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^{3}AAWG
MESSAGING MALWARE MOBILE

M^{3}AAWG 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 6 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

U.S. FCC's Anti-Botnet Code of Conduct (ABCs for ISPs):

Overview & Code on a Shoestring Budget

Segment 6 of 6

Barry Raveendran Greene, bgreene@senki.org

October 22, 2012, Baltimore, Maryland, USA

M3AAWG
MESSAGING MALWARE MOBILE

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).

CSRIC III

Communications Security, Reliability and Interoperability Council

US FCC’s Anti-Botnet Code of Conduct

What is CSRIC?

- The **Communications Security, Reliability and Interoperability Council's (CSRIC)** mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety.
  - We're currently in the middle of CSRIC III (see http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii)

CSRIC III

- CSRIC III is covering these areas:
  - WG 1: NG 9-1-1
  - WG 2: Next Generation Alerting
  - WG 3: E9-1-1 Location Accuracy
  - WG 4: Network Security Best Practices
  - WG 5: DNSSEC Implementation Practices for ISPs
  - WG 6: Secure BGP Deployment
  - **WG 7: Botnet Remediation**
  - WG 8: E9-1-1 Best Practices
  - WG 9: Alerting Issues Associated With CAP Migration
  - WG 10: 9-1-1 Prioritization

CSRIC III BOTNET Remediation

- This Working Group will review the efforts undertaken within the international community, such as the Australian Internet Industry Code of Practice, and among domestic stakeholder groups, such as IETF and the Messaging Anti-Abuse Working Group, for applicability to U.S. ISPs. Building on the work of CSRIC II Working Group 8 ISP Network Protection Practices, the Botnet Remediation Working Group shall propose a set of agreed-upon voluntary practices that would constitute the framework for an opt-in implementation model for ISPs. The Working Group will propose a method for ISPs to express their intent to op-into the framework proposed by the Working Group.

- The Working Group will also identify potential ISP implementation obstacles to the newly drafted Botnet Remediation business practices and identify steps the FCC can take that may help overcome these obstacles.

- Finally, the Working Group shall identify performance metrics to evaluate the effectiveness of the ISP Botnet Remediation Business Practices at curbing the spread of botnet infections.

Anti-Botnet Code of Practice

- A voluntary code of practice was adopted to insure no unrealistic cost are imposed on the industry.
- Each SP is now asked to public state if they will comply with the code of practice.

CSRIC III

Communications Security, Reliability and Interoperability Council

March 2012

Final Report

U.S. Anti-Bot Code of Conduct (ABCs)
for Internet Service Providers (ISPs)

(A Voluntary Code)

"This Code of Conduct would be a major step forward and a significant complement to the Administration's broader efforts against botnets."

FCC Chairman Julius Genachowski
February 22, 2012

WORKING GROUP 7 - Botnet Remediation

What is the ABC?

- Encourage ISPs to
  - Educate end-users of the threat posed by bots and of actions end-users can take to help prevent bot infections;
  - Detect bot activities or obtain information, including from credible third parties, on bot infections among their end-user base;
  - Notify end-users of suspected bot infections or help enable end-users to determine if they are potentially infected by bots; and
  - Provide information and resources, directly or by reference to other sources, to end-users to assist them in remediating bot infections.

ABC’s Implementation

- Implementation of the Code will be guided by the following principles:
  1. **Voluntary** — participation is voluntary and encourages types of actions to be taken by ISPs, however this Code does not require any particular activity.
  2. **Technology neutral** — this Code does not prescribe any particular means or methods.
  3. **Approach neutrality** — this Code does not prescribe any particular approach to implement any part of this Code.
  4. **Respect for privacy** — ISPs must address privacy issues in an appropriate manner consistent with applicable laws.

ABC’s Implementation (cont)

5. **Legal compliance** — activities must comply with applicable law.
6. **Shared responsibility** — ISPs, acting alone, cannot fully address the threat posed by bots. Other Internet ecosystem participants must also do their part.
7. **Sustainability** — ISPs should seek activities that are cost-effective and sustainable within the context of their business models.
8. **Information sharing** — ISPs should indicate how they are participating in the Code and share lessons-learned from their activities with other appropriate stakeholders. All information sharing between ISPs and other involved parties must be performed in accordance with applicable laws including, but not limited to, antitrust and privacy laws.

ABC Implementation (cont)

9. **Effectiveness** — ISPs should be encouraged to engage in activities that have been demonstrated to be appropriate and effective.
10. **Effective Communication** — Communication with customers* should take into account various issues such as language and make sure that information is provided in a manner that is reasonably expected to be understood and accessible by the recipients.

Participation Requirements

- To participate in this Code, an ISP will engage in at least one activity (i.e., take meaningful action) in each of the following general areas:
  - ✓ **Education** - an activity intended to help increase end-user education and awareness of botnet issues and how to help prevent bot infections;
  - ✓ **Detection** - an activity intended to identify botnet activity in the ISP’s network, obtain information on botnet activity in the ISP’s network, or enable end-users to self-determine potential bot infections on their end-user devices;
  - ✓ **Notification** - an activity intended to notify customers of suspected bot infections or enable customers to determine if they may be infected by a bot;
  - ✓ **Remediation** - an activity intended to provide information to end-users about how they can remediate bot infections, or to assist end-users in remediating bot infections.
  - ✓ **Collaboration** - an activity to share with other ISPs feedback and experience learned from the participating ISP’s Code activities.

Education

- End-users are ultimately responsible for protection of their devices and for remediating an infected device. ISPs, like many other Internet participants and government actors, can assist in helping to educate end-users about the threats presented by bots and the steps end-users can take to protect their devices and remediate infections.
  - Education about bot prevention
  - Support of end-user bot remediation efforts

Education

Guidelines: In addressing the above requirements, ISPs should consider these guidelines:

- Offer educational information and resources directly or through referral to third party services.
- Keep educational content concise and focused on the most important things users need to know.
- Ensure that instructions can be followed by an audience of non-technical users.
- Use multiple media, e.g., images, videos, text, captions, etc., and, where helpful, multiple languages to maximize customer understanding and accessibility.
- Help end-users determine if they have a bot infection by providing information or pointing to resources that describe anomalous behaviors of bot infected devices and the availability and use of bot detection software tools or services.

Detection

- ISPs can find out about malicious activity and bot compromised end-user devices in a variety of ways:
  - Receiving notifications from external entities, particularly those designed to aid with the overall understanding and real-time dissemination of bot related data. A list of resources is listed in Appendix 2.
  - Deploying capabilities within their networks that aid in identifying potential bot infections.
  - Directing customers to tools, a web portal, or other resources that enable customers to self-identify a potential bot infection.

Notification

- Recommended Action: Provide communication of a suspected bot infection to the customer or help enable customers to determine if they are potentially infected by bots. Many notification methods are outlined in references in Appendix 2; however, other methods may be used.

- The problem: Appendix 2 did not reference “other methods.”

Remediation

Recommended Action:

1. Bots are designed to be stealthy and difficult to remove. As part of the notification, ISPs should offer guidance, as described above. This may include links to a variety of publically available online and third party sources of information, software, and tools. It might also include links to professional services. These need not be offered by the ISP itself but may be offered by third parties.

Remediation (cont)

2. An ISP may provide remediation tools to the end-user, either during or after the notification process. However, the ISP should not mandate that the end-user run remediation tools. If the ISP provides tools to the end-user, the end-user should be allowed to exit the process without running any suggested tools or procedures.
3. As part of the notification process, ISPs may wish to include guidance (depending on the nature of the bot in question) that settings on customer owned network equipment such as home gateways and routers may have been altered and should be restored to a secure state, depending on the nature of the bot infection.

Collaboration

Recommended Action: Code participation requires collaboration within ISP, industry, or broader fora through collaborative activities, of which the following are examples:

- Sharing detection, notification, or mitigation methods planned for or deployed in ISP networks, and where practical an evaluation of their effectiveness.
- Sharing of intelligence or operational attack data that may be useful in bot prevention, defense, or remediation.
- Identification of key data or technical resources that are needed from systems or actors beyond the ISP network.
- Participation in definition, development, or operation of integrated defense strategies or systems which extend beyond the boundaries of the ISP network.
- Other collaboration activities involving the sharing of information with parties outside the ISP or data with systems outside of the ISP network.

Impact to the Business (No ABC)

CAPEX – Capital expense on equipment	**Violated customer require more resources from "over the top" cyber-criminals.**
OPSEC – The over all Operational cost of certification, deployment, testing, integration, and maintenance.	**Help desk calls, excess bandwidth consumption, and abuse process all increase OPSEC**
CPGA – Cost per gross subscriber add (primarily subsidies & provisioning)	**No impact.**
ARPU – Average revenue per user month	**Basic services – no extra security services**
CCPU – Cash cost per user per month, ex-marketing (backhaul, customer support, maintenance, & overhead)	**BOTNET violated customer take on more resources on the overall system.**
Churn - % number of subscribers disconnecting each month	**Perception of slow internet services churn the customer.**

Impact to the Business (w/ ABC)

CAPEX – Capital expense on equipment	Additional CAPEX to deploy the ABCs
OPSEC – The over all Operational cost of certification, deployment, testing, integration, and maintenance.	Automated notification systems facilitate call deflection.
CPGA – Cost per gross subscriber add (primarily subsidies & provisioning)	"Security" add on features have new cost – with new revenue.
ARPU – Average revenue per user month	Security features increase ARPU.
CCPU – Cash cost per user per month, ex-marketing (backhaul, customer support, maintenance, & overhead)	Clean customs with new security capabilities have over all savings on the system.
Churn - % number of subscribers disconnecting each month	Big SPs who deploy something like the ABCs report lower churn.

Shoestring ABC Compliance

- Education – Create a /security page – team up with a non-profit industry organization to provide education.
- Detection – Subscribe to the free feeds from Shadowserver, Team CYMRU, and Microsoft. Notification – Deploy a E-mail notification system and a billing notification system.
- Remediation – Same as education.
- Collaboration - Deploy Passive DNS on your DNS Resolvers. Deploy a Dragon Research, Arbor Atlas, and Shadowserver.org box in your Sink Hole (dark IP monitoring). Join groups like MAAWG, OPSEC Trust, NSP-SEC and others.

Home Work

- Sitting around waiting for your customers violated by malware to adversely impact your business is not a wise business decision.
- Recommend action – given that there are cost effective means to take action now.

Bot Mitigation for ISPs – Link to Materials

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

M^{3}AAWG
MESSAGING MALWARE MOBILE

This has been the sixth 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

M^{3}AAWG
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