M3AAWG

MESSAGING MALWARE MOBILE

Techniques, Tools and Processes to Help Service Providers Clean Malware from Subscriber Systems

Barry Raveendran Greene, bgreene@senki.org

October 22, 2012, Baltimore, Maryland, USA

M^3AAWG
MESSAGING MALWARE MOBILE

M^3AAWG Training Video Series

Techniques, Tools and Processes to Help Service Providers Clean Malware from Subscriber Systems

(more than 2.25 hours of training)

This is Segment 5 of 6

The complete series is available at: https://www.m3aawg.org/activities/maawg-training-series-videos

Segment 1 **Top SP Security Essential Techniques** **(about 20 minutes)**	**Segment 2** **Types of Malware Problems ISPs Encounter** **(about 20 minutes)**	**Segment 3** **Understanding the Threat:** **A Cyber-Criminal's Work Day & Cyber-Criminal Behavior Drivers** **(about 30 minutes)**
Segment 4 **Turning Point** **(about 12 minutes)**	**Segment 5** **Remediating Violated Customers** **(about 35 minutes)**	**Segment 6** **U.S. FCC's Anti-Botnet Code of Conduct (ABCs for ISPs)** **Overview &** **Code on a Shoestring Budget** **(about 20 minutes)**

MESSAGING MALWARE MOBILE

Remediating Violated Customers

Segment 5 of 6

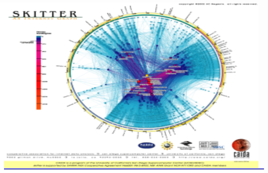
Barry Raveendran Greene, bgreene@senki.org

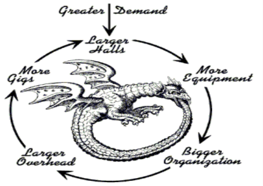
October 22, 2012, Baltimore, Maryland, USA

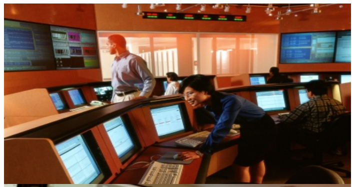
Barry Greene has over 30 years industry experience including having served as president of the ISC (Internet Systems Consortium). He is a pioneer in service provider security and operational security reaction teams.

Barry is currently a participant on the U.S. Federal Communications Commission’s (FCC’s) Communications Security, Reliability and Interoperability Council (CSRIC).

Remediating Violated Customers







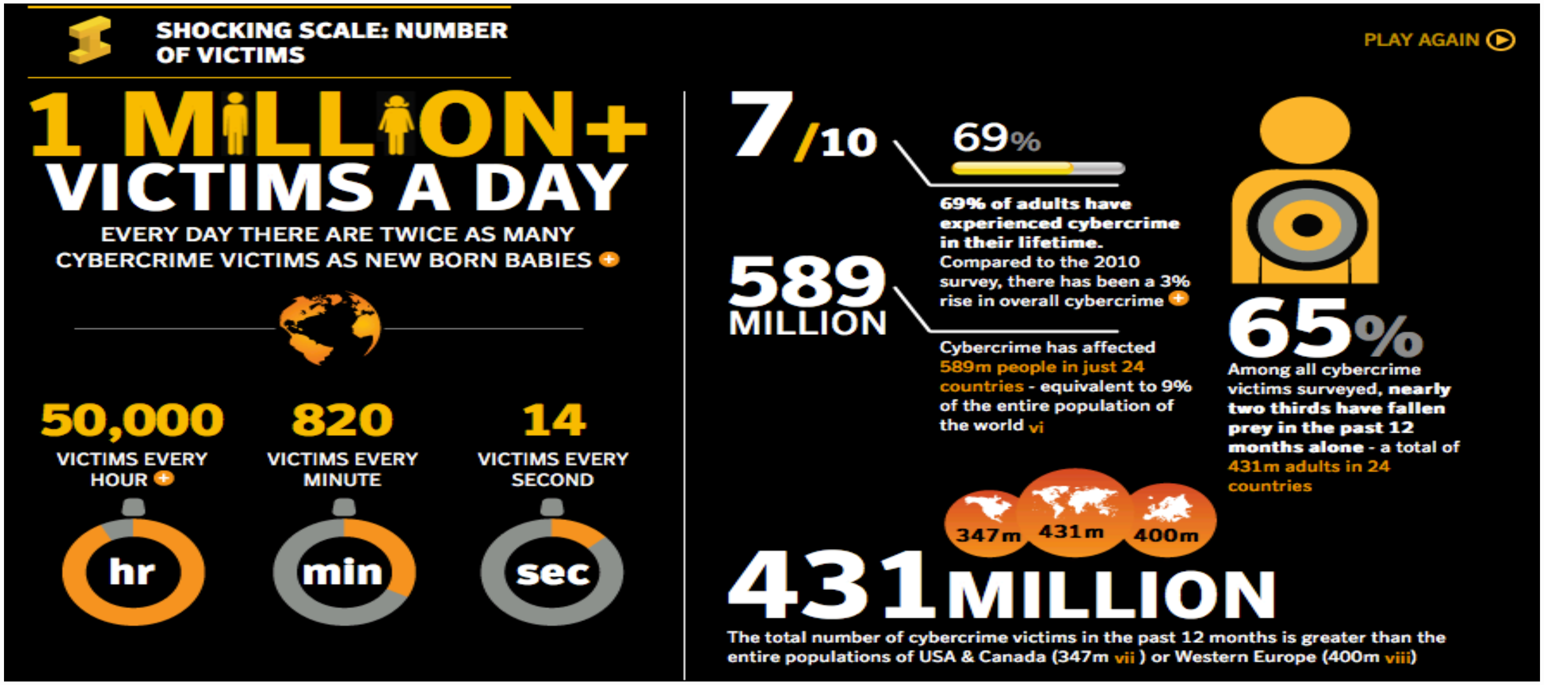
Time for Remediation Action

- The cyber-civic society will be expecting all parties to do their part to protect against cyber-threats.
- This includes Service Providers.
- This module is based on the work in the IETF RFC 6561 ***Recommendations for the Remediation of Bots in ISP Networks (http://tools.ietf.org/html/rfc6561)***

Your Customers are Not the Problem!

- There was a time where “users” and “customers” were blamed for doing dumb things to get their systems infected.
- When users who have up to date hardware, operating systems, software, anti-virus, anti-malware, and is mindfully doing the right think still getting infected, then we have to consider that the real problem is beyond the user!

This is your Network!



SHOCKING SCALE: NUMBER OF VICTIMS

PLAY AGAIN

1 MILLION+ VICTIMS A DAY

EVERY DAY THERE ARE TWICE AS MANY CYBERCRIME VICTIMS AS NEW BORN BABIES

50,000 VICTIMS EVERY HOUR

820 VICTIMS EVERY MINUTE

14 VICTIMS EVERY SECOND

7/10

69%

69% of adults have experienced cybercrime in their lifetime. Compared to the 2010 survey, there has been a 3% rise in overall cybercrime

589 MILLION

Cybercrime has affected 589m people in just 24 countries - equivalent to 9% of the entire population of the world vi

65%

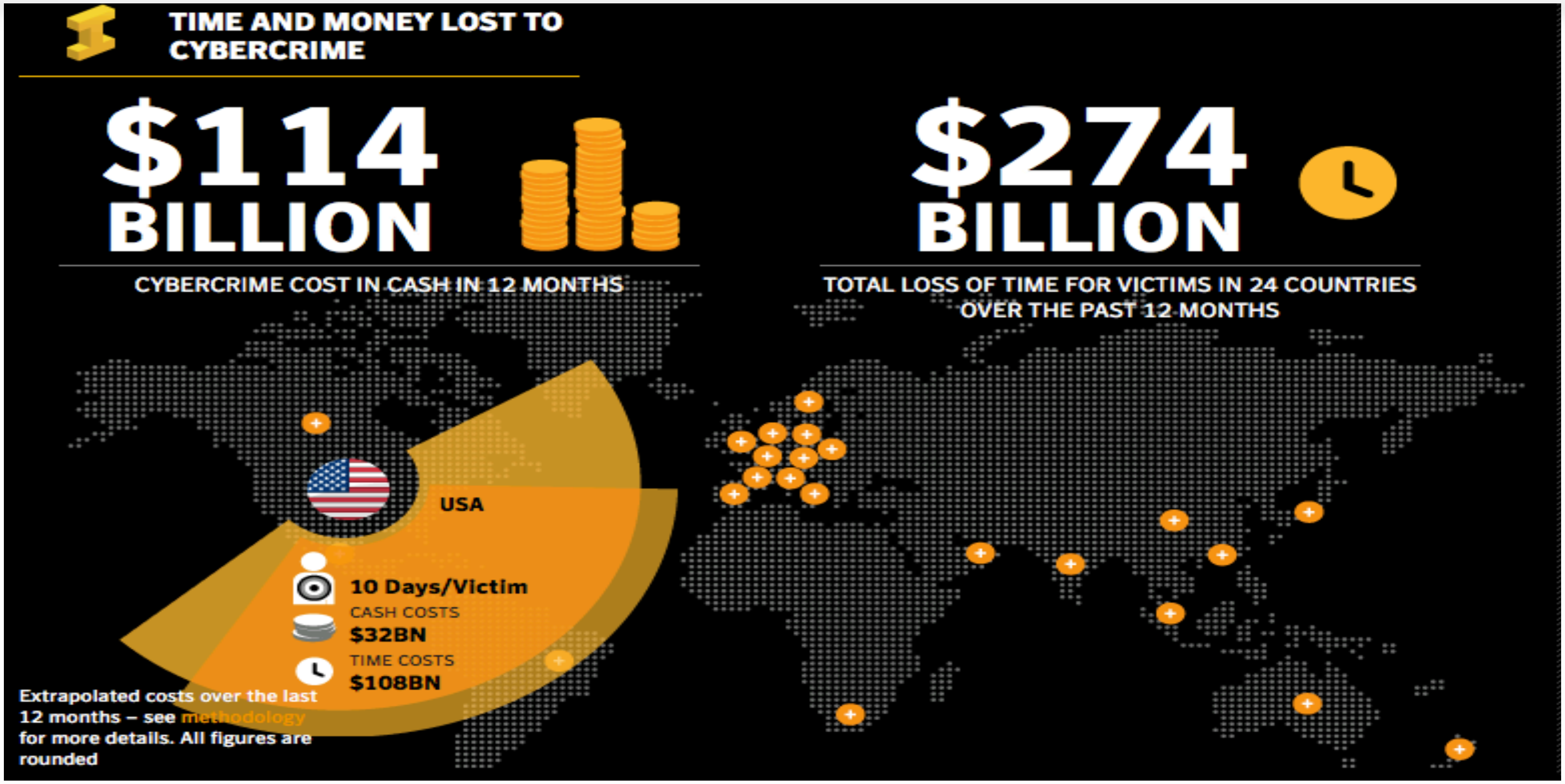
Among all cybercrime victims surveyed, **nearly two thirds have fallen prey in the past 12 months alone** - a total of 431m adults in 24 countries

431 MILLION

The total number of cybercrime victims in the past 12 months is greater than the entire populations of USA & Canada (347m vii) or Western Europe (400m viii)

See http://norton.com/cybercrimereport.

Victimization Cost



TIME AND MONEY LOST TO CYBERCRIME

$114 BILLION

CYBERCRIME COST IN CASH IN 12 MONTHS

$274 BILLION

TOTAL LOSS OF TIME FOR VICTIMS IN 24 COUNTRIES OVER THE PAST 12 MONTHS

10 Days/Victim

CASH COSTS

$32BN

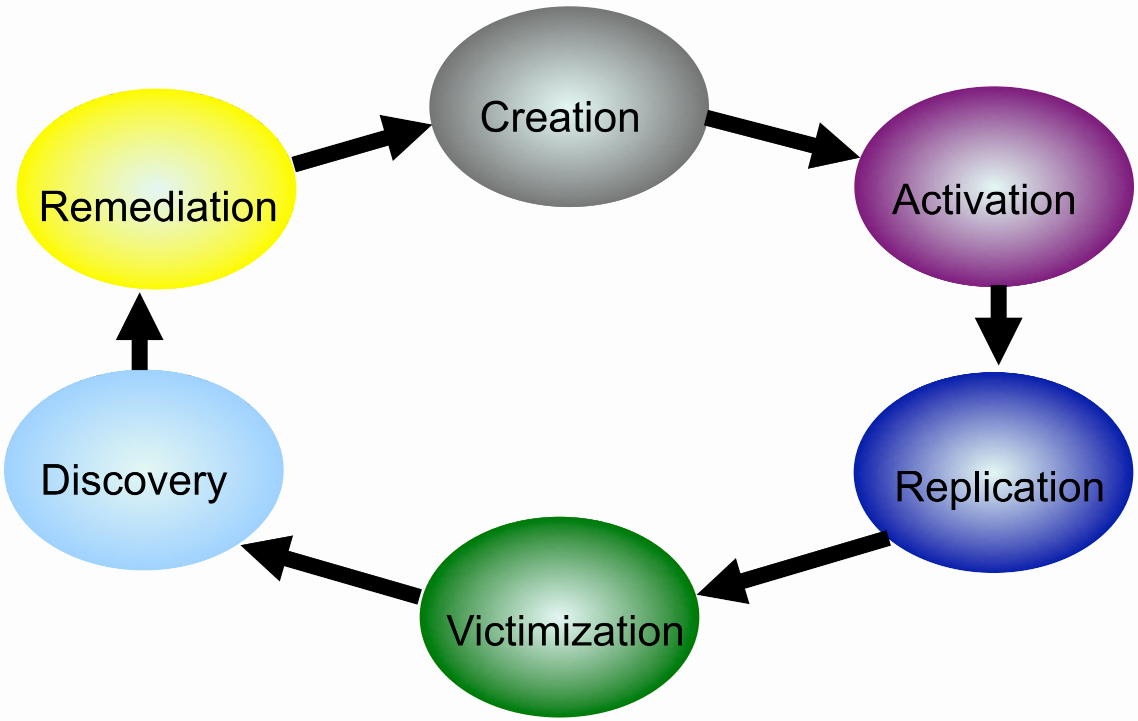
TIME COSTS

$108BN

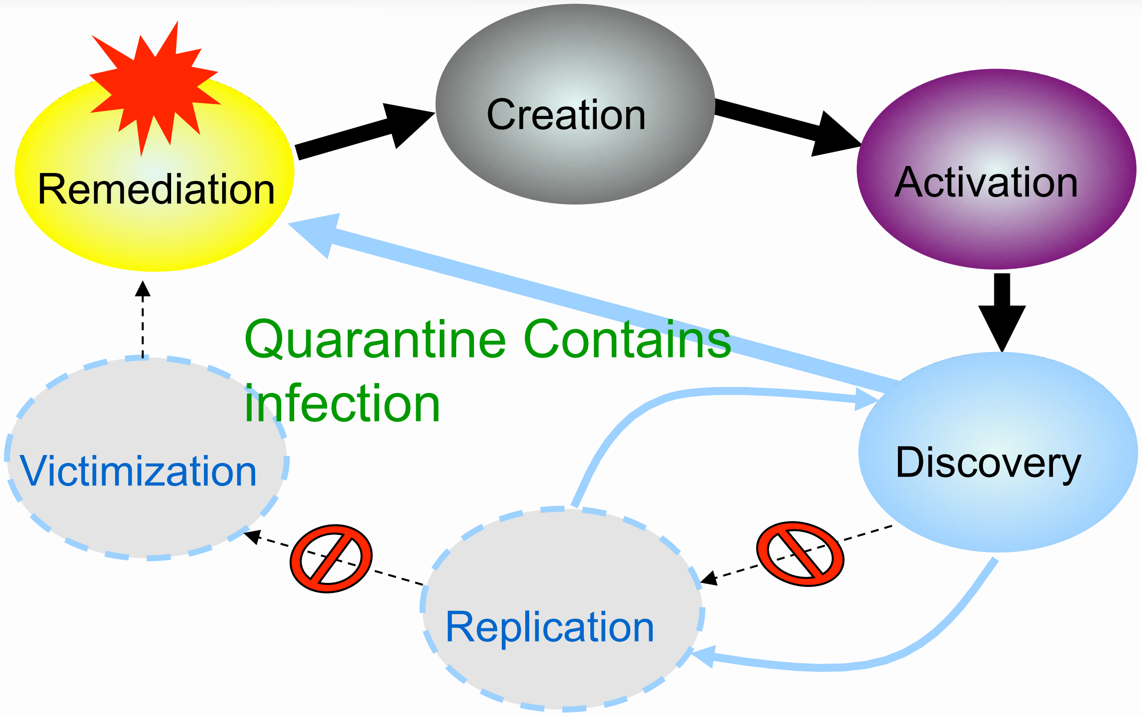
Extrapolated costs over the last 12 months – see methodology for more details. All figures are rounded

See http://norton.com/cybercrimereport.

Normal Malware Cycle



Remediation Shortens the Cycle



Remediation

Creation

Activation

Discovery

Replication

Victimization

Quarantine Contains infection

Proactive Detection
Discovers Infection
In Early stage

Minimizing Replication and Assimilation
Is the key to damage control

Principles of Remediation

- No one party can remediate a violated customer.
- It takes a team that involves the entire eco-system of operating system vendors, application providers, on-line content, anti-virus vendors, service providers, professional computer repair organizations, and the ***user of the device***.

Expectations of Remedation

- No way guarantee the remediation of all bots.
- Bot removal is potentially a task requiring specialized knowledge, skills and tools, and may be beyond the ability of average users.
- Attempts at bot removal may frequently be unsuccessful, or only partially successful, leaving the user's system in an unstable and unsatisfactory state or even in a state where it is still infected.
- Attempts at bot removal can result in side effects ranging from a loss of data to partial or complete loss of system usability.

When a when a customer’s computer gets infected, we ask them to go buy a new PC. We’re in Hong Kong. New PCs are cheaper than trying to clean up our customer’s computer. ***(anonymous CTO in an SP)***

Detecting BOTNET & Malware

- Service Providers have a range that gives them insight into which of their customers are infected.
  - Reports (free and subscription) from external parties.
  - Service Provider Telemetry.
  - Partnership with Anti-Virus Vendors
  - Helpdesk calls

Where to Start

- We currently have a multitude of organizations who will provide detailed and traceable (i.e. through account logs and NATs) reports.
  - Arbor - Atlas, see http://atlas.arbor.net/
  - Internet Systems Consortium - Secure Information Exchange (SIE), see https://sie.isc.org/
  - Microsoft - Smart Network Data Services (SNDS), see https://postmaster.live.com/snds/
  - SANS Institute / Internet Storm Center - DShield Distributed Intrusion Detection System, see http://www.dshield.org/about.html
  - ShadowServer Foundation, see http://www.shadowserver.org/
  - Spamhaus - Policy Block List (PBL), see http://www.spamhaus.org/pbl/
  - Spamhaus - Exploits Block List (XBL), see http://www.spamhaus.org/xbl/
  - Team Cymru - Community Services, see http://www.team-cymru.org/

Alerting Violated Customers

- Communicating with customers is core to modern customer experience.
- Customer persistence and stickiness is core to reducing churn.
- Any rational SP strategy to reduce churn will have customer communications tools that include:
    - Email
    - Phone
    - Walled Garden
    - IM
    - Web Alert
    - Home Page Alert
    - SMS
    - TV Screen Alerts

Alerting Violated Customers

- If you know that a customer has been violated, then there are civic society expectations to let them know they are being victimized.
- SPs doing this today find that it is a tool to increase customer loyalty and decrease churn.
- Tracking violated customers means that the Service Provider must update their customer tracking & support system to know which are identified as victimized and which have been notified.

Alerting Violated Customers

- **Email Notification** – E-mail with customers sometimes work – but with all the SPAM, how do they know it is from you? Email notification with another approach to validate the source works best.
- **Telephone Call Notification** – A simple phone call does wonders. But also needs a secondary source to validate (fake support phone calls do happen).
- **Postal Mail Notification** – People do look at mail from their service provider. The notification letter can have all the information needed to help the violated customers start their remediation work.

Alerting Violated Customers

- **Walled Garden Notification** – Violated customers who are not paying attention or may be other devices in the residence/ business may need to be put into a walled garden to notify. Careful attention is needed to insure collateral impact to other devices in the residence/business are not impacted (i.e. medial monitoring or emergency services).
- **Instant Message Notification** – Many people live on chat. A chat pop-up can be a way to get the attention of a violated customer.
- **Short Message Service (SMS) Notification** – Mobile phone operators can send free SMS – asking the violated customer to go to a site and run a security check.
- **Web Browser Notification - In**
- **Social Media -**

Alerting Violated Customers

- **Web Browser Notification** – If the browser is where the customer lives, then explore tools that help interact at the browser level (i.e. plugins or toolbars).
- **Social Media** – A large majority of customers live in social media. The same tools can be used to get the word out to violated customers.

Notification Factor

- **Notification to Public Access Points.** Alerting violated customers that are tracked from a public WIFI point may or may not be the best time to notify. A coffee shop would not be a good place to try to recover your system from a malware infection.
- **Shared IP addresses.** Many residence and businesses are behind NAT with no logging (or they will have not clue about "NAT logging"). Tools to help them figure out which computer, device, or appliance is infected will be needed.
  - Q. How do you remediate a violated Internet connected refrigerator?
  - Q. How do you remediate a violated diabetic monitoring device?
- **Law Enforcement Lessons on how to help a Victim of Crime are useful.** The SP's support team can draw on lesson used in the LE community to help people productively cope.

I’ve checked everything!

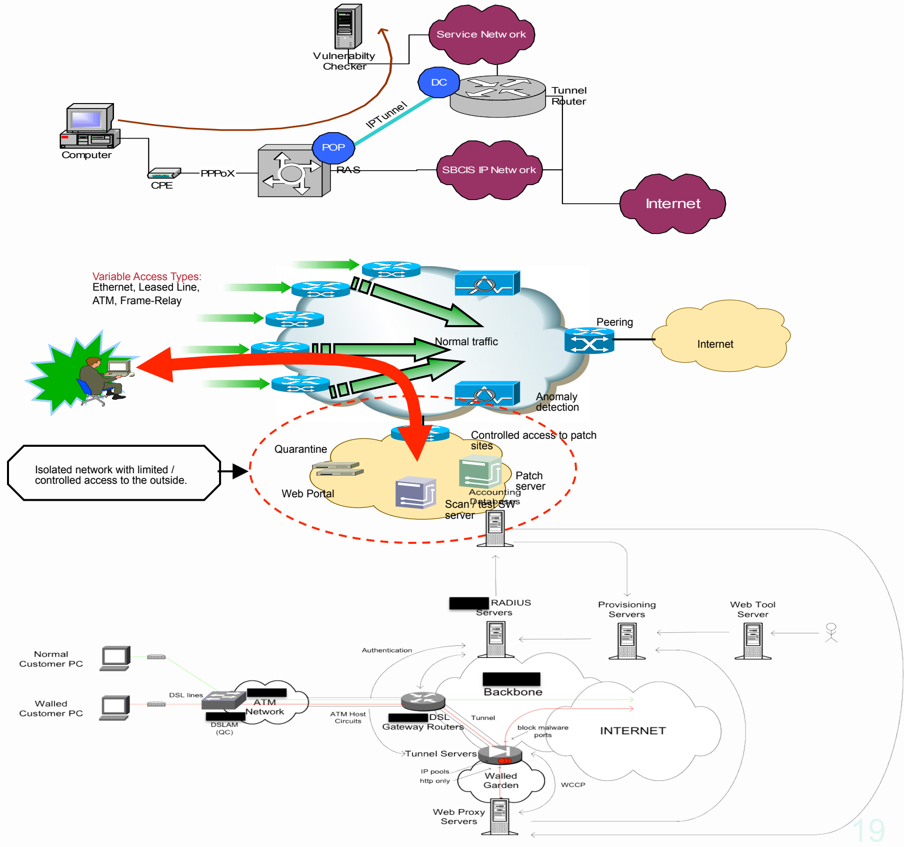
- Customer: “I’ve checked all my computers, my kids computers, my phones, my tables, my X-box, my Tivo, my printers, my furnace, my light controls, my home security system, my health monitoring system, my electric vehicle charging station, my soar panel monitoring system …. Everything is patched and fixed – why are you still saying I’m infected with malware!?”

- Support Team “Have you checked to see if your neighbors are using your wireless?”

- Customer: “How do I do that?”

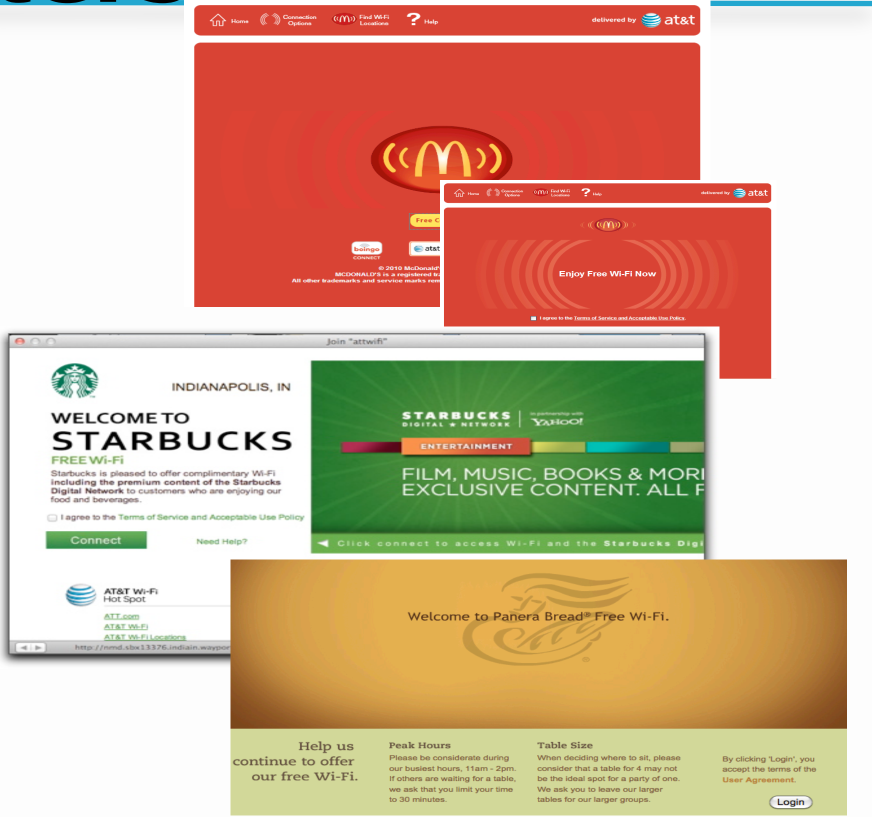
Walled Garden Systems do Work

- Several major providers now have ½ a decade of experience with production walled garden/quarantine systems.
- These systems work, they have not turn off customers, and have been updated to work with E.911 and medical devices.



Walled Gardens are Everyday Encounters

- We, as an industry, know how to set up our AAA to trigger a interactive user response.
- This is now an every day activity. There no longer a surprise factor with end-users.



© 2010 McDonald's
MCDONALD'S is a registered tr
All other trademarks and service marks rem

Enjoy Free Wi-Fi Now

□ I agree to the Terms of Service and Acceptable Use Policy.

Join "attwifi"

INDIANAPOLIS, IN

WELCOME TO STARBUCKS

FREE Wi-Fi

Starbucks is pleased to offer complimentary Wi-Fi **including the premium content of the Starbucks Digital Network** to customers who are enjoying our food and beverages.

□ I agree to the Terms of Service and Acceptable Use Policy

FILM, MUSIC, BOOKS & MORI
EXCLUSIVE CONTENT. ALL F

Click connect to access Wi-Fi and the Starbucks Digi

Welcome to Panera Bread® Free Wi-Fi.

Help us continue to offer our free Wi-Fi.

Peak Hours
Please be considerate during our busiest hours, 11am - 2pm. If others are waiting for a table, we ask that you limit your time to 30 minutes.

Table Size
When deciding where to sit, please consider that a table for 4 may not be the ideal spot for a party of one. We ask you to leave our larger tables for our larger groups.

By clicking 'Login', you accept the terms of the User Agreement.

Remediation Guidelines

- Three approaches:
  - **Self Help** – Point customers to a self-help site or create your own security landing page.
  - **Professional Help** – Ask for the user to use a professional service to clean up the malware. The professional service might offer help with the other consequence of the violation (i.e. identity theft or some other crime).
  - **Get a new computer or device** – Unfortunately, we could see malware evolving to the point where the hardware is violated and the only remediation is to get a new device (ask the industry for consumer capable re-imaging).

Consequences of In-Action

- We as an industry are at a stage where Service Providers need to play their part in the remediation eco-system.
- Cyber-Civic society will drive for action through:
  - Government Guidelines, Regulation, and Laws
  - Through market forces (customer churn)
  - Through civic legal action
  - Through insurance underwriters demanding actions that reduce the over all risk to a system.

Homework

- Read through the IETF draft IETF RFC 6561 ***Recommendations for the Remediation of Bots in ISP Networks (*** ***http://tools.ietf.org/html/rfc6561)***
- Talk to your peers at operations meeting like NANOG, RIPE, APRICOT, etc to find out what they are doing.
- Join the SP Security effort that will document, build, and teach remediation techniques that work.
  - E-mail bgreene@senki.org for more information or go to http://confluence.senki.org and select "SP Security."

Bot Mitigation for ISPs – Link to Materials

http://confluence.senki.org/display/SPSec/MAAWG+26+-+Workshop

This has been the fifth of six video segments

View the entire

Techniques, Tools and Processes to Help Service Providers Clean Malware from Subscriber Systems

from the public training video pages on the M^{3}AAWG website at:
https://www.m3aawg.org/activities/maawg-training-series-videos

Our thanks to Barry Raveendran Greene
for developing and presenting the material in this series
and allowing M^{3}AAWG to videotape it for professionals worldwide.

This video is presented by the
Messaging, Malware and Mobile Anti-Abuse Working Group

M3AAWG

MESSAGING MALWARE MOBILE

For information about M^{3}AAWG:

www.m3aawg.org

www.facebook.com/maawg

www.twitter.com/maawg

www.youtube.com/maawg

Contact us at:

https://www.m3aawg.org/contact_form