares en términos de fraude, phishing, malware y spyware. En la mayoría de los casos (por ejemplo, el spam y el malware de defensa), se ha encontrado que es necesario detener el ataque en el origen, ya que las naciones receptoras pueden no

ser capaces de identificar el ataque oculto en los flujos de comunicaciones de alto volumen. Al igual que la Internet, las redes de comunicaciones móviles son globales y requieren un enfoque de defensa y colaboración internacional.

CONSIDERACIONES INTERNACIONALES

Los ciberdelincuentes tienen una fuerte preferencia por operar en un entorno internacional. Por ejemplo, un vendedor en línea de medicamentos ilegales que vive en los Estados Unidos podría enviar correo electrónico no deseado publicitando sus medicamentos de un equipo afectados en Brasil, dirigiendo a potenciales compradores a un sitio web con un nombre de dominio ruso, mientras que físicamente el servidor de ese sitio web está ubicado en Francia El pago de la compra con tarjeta de crédito se podría procesar a través de un banco en Azerbaiyán, el pedido podría ser enviado en barco desde un sitio en la India y el ingreso podría ser canalizado hacia un banco en Chipre. Los delincuentes saben que al actuar de esta manera existen muchos factores que complican las investigaciones oficiales de sus delitos en línea y reducen su probabilidad de captura. Estos factores son la falta de colaboración, las diferencias entre jurisdicciones y el costo de las investigaciones internacionales.



COOPERACIÓN INTERNACIONAL Y JURISDICCIÓN

Los agentes del orden público no poseen un poder ilimitado. En particular, un oficial de policía de una ciudad o país, normalmente no competente para citar documentos o detener a un criminal más allá de su propia jurisdicción. Las investigaciones transfronterizas requieren la cooperación internacional entre los organismos policiales nacionales e internacionales, un proceso que puede implicar procesos formales enormemente complejos, por no mencionar el tiempo y los recursos necesarios. Las complicaciones asociadas con estos procesos pueden demorar las investigaciones, o hacer que algunas investigaciones sean imposibles.

COBERTURA LEGAL Y JURISPRUDENCIA

Una actividad que es ilegal en un país puede no ser ilegal en otro. Por ejemplo, algunos países no tienen leyes relativas a spam por correo electrónico, ni han penalizado la difusión de malware. En otras jurisdicciones, el sistema legal no puede ser capaz de mantenerse al día con un flujo constante de nuevos fármacos, químicamente diferentes pero equivalentes. En otros casos, una ley puede estar en los libros, pero el país puede no tener antecedentes de procesar con éxito a aquellos que han violado ese estatuto. Cada una de estas condiciones son un desafío para las agencias de orden público y la colaboración.

Ejemplo: Estafa en un call center en India

Aproximadamente 60 000 personas en el Reino Unido fueron recientemente víctimas de una estafa multimillonaria en libras esterlinas. Los investigadores creen que el gran número de víctimas por la estafa de préstamos convierte a este hecho en uno de los fraudes más grandes jamás vistos en el Reino Unido. En su apogeo, más de 1000 personas por día que habían solicitado legítimamente préstamos sin garantía con bancos y compañías financieras recibían la "llamada fría" de los call center en Nueva Delhi; aproximadamente 100 personas por día fueron engañadas para firmar y pagar los gastos de procesamiento de un préstamo inexistente. Según la policía de India se robaron al menos £10 millones.

EL COSTO DE LAS INVESTIGACIONES INTERNACIONALES

El costo de operación internacional ocasiona que las agencias de orden público sólo se ocupen de los casos estrictamente locales. Si un investigador tiene que viajar a un país extranjero, el costo de los pasajes aéreos y otros gastos de viaje pueden ser considerables. Por lo tanto, las agencias con problemas de liquidez simplemente pueden no ser capaces de darse el lujo de trabajar en casos internacionales.

Irónicamente, al mismo tiempo que es caro para el oficial de policía trabajar en un delito de aspecto internacional, los delincuentes cibernéticos son a menudo capaces de adquirir bienes o servicios ilegales en el extranjero a través de Internet a precios irrisorios. Por ejemplo, un talentoso autor de malware de una nación económicamente devastada podría estar dispuesto a crear un malware que provocará millones de dólares en daños y perjuicios por unos pocos cientos de dólares. Estas condiciones generan en los ciberdelincuentes un gran incentivo para trabajar internacionalmente, y muchos, de hecho, lo hacen.

LAS MEJORES RECOMENDACIONES PARA EL GOBIERNO Y LA INDUSTRIA DE ACUERDO CON CUESTIONES DE COLABORACIÓN CRUZADA:

1. **Colaboración:** La clave de una defensa internacional efectiva es la colaboración. En primer lugar, los organismos gubernamentales y no gubernamentales en las naciones afectadas deben tomar conciencia de la cuestión. Luego, se requiere la colaboración para diseñar e implementar estrategias y una infraestructura de defensa que implican entidades técnicas, políticas, policiales y jurídicas en varios países. Los principales desafíos para lograr la colaboración necesaria son identificar el conjunto adecuado de foros y obtener la asistencia adecuada.

2. **Intercambio de información sobre amenazas/ataques:** El intercambio de información sobre amenazas y ataques es esencial para afrontar los desafíos que exceden las fronteras. Si bien se necesitan comunicaciones de humano a humano, la amplitud y magnitud de los ataques (por ejemplo, los miles de millones de mensajes de spam y de phishing recibidos diariamente) dictan la necesidad de enfoques mecanizados. También en este caso, para una infraestructura internacional mecanizada que sea implementada con éxito, se deben considerar los obstáculos para una implementación y la adopción generalizada, que incluye la fragmentación entre muchos sistemas dispares, diferentes necesidades funcionales de los diferentes países (incluso los impedimentos legales y cuestiones técnicas/tecnológicas) y las diferentes necesidades de los diferentes operadores. Una infraestructura general para el intercambio de información sobre ataques también deberá respaldar modelos de servidores centralizados y punto a punto e identificar los protocolos de formato y transferencia.
3. **Capacitación:** Con el fin de reconocer y responder a las amenazas móviles, los profesionales y las agencias de orden público tienen que estar al día con las nuevas tendencias y amenazas.

AMENAZAS TELEFÓNICAS DE VOZ

EL ENTORNO DE LA TELEFONÍA DE VOZ

Los consumidores tienen muchas opciones con respecto a las llamadas telefónicas de voz: conectados, inalámbricos, fuentes alternativas (por ejemplo, equipos). Estas llamadas pueden atravesar la red telefónica pública conmutada (PSTN) mediante un servicio de multiplexación por división de tiempo (TDM), voz sobre protocolo de Internet (VoIP), o una combinación de TDM y VoIP. La telefonía por Internet se refiere a la integración de los servicios de telefonía en las redes informáticas. Básicamente, el proceso convierte las señales de voz analógicas que fueron enviadas tradicionalmente a través de un teléfono fijo en señales digitales. Estas señales se transmiten a través de Internet y luego se convierten de nuevo en señales analógicas de voz.

El número de suscripciones de telefonía fija en todo el mundo alcanzó su punto máximo en 2006 y ha disminuido en forma anual desde entonces. Por ejemplo, las suscripciones de telefonía fija eran poco menos de 1110 millones de suscripciones en 2014, frente a los más de 1,14 millones de dólares en 2013. Al mismo tiempo, el número de abonados móviles y celulares está aumentando en todo el mundo, y se acerca rápidamente el número de personas en la tierra. Los abonados a la telefonía móvil alcanzaron los casi 7000 millones a finales de 2014, que corresponde a una tasa de penetración del 96 %, pero las tasas de crecimiento estuvieron en el nivel más bajo de la historia (del 2,6 % a nivel mundial), lo que indica que el mercado se está acercando rápidamente a niveles de saturación.

El protocolo de inicio de sesión (SIP) es un protocolo de comunicaciones para la señalización y el control de las sesiones de comunicación multimedia y se encuentra más frecuentemente en aplicaciones de telefonía por VoIP o Internet.

La TDM es un método de transmisión y recepción de señales independientes en una ruta de señales comunes por medio de conmutadores sincronizados en cada extremo de la línea de transmisión.

A finales de 2014, el número de suscripciones de banda ancha móvil alcanzó los 2,3 millones a nivel mundial, casi 5 veces más que tan sólo seis años antes (en 2008). Las suscripciones de banda ancha móvil fueron de 2,1 millones en 2013. La penetración de la banda ancha fija sigue creciendo, aunque lentamente (en un 4,4 % a nivel mundial en el año 2014). Dado que los servicios son cada vez

más accesibles, la adopción de la banda ancha fija ha mostrado un fuerte crecimiento, y para el año 2013 había casi 700 millones de suscripciones de banda ancha fija, que corresponde a una tasa de penetración global del 9,8 %.

El número de usuarios de Internet a nivel mundial habrá alcanzado los casi 3000 millones a finales del año 2014, en comparación con los 2700 millones de personas en 2013[lvi].

Con el crecimiento generalizado de la telefonía por Internet, es vital que la infraestructura que soporta esta tecnología siga siendo segura y esté disponible. Una pequeña cantidad de "inactividad" tiene el potencial de costar a las empresas millones de dólares en ingresos perdidos y problemas de soporte al cliente.

AMENAZAS POR VOIP

Esta sección ofrece una taxonomía de amenaza de telefonía de voz simple, cubriendo los problemas que afectan la voz y los sistemas de comunicaciones unificadas (UC) y mejores prácticas recomendadas para prevenir y remediar estas amenazas. Esta sección se centra en la voz, pero las amenazas pueden afectar otras formas de comunicación, incluso el video y la mensajería. Estas amenazas se aplican principalmente a empresas, pero también pueden afectar a los proveedores de servicios, pequeñas empresas y los consumidores.

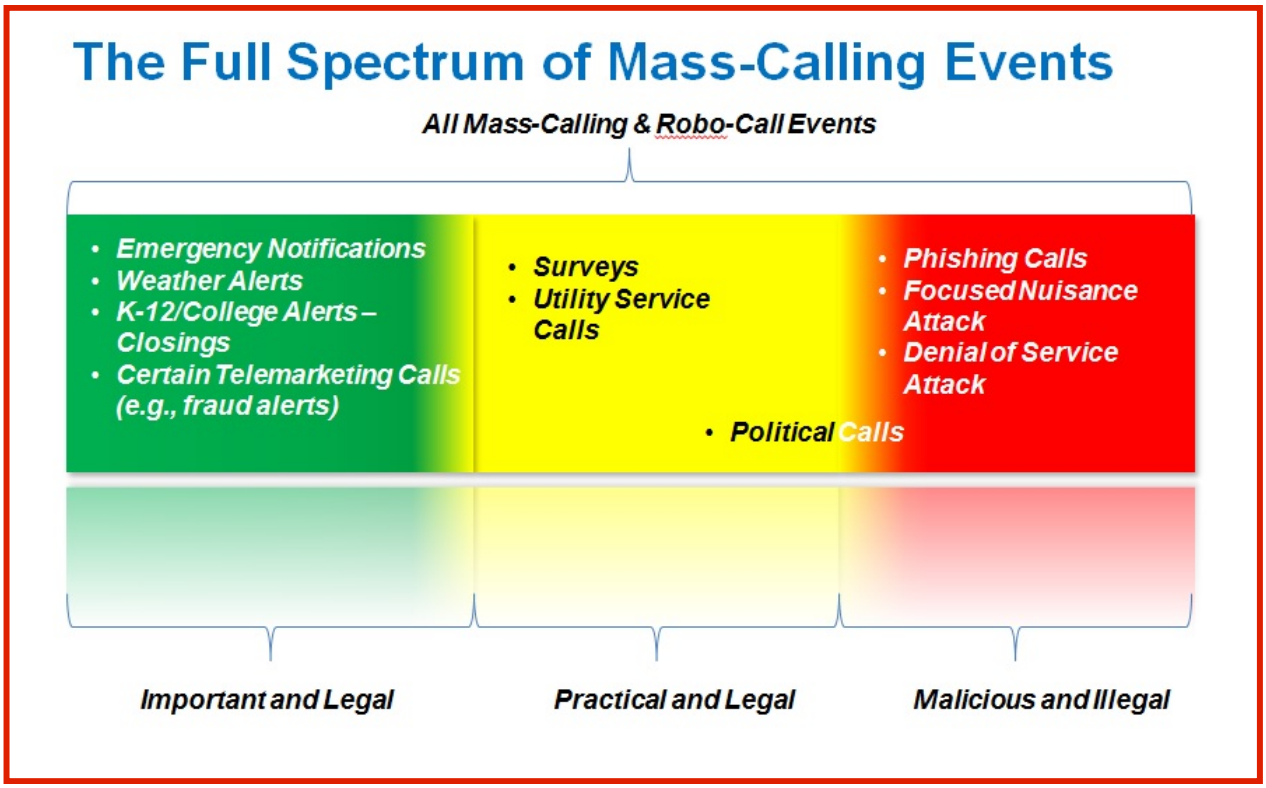
Estafas con un ring: Los consumidores inalámbricos reciben llamadas telefónicas automatizadas de números de teléfono que tienen códigos de área que imitan números locales, pero en realidad están asociados con números internacionales por pagar. Estas llamadas automatizadas por lo general se desconectan luego de hacer un ring, y no le da tiempo al consumidor para responder y lo tientan a devolver la llamada. Los consumidores que devuelven las llamadas dirigen un tráfico adicional a esos operadores internacionales y el scammer puede recibir una porción de los cargos finales (o posiblemente por cargos premium) que el operador internacional del servicio cobra del operador inalámbrico del cliente.

LLAMADAS AUTOMATIZADAS

Las llamadas automatizadas, que utilizan sistemas de marcación automática para realizar llamadas de voz, es una forma cada vez más problemática de abuso de servicio de voz. Se utilizan normalmente para llamadas relacionadas con ventas, marketing o encuestas. Por ejemplo, cuando una opinión o algún otro tipo de encuesta se lleva a cabo, el mensaje pregrabado le puede solicitar a la persona que pulse un dígito correspondiente a la respuesta preestablecida de su elección. Otro uso común es para notificaciones de emergencia, avisos o recordatorios. Esto se utiliza con frecuencia por funcionarios de seguridad pública mediante un sistema llamado un sistema de notificación de emergencia (SNE). Sin embargo, las llamadas automatizadas son también utilizadas generalmente para estafar consumidores o para otros fines ilícitos.

En los Estados Unidos, por ejemplo, las llamadas automatizadas afectan especialmente a los clientes fijos, que son dirigidos a menudo por vendedores sin escrúpulos y los estafadores.[lvii] Las llamadas automatizadas representaron el reclamo más frecuente de consumidores según la FTC en 2014. Recientemente, las empresas también han comenzado a presentar un número creciente de reclamos de clientes inalámbricos. Por ejemplo, la estafa de "un ring" apuntó recientemente a inducir a clientes inalámbricos a marcar de forma involuntaria números de pago por llamada internacionales sin su consentimiento.[lviii] Las llamadas de phishing específicamente dirigidas a obtener el acceso a información confidencial, personal y financiera, conocido como vishing, también son frecuentes.

Se utilizan también con frecuencia las llamadas automatizadas para abrumar a clientes conectados e inalámbricos mediante ataques TDoS: se crean llamadas en masa que evitan la realización de llamadas legítimas.



LAS MEJORES PRÁCTICAS RECOMENDADAS PARA COMBATIR LAS LLAMADAS AUTOMATIZADAS:
Los operadores o proveedores pueden ofrecer herramientas y soluciones para combatir las llamadas automatizadas. Sin embargo, no existe una única solución para eliminar todas las llamadas automatizadas ilegales o no deseadas.

Anzuelos: Un anzuelo es una trampa para detectar, desviar o contrarrestar intentos de uso no autorizado de una red o sistema. En general, los anzuelos imitan un equipo, datos o un sitio de la red, pero realmente son aislados, protegidos y supervisados. Están construidos específicamente para atrapar a los atacantes. Una vez que muerden el anzuelo, es posible rastrear y vigilar a los delincuentes.

Recopilación de datos y herramientas de análisis: La información es una potente herramienta en la prevención de las llamadas automatizadas. Recogiendo información sobre flujos de tráfico en una red particular y combinando datos con análisis para identificar patrones sospechosos de llamadas según el volumen, el enrutamiento, el destino y la duración de llamada y las tasas de realización, los proveedores pueden identificar e investigar patrones sospechosos para identificar llamadas automatizadas ilegales. Es posible utilizar esta información para establecer listas negras y bloquear llamadas de ciertos números, o listas blancas, que definen las llamadas que se pueden recibir. Una vez que se identifica un patrón de llamadas automatizadas, los operadoras y las agencias de orden público pueden utilizar técnicas de rastreo para identificar y perseguir a los responsables.

Equipo local del cliente (CPE): Se disponen de herramientas de compañías y proveedores para gestionar las llamadas en los teléfonos: Los tipos frecuentes de equipo son:

- ***Identificador de llamadas:*** El identificador de llamadas muestra el número que está llamando. Los clientes pueden utilizar esta tecnología bien conocida para filtrar llamadas desde fuentes desconocidas. Los servicios y dispositivos de bloqueo de llamadas se basan en la información del identificador de llamadas y en las llamadas entrantes con el fin de colocar los números en una lista negra.
- ***Dispositivos CAPTCHA[lix]:*** hacer que ciertas llamadas atraviesen menús diseñados para eliminar los llamadores no humanos.[lx]
- ***Aplicaciones:*** Los clientes inalámbricos pueden descargar una variedad de aplicaciones que utilizan la funcionalidad de identificador de llamadas para rechazar o supervisen llamadas desde números de teléfono que las aplicaciones identifican como sospechosos según las diversas técnicas, como el crowdsourcing, algoritmos o listas negras.[lxi] Los usuarios también pueden aprovechar las características integradas de sus teléfonos inteligentes que permiten configurar qué llamadas suenan en sus teléfonos y cuáles no.
- ***Identificación de clave pública/privada:*** este sistema está siendo desarrollado para autenticar la dirección de la red o la persona que llama asociada con el originador de la llamada.

Regímenes regulatorios: Muchos comercializadores han utilizado la telefonía para promover campañas de marketing. La mayoría de los regímenes no prohíben las llamadas automatizadas a menos que el consumidor haya dado su consentimiento para recibir este tipo de llamadas desde la entidad que llama. Por otra parte, la molestia generada en el consumidor por las solicitudes no deseadas ha llevado a muchos países para regular todas las llamadas comerciales: algunas jurisdicciones operan regímenes que seleccionan la opción "no llamar" (por ejemplo Alemania, Austria e Israel) y otros operan regímenes que no seleccionan la opción "no llamar" (obligatorios o voluntarios). En países como Australia, los Estados Unidos y Canadá, los registros nacionales "no llamar" se complementan con leyes que regulan a los telemarketers en cuanto a las normas sobre tiempos de llamada, identificación de la empresa que llama (CLI) y declaraciones obligatorias.

Las sanciones pueden ser importantes y, junto con el alto riesgo de daños a la reputación, han sido fundamentales para asegurar que los buenos ciudadanos corporativos cumplan políticas y procedimientos.

La Red Internacional No Llamar, parte del LAP, estableció un foro anual y llamadas de conferencia periódicas para la discusión de temas comunes y emergentes en la gestión de llamadas no solicitadas de telemarketing a nivel mundial y las oportunidades de aplicación de la ley de colaboración.

Estándares de la industria: Los proveedores de servicios, organismos de estándares de la industria y agencias han estado trabajando conjuntamente y de manera independiente para mitigar este tipo de llamadas ilegales. Los proveedores de servicios y las entidades privadas están desarrollando o actualmente tienen servicios e instalaciones disponibles para que los consumidores aborden las llamadas automatizadas ilegales[lxii] y deberán seguir desarrollando e implementando estos estándares.

Los proveedores de servicios también deben considerar una mejora en la atención de primera línea u otros call center de llamadas entrantes, en el acceso en línea para los clientes, así como en la corrección y centros de soporte técnico y debe capacitar a su personal sobre las características del identificador de llamadas, los usos legítimos de suplantación de llamadas y suplantaciones malintencionadas y reconocidas actualmente.

Algunos proveedores pueden considerar el establecimiento oficinas de llamadas molestas o equipos de seguridad para tratar temas como estos. Los clientes que continúan con problemas después de su contacto con empleados de atención al cliente o recursos en línea se pueden derivar a ese grupo para una asistencia adicional según los procesos específicos de los proveedores. Se puede solicitar a los clientes que compartan información relevante como las fechas y épocas en las que han recibido llamadas de este tipo y otras características apropiadas para la investigación de las llamadas. La oficina de llamadas molestas o los equipos de seguridad pueden proporcionar valiosos esfuerzos para abordar estas cuestiones, como:

- Aprovisionamiento y control de equipo de seguimiento de llamada en servicios telefónicos de los clientes;
- Seguimiento, traducción e identificación de fuentes de llamada mediante ubicaciones de conmutadores de la oficina central y sistemas de supervisión y análisis de red;
- Utilización la dirección de facturación y los sistemas de instalaciones para identificar fuentes de llamadas siempre que sea posible;
- Trabajo directo con operadores locales, a distancia, inalámbricos y otros proveedores de comunicación y oficinas de llamadas molestas;
- Colaboración con las agencias de orden público para comunicar información identificada; y
- Contacto con partes identificadas en nombre del cliente cuando sea apropiado para resolver los problemas con llamadas que ponen en riesgo la vida o acosan al destinatario y llamadas generadas por equipos y automarcadas, suplantación de llamadas, fax que explosivos y cualquier otra tipo de llamadas molestas identificadas por los clientes.

Organismos encargados del cumplimiento de la ley: Mientras que los regímenes de cumplimiento pueden frente a llamadas no deseadas de negocios legítimos, no son una adecuada disuasión a quienes pretenden engañar al público. Para aquellos actores, aplicación de la ley fuerte es a menudo el único medio para abordar estos abusos. Algunas naciones han adoptado una postura agresiva contra el uso de la telefonía, ya sea a través de VoIP o de otros medios, para engañar a los consumidores. El procesamiento de casos bajo las leyes de protección al consumidor en procesos civiles y penales ha dado lugar a sanciones sustantivas así como penas de prisión. Para abordar plenamente el problema del fraude por telemarketing, es esencial que los reguladores, la industria y la aplicación de la ley continúen ubicando y denunciando a los estafadores cuyo uso de la suplantación de llamadas y llamadas automatizadas han resultado en cientos de millones de dólares en el fraude en todo el mundo.

ATAQUES TELEFÓNICOS POR DENEGACIÓN DE SERVICIO (TDOS)

El TDoS es un ataque que apunta a desactivar el sistema de teléfono de una empresa o servicio público. Al saturar un número de teléfono desde el exterior, o incluso la totalidad de los canales de comunicación de la entidad, los atacantes pueden desactivar rápidamente todas las llamadas entrantes y salientes. El TDoS es muy similar a la ataque de denegación de servicio (DDoS) puntual en sitios web. Los atacantes se benefician porque mantienen el sistema de teléfono como rehén y perturbar el sistema hasta que la víctima paga una suma especificada.

Para iniciar un ataque TDoS, el atacante debe tener acceso a varios canales de comunicación o cuentas de protocolo de inicio de sesión (SIP) (generalmente pirateadas). Entonces utilizan máquinas automatizadas que realizan llamadas simultáneas y en varias ocasiones llaman a uno o varios

números de teléfono de la víctima. Las "herramientas" o el "kit" para el ataque TDoS se encuentran fácilmente en Internet. También es muy fácil solicitar que dicho ataque lo realicen terceros sin escrúpulos. Este es el tipo de ataque generalmente se hace por perturbación, extorsión, o para encubrir un fraude.

LAS MEJORES PRÁCTICAS RECOMENDADAS SOBRE TDOS:

Puertas de enlace de nivel de aplicación: Es importante que las empresas de todos los tamaños aseguren sus sistemas de VoIP y telefonía. Los sistemas de VoIP son como cualquier otro sistema informático de red y por lo tanto requieren protección de las mismas clases de ataques cibernéticos como cualquier otro servidor de red. Mientras que los firewalls obsoletos pueden tener problemas para manejar adecuadamente los requerimientos únicos de sistemas VoIP, muchos dispositivos de seguridad modernos tienen puertas de enlace de capas de aplicación (ALG) diseñados específicamente para manejar protocolos específicos de VoIP. Algunos de estos algoritmos pueden proporcionar incluso una funcionalidad de seguridad específica de VoIP, como la prevención de la cosecha de directorios SIP o ataques DoS de nivel de red.

Protección de los servicios básicos
El Comité Canadiense de Interconexión (CISC) exploró el tema de ataques de denegación de servicio de telefonía dentro de los grupos de trabajo de red y servicios de emergencia y ha sugerido las mejores prácticas recomendadas para la protección de sistemas esenciales.

http://www.crtc.gc.ca/public/cisc/nt/NTCO0570.doc

Informe al orden público: Los ataque de TDoS tienen el potencial para desactivar la infraestructura crítica y clave, que incluye servicios de emergencia, hospitales y primeros auxilios. Esto puede plantear cuestiones de seguridad nacional y por lo tanto se debe referir a la agencia de orden público apenas se detecte un ataque.

SUPLANTACIÓN DE LLAMADAS

La suplantación de llamadas es un método de falsificación de la información de la llamada de origen. Mientras que esto no es un ataque *per se*, se utiliza comúnmente para ocultar la identidad de un atacante o realizar ataques más eficaces. A través de tal suplantación, los estafadores tienen por objetivo a consumidores y realizan llamadas que imitan la ciudad del consumidor, el código de área o una fuente de confianza. Algunas personas han utilizado números asociados con las agencias gubernamentales y han suplantado a funcionarios del gobierno en fraudes de impuestos e inmigración. A menudo, el origen de estas llamadas es de otro continente, añadiendo más complejidad para el seguimiento y la detención fraudes.

Informe/Bloqueo selectivo de llamadas (*09)
Los códigos de servicio verticales, como *09, se deben definirse por la industria para permitir a los consumidores iniciar fácilmente la captura automática y el análisis de la información de la red relacionadas con llamadas no deseadas. Este sistema funciona al permitir que un consumidor reciba una llamada de telemarketing fraudulenta u otro tipo de llamada no deseada, para colgar el teléfono y oprima *09 para revelar la información completa sobre la llamada a su operador, agencias de orden público y reguladores, y también bloquear automáticamente futuras llamadas de ese

LAS MEJORES PRÁCTICAS RECOMENDADAS PARA PREVENIR LA SUPLANTACIÓN DE LLAMADAS:

Legislación sobre fraude: En general, debería ser ilegal en todo el mundo transmitir información engañosa o inexacta sobre identificación de llamadas con la intención de defraudar, dañar u obtener indebidamente algo de valor.[lxiii]

En los Estados Unidos, por ejemplo, la Ley sobre identificación de llamadas legítimas de 2010 prohíbe la suplantación de llamadas o la falsificación deliberada de número telefónicos o el nombre identificado como información del identificador de llamadas para disfrazar la identidad de la llamada con fines perjudiciales o fraudulentos. [lxiv] Este tipo de definición permite el uso de suplantación de identidad con fines no fraudulentos, como el uso de número del consultorio de un médico cuando llama de su línea privada.

Educación al consumidor: La confianza del consumidor en el sistema de telefonía está en riesgo, con el aumento de suplantación de llamadas y las llamadas automatizadas. Para proteger a los consumidores de fraudes y otros daños que dependen de mal uso de la plataforma telefónica, las agencias gubernamentales han lanzado campañas de educación. Por ejemplo, la Comisión Federal de Comercio de Estados Unidos (FTC) ha publicado advertencias en sus páginas web, publicado entradas en el blog y promovido sus esfuerzos de aplicación de la ley para concientizar al consumidor sobre las llamadas automatizadas y la suplantación de identificadores de llamadas.[lxv] Fomentar una mayor conciencia de los consumidores del uso de la suplantación de identidad puede ayudar a reducir el daño resultante que puede resultar de los fraudes que se promueven a través de esta técnica. Los esfuerzos de educación al consumidor también deben dar a conocer las diversas herramientas que pueden utilizar los consumidores para protegerse de llamadas no deseadas.

SERVICIOS DE HOSTING Y EN LA NUBE

Los servicios de hosting y de la nube representan uno de los cambios recientes más significativos en la tecnología de la información. Las empresas están entusiasmadas por la oportunidad de mejorar el control de los costos de capital, de aumentar la agilidad y eliminar la infraestructura compleja de tecnología de información. Sin embargo, las cuestiones sobre la seguridad y la pérdida de control directo están sofocando la adopción y el crecimiento de esta nueva tecnología.

Las amenazas móviles y en línea aumentan para los servicios de hosting y en la nube. Según un reciente artículo publicado en The Economist, se espera que el mercado mundial para los servicios de informática en la nube alcance USD 176 000 millones en 2015. Esta cantidad aún representa una pequeña porción del total de gastos de IT, pero el gasto en servicios de hosting y de la nube está creciendo rápidamente. Actualmente, muchas otras partes de la industria están estancadas o incluso en vías de desaparición, pero para 2017 se espera que el gasto derivado de la nube alcance a un total de USD 240 000 millones por año[lxvi].

Esta sección clasifica los tipos de hosting y describe las áreas de interés. Proporciona un análisis del panorama actual de las amenazas en la nube y en línea, y un breve recorrido por los métodos de corrección que se utilizan para abordar estas cuestiones críticas.

TIPOS DE HOSTING

Los proveedores de hosting facilitan la operación de la Internet global y operan los aspectos básicos que hacen funcionar Internet. Los proveedores de hosting varían en tamaño, desde empresas unipersonales hasta empresas internacionales de renombre mundial. Lo que diferencia a los proveedores de infraestructura de Internet de otros aspectos de Internet es su relativo anonimato. Estos negocios generalmente operan detrás de escena para facilitar el uso de Internet para negocios muy diversos, desde una tintorería local o un banco internacional.

FORMATO DE LA INFRAESTRUCTURA DE INTERNET:

Los servicios de infraestructura de Internet se comprenden mejor en términos de las formatos subyacentes utilizadas por el proveedor de servicios para brindar los servicios al usuario final. Existen tres componentes de estos formatos subyacentes:

- **Instalaciones**: Las instalaciones, frecuentemente conocidas como centro de datos, son el pilar de un proveedor de infraestructura de Internet. Puede ser propiedad del propio proveedor de infraestructura o estar operado por un tercero. Esta instalación alberga los enrutadores y conmutadores que se conectan a Internet junto con los servidores, físicos y virtuales, que poseen el contenido, los datos y las aplicaciones.
- **Servidor físico**: El servidor físico reside en un gabinete o una estantería y se ubica en un centro de datos. Es donde se almacenan y se aseguran contenidos y aplicaciones.
- **Servidor virtual:** El servidor virtual es una partición virtualizada de un servidor físico. El servidor virtual actúa y se ejecuta como un servidor físico con una diferencia marginal en el rendimiento. Un único servidor puede albergar literalmente hasta docenas de servidores virtuales.

Los proveedores de hosting generalmente se pueden clasificar en una de cinco categorías principales:

i. Hosting compartido
ii. Hosting estándar administrado
iii. Hosting complejo administrado
iv. Infraestructura en la nube
v. Colocación

CATEGORÍAS DE INFRAESTRUCTURA DE INTERNET

Hosting compartido: El hosting compartido es el espacio compartido en un servidor físico que no aísla usuarios y ni asigna de recursos definidos. Se comparten los recursos finitos de un servidor físico, a menudo en forma desigual, entre todos los clientes que residen en él. Los proveedores pueden albergar literalmente cientos de clientes en un único servidor.

El hosting compartido se utiliza frecuentemente para publicar contenido web estático o dinámico. Las plataformas de blogs, como WordPress y aplicaciones simples de comercio electrónico, a menudo se ejecutan en entornos de hosting compartidos y están habilitados con instalación automática.

Las organizaciones con recursos muy limitados utilizan el hosting compartido para comunicarse y construir una presencia en Internet. El hosting compartido existe normalmente en el punto inferior del mercado de la infraestructura. Los usuarios frecuentes son: consumidores, pequeñas empresas, oficinas domésticas y blogueros.

Hosting estándar administrado: Un proveedor de infraestructura que proporciona un hosting estándar administrado en general alquila servidores físicos dedicados (a veces se denominan servidores desnudos de metal) o servidores virtuales alojados en las instalaciones del centro de datos del proveedor de infraestructura. Los clientes suelen alquilar los recursos del servidor según un contrato fijo.

En el hosting estándar administrado, los clientes poseen un acceso raíz al servidor y por lo general se auto administran. El proveedor de infraestructura proporciona un nivel básico de soporte y maneja ciertas tareas de administración, aunque limitadas, como el mantenimiento del hardware, la realización de copias de seguridad y la instalación de software de servidor web y sistema operativo.

El servidor real es propiedad del proveedor y el cliente lo alquila. Como resultado, el cliente no se enfrenta a un ciclo de actualización de IT. Simplemente se pueden mover a otro servidor que se ajuste a sus necesidades. No suelen pagar las actualizaciones de hardware o tienen la obligación de permanecer en el servidor que han alquilado.

El hosting estándar administrado está diseñado para acomodar las cargas de trabajo y configuraciones relativamente sencillas. Las pequeñas empresas generalmente utilizan el hosting estándar administrado como una alternativa a la compra e instalación de activos de IT.

Hosting complejo administrado: El hosting complejo administrado también se aplica a servidores virtuales y servidores físicos dedicados. Hay muchas similitudes entre el hosting estándar administrado y el hosting complejo administrado; pero la diferencia clave es el nivel de soporte administrativo y de ingeniería que paga el cliente. Estas diferencias surgen del aumento en el tamaño y la complejidad de la implementación de infraestructura. El proveedor de infraestructura asume el control de la mayor parte de la administración.

El hosting complejo administrado implica adquirir una amplia gama de conocimientos y capacidades en la administración de sistemas, gestión de bases de datos, seguridad, supervisión, administración de registros, recuperación ante desastres y respaldo de datos. Los servicios de administración se pueden extender incluso a la capa de aplicación, aunque esto tiende a ser infrecuente fuera de la mayoría de las aplicaciones estándar de la empresa. Una implementación típica de un hosting administrado tendrá un número de dispositivos adicionales, como bases de datos, servidores web y aplicaciones, firewalls y equilibradores de carga. En lugar de utilizar almacenamiento local, los clientes a menudo usan redes de almacenamiento o adjuntos a la red. También adquirirán servicios de copias de seguridad y servicios de replicación o escenarios de recuperación ante desastres. Algunos proveedores de infraestructura aumentan su oferta estándar proporcionando servicios de consultoría que van más allá de la capa de nivel de servicios administrados.

Cuando se trata un servicio de hosting complejo administrado, la relación del hosting se tiende a limitar a un número pequeño de aplicaciones versus el total que existe dentro de la empresa. El hosting complejo administrado es utilizado como una extensión del centro de datos local.

El hosting complejo administrado se utiliza para cargas de trabajo y configuraciones grandes y complejas. También es una opción cuando las empresas necesitan una capacidad muy específica y especializada, como la seguridad y la conformidad. El hosting administrado es una alternativa a la compra e instalación de activos de IT y tiene un componente de ahorro de costos. Es una manera de aliviar la carga de personal de IT interno y liberar recursos.

Infraestructura en la nube: La infraestructura de nube es básicamente una forma más flexible y escalable de servidor de hosting virtual. La característica clave de la infraestructura en la nube es la disponibilidad de recursos. El tamaño de un servidor aumentar o disminuir sobre la marcha o dentro de un plazo de tiempo muy breve. Así que en lugar de una cantidad fija de recursos, el usuario final puede ajustar capacidad de infraestructura según la demanda (o la falta de ella). Por lo general, la nube se consume por hora, pero incluso se está comenzando a facturar por minuto, permitiendo el consumo basado en la utilidad.

La nube es también altamente resistente, y no tiene un único punto de falla. Los recursos en la nube son móviles y se pueden conmutar automáticamente hacia otro host físico. Se puede reiniciar en cualquier lugar y en cualquier momento con el conjunto adecuado de herramientas y capacidades. Esta flexibilidad le permite a la nube integrarse en entornos híbridos en cualquier centro de datos local o tercerizado.

Colocación: La colocación es el suministro de capacidad de la fuente del centro de datos para empresas que necesitan un lugar externo para alojar o "colocar" los servidores, el almacenamiento y los equipos de redes que poseen y administran. Los pilares de la colocación son el espacio, la potencia, la refrigeración y la conectividad a Internet. En el modelo de colocación, el cliente tiene acceso a un área designada dentro de un centro donde se instale el equipamiento propio o alquilado. Muchos proveedores de colocación también ofrecen servicios de supervisión y administración remota. Algunos proveedores le alquilan los equipos a los clientes.

La realidad de la industria de la infraestructura de Internet puede llegar a ser más compleja, dado que los segmentos de servicio de infraestructura se siguen confundiendo. Por ejemplo, el límite entre el hosting estándar administrado y el hosting complejo administrado está cada vez más claro, dado que los proveedores amplían el mercado y se expanden hacia servicios de valor agregado. Lo mismo se puede decir del límite entre hosting administrado, de la variedad de servidores virtuales, y la

infraestructura en la nube. Un número de ofertas de hosting con servidor virtual parecen ser parte de la infraestructura en la nube. Es posible que no tengan todas las características de la nube, pero muestran lo suficiente para difuminar el límite y crear algunas zonas grises.

EL ESCENARIO DE LAS AMENAZAS

A continuación, se enumeran los tipos de ataques más frecuentes en los proveedores de servicios de hosting y en la nube. La lista no pretende ser completa y siempre va a cambiar con el tiempo.

- **Spam (saliente)**: El spam es cualquier correo electrónico comercial no deseado o no solicitado. Los proveedores deben garantizar que los usuarios finales respeten las Mejores prácticas recomendadas actuales del M³AAWG.[lxvii] Los proveedores de hosting también querrán suscribirse a tantos informes sobre bucles de retroalimentación pertinentes como sea posible procesar.
- **Spamvertising (redirigido y carga)**: El spamvertising ocurre cuando un usuario del proveedor de hosting contrata a un tercero para que anuncie su presencia en la Web. La mayoría de los reclamos de spam se originan porque los usuarios finales envían correos electrónicos a sus clientes potenciales que solicitan algún producto o servicio sobrevaluado. Lo más probable es que los proveedores que reciben uno de estos reclamos estén en el bucle como el remitente del correo electrónico o como el host del sitio que se anuncia.
- **Phishing saliente (hosting y saliente para las credenciales del cliente)**: El phishing ocurre principalmente cuando la cuenta de un usuario final ha sido afectada, casi siempre como resultado de un script obsoleto ejecutado por el usuario final. Un sitio de phishing es un sitio fraudulento que pretende ser una empresa legítima, como un banco, una tarjeta de crédito o PayPal que dirige al individuo a ingresar información confidencial. Los suplantadores entonces tienen todo que lo necesario para defraudar a la persona. (Véase la sección Phishing e ingeniería Social para obtener mayor información).
- **Sitios desfigurados o pirateados (servicio de hosting por parte del cliente)**: Mientras que los reclamos de phishing con frecuencia caerán en esta categoría, no todas las cuentas pirateadas se utilizarán para phishing. Algunas simplemente pueden ser desfiguradas y los datos de los usuarios finales pueden ser dañados o destruidos. Con frecuencia los piratas informáticos también insertan un código malicioso o cargan bots que se configuran para causar otros problemas, como ataque a sitios, descargas cultas o redireccionamiento a contenido malicioso. Los terceros y las agencias de orden público analizan estos eventos y proporcionan información sobre cómo corregir sitios pirateados. La mayoría de las cuentas está en peligro debido a la instalación de un sistema de administración de contenidos (CMS) no actualizados, por ejemplo Joomla o WordPress.
- **Material sobre abuso sexual de menores (servicio de hosting por parte del cliente)**: Para el manejo adecuado de estos temas, lea las Mejores Recomendaciones sobre Material sobre Abuso Sexual de Menores del M³AAWG (https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Disposition_CAM-2015-02.pdf).
- **Cuestiones sobre derechos de autor y de propiedad intelectual/de marcas comerciales (servicio de hosting por parte del cliente)**: Para consultar la ley sobre derechos de autor de los Estados Unidos, haga clic en http://www.copyright.gov/reports/studies/dmca/dmca_executive.html. Otros regímenes de derechos de autor se aplican en otras jurisdicciones.

- **Denegación de Servicio Distribuido y otro tipo de tráfico hostil saliente:** Mientras los proveedores de hosting o servicios en la nube pueden tener una mejor protección que las pequeñas empresas unipersonales, estos proveedores de servicios también sufren un riesgo mayor de ataques DDoS que otras empresas en línea debido a que, en efecto, acumulan el riesgo de sus clientes. Un ataque a un cliente puede afectar a otros y potencialmente a toda la operación de hosting debido a la fuerte dependencia en la infraestructura compartida.
- **Inicios de sesión maliciosos:** Los piratas informáticos construyen un botnet sólo con las pruebas gratis y las cuentas "freemium" de los servicios de hosting de aplicaciones en línea. Utilizan un proceso automatizado para generar direcciones de correo electrónico únicas y suscribirse en masa a las cuentas gratis, creando un botnet basado en la nube de miles de computadoras.

PRINCIPALES ÁREAS DE INTERÉS

Instalaciones CRM vulnerables/desactualizadas:
Si consideramos que existen más de 67 millones de sitios WordPress, que representa el 23 por ciento de todos de sitios web[lxviii], del mundo —y que los editores utilizan la plataforma para crear blogs, sitios de noticias, sitios de la empresa, revistas, redes sociales, sitios de los deportes y otros— no es de extrañar que muchos delincuentes en línea tienen su mirada puesta en obtener acceso a través de este sistema de gestión de contenidos (CMS). Por ejemplo, Drupal, una plataforma CMS en rápido desarrollo, fue atacada en el 2014 mediante software de terceros instalado en la infraestructura de servidores de Drupal.org.

No es sólo la popularidad de estos sistemas lo que los hace objetivos atractivos. Muchos de los sitios de estos servidores, aunque estén activos, han sido abandonados por sus propietarios. Probablemente, existen millones de blogs abandonados y dominios comprados sin uso, y es probable que muchos de estos sitios han sido corrompidos por los ciberdelincuentes. Los expertos en seguridad de Cisco predicen que el problema sólo empeorará dado que cada vez más personas en los mercados emergentes de Internet en el mundo establecen un blog o un sitio web y lo abandonan más adelante.

También se ha demostrado que el uso generalizado de plugins, que son diseñados para ampliar la funcionalidad de un CMS de contenidos y juegos, animaciones y videos potentes, es una bendición para los ciberdelincuentes que buscan obtener acceso no autorizado a las plataformas. Para exacerbar este problema muchos plugins quedan sin actualizar por sus autores y fuerzan a aquellos que usan y dependen de los plugins a no actualizar su instalación actual a costas de perder negocios o funcionalidades del sitio. Muchas afecciones del CMS observadas por los investigadores de Cisco en 2013 se remontan a plugins escritos en el lenguaje de código de escritura web PHP que fueron mal diseñados y sin considerar la seguridad.

Las estadísticas recogidas por la empresa de seguridad Sucuri muestran un total de 3143 vulnerabilidades en WordPress en 15 categorías diferentes.[lxix] Con esta cantidad de vulnerabilidades, los consumidores de WordPress han comenzado a mantener su software actualizado; pero más del 30 % de los sitios de WordPress sigue utilizando la versión 3 o inferior[lxx] y deja a sus sitios al acecho de terceros maliciosos.

Ataques DDoS:
Dado que los ataques DDoS se habían considerado "noticias viejas" en términos de técnicas de ciberdelincuencia, muchas empresas estaban seguras de que las medidas de seguridad que tenían vigentes proporcionarían una protección adecuada. Esa confianza, recientemente ha sido sacudida por ataques DDoS a gran escala entre 2012 y 2013, que incluye la operación Ababil, que apuntó a varias instituciones financieras, probablemente por motivos políticos.

Los líderes de la industria advierten que los ataques DDoS deben ser una cuestión de alta seguridad para las organizaciones del sector público y privado porque se esperan futuras campañas aún más extensivas. Las organizaciones, particularmente las que operan o tienen intereses en las industrias que ya son blanco, como el sector financiero y el sector energético, deben ser extraordinariamente cautelosas. Entre 2010 y 2013, las interrupciones no planificadas por ataques DDoS aumentaron del 2 % al 13 % en total.[lxxi] De hecho, una comparación entre el último trimestre de 2013 y el de 2014 mostró un aumento de los ataques DDoS en un 90 %, resaltando que los ataques continúan en aumento.[lxxii] El costo promedio total de estas interrupciones también ha aumentado de USD 613 000 a USD 822 000 en el mismo período. [lxxiii]

Algunos ataques por DDoS han dado un giro preocupante. Se han utilizado para desviar la atención de otras actividades nefastas, tales como fraude por cable. Estos ataques pueden abrumar a personal del banco, impedir el envío de notificaciones a los clientes y evitar que los clientes informen el fraude. Las instituciones financieras raramente son capaces de recuperar sus pérdidas financieras. Un ataque que tuvo lugar el 24 de diciembre de 2012 que apuntaba al sitio web de una institución financiera regional con sede en California y ayudó a distraer a los empleados bancarios mientras se tomaba el control de una cuenta en línea de uno de sus clientes, que se tradujo en USD 900 000 en manos de los delincuentes.

Los conocimientos que rápidamente se profundizan sobre cómo afectar un servidor de hosting sólo les facilitará a los ciberdelincuentes lanzar ataques DDoS y robar organizaciones específicas. Por ingresar a una parte de la infraestructura de Internet, los actores maliciosos se pueden aprovechar de grandes cantidades de ancho de banda, posicionándose para lanzar cualquier cantidad de campañas de gran alcance. Ya está sucediendo: en agosto de 2013, el gobierno chino informó que el mayor ataque DDoS en la historia había interrumpido el servicio de Internet en China durante aproximadamente cuatro horas.

Incluso los spammers están usando ataques DDoS para contraatacar a las organizaciones que se cruzan en el camino de su generación de ingresos. En marzo de 2013, la organización sin fines de lucro Spamhaus (que rastrea a los spammers y ha creado la lista de bloqueo de Spamhaus, un directorio que contiene direcciones IP sospechosas) fue blanco de un ataque DDoS que temporalmente interrumpió su sitio web y redujo el tráfico de Internet en todo el mundo. Los atacantes supuestamente estaban afiliados CyberBunker, un proveedor de hosting, con sede en los Países Bajos, que posee condiciones de uso permisivas y STOPhaus, que ha expresado públicamente su desagrado por las actividades de Spamhaus. El ataque DDoS siguió al servicio ampliamente utilizado de Spamhaus, que había colocado a CyberBunker en su lista negra.

Servidores mal configurados en entornos no administrados:
Con la llegada de la nube, los usuarios ahora tienen la capacidad de crear y configurar un entorno de servidor completo en una fracción del tiempo que se requería para el hardware físico. Esto ha permitido que los usuarios puedan crear fácilmente su propia infraestructura con poco o ningún conocimiento de cómo los sistemas son creación de trabajo. Mientras que este cambio le ha permitido

a los usuarios la capacidad para hacer mucho más de lo que han hecho antes de abrir un nuevo desafío en la prevención y detención de ataques a estos sistemas.

Muchos de los servidores virtualizados y no administrados no reciben el mantenimiento que ya se ha definido en el mundo del hardware físico administrado. Los sistemas operativos y programas no se actualizan correctamente (o no se actualizan) para tratar parches y vulnerabilidades de seguridad. Los permisos se cambian raramente o se establecen en donde cualquier persona con acceso al servidor pueda realizar cambios, dejando la puerta abierta del servidor hacia el mundo exterior susceptible a la actividad malintencionada.

Algunos programas usan métodos de comunicación entrante y saliente que si no se configura correctamente convierte al servidor en un arma que se puede utilizar en una reflexión DDoS, inicio de sesión SSH, inyección de SQL y otros ataques con capacidad para interrumpir los sistemas específicos durante un período significativo. Además, estos errores de configuración les permiten a los actores maliciosos acceder a sitios o información alojada en el servidor que resultan en el robo de datos, sitios de phishing y hosting de malware.

El seguimiento de estos sistemas mal configurados y actualizados es una tarea monumental para las compañías que ofrecen estos servidores; por lo tanto, poco se le hace a estos sistemas hasta que ya han sido atacados.

LAS MEJORES RECOMENDACIONES

Prevención:

1) **Investigar a los clientes antes de que causen problemas**: Los proveedores de hosting están a merced de las peores prácticas de sus clientes. Los proveedores deben incorporar un proceso de investigación para identificar de forma proactiva clientes maliciosos antes de que realicen actividades ilegales. realizar esfuerzos para seleccionar clientes que tendrán un buen comportamiento para la empresa de hosting es otra forma de preservar la seguridad del entorno de hosting.

2) **Requerir a los clientes que mantengan el software actualizado:** La imposibilidad de mantener actualizado el software y hardware o firmware en el entorno es una de las principales causas de abuso en el espacio de hosting. Los acuerdos con los clientes deberían especificar que los clientes harán un mejor esfuerzo para mantener sus sistemas actualizados.

3) **Capacitar al personal de atención al cliente en la concientización sobre seguridad:** Los equipos orientados al cliente, como soporte, ventas y marketing no se enfrentan a la mayoría de los desafíos diarios que son la norma para los equipos de seguridad o de contraataques. La capacitación debe brindarle a estos equipos el conocimiento de cuándo decirle a un cliente o prospecto que sus prácticas no se rigen por los términos y las políticas de uso aceptable del sistema en el que están, o en donde están tratando de proporcionar un entorno.

4) **Prevenir el abuso en el borde de la red:**
   a) Considere utilizar un sistema de detección de intrusiones de hardware (IDS).
   b) Utilice un software de seguridad y un firewall.
   c) Promueva el uso de firewall de aplicación web.
   d) Utilice la asignación por niveles para clientes valiosos.
   e) Contrate clientes para proteger la seguridad.
   f) Maximice el contacto con los clientes y proteja la identidad del cliente.

g) Fomente el uso de contraseñas seguras.
h) Utilice las mejores prácticas recomendadas en redes IPv6: El IPv6 proporciona tantas direcciones que no es necesario —y no hay razón— compartir una única dirección IP entre varios clientes. La mejor práctica es asignar a cada cliente 1/64 del espacio de direcciones IPV6. Incluso en los sistemas físicos y compartidos más pequeños, cada cliente y cada sitio web debería tener una dirección única. Esto facilita el rastreo de la fuente del ataque, posibilita que los destinatarios del ataque bloqueen al cliente infractor sin bloquear al resto de los clientes del mismo host y puede facilitar la suspensión y renovación del servicio cuando sea necesario.
i) Los proveedores de hosting deben mantener sistemas y prácticas de seguridad interna. Todas las medidas recomendadas anteriormente son inútiles si los actores maliciosos pueden adivinar las contraseñas que utiliza el personal del proveedor. Los proveedores de hosting deben cumplir los estándares de cumplimiento de PCI.

Detección e identificación:

1) **Utilizar identificadores confidenciales del cliente:** Las empresas deben crear un identificador único para cada cliente específico. Este identificador debe ser evidente sólo para la empresa de hosting y ser incomprensible para terceros. Esto mantiene la privacidad de la identidad del cliente y, sin embargo, le otorga a la empresa de hosting una manera simple y efectiva para identificar a los clientes.

2) **Establecer cuentas de papel para los dominios de la red:** Las cuentas de correo electrónico de práctica común y roles definidos por RFC se deben configurar para cada dominio y dominio del cliente suministrado en una red.

3) **Mantener registros precisos de SWIP e IP WHOIS:** Las empresas deben mantener ingresos claros y precisos en su RIR para la asignación de espacio IP, e incluyen las subasignaciones mayores al 1/27 de los clientes. Las listas WHOIS deberían incluir cuentas funcionales para informar sobre ataques.

4) **Configurar la telemetría interna que informa el estado de la red:** Los ejemplos son:
   a) Autoverificación de la red;
   b) Análisis del tráfico; y
   c) Verificación del filtro de spam saliente.

5) **Facilitar el informe de ataques:** Los proveedores de hosting deben proporcionar instalaciones para que los miembros del público puedan presentar informes sobre el ataque que perciben desde de la red en cuestión. Los proveedores deben entonces reconocer la presentación de estos informes y actuar según corresponda. Deben mantener canales de comunicación redundantes que fundamenten la falla de un canal dado.
   a) Correo electrónico;
   b) Teléfono;
   c) Mensajería instantánea (chat);
   d) Sistemas de ventas de boletos;
   e) Informes de estado del sitio; y
   f) Participación en redes sociales.

6) **Responder con rapidez los reclamos:** Las presentaciones individuales deben tener un mensaje automático de reconocimiento (AUTO-ACK) con suficiente especificidad para ser discretos entre otras presentaciones que la organización querellante haya hecho. Deben incluir la denuncia original, un número de reclamo original y cualquier otra información que le garantice al usuario que el reclamo ha sido recibido y está siendo analizado.

7) **Considerar la designación de informantes de confianza:** Quienes presenten un reclamo se pueden definir como de alta calidad o de alta prioridad. Estas fuentes pueden ser internas y externas. Se debe prever un servicio prioritario manteniendo niveles de prioridad especificada. Por ejemplo, es posible designar el contacto de una DNSBL ampliamente utilizada como un informante adecuado de prioridad, aunque un reclamo de spam de esa fuente obviamente sería menos significativo que una cuestión DDoS que sucede simultáneamente.

8) **Establecer bucles de retroalimentación (FBL) e informes automatizados:** El consumo del registro de datos por FBL para FBL colabora en que el proveedor evite las listas DNSBL, restrinja el daño de reputación y permita que el personal trate en forma proactiva con los clientes atacantes y atacados (afectados).

9) **Implementar una métrica de comparación:** Establecer métricas sistemáticas para que los proveedores de hosting las utilicen les permite a estos y a las agencias de orden público identificar casos de ataque y comparar eficazmente los datos en toda la industria.[lxxiv]

Corrección:

Las prioridades de corrección proporcionan a las empresas de hosting y a los clientes con las pautas para resolver problemas. Las recomendaciones acerca de la prioridad de los reclamos también deben considerar la gravedad y la seriedad del ataque y el alcance de una cuestión determinada. Además, se deben tener en cuenta la fuente del informe y la gravedad de los daños a la reputación de la empresa de hosting y del cliente. Una campaña de spam masivo puede ser de mayor prioridad que la presencia de un botnet latente. Debe haber una evaluación caso por caso de cuestiones que puedan alterar el nivel de prioridad de un determinado proveedor o cliente.

Responder rápidamente a las cuestiones de alta calidad/alta prioridad:

La mayoría de las denuncias recibidas desde cualquier empresa de hosting sólo requiere un acuse de recibo. Sin embargo, en algunos casos, como reclamos de alto perfil, solicitudes de cierre y eliminación de la lista negra, se exigen una respuesta adicional. El cliente o la agencia informante se debe contactar inicialmente para comunicar que el reclamo se encuentra en análisis. Se debe realizar un segundo contacto una vez que se resuelve la cuestión. Sólo en el caso de cuestiones persistentes o excepcionales, se deberán realizar las comunicaciones que sean necesarias.
Comuníquese proactivamente cuando ocurren eventos que afectan a la industria o a toda una empresa.

En caso de un ataque o una vulnerabilidad grave que podría poner varios clientes o un grupo específico de clientes en peligro, se deberá desarrollar un plan de comunicación informarles del problema y proporcionarles instrucciones generales sobre cómo resolverlo. Si la violación implicó el acceso a la información de identificación personal, se debe saber cuáles son sus obligaciones según los requisitos regionales o nacionales, incluso el alcance de la notificación a las personas afectadas y el aviso a las autoridades policiales correspondientes. Estas comunicaciones se deben enviar en tiempo y forma. Además, el personal deberá tomar conciencia de la cuestión y disponer de las instrucciones adecuadas para resolver el asunto en caso de que un cliente necesite asistencia.

Tratar con clientes difíciles:

1) Confirme la validez del reclamo.
2) Notifíquele al cliente de un ataque. Infórmele al cliente las instrucciones aprobadas que le ayudarán a resolver la cuestión.
3) Proporciónele al cliente los términos y las condiciones pertinentes y cualquier regulación gubernamental aplicable que puedan haber sido incumplidos y haber causado la notificación de la violación o la suspensión del servicio. Con estas acciones, el acuerdo con el cliente permanece intacto. La notificación del cliente protege la empresa de hosting de posibles reclamos del cliente o del tercero querellante que podrían provocar litigios.
4) Concédale tiempo al cliente para solucionar el problema o, si existe un acuerdo en vigencia, permítale al proveedor solucionarlo.
5) Confirme que el reclamo se ha resuelto.
6) Cierre el incidente. Si es necesario, notifíquele a la parte informante que el problema ha sido resuelto. Suspenda el servicio de a los clientes que no respondan.

ACOSO EN LÍNEA

No pasa un día sin recibir un informe de los medios en línea y tradicionales sobre algún tipo de acoso en línea. A pesar de que varía entre las molestias y las acciones que son en verdad graves, queda claro que como los servicios de Internet están cada vez más disponibles a nivel mundial lo mismo sucede con el problema del acoso en línea. El acoso en línea puede incluir desde la publicación en línea de mensajes o fotos digitales perturbantes o crueles, amenazas en línea, casos de bullying o comentarios negativos hasta el acoso mediante correos electrónicos, sitios web, redes sociales y mensajes de texto.

Cada grupo de edad es vulnerable al acoso en línea, que es un problema creciente en las escuelas en los campus universitarios e incluso en el lugar de trabajo. El acoso en línea se ha convertido en un problema porque Internet ofrece un anonimato que es atractivo a agresores porque es difícil rastrear su intimidación. Lamentablemente, los rumores, las amenazas y las fotos se pueden difundir en Internet muy rápidamente.

Se han producido intentos de viabilidad para regular [lxxv] e incluso sancionar leyes[lxxvi, lxxvii]para combatir algunos aspectos de la cuestión, pero en general se trata de una zona que es, todavía, omnipresente y en necesidad de examen y desarrollo de buenas prácticas.

A continuación, se proporciona una lista de las diferentes formas de acoso en línea y seguida de una guía simple sobre cómo evitar el acoso.

Catfishing: Se configura un perfil falso en sitios de citas y redes sociales para engañar a una posible víctima en una relación en línea mediante una estafa con su dinero.

Acoso clasificado (Craigslist): Se crean anuncios que afirman que una persona busca sexo duro u otro tipo de comportamiento atípico con respuestas configuradas para dirigirse al teléfono de la casa de la víctima o dirección de correo electrónico.

Cyberbullying: Básicamente es un caso de cyberstalking, pero se asocia más con niños y adolescentes que son acosados en línea por otros estudiantes a través de sitios web, redes sociales, tableros de mensajes, correo electrónico o aplicaciones de teléfonos inteligentes o mensajería de texto.

Cyberstalking: Cuando se le ha solicitado al acosador en línea que se detenga y continúa contactando en línea en repetidas oportunidades a la víctima. Esto puede tomar muchas formas: correo electrónico, sitio web, mensajes o comentarios, tableros de mensajes, mensajes de texto en el teléfono móvil, comentarios y mensajes mediante en aplicaciones para teléfonos inteligentes, etc.

Doxing: Averiguación de información personal identificable sobre un individuo; a continuación, se publicar la información en línea, con dirección, número de teléfono particular, teléfono móvil, dirección y número de teléfono laborales, información sobre familiares, etc.[lxxviii]

Imitación: Cuando un usuario crea perfiles o cuentas con otro nombre, fotos e información de identificación, y luego publica como si fuera esa persona. Esto puede usarse para desacreditar a la víctima, o en algunos casos como un primer paso hacia actividades fraudulentas para beneficio económico. Por ejemplo, mediante el robo de fotos e información de un perfil de redes sociales y la creación de uno nuevo, un delincuente puede entablar amistad con amigos y parientes de la víctima y contactarlos mediante un esquema de "viajero varado"[lxxix] en donde la persona que afirma haber viajado hacia alguna parte pero ha perdido su billetera. Los amigos cercanos son más propensos a caer en esta trampa y envían dinero porque creen que el perfil falsificado es real.

Mobbing: Cuando un grupo de usuarios en línea apunta hacia uno o más individuos y como una "banda" acosa y acecha a las víctimas, con la esperanza de expulsarlos de Internet, de la escuela o de su trabajo. [lxxx]

Outing: Revelar (o denunciar) el hecho de que alguien sea gay, lesbiana, transgénero o compartir información sobre fetiches, condiciones médicas, etc. en línea sin autorización.

Robo de identidad en línea: Robar información personal y asumir la identidad o vender la información, para obtener tarjetas de crédito u otros instrumentos financieros, en forma fraudulenta, como préstamos o hipotecas.

Comentarios por venganza: Publicar comentarios falsos o extremadamente críticos en sitios como ripofferport.com. También es posible publicar información personal, prejuicios sobre una persona en sitios como thedirty.com.

Pornografía de venganza: Publicación de fotos o videos con desnudos o semidesnudos en sitios web y en otros foros sin el consentimiento de la parte. Como sucede con otros métodos de acoso en línea, la mayoría de los autores intentan permanecer en el anonimato al realizar la pornovenganza creando perfiles falsos o cuentas de correo electrónico gratuitas para publicar sobre sus víctimas.

Sexting: Intercambio de fotos o videos con desnudos o semidesnudos en línea a través de aplicaciones como Snapchat, Instagram, Vine o sitios web como Facebook. Mientras que el "sexting" en sí mismo no es acoso en línea, se puede convertir en acoso si las fotos se envían a destinatarios que no las han solicitado o si el receptor a su vez los redistribuye.

SWATting: Hacer una llamada falsa a la policía para invocar una respuesta armada, generalmente por el equipo SWAT[lxxxi]. Esto a veces parece una amenaza falsa de bomba o un informe falso sobre una toma de rehenes.

Trolling: Los usuarios en línea que tratan de incitar a la reacción por publicar comentarios intencionalmente tangenciales o agresivamente groseros. Esto también incluye *trolls* contratados: por ejemplo, personas relacionadas con campañas políticas pueden recibir un pago para iniciar discusiones o publicar puntos de vista ridículos y extremos sobre sus oponentes para desacreditarlos.

Las mejores prácticas recomendadas para restringir el acoso en línea[lxxxii]:

Restringir los lugares dónde publicar información personal: Sea consciente de quién puede acceder a información de contacto o la información sobre sus intereses, hábitos o trabajo para reducir la exposición a los agresores. Esto puede restringir el riesgo de convertirse en víctima; puede resultar más fácil identificar al agresor si se convierte en víctima.
Evitar la escalación de la situación: Responder con hostilidad probablemente provoque a un agresor. Según las circunstancias, considere ignorar la cuestión. A menudo, los cyberbullies y agresores prosperan en la reacción de sus víctimas. Si usted o su hijo reciben mensajes electrónicos no deseados, ya sean mensajes SMS o correo
electrónico, considere cambiar la dirección electrónica. Es posible detener el problema. Si continúa recibiendo mensajes en la cuenta nueva, puede llevar su caso a una acción legal.
Documentar el cyberbullying: Registrar cualquier actividad en línea (correos electrónicos, sitios web, mensajes en redes sociales, etc.), incluyendo las fechas y horas. Mantener una versión electrónica y una copia impresa.

Informar el acoso cibernético a las autoridades competentes: Si usted o su hijo está siendo acosado o amenazado, informe de la actividad a las autoridades locales. La policía local o nacional a menudo es un buen punto de partida. Hay una distinción entre libertad de expresión y la agresión punible. Los fiscales y funcionarios encargados de hacer cumplir la ley pueden ayudar a clasificar las implicaciones legales. También puede ser apropiado informar a los directivos de la escuela quienes pueden disponer de diferentes políticas para abordar la actividad que involucra a los estudiantes.

Ser propietario de su propia participación en línea: Cuando sea posible, establezca la configuración de privacidad y seguridad en los sitios web a su nivel de comodidad para el intercambio de información. Por ejemplo, cambie la configuración de sus sitios de redes sociales para limitar la visibilidad de los mensajes a "sólo amigos". Es aceptable limitar el intercambio de información.

Utilizar contraseñas seguras y preguntas de seguridad: No utilizar la misma contraseña en diferentes sitios. Si tiene problemas para recordar las contraseñas, utilice un gestor de contraseñas como iPassword (Agilebits) y autenticación bifactorial siempre que sea posible en las redes sociales y cuentas de correo electrónico. Si publica información personal como su escuela y el nombre de soltera de su madre a los medios de comunicación social, utilice diferentes respuestas a preguntas que se le puede pedir a su institución financiera, para que las respuestas no se puedan determinar fácilmente. También, en lugar de utilizar la información real personal, considere elegir una frase absurda que pueda recordar y que usa para estas cuestiones (por ejemplo, nombre de soltera de la madre: Batman).

Más seguro para mí, más seguro para todos: Lo que usted hace en línea puede afectar a todos: en casa, en el trabajo y todo el mundo. Practicar buenos hábitos en línea beneficia a la comunidad digital mundial.

Educar a la comunidad: Hay muchos recursos disponibles que pueden ayudar a desalentar el acoso cibernético. Provistos a través de las autoridades gubernamentales[lxxxiii]

CONCLUSIÓN

En los últimos años, el ambiente de las amenazas en línea y móviles ha cambiado dramáticamente, y apunta a una gama más amplia de individuos, empresas y redes. La aparición de nuevas tecnologías permite ataques más sofisticados que se desarrollarán mediante el aprovechamiento de vulnerabilidades de una gama más amplia de servicios, canales y plataformas.

Los métodos tradicionales para abordar las amenazas en línea, con antivirus, firewalls y campañas de educación siguen siendo una parte importante de la defensa. El malware y las botnets que surgieron en los últimos años se han transformado para evitar su detección y corrección. Para hacer frente a estas amenazas nuevas y emergentes, la comunidad internacional debe dar un paso más en el ecosistema de Internet y, de manera colaborativa, desarrollar enfoques polifacéticos y multilaterales para combatirlas.

Este informe proporciona las mejores prácticas recomendadas para que los consumidores, la industria y los gobiernos aborden las amenazas móviles y en línea. Se incluyen recomendaciones para que los consumidores sean más proactivos en la protección de sus propios dispositivos; para que los proveedores de servicios implementen prácticas y tecnologías de seguridad recomendadas de inmediato; para que los gobiernos garanticen entornos regulatorios y legislativos modernos vigentes y trabajen con las organizaciones internacionales para lograr esfuerzos de colaboración.

Estas recomendaciones son un conjunto de herramientas para manejar amenazas móviles, en línea y de voz. Sin embargo, las amenazas descritas en este informe son sólo un panorama del entorno actual de las amenazas. Dado que las actividades en línea cambian, el uso de la informática móvil aumenta, y los usuarios de Internet y las empresas cambian sus respuestas y defensas a las amenazas existentes, estas amenazas se modifican y adaptan para atacar otras vulnerabilidades y perseguir nuevos objetivos.

La implementación de estas recomendaciones tendrá un enfoque multilateral y coordinado. Con ese fin, los autores de este informe recomendamos a la OCDE y otras organizaciones internacionales unirse al M^{3}AAWG y al LAP y participar con las organizaciones que gobiernan y administran las infraestructuras de Internet. Además, para hacerle frente del entorno cambiante de las amenazas, las organizaciones interesadas deberían colaborar más proactivamente en la supervisión de amenazas y la implementación de nuevas medidas como sea necesario.

GLOSARIO

- **Estafa del 419** Llamada así a partir del Capítulo 38, Sección 419, del Código Penal nigeriano que aborda el tema del fraude. "Cualquier persona que mediante un pretexto falso, y con intención de defraudar, obtenga de otra persona cualquier cosa pasible de ser robado, o induzca a otra persona a entregar a un tercero cualquier cosa pasible de ser robado, es culpable de delito y será castigado con prisión de tres años". Estas fueron los famosos correos electrónicos o esquemas de pago por adelantado del príncipe nigeriano en los que se solicita gastar dinero a cambio de obtener riquezas incalculables a final del régimen.

- **Fraude por pago adelantado:** Se trata de correos electrónicos que ofrecen un pago adelantado, por ejemplo un sobrepago, por servicios ofrecidos. En la forma más frecuente, se solicita que el sobrepago se realice a un tercero. Después de que el tercero liquida el pago, se descubre que el pago original es falso y se retira del estado de cuenta del banco de la víctima.

- **Protocolo de puerta de enlace de borde (BGP):** Es el protocolo que toma decisiones sobre enrutamiento central en Internet. Mantiene una tabla de "prefijos" o redes IP que designan la capacidad de alcance de la red entre sistemas autónomos.[1]

- **Memoria caché:** Almacenamiento de información utilizada recientemente en un lugar donde se puede acceder muy rápidamente. Por ejemplo, un navegador web utiliza una memoria caché para almacenar información sobre páginas web recientemente visitadas en el disco rígido. Dado que el acceso al disco rígido del equipo es mucho más rápido que el acceso a Internet, el almacenamiento en la memoria caché de páginas web puede acelerar significativamente la navegación web. [2]

- **Denegación de servicio distribuido (DDoS):** Es un tipo de ataque cibernético que apunta a avasallar o interrumpir de manera alguna la capacidad del sistema blanco para recibir información e interactuar con otros sistemas. Por ejemplo, el envío de uno o un enorme número de mensajes no deseados para evitar que un servidor o una red funciona correctamente.

- **Descarga oculta:** Se trata de la descarga involuntaria de software desde Internet. Un usuario puede autorizar una descarga sin entender las consecuencias, por ejemplo un programa ejecutable falso, o la descarga puede ocurrir sin conocimiento alguno del usuario.[3]

- **Proveedores de servicios de correo electrónico (ESP):** Es una empresa que ofrece servicios de correo electrónico a otras empresas. Estos servicios pueden incluir la recolección y armado de listas de direcciones de correo electrónico, el envío de correo masivo a las direcciones de la lista, la eliminación de direcciones que rebotan los correos y el manejo de reclamos e informes de ataques causados por correos electrónicos masivos.

- **Firewall:** Es un dispositivo de hardware o software instalado en un equipo que controla el acceso entre una red privada y una red pública, como Internet. Un firewall está diseñado para proporcionar protección mediante el bloqueo del acceso no autorizado al equipo o a la red.

- **Sistema global para comunicación móvil (GSM):** Es un conjunto estándar desarrollado por el Instituto Europeo de Estándares de Telecomunicaciones (ETSI) para describir los protocolos de segunda generación (2G) para redes móviles y digitales utilizadas por los teléfonos móviles. [4]

- **Filtrado de ingresos:** Es una técnica que se utiliza para garantizar que los paquetes entrantes pertenezcan en verdad a las redes que dicen pertenecer mediante el bloqueo de paquetes que provienen de direcciones de IP falsas. [5]

- **Corporación para la asignación de números y nombres en Internet (ICANN):** Es el organismo que coordina el Sistema de Nombres de Dominio (DNS), la asignación de espacio de direcciones IP (Protocolo de Internet), la asignación del protocolo de identificación, la gestión del Sistema de Nombres de Dominio genéricos (gTLD) y de nivel superior con código de país (ccTLD) y las funciones de gestión del sistema de servidor raíz.[6]

- **Mula de dinero:** Se llama así a una persona que transfiere dinero robado o mercancías de un país a otro, ya sea en persona, a través de un servicio de mensajería o por medios electrónicos. Las mulas de dinero en línea generalmente existen como resultado de estafas por phishing o malware[7]

- **Nodo:** En la comunicación de datos, un nodo de red física puede ser un equipo de terminación de circuito de datos (DCE), por ejemplo un módem, un núcleo, un puente o un conmutador; o un equipo terminal de datos (DTE), como un teléfono digital, una impresora o un equipo host, por ejemplo un enrutador, una estación de trabajo o un servidor.

- **JavaScript:** Es un lenguaje de código de escritura que permite a los autores diseñar de páginas web interactivas.

- **Phishing:** Es el intento de obtener información personal para robar una identidad u otra información confidencial, como números de tarjeta de crédito o datos bancarios con fines fraudulentos. Por ejemplo, un mensaje de correo electrónico que parece ser del banco del destinatario le solicita que visite un sitio web para confirmar los detalles de la cuenta, pero en cambio lo dirige a un sitio web falso donde se recopila la información personal.

- **SMShing o phishing mediante SMS o mensaje de texto:** Se envía un enlace que conduce a un sitio web falso vía SMS, o el mensaje le solicita al destinatario que llame a un número de teléfono donde continuará el ataque de ingeniería social.

- **Spoofing**: Es fingir ser otra persona u organización y hacer que un mensaje de correo electrónico o una llamada telefónica originada en un lugar que dista de su origen legítimo parezca real.

- **Dominios de Alto Nivel (TLD):** Los TDL son el más alto nivel en la jerarquía del Sistema de Nombres de Dominio de Internet y representa la última porción del nombre de dominio. Por ejemplo, en el nombre de dominio www.example.com, el dominio de alto nivel es .com. La responsabilidad de gestionar dominios de más alto nivel es delegada a ciertos organismos por la Corporación para la Asignación de Nombres y Números en Internet (ICANN), que maneja la Autoridad de Números Asignados en Internet (IANA), y tiene a cargo el mantenimiento de la zona raíz del DNS.

- **Typosquatters:** Son errores tipográficos que cometen los usuarios de Internet cuando escriben la dirección de un sitio web en un navegador web. En caso de que un usuario accidentalmente ingrese una dirección web incorrecta, puede conducir a un sitio web alternativo de un cybersquatter. Una vez en el sitio del typosquatter, el usuario puede también ser engañado pensando que son de hecho en el sitio real mediante el uso de copiado o similares logotipos, diseños web o contenido.[8]

- **VoIP**: Es el enrutamiento de conversaciones de voz por Internet. Difiere de una llamada telefónica, que se hace desde el teléfono del hogar o la oficina que pasa a través de la red telefónica pública conmutada.

- **Vishing o phishing mediante voz sobre IP:** Se realiza una llamada al destinatario, utilizando a menudo una capacidad común de VoIP para establecer un identificador falso de llamadas, se le solicita a la persona que llama a visitar un sitio web o a llamar a un número de teléfono donde

continuará el ataque mediante ingeniería social. Varios esquemas comunes incluyen un "soporte técnico de Microsoft", cuestiones de impuestos atrasados o "usted será arrestado si no paga una multa".

- **Inyecciones web:** Es un tipo de ataque a la seguridad en el que el atacante añade código a un cuadro de formulario web para acceder a recursos o realizar cambios en los datos. Los cuadros de entrada se suelen utilizar para la autenticación de un usuario; sin embargo, la mayoría de los formularios web no tienen mecanismos que bloqueen la entrada de distintos nombres y contraseñas. Si no se toman precauciones, un atacante puede utilizar los cuadros de entrada para enviar su solicitud a la base de datos, que podría permitirle descargar la base de datos o interactuar otra manera ilícita. [9]

REFERENCIAS

- 1. http://en.wikipedia.org/wiki/Border_Gateway_Protocol
- 2. http://www.techterms.com/definition/cache
- 3. http://en.wikipedia.org/wiki/Drive-by_download
- 4. http://en.wikipedia.org/wiki/GSM
- 5. http://www.expertglossary.com/security/definition/ingress-filtering
- 6. http://www.icann.org/en/about/welcome
- 7. http://en.wikipedia.org/wiki/Money_mule
- 8. http://en.wikipedia.org/wiki/Typosquatters
- 9. http://searchsoftwarequality.techtarget.com/definition/SQL-injection

[i] DCWG, http://www.dcwg.org/
[ii] Grupo de Trabajo para Conficker, http://www.confickerworkinggroup.org/
[iii] WinFixer, Wikipedia, http://en.wikipedia.org/wiki/WinFixer
[iv] Symantec, 2015 Internet Security Threat Report, Volume 20, http://www.symantec.com/security_response/publications/threatreport.jsp
[v] McAfee, McAfee Labs 2014 Threats Predictions, http://www.mcafee.com/ca/resources/reports/rp-threats-predictions-2014.pdf
[vi] Microsoft, Download Center, http://www.microsoft.com/en-us/download/details.aspx?id=44937
[vii] Secunia, http://secunia.com/vulnerability_scanning/personal/
[viii] PCMag, "The Best Password Managers for 2015", http://www.pcmag.com/article2/0,2817,2407168,00.asp; PCMag, "You Can't Remember Good Passwords, So You Need a Password Manager", http://securitywatch.pcmag.com/security-software/332153-you-can-t-remember-good-passwords-so-you-need-a-password-manager
[ix] PCMag, "The Best Free Antivirus for 2015", http://www.pcmag.com/article2/0,2817,2388652,00.asp
[x] Internet Engineering Task Force (IETF), "Recommendations for the Remediation of Bots in ISP Networks", http://tools.ietf.org/html/rfc6561
[xi] Aquilina, James, Eoghan Casey y Cameron Malin, Malware Forensics: Investigating and Analyzing Malicious Code, Elsevier, Inc., 2008.
[xii] Safe Code, http://www.safecode.org
[xiii] M3AAWG, "ABCs for ISPs", https://www.m3aawg.org/abcs-for-ISP-code
[xiv] National Security Agency, Security Configuration Guides, http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml
[xv] National Vulnerability Database, "National Checklist Program Repository", http://web.nvd.nist.gov/view/ncp/repository
[xvi] Verizon, 2014 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2014/
[xvii] *Ibid.*
[xviii] APWG, "APWG Phishing Attack Trends Reports", https://apwg.org/resources/apwg-reports/
[xix] APWG, "APWG Global Phishing Survey 1H2014: Trends and Domain Name Use", http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf
[xx] RSA, "2014 Cybercrime Roundup", www.emc.com/collateral/fraud-report/h13929-rsa-fraud-report-jan-2015.pdf
[xxi] Center for Strategic and International Studies, "2014 McAfee Report on the Global Cost of Cybercrime", http://csis.org/event/2014-mcafee-report-global-cost-cybercrime
[xxii] O'Connor, Fred, PCWorld, "Monetising Medical Data is Becoming the Next Revenue Stream for Hackers", March 21, 2015
[xxiii] IT Governance, "123 Million Health Care Records Breached so far this Year", March 26, 2015, http://www.itgovernanceusa.com/blog/123-million-health-care-records-breached-so-far-this-year/
[xxiv] Sender Policy Framework, "Project Overview", http://www.openspf.org/
[xxv] DKIM.org, http://dkim.org/
[xxvi] ICANN, http://www.icann.org/
[xxvii] DMARC, http://dmarc.org
[xxviii] En la mayoría de los países de occidente, las instituciones financieras les reembolsará a los consumidores las pérdidas por fraude generadas mediante la institución financiera.
[xxix] McAfee, "McAfee Labs Report Highlights Success of Phishing Attacks with 80% of Business Users Unable to Detect Scams", September 4, 2014, http://www.mcafee.com/us/about/news/2014/q3/20140904-01.aspx
[xxx] SANS, "Building an Effective Phishing Program", http://www.securingthehuman.org/media/resources/presentations/STH-Presentation-PhishingYourEmployees.pdf
[xxxi] Stop. Think. Connect., "Resources", www.stopthinkconnect.org/resources/
[xxxii] StaySafeOnline.org, "National Cyber Security Awareness Month", https://www.staysafeonline.org/ncsam/
[xxxiii] APWG, "How to Redirect a Phishing Site Web Page to the APWG.ORG Phishing Education Page", http://phish-education.apwg.org/r/how_to.html
[xxxiv] Grupo de Trabajo Anti-Phishing (APWG, en inglés), www.apwg.org
[xxxv] Grupo de Trabajo Anti-Abuso de Mensajes, Malware y Móvil, www.m3aawg.org
[xxxvi] Alianza de Confianza en Línea, otalliance.org
[xxxvii] Consejo de Riego del Comerciante, merchantriskcouncil.org
[xxxviii] Foro de los Equipos de Respuesta a Incidentes y Seguridad, first.org
[xxxix] FBI, "DNS Changer Malware" November 9, 2011, http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

[xl] RFC Editor, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", May 2000, http://www.rfc-editor.org/info/bcp38
[xli] RFC Editor, "Ingress Filtering for Multihomed Networks", March 2004, http://www.rfc-editor.org/info/bcp84
[xli] https://www.arin.net/policy/nrpm.html
[xlii] RFC Editor, "Ingress Filtering for Multihomed Networks", March 2004, http://www.rfc-editor.org/info/bcp84
[xliii] https://www.arin.net/policy/nrpm.html
[xliv] Counterpoint, "Market Monitor: Handset and Spartphone Markets Q4 2014", January 29, 2015, http://www.counterpointresearch.com/marketmonitor2014q4
[xlv] The Realtime Report, "Mobile Comemerce: Online Retail Sales from Mobile Devices Double in Last Year", May 3, 2012, http://therealtimereport.com/2012/05/03/mobile-commerce-online-retail-sales-from-mobile-devices-double-in-last-year/
[xlvi] Corra, "Mobile Shopping Trends by Device", February 3, 2015, http://corra.com/mobile-ecommerce-trends-2015
[xlvii] GSMA Intelligence, "Global Data", https://gsmaintelligence.com/
[xlviii] Worldometers, "Current World Population", http://www.worldometers.info/world-population/
[xlix] IDC, Llamas, Ramon, Anthony Scarsella, William Stofega, "Worldwide Mobile Phone 2015-2019 Forecast and Analysis", April 2015, http://www.idc.com/getdoc.jsp?containerId=prUS23455612 (subscription required)
[l] Symantec, "Internet Security Threat Report", April 2015, Volume 20, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA- internet-security-threat-report-volume-20-2015-social_v2.pdf
[li] *Ibid.*
[lii] Adaptive Mobile, "Selfmite: Attack Using SMS Worm to Increase Pay-Per-Install Income", June 25, 2014, http://www.adaptivemobile.com/blog/selfmite-worm
[liii] Australia, Bulgaria, Belgium, France, Germany, Ghana, Greece, Ireland, Kenya, Netherlands, USA, South Africa, Spain, Sweden, Switzerland
[liv] Lookout, "2014 Mobile Threat Report," https://www.lookout.com/static/ee_images/Consumer_Threat_Report_Final_ENGLISH_1.14.pdf
[lv] Bibat, Aerol, "GGTracker Malware Hides as Android Market", Android Authority, June 21, 2011 http://www.androidauthority.com/ggtracker-malware-hides-as-android-market-17281/
[lvi] ICT, "Statistics", http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
ICT, "ICT Facts and Figures, The World in 2014", http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf; http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf
[lvii] *Compare for example:* 47 U.S.C. § 227(b)(1)(A)(iii) *with* 47 U.S.C. § 227(b)(1)(B) and 47 U.S.C. § 227(b)(2)(B).
[lviii] FCC, "'One Ring' Phone Scam," *available at* http://www.fcc.gov/guides/one-ring-wireless-phone-scam.
[lix] CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart"
[lx] See for e.g., T-Lock Call Blocker – Version N2, http://hqtelecom.com/callblocker?gclid=CMmt_raT6cECFc1_MgodhnEAWg; CPR Call Blocker Product Page, http://www.cprcallblocker.com/purchase.html; Digitone Call Blocker Plus, http://www.digitone.com; and Sentry Dual Mode Call Blocker, http://www.plugnblock.com/?gclid=CJmKkbaT6cECFSFgMgodJRIAGA; Privacy Corp Caller ID Manager, http://www.privacycorps.com/products/ .
[lxi] Weisbaum, Herb, "Want to get rid of those $#%@ robocalls? There's an app for that," http://www.cnbc.com/id/101758815# .
[lxii] Alliance for Telecommunications Industry Solutions, "Next Generation Interconnection Interoperability Forum (NGIIF) Auto Dialers Reference Document," https://www.atis.org/docstore/product.aspx?id=26137
[lxiii] Prepared Statement of The Federal Trade Commission Before the United States Senate Committee on Commerce, Science and Transportation, Subcommittee on Consumer Protection, Product Safety, and Insurance on 'Stopping Fraudulent Robocall Scams: Can More Be Done?', Washington, DC, July 10, 2013 ("Senate Hearing"), http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=c1eec086-3512-4182-ae63-d60e68f4a532&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=7&YearDisplay=2013
[lxiv] *Truth in Caller ID Act*, 47 U.S.C. § 227(e); cf. 16 C.F.R. Part 310.4(a)(8).
[lxv] Federal Trade Commission, "Robocalls Gone Wrong", https://www.consumer.ftc.gov/media/video-0027-robocalls-gone-wrong
[lxvi] The Economist, "The Cheap, Convenient Cloud," April 18, 2015, http://www.economist.com/news/business/21648685-cloud-computing-prices-keep-falling-whole-it-business-will-change-cheap-convenient?fsrc=scn/tw/te/pe/ed/thecheapconvenientcloud
[lxvii] M³AAWG, "M³AAWG Sender Best Common Practices, Version 3, Updated February 2015," https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

[lxviii] http://w3techs.com/technologies/history_overview/content_management/all/y
[lxix] https://wpvulndb.com/statistics
[lxx] http://w3techs.com/technologies/details/cm-wordpress/all/all
[lxxi] http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white%20papers/2013_emerson_data_center_cost_downtime_sl-24680.pdf Page 13
[lxxii] http://www.stateoftheinternet.com/resources-web-security-2014-q4-internet-security-report.html
[lxxiii] http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white%20papers/2013_emerson_data_center_cost_downtime_sl-24680.pdf Page 14
[lxxiv] Noroozian, A. et al., "Developing Security Reputation Metrics for Hosting Providers, http://www.tudelft.nl/fileadmin/Faculteit/TBM/Onderzoek/Publicaties/hosting-metrics.pdf
[lxxv] Twitter boss vows to crack down on trolls and abuse: http://www.theguardian.com/technology/2015/feb/26/twitter-costs-dealing-abuse-harassing-dick-costolo
[lxxvi] Suicide of Rehtaeh Parsons: https://en.wikipedia.org/wiki/Suicide_of_Rehtaeh_Parsons
[lxxvii] Granby, Quebec, Canada moves to fine people insulting police on social media: http://www.cbc.ca/news/canada/montreal/granby-moves-to-fine-people-insulting-police-on-social-media-1.3045816
[lxxviii] 4chan Bullies Fitness Guru Scooby Off YouTube With Doxxing and Threats: http://newmediarockstars.com/2013/07/4chan-bullies-fitness-guru-scooby-off-youtube-with-doxxing-and-threats-video/
[lxxix] How I got caught up in a 'stranded traveller' phishing scam: http://www.theguardian.com/money/2013/nov/13/stranded-traveller-phishing-scam
[lxxx] How One Stupid Tweet Blew Up Justine Sacco's Life: http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html?_r=0
[lxxxi] The World Has No Room For Cowards: http://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards/
[lxxxii]Stay Safe Online, https://www.staysafeonline.org/stay-safe-online/for-parents/cyberbullying-and-harassment
[lxxxiii] From the US FTC, https://www.consumer.ftc.gov/articles/0028-cyberbullying;
Nigeria, http://www.mamalette.com/parenting-3/cyber-bullying-nigerian-parents-need-know/;
ACMA, http://www.cybersmart.gov.au/Schools/Cyber%20issues/Cyberbullying.aspx;
RCMP, http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/index-eng.htm;
South African Police Service, http://www.saps.gov.za/child_safety/teens/cyber_bullying.php;

Steering Committee

Andre Leduc, Manager, National Anti-Spam Coordinating Body, Industry Canada

Alyson Hawkins, Policy Analyst, Industry Canada

Christina Adam, Policy Analyst, Industry Canada

Jerry Upton, Executive Director, Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)

Lisa Foley, Policy Analyst, Industry Canada

Neil Schwartzman, Executive Director, CAUCE.org

Contributors

Alex Bobotek, Lead, Mobile Messaging Anti-Abuse Strategy and Architecture, AT&T

Amy Hindman, Principal Engineer, Verizon

Betsy Broder, Counsel for International Consumer Protection, Federal Trade Commission

Bruce Matthews, Manager, Anti-spam Team, Australian Communications & Media Authority

Carlo Catajan, iCloud Mail & iMessage Anti-Abuse, Apple Inc.

Carlos Alvarez, Sr. Manager, Security Engagement, SSR Team, ICANN

Chris Boyer, Assistant Vice President, Global Public Policy, AT&T

Christian Dawson, President, ServInt and Chairman, i2Coalition

David Jevans, Chairman, Anti-Phishing Working Group (APWG)

Eric Freyssinet, Ministère de l'intérieur, France

Foy Shiver, Deputy Secretary-General, APWG

Francis Louis Tucci, Manager, Network Repair Bureau, Verizon Wireless

Frank Ackermann, M³AAWG Public Policy Committee Co-chair

Gary Warner, Director of Research in Computer Forensics, University of Alabama at Birmingham

Jay Opperman, General Manager, CSP, Damballa

Jayne Hitchcock, President, WOAH

Jeff Williams, Dell SecureWorks

Jessica Malekos Smith, Student, UC Davis School of Law

John Levine, President, CAUCE.org

Jonathan Curtis, Norse Corporation

Justin Lane, Anti-Abuse Manager, Endurance International

Karen Mulberry, ISOC

Lee Armet, Senior Investigator, TD Bank Group

Mary Retka, Director, Network Policy, CenturyLink

Matthew Bryant, Ofcom

Matthew C Stith, Manager, Anti-abuse, Rackspace Hosting

Michael Hammer, American Greetings

Michael O'Reirdan, Comcast Fellow

Patrick Tarpey, Ofcom

Paul Vixie, CEO, Farsight Security

Peter Merrigan, Government of New Zealand

Phil Shih, Structure Research

Richard Feller, Hedgehog Hosting

Rod Rasmussen, President and CTO, Internet Identity (IID)

Sanjay Mishra, Distinguished Member of Technical Staff, Verizon

Sara Roper, Manager Information Security, CenturyLink

Sid Harshavat, Symantec

Steven Champeon, Enemieslist

Terry Zink, Program Manager, Microsoft

TR Shaw, SURBL

Venkata Atluri, Associate Professor, Alabama A&M University

Participants

Adam Panagia, Adria Richards, Alexander Falatovich, April Lorenzen, Autumn Tyr-Salvia, Bill Wilson, Bulent Egilmez, Chris Lewis, Dave Crocker, David Dewey, David Levitt, Donald McCarthy, Donald Smith, Dylan Sachs, Eric Chien, Franck Martin, Hein Dries-Ziekenheiner, Jacek Materna, Jack Johnson, Jared Mauch, Jean Marie Norman, John Cunningham, Julia Cornwell McKean, Kaio Rafael, Karmyn Lyons, Ken Simpson, Lucas Moura, Mark Collier, Matteo Lucchetti, Michael Shoukrey, Mustaque Ahamad, Nabeel Koya, Nitin Lachhani, Olivier Caleff, Patricia B. Hsue, Paul Ebersman, Peter Cassidy, Raymond Choo, Richard Clayton, Richard Gane, Rudy Brioche, Sid Harshavat, Steve Jones, Steven M. Wernikoff, Suresh Ramasubramanian, Toni Demetriou, Trent Adams, Will Clurman