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

M³AAWG
MESSAGING MALWARE MOBILE

M³AAWG 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 4 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)**

Turning Point

Segment 4 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).

2012 is Cyber Security's Turning Point

Barry Greene bgreene@senki.org

Version 1.1

Thursday, January 10, 13

Takeaways

- Aggressive Private Industry to Private Industry Collaboration is critical before any successful "pubic – private partnership".
- There **are effective Private Industry "Operational Security" Communities** that specialize and success.
- Effective Incident Response, Cyber-Risk Management, and Investigations requires active participation and collaboration in these "Operational Security Communities."
- These communities have rules, expectations, "trust networks," and paranoia that makes it hard to find and hard to gain access. The investment in Trust does turn into results.

Example of Specializations

- Situational Consultation (Map the Crime Vector): **OPSEC Trust's Main Team**
- Situational Awareness: BTFC, Anti-S, SCADASEC (and others)
- Dissecting Malware: **YASMIL, II** (perhaps MWP)
- Big Back Bone Security and IP Based Remediation: **NSP-SEC**
- Domain Name Takedown: **NX-Domain**
- DNS System Security: **DNS-OARC**
- Anti SPAM, Phishing, and Crime: **MAAWG & APWG**
- Vulnerability Management: **FIRST**
- Many other Confidential Groups specializing into specific areas, issues, incidents, and vulnerabilities.
- Investigative Portals providing focused, confidential investigation: **OPSEC Trust Investigative Teams**

2012 - Optimistically

- Every January we have many throughout the industry predicting cyber-doom and cyber-pessimism.
- 2012 is a year where we're going to see a dramatic change.
- Conficker, McColo, Coreflood, Zeus, Gozi, Waledec, Rustoc, DNS Changer, and many other operations have taught us what is needed to effectively collaborate to succeed.
- We can not turn these lessons into a **Cyber Security Strategy of Action**.

Cyber Strategy of Action

- **Private-to-Private Collaboration with Public participation.** Public policy around the world needs to facility the flexibility of private industry to collaboration with each other and with global public partners – moving beyond National constraints.
- **Public – Private Partnership activities need to optimize around private industry flexibility, clarity, and action**. Models like NCFTA are successful because of the interface with aggressive Private-to-Private Collaboration Communities. **We know this works through our results.**

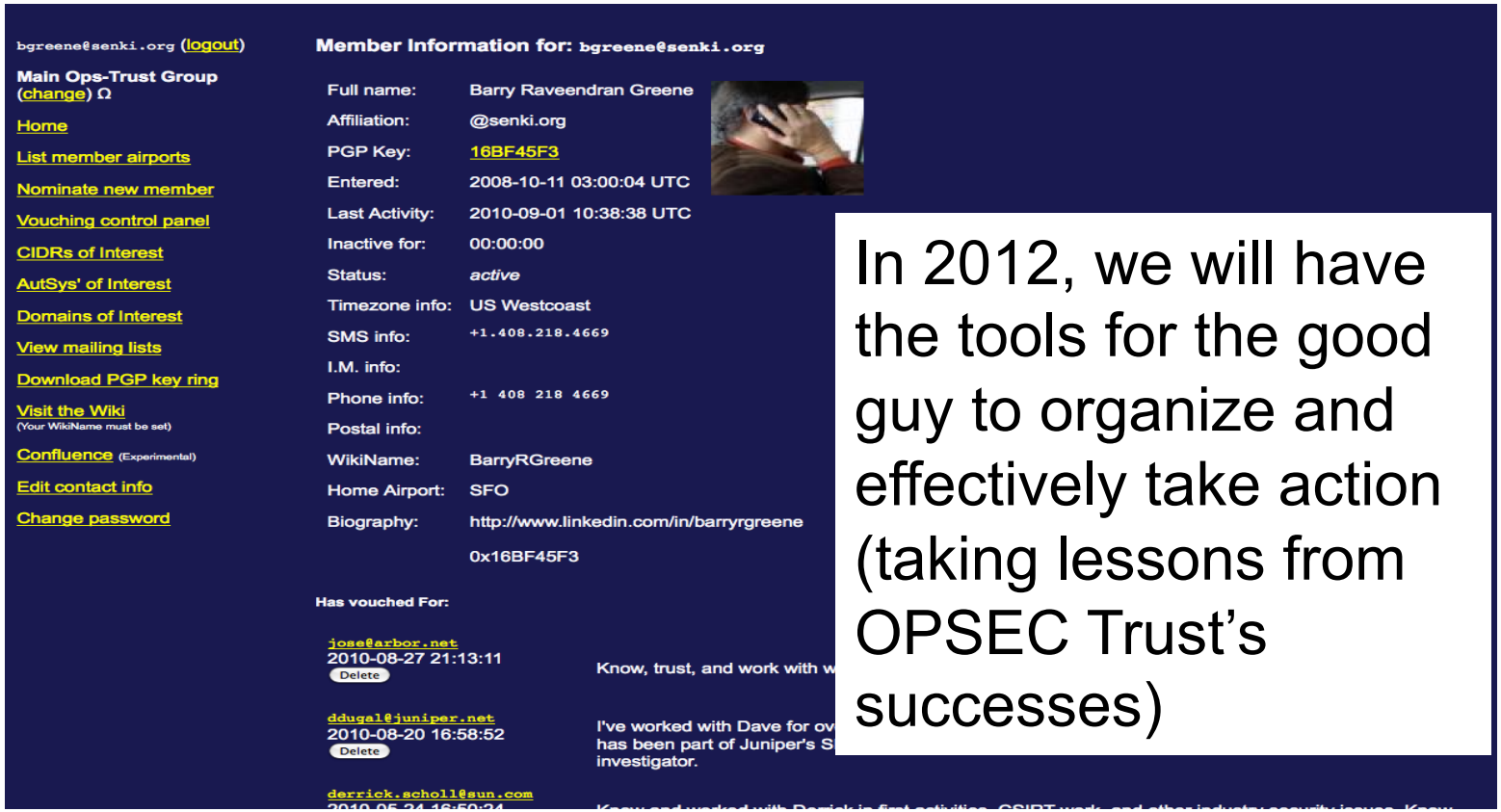
Cyber Strategy of Action

- **Existing Technology for Detecting, Tracking, and Identifying malicious activity is at a level to allow for broad adoption – resulting in new levels of cyber-criminal visibility**. This technology has been validated in enough small and large commercial networks to have a good grape on the operational cost and impact.
- **Existing Technologies for Remediation have proven to work.** Industry who have deployed remediation are prepared to share the business model impact to foster a sustainable and persistent remediation effort.

Cyber Strategy of Action

- **Action Now is the key to preparing for Cyber-Security Defense.** It is imperative for industry to prepare for critical cyber security incidents. Action now is the best way to prepare and build new security capability/capacity. DCWG, Conficker, and other malware take downs are golden opportunities to build the remediation tools that might save the business in the future.

Effective Collaboration



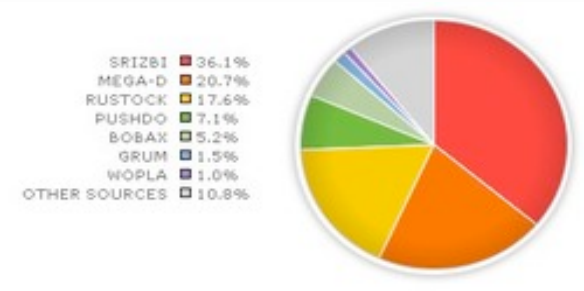
In 2012, we will have the tools for the good guy to organize and effectively take action (taking lessons from OPSEC Trust's successes)

Cyber Strategy of Action

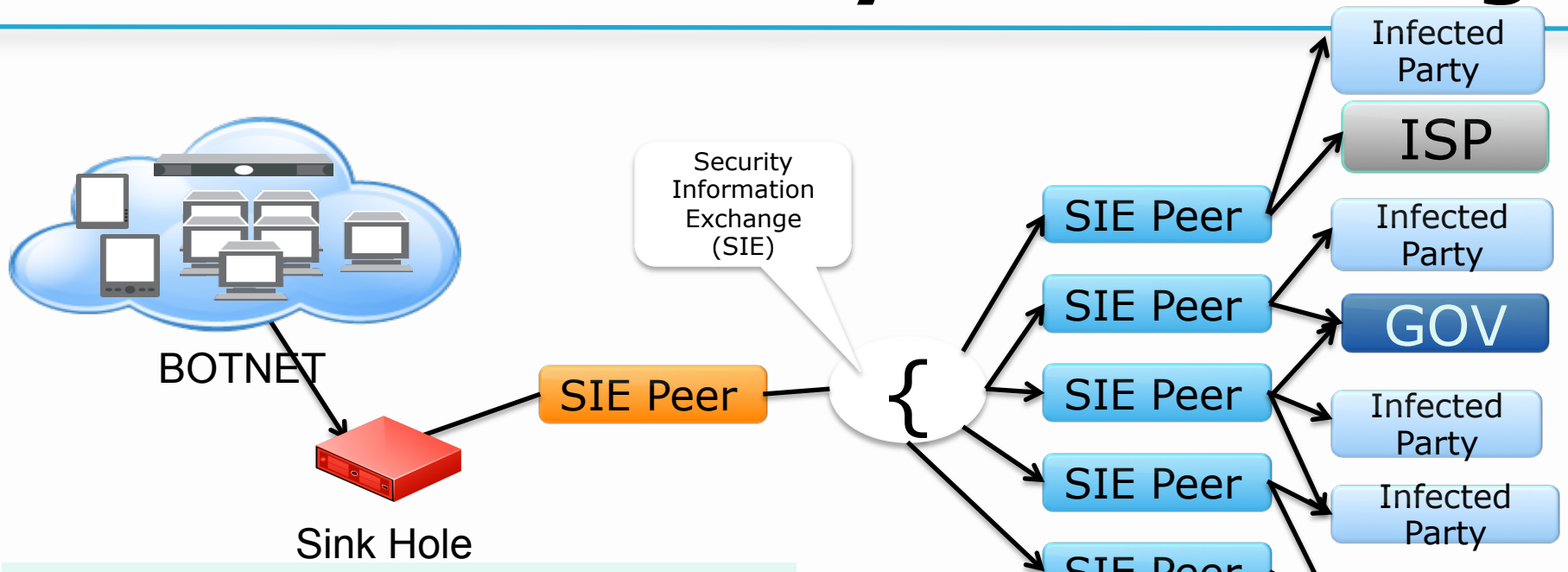
- **Exercise the Court with Criminal and Civil Action. Laws are driven by cases in the court.** We are consistently working on criminal action, but that is one side of the legal system. Civil action is as important as the criminal action. As seen by Microsoft, damages to a company can be used as a bases for civil action that results in impact against the perceived criminal damage.

Cyber Strategy of Action

- **Autonomous System (ASN) Sovereignty, Contract Law, and AUPs can be used to embargo peers who are damaging the business.** Each ASN can choose to whom they communicate. While it is a general principle to maintain global connectivity with every ASN in the world, it is by no means a requirement. Problem ASNs have been temporarily "filtered" for the best interest of the Internet. This filtering is done within each ASN.



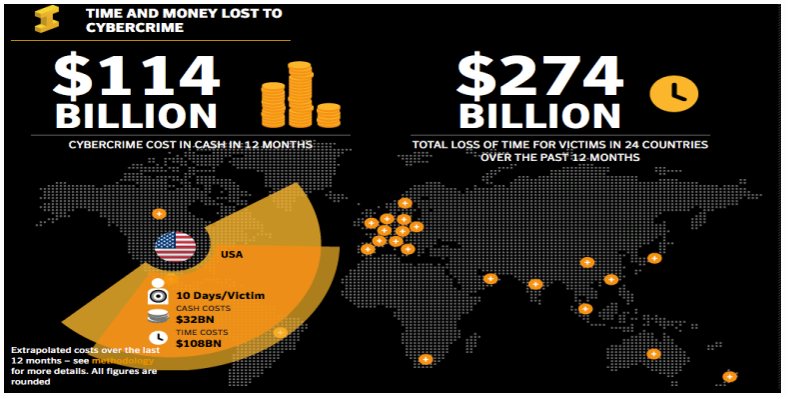
Real Time Security Data Sharing



BOTNETs whose C&C is Sinkholed has their log details sanitized and shared to the private industry through tools like the Security Information Exchange

Cyber Strategy of Action

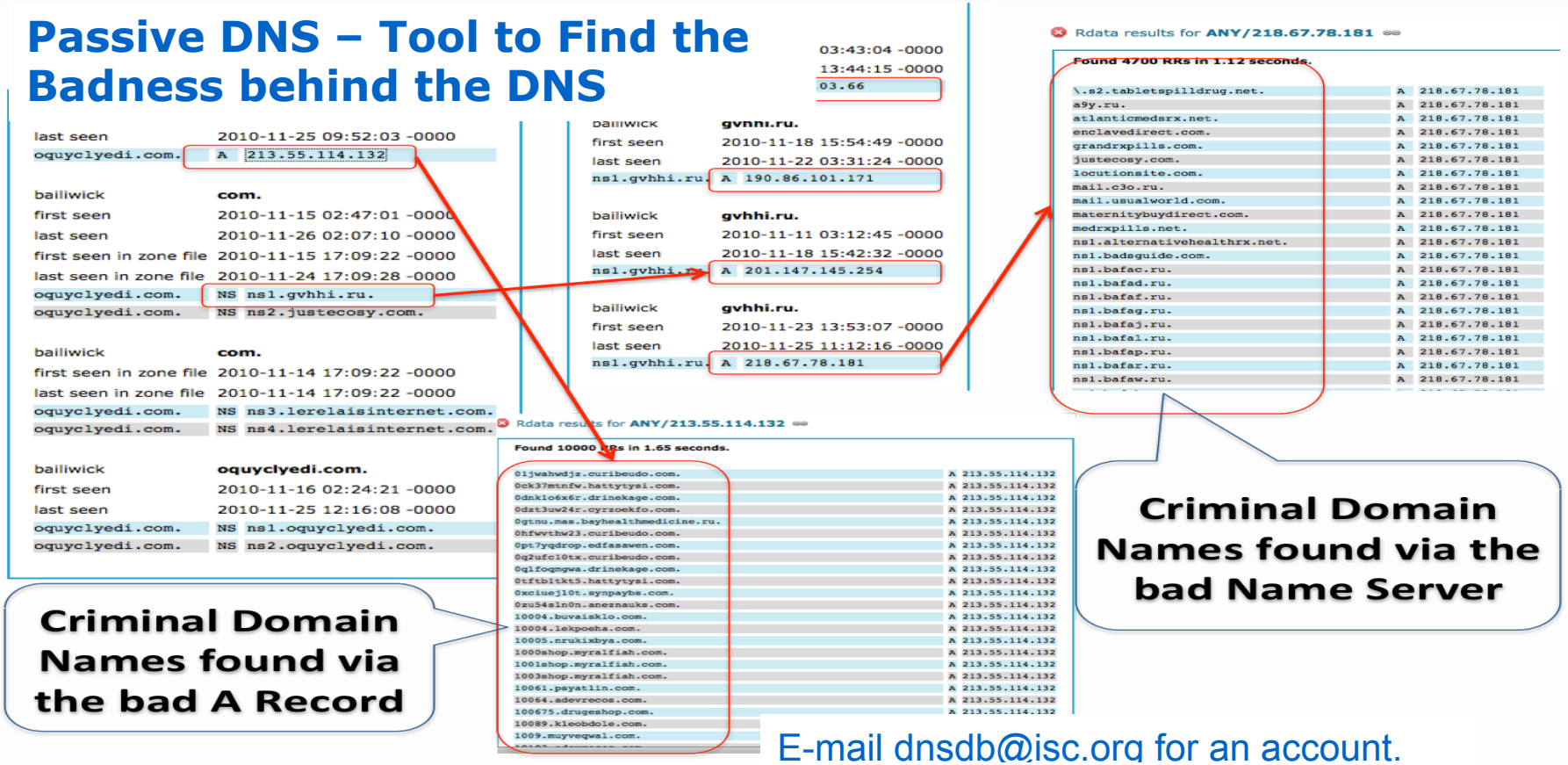
- **Monetizing Cyber-Security Cost and Risk to the Global Economy will happen in 2012.** Symantec's commissioned study takes expectations to a new level (i.e value of risk can be quantified.) More studies are coming along with the consequence of those studies.



See http://norton.com/cybercrimereport.

Take Back the DNS!

Passive DNS – Tool to Find the Badness behind the DNS

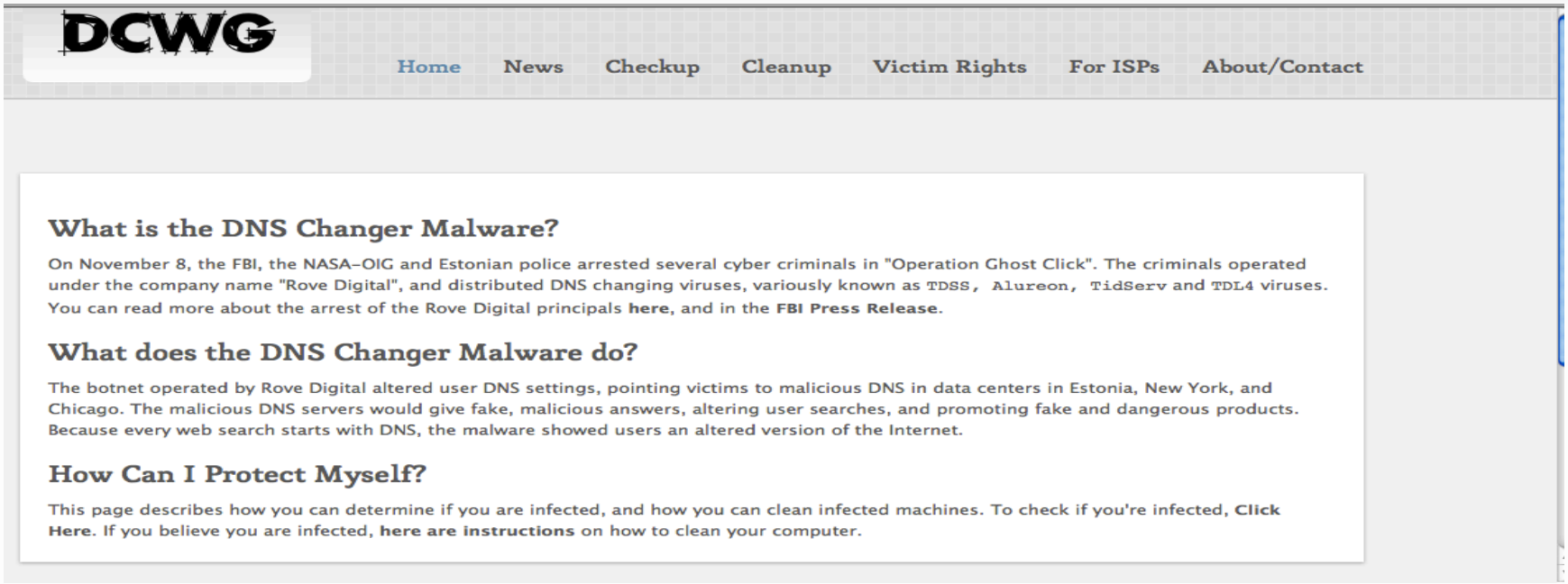


E-mail dnsdb@isc.org for an account.

Summary = Action

- Make 2012 your year of action.
  - **Foster Private-to-Private Collaboration with Public participation.**
  - **Invest in Public – Private Partnership activities like NCFTA**
  - **Action Now is the key to preparing for Cyber-Security Defense**
  - **Reach out and participate in the Operational Security Portals**
  - **Exercise the Court with Criminal and Civil Action.**
  - **Have your service providers each out an empower their *Autonomous System (ASN) Sovereignty*.**
  - **Real Time Security Data Sharing**
  - **Monetizing Cyber-Security Cost and Risk to the Global Economy will happen in 2012.**
  - **Take Back the DNS – Get a DNSDB Account**

Start with an Active Operation



DCWG.ORG

M3AAWG
MESSAGING MALWARE MOBILE

Bot Mitigation for ISPs – Link to Materials

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

This has been the fourth 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 M3AAWG 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 M3AAWG to videotape it for professionals worldwide.

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

For information about M3AAWG:
www.m3aawg.org
www.facebook.com/maawg
www.twitter.com/maawg
www.youtube.com/maawg

Contact us at:
https://www.m3aawg.org/contact_form