News Release - For Immediate Release

Se definen los requisitos mínimos de seguridad para la adquisición de equipos en las instalaciones del cliente en las Nuevas Mejores Prácticas Operativas Conjuntas de LACNOG y M³AAWG

MONTEVIDEO, Uruguay y SAN FRANCISCO, 2019/06/03 – Las nuevas recomendaciones de mejores prácticas para los proveedores locales de servicios de Internet (Internet Service Providers, ISP), emitidas por LACNOG y M³AAWG este mes, definen los criterios básicos de seguridad para enrutadores domésticos y otros equipos locales del cliente (customer premise equipment, CPE). Se espera que ayuden a proteger Internet contra ataques comunes, especialmente contra ataques de denegación de servicios (Denial of Service, DoS) que surgen del abuso de estos dispositivos. Las directrices fortalecerán los esfuerzos de seguridad de los proveedores de servicios de Internet al identificar los requisitos para los dispositivos de hardware conectados a sus redes que son susceptibles de explotación cuando se ignoran las salvaguardas básicas.

El documento de mejores prácticas operativas actuales realizado en conjunto por LACNOG y M³AAWG sobre los requisitos mínimos de seguridad para la adquisición de equipos locales del cliente (CPE) (Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition) se está traduciendo a múltiples idiomas para que sean utilizados por los proveedores de servicios de Internet de todo el mundo. Fue publicado por el Grupo de Operadores de Redes de América Latina y el Caribe (Latin American and Caribbean Network Operators Group, LACNOG) y por el Grupo Contra el Abuso de Mensajería, Malware y Dispositivos Móviles (Messaging, Malware and Mobile Anti-Abuse Group, M3 AAWG), y está disponible en www.lacnog.net/docs/lac-bcop-1 y en www.m3aawg.org/CPESecurityBP o las traducciones actuales en https://www.m3aawg.org/published-documents.

La configuración y funcionalidad de seguridad recomendadas se basan en la experiencia de la industria y son esenciales para evitar los ataques de denegación de servicios (DoS) que hacen uso de dispositivos de infraestructura de redes vulnerables, dispositivos de Internet de las cosas (Internet of Things, IoT) e infecciones de malware. Se proporciona una Tabla de Requisitos para ayudar a los ISP a personalizar las recomendaciones de seguridad para sus redes en un formato conciso que pueden proporcionarse a los fabricantes de CPE.

Esfuerzo mundial para fortalecer la protección en línea

El documento se está traduciendo actualmente al portugués, español, francés, alemán y japonés, y se espera que sigan otros idiomas. Las mejores prácticas traducidas serán útiles en todo el mundo como una herramienta para que los proveedores de servicios de Internet establezcan los requisitos para la configuración predeterminada de los equipos de las instalaciones del cliente que se conectarán a sus redes, sostiene la editora del documento: Lucimara Desiderá, directora del Grupo de Trabajo Contra el Abuso para América Latina y el Caribe (Latin American and Caribbean Anti-Abuse Working Group, LAC-AAWG) y analista de seguridad en CERT.br (el Equipo nacional de respuesta a emergencias informáticas del Brasil).

"Los equipos latinoamericanos de respuesta a incidentes de seguridad informática han identificado la falta de seguridad de los CPE como un grave problema de ataques durante los últimos años. Estas nuevas prácticas recomendadas les permitirán a los proveedores de servicios de Internet negociar con los proveedores de CPE para garantizar que los equipos que se conectan a sus redes cumplan con los requisitos mínimos de seguridad, lo que ayudará a reducir la

cantidad y la intensidad de ataques en Internet en general y, como resultado, el impacto negativo que causan en las operaciones de los proveedores de servicios de Internet", comentó Desiderá.

Las directrices cubren la documentación y la información de contacto del proveedor, la seguridad del software, las actualizaciones remotas y la funcionalidad de administración de los dispositivos, las preferencias de configuración predeterminadas y las políticas de soporte relacionadas con las correcciones de seguridad. Entre las recomendaciones figuran las siguientes:

- Las contraseñas no deben incluirse en el firmware, deben ser modificables y los proveedores no deben usar la misma contraseña predeterminada para todos los dispositivos.
- Es necesario que exista un mecanismo para las actualizaciones periódicas y remotas de software, incluido un método para verificar la autenticidad de un archivo de actualización descargable.
- El equipo debe configurarse de forma restrictiva, en lugar de configurarse de manera permisiva.

Como ejemplo del alcance del problema, el malware Mirai, responsable de varios ataques importantes al sitio web, contiene una tabla con más de 60 nombres de usuario y contraseñas predeterminados de fábrica comunes a los que hace referencia para iniciar sesión e infectar cámaras de seguridad domésticas, enrutadores domésticos y otros dispositivos de IoT. Las nuevas directrices harían que la tabla de inicio de sesión fuera ineficaz, de acuerdo con los dichos del presidente de la Junta Directiva de M³AAWG, Severin Walker.

Walker señaló: "La colaboración de M³AAWG con LACNOG y su Grupo de Trabajo de América Latina y el Caribe, en este documento fue una prioridad, en parte, debido a nuestro trabajo continuo con los operadores de redes regionales y los grupos de respuesta a incidentes para enfrentar las amenazas globales a las comunicaciones seguras. También fue importante porque tenemos que seguir cambiando el enfoque de nuestros miembros en la seguridad de IoT, los dispositivos móviles y otros dispositivos de consumo para ayudar a prevenir los ataques cada vez más grandes que se originan en ellos".

El documento de mejores prácticas fue desarrollado por LACNOG y M³AAWG y expuesto en la reunión LACNIC 31 en República Dominicana el 8 de mayo. Se basa en la experiencia de los grupos de trabajo de LACNOG LAC-AAWG y el Grupo de Trabajo BCOP, en colaboración con los miembros de M³AAWG, sus asesores técnicos principales y el Comité Técnico de M³AAWG.

Acerca de LACNOG

LACNOG (www.lacnog.net) es el Grupo de Operadores de Redes de América Latina y el Caribe que cuenta con una Junta Directiva, un Comité de Programa y diferentes Grupos de Trabajo. Proporciona un ámbito para que los operadores de redes y las partes interesadas intercambien experiencias y conocimientos a través de listas de correo, grupos de trabajo y reuniones anuales. LACNOG también promueve los Grupos de Operadores de Redes (Network Operators Groups, NOGs) locales y los foros de intercambio de información, el desarrollo, la adopción de mejores prácticas y las actividades de capacitación técnica y tutoriales.

Acerca del Grupo de Trabajo Contra el Abuso de Mensajería, Malware y Dispositivos Móviles (Messaging, Malware and Mobile Anti-Abuse Working Group, M3AAWG)

El Grupo de Trabajo Contra el Abuso de Mensajería, Malware y Dispositivos Móviles (M³AAWG) es donde se une el sector para trabajar contra bots, malware, spam, virus, ataques de denegación de servicio y otras explotaciones en línea. Los miembros de M³AAWG (www.m3aawg.org) representan más de dos mil millones de buzones de correo de algunos de los operadores de redes más grandes del mundo. Aprovecha la profundidad y experiencia de su membresía global para abordar el abuso en las redes existentes y los nuevos servicios emergentes a través de la tecnología, la colaboración y las políticas públicas. También trabaja para educar a los creadores de políticas globales sobre los problemas técnicos y operacionales relacionados con el abuso y con la mensajería en línea. Con sede en San Francisco,

Calif., M³AAWG se basa en las necesidades del mercado y está respaldado por las principales operadores de redes y proveedores de mensajería.

Junta Directiva y patrocinadores de M³AAWG: 1 & 1 Internet SE; Adobe Systems Inc.; AT&T Comcast; Endurance International Group; Facebook; Google, Inc.; LinkedIn; Mailchimp; Marketo, Inc.; Microsoft Corp.; Orange; Proofpoint; Rackspace; Return Path, Inc.; SendGrid, Inc.; Vade Secure; Valimail; VeriSign, Inc. y Verizon Media (Yahoo y AOL).

Miembros de pleno derecho de M³AAWG: Agora, Inc.; Broadband Security, Inc.; Campaign Monitor; Cisco Systems, Inc.; CloudFlare, Inc.; dotmailer; eDataSource Inc.; ExactTarget, Inc.; IBM; iContact; Internet Initiative Japan (IIJ); Liberty Global; Listrak; Litmus; McAfee; Mimecast; Oracle Marketing Cloud; OVH; Spamhaus; Splio; Symantec; USAA y Wish.

Una lista completa de miembros está disponible en http://www.m3aawg.org/about/roster.

El texto original en el idioma fuente de este comunicado es la versión oficial autorizada. Las traducciones solo se suministran como adaptación y deben cotejarse con el texto en el idioma fuente, que es la única versión del texto que tendrá un efecto legal.

# # #

Contacto con los medios: Astra Communications, Linda Marcus, APR, +1-714-974-7973 (Pacífico de los EE. UU.), LMarcus@astra.cc

unta Directiva y patrocinadores de M³AAWG: 1 & 1 Internet SE; Adobe Systems Inc.; AT&T; Comcast; Endurance International Group; Facebook; Google, Inc.; LinkedIn; Mailchimp; Marketo, Inc.; Microsoft Corp.; Orange; Proofpoint; Rackspace; Return Path, Inc.; SendGrid, Inc.; Vade Secure; Valimail; VeriSign, Inc., y Verizon Media (Yahoo & AOL).

Miembros de pleno derecho de M³AAWG: Agora, Inc.; Broadband Security, Inc.; Campaign Monitor; Cisco Systems, Inc.; CloudFlare, Inc.; dotmailer; eDataSource Inc; ExactTarget, Inc.; IBM; iContact; Internet Initiative Japan (IIJ); Liberty Global; Listrak; Litmus; McAfee; Mimecast; Oracle Marketing Cloud; OVH; Spamhaus; Splio; Symantec; USAA; y Wish.

Una lista completa de miembros está disponible en http://www.m3aawg.org/about/roster.