

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 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 1 of 6

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

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

Top SP Security Essential Techniques

Segment 1 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).

SP Security Primer 101

Peers working together to battle
Attacks to the Net

Barry Raveendran Greene
bgreene@senki.org

Goals

- Provide core techniques/task that any SP can do to improve their resistance to security issues.
- These core techniques can be done on any core routing vendor's equipment.
- Each of these techniques have proven to make a difference.
- New Drivers: New levels of security capability are being expected from Service Providers.
- Australia's I-code, FCC's CSRIC, expectations from the cyber-civic society and successful take downs are shaping these expectations.

“Never underestimate the power of human communications as a tool to solve security problems. Our history demonstrates that since the Morris Worm, peer communication has been *the* most effect security tool.”

Barry Raveendran Greene

Agenda

- Overview
- Understanding the Threat: *A Typical Cyber-Criminal's Work Day*
- Why Cyber-Crime is Institutionalized?
- A 2012 SP Security Strategy for Action
- Top 10 SP Security Techniques: The Executive Summary
 - Prepare your NOC
 - The New Internet "Civic Society": OPSEC Communities
 - Working with your Peers with "Out of Band" Communications: iNOC DBA
 - Point Protection
 - Edge Protection
 - Remote Trigger Black Hole
 - Sink Holes
 - Source Address Validation
 - Control Plane Protection
 - Total Visibility
- (cont_)

Agenda

- Prepare your NOC
- Operational Security Community
- Putting the Tools to Work – DDOS Attack
- Remote Triggered Black Hole Routing
- Sink Holes
- Remediating Violated Customers
- Summary

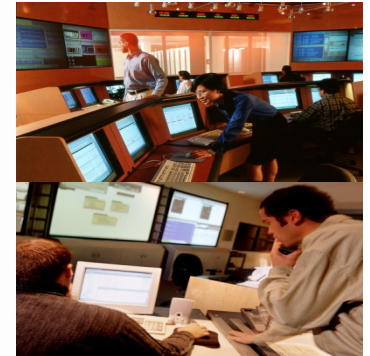
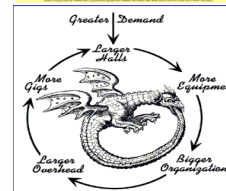
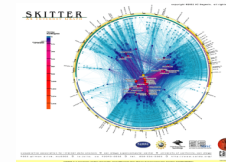
Expectations

- Today's tutorial is about the fundamentals for which new solutions and technique can be built.
- Everything cannot be covered today (more than a week's worth of materials).
- We cannot go in-depth on everything.

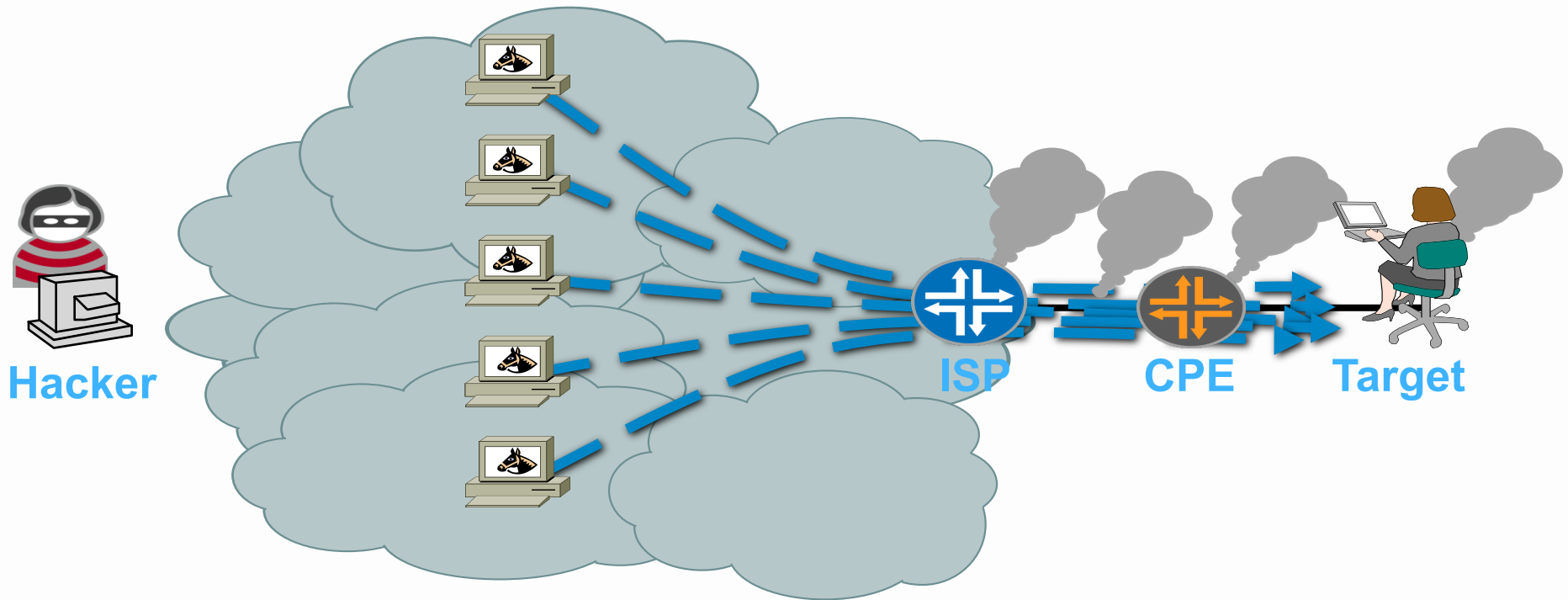
Invitation to Participate

- The current materials are based on the contributions of many people from the industry. Cisco, Juniper, Arbor Networks, and many of the largest SPs in the industry have all been generous to add to the volume of materials.
- The materials require refreshing.
- ***Invitation: If you are really interested in the security and resiliency of your network, please join the community who are working to craft and deploy the foundation techniques while creating new techniques that will security the network.***
 - E-mail: bgreene@senki.org

Overview



What Do You Tell the Boss?



The SP's Watershed - Feb 2000

The screenshot shows the CNN.com website interface. At the top left is the CNN.com logo. A navigation menu on the left lists categories: MAIN PAGE, WORLD, U.S., LOCAL, POLITICS, WEATHER, BUSINESS, SPORTS, TECHNOLOGY, computing, personal technology, SPACE, HEALTH, ENTERTAINMENT, BOOKS, TRAVEL, FOOD, ARTS & STYLE, NATURE, IN-DEPTH, ANALYSIS, and mvCNN. Below this is a 'Headline News brief' section. The main content area shows a breadcrumb trail: sci-tech > computing > story page. The article title is "'Immense' network assault takes down Yahoo". Below the title is a sub-header: "From... COMPUTERWORLD AN IDG.net SITE". The article is part of a series titled "INSURGENCY on the internet" with an "in-depth reports" link. The main headline is "Cyber-attacks batter Web heavyweights" with a sub-headline "Strikes on eBay, Amazon, CNN.com follow Monday Yahoo! attack". The date is February 9, 2000, and the article was posted at 9:56 a.m. EST (1456 GMT). A small image shows a computer keyboard with a glowing cursor. The bottom of the page says "In this story:".



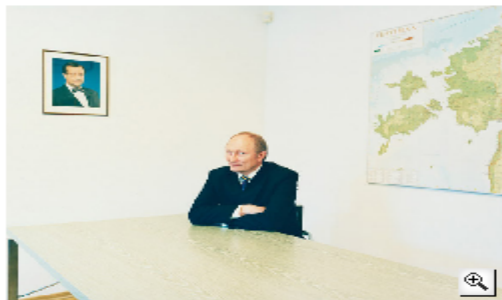
The Vetted – Battling the Bad Guys

WIRED MAGAZINE: ISSUE 15.09

POLITICS : SECURITY [RSS](#)

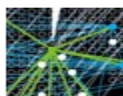
Hackers Take Down the Most Wired Country in Europe

By Joshua Davis [✉](#) 08.21.07 | 2:00 AM



Defense minister Jaak Aaviksoo got help from NATO in the wake of the cyberattacks. Photo: Donald Milne

FEATURE



[When Bots Attack](#)



[Washington Ignores](#)

The minister of defense checked the Web page again — still nothing. He stared at the error message: For some reason, the site for Estonia's leading newspaper, the Postimees, wasn't responding. Jaak Aaviksoo attempted to pull up the sites of a couple of other papers. They were all down. The former director of the University of Tartu Institute of Experimental Physics and Technology had been the Estonian defense minister for only four weeks. He hadn't even changed the art on the walls.

An aide rushed in with a report. It wasn't just the newspapers. The leading bank was under siege. Government communications were going down. An enemy had invaded and was assaulting dozens of targets.

Outside, everything was quiet. The border guards had reported no incursions, and Estonian airspace had not been violated. The aide explained what was going on: They were under attack by a rogue computer network.

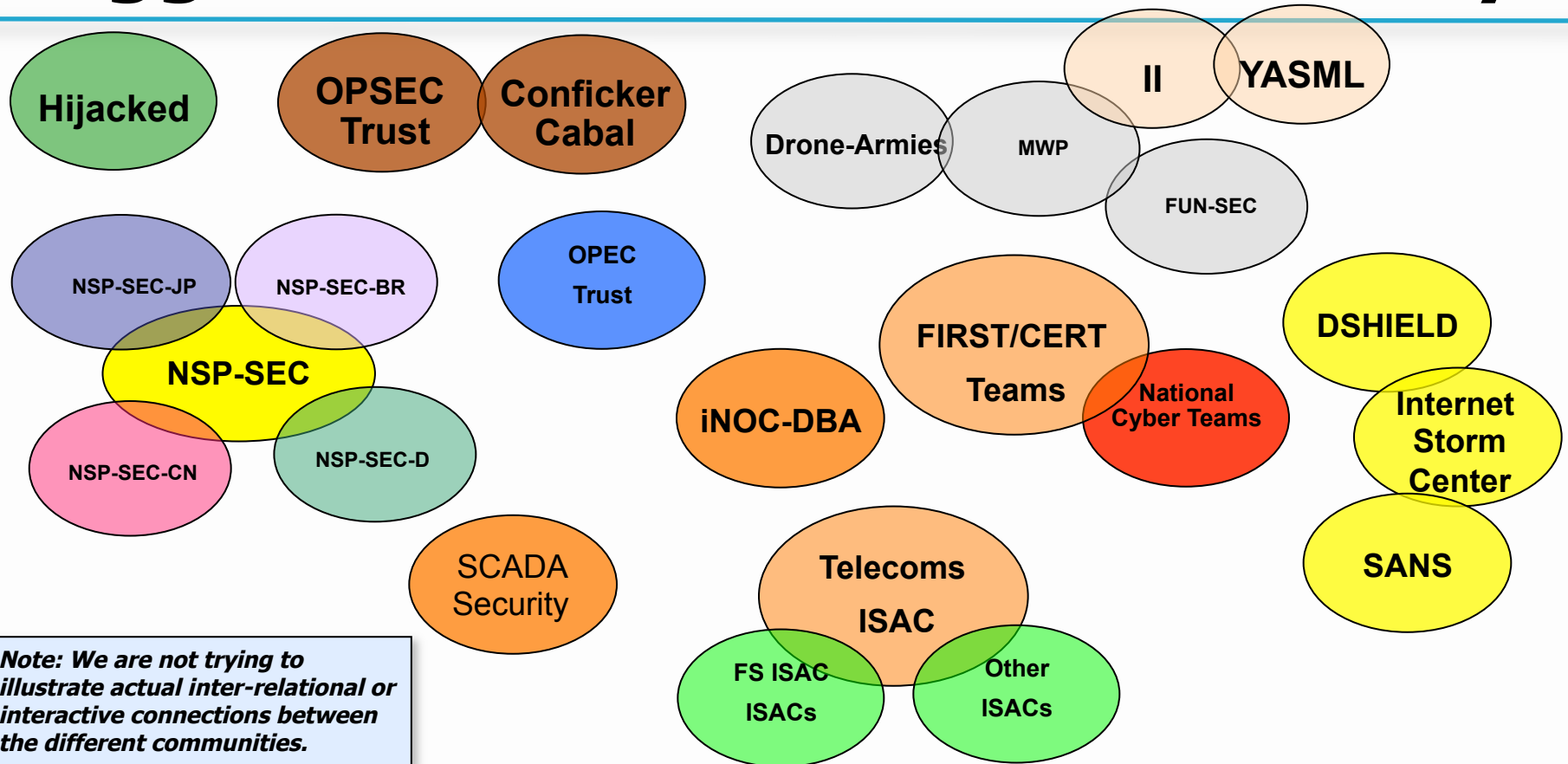
It is known as a botnet, and it had slipped into the country through its least protected border — the Internet

When BOTs Attack – Inter AS



http://www.wired.com/politics/security/magazine/15-09/ff_estonia_bots

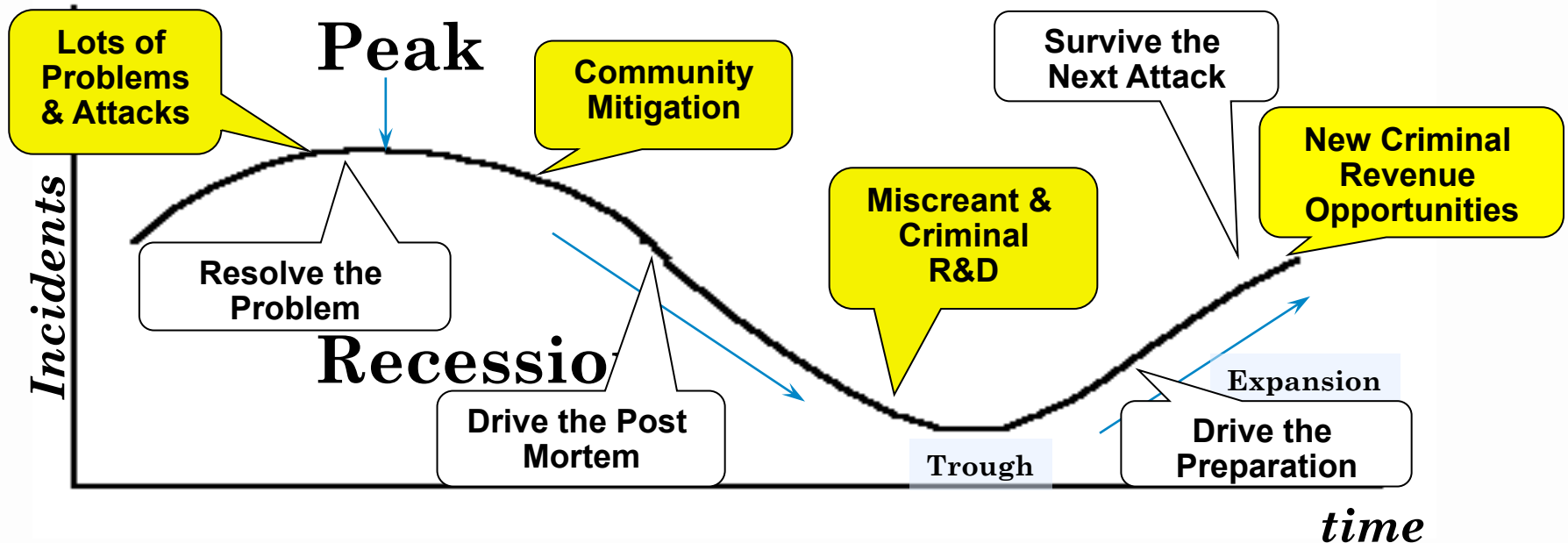
Aggressive Collaboration is the Key



What is NSP-SEC

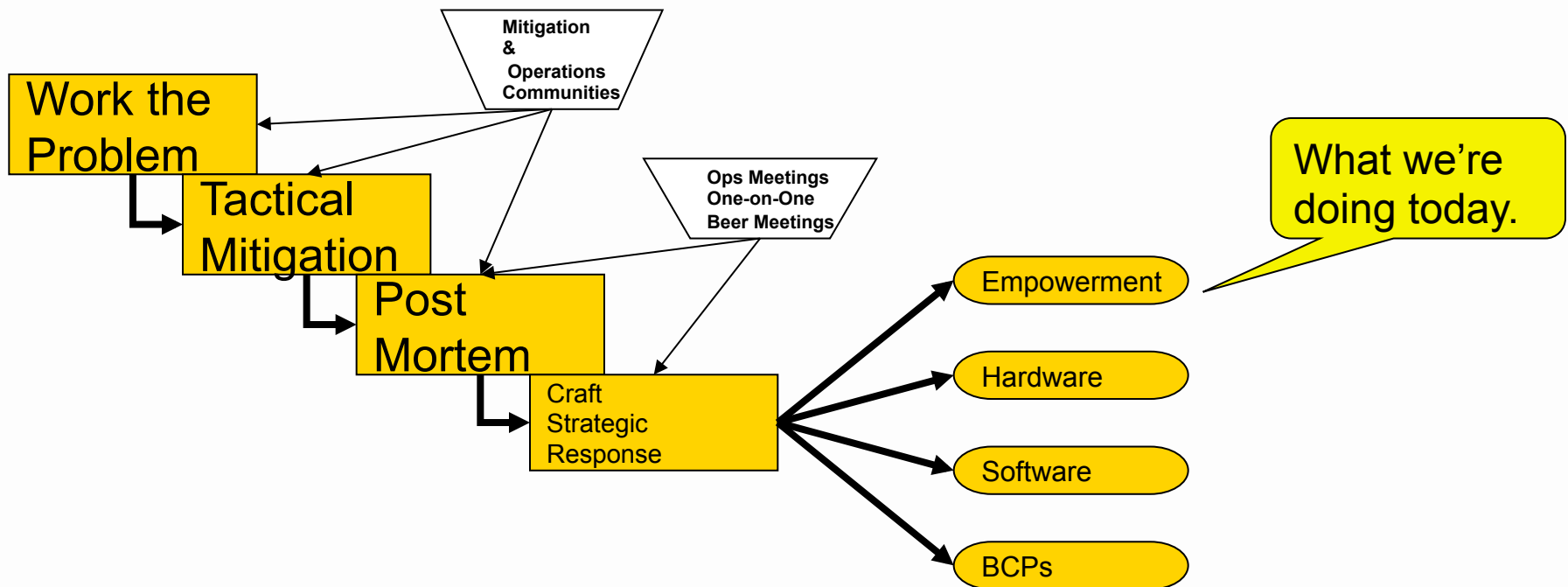
- NSP-SEC – *Closed* Security Operations
Alias for engineers actively working with NSPs/ISPs to mitigate security incidents.
- Multiple Layers of sanity checking the applicability and trust levels of individuals.
- Not meant to be perfect – just better than what we had before.
- <http://puck.nether.net/mailman/listinfo/nsp-security>

Miscreant - Incident Economic Cycles



These Cycles Repeat

Where is This Coming From?



Working the 40/40/20 Rule

- Sean Donelan's (back in his SBC days) [sean@donelan.com] rule for end point patching:
 - 40% of the customers care and will proactively patch
 - 40% of the customers may someday care and fix/patch/delouse their machines
 - 20% of the customers just do not care and have never responded to any effort to fix them.

Top Ten List of SP Security Fundamentals

1. Prepare your NOC
2. Mitigation Communities
3. iNOC-DBA Hotline
4. Point Protection on Every Device
5. Edge Protection
6. Remote triggered black hole filtering
7. Sink holes
8. Source address validation on all customer traffic
9. Control Plane Protection
10. Total Visibility (Data Harvesting – Data Mining)
11. Remediating Victimized Customers

The Fundamentals are Building Blocks for ...

- Clean Pipes – DDOS Mitigation Services
- Malware Remediation Services

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

Sun Tzu - Art of War



This has been the first 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

© slide PDF files and video copyrighted by the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)

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 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 2 of 6

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

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

Types of Malware Problems ISPs Encounter

Segment 2 of 6

Barry Raveendran Greene, bgreene@senki.org

October 22, 2012, Baltimore, Maryland, USA



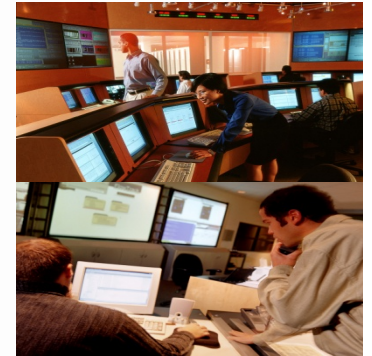
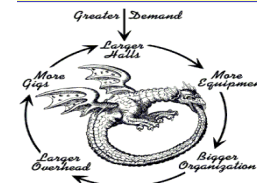
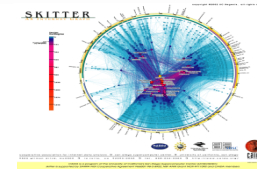


Barry Greene has over 30 years industry experience including having served as president of the ISC (Internet Systems Consortium). He is a pioneer in service provider security and operational security reaction teams.

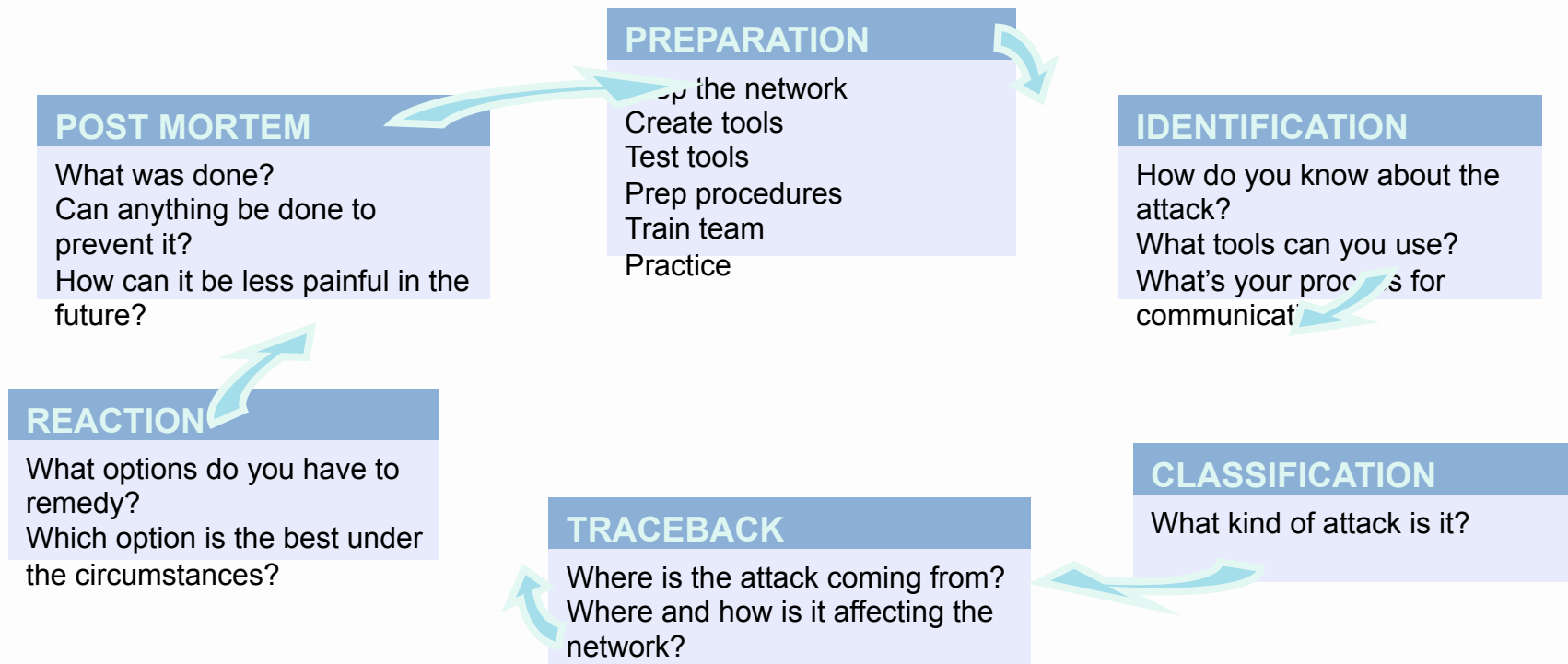
Barry is currently a participant on the U.S. Federal Communications Commission's (FCC's) Communications Security, Reliability and Interoperability Council (CSRIC).

Top SP Security Essential Techniques

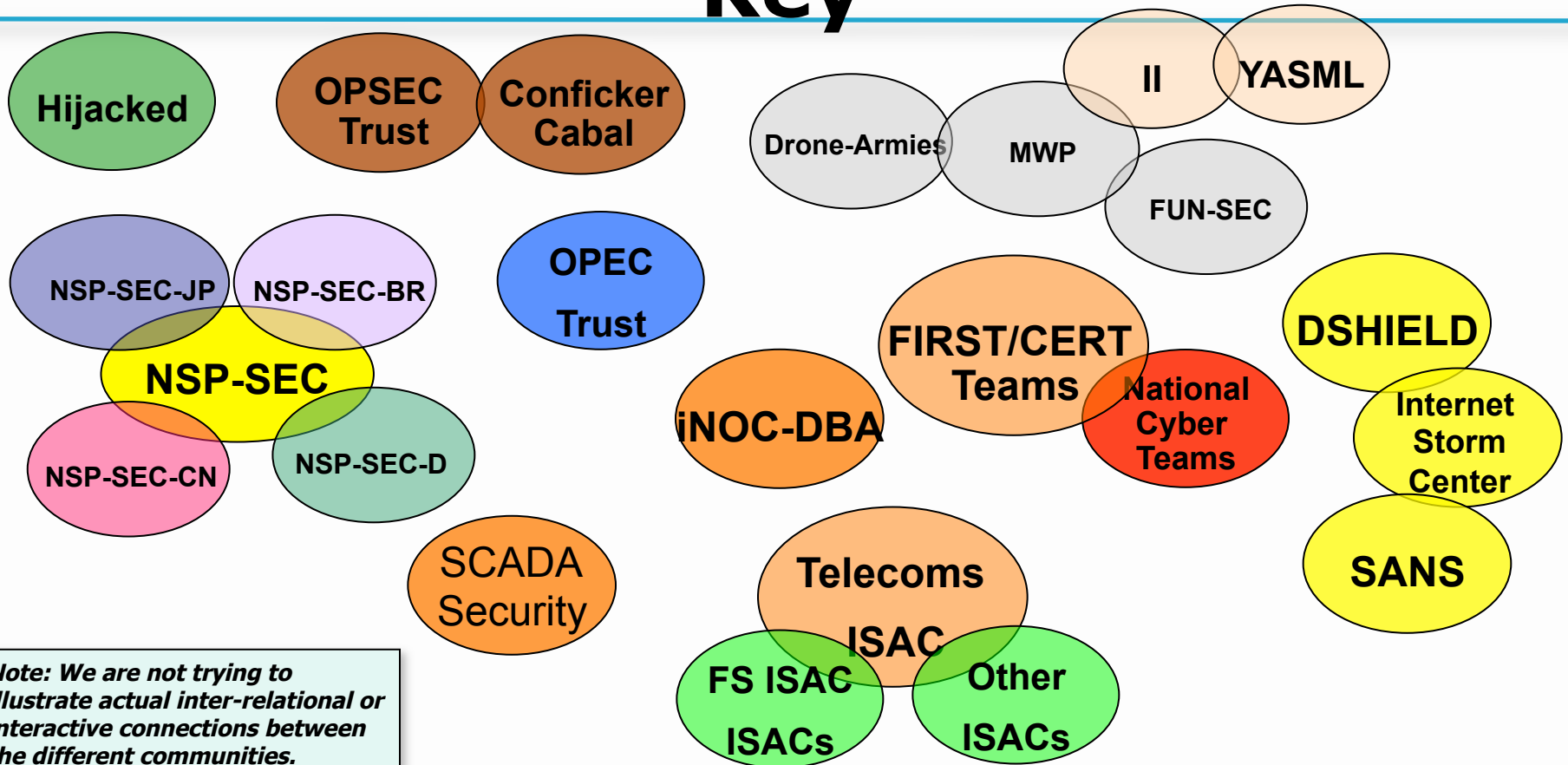
The Executive Summary



SP Security in the NOC - Prepare



Aggressive Collaboration is the Key



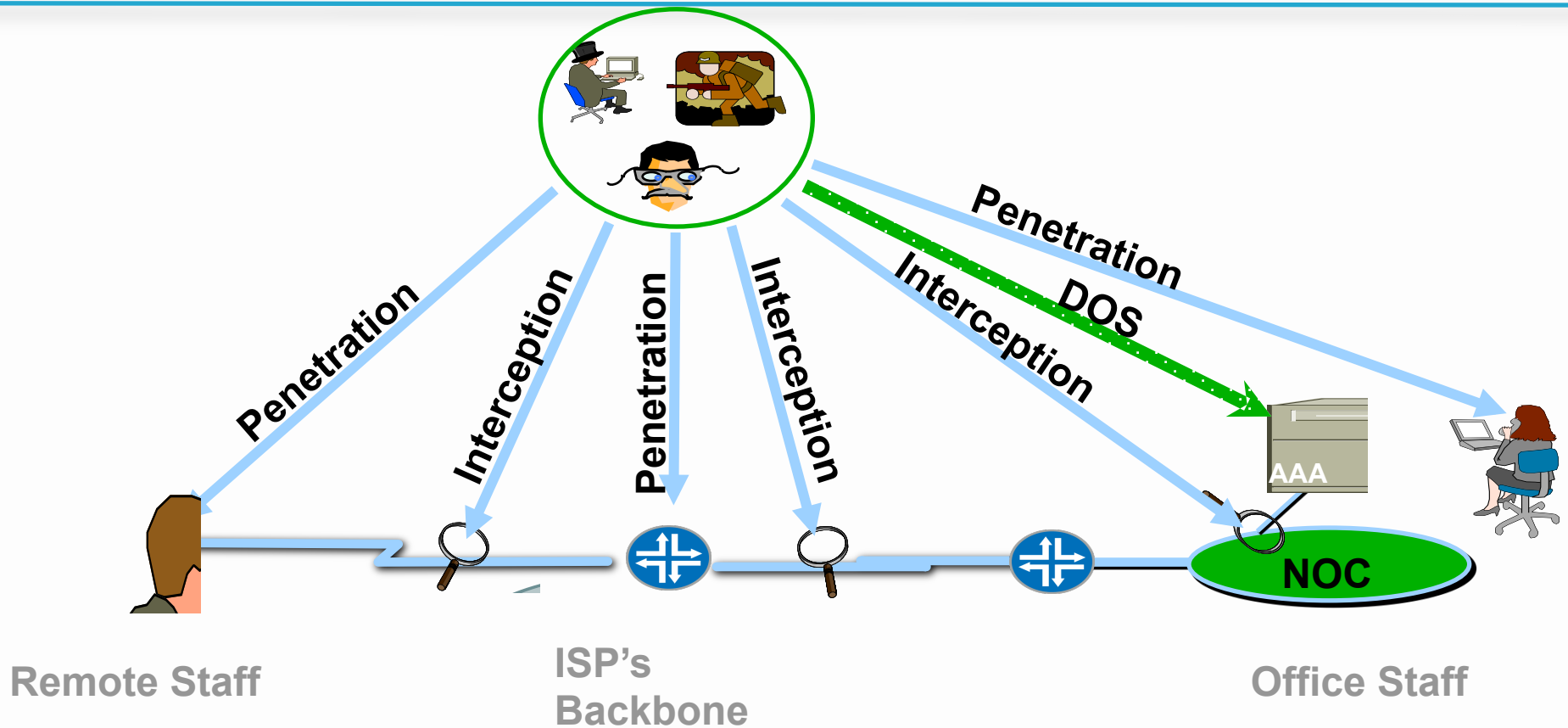
Note: We are not trying to illustrate actual inter-relational or interactive connections between the different communities.

iNOC DBA Hotline

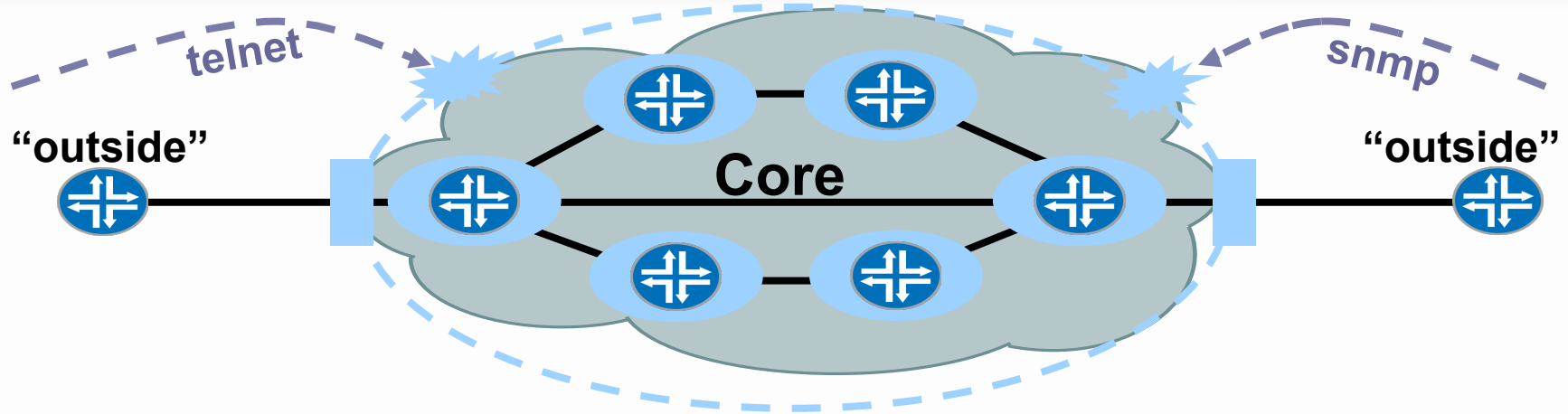


- INOC-DBA: *Inter-NOC Dial-By-ASN*
- The iNOC Hotline was used to get directly to their peers.
- Numbering system based on the Internet:
 - ASnumber:phone
 - 109:100 is Barry's house.
- SIP Based VoIP system, managed by www.pch.net

Point Protection

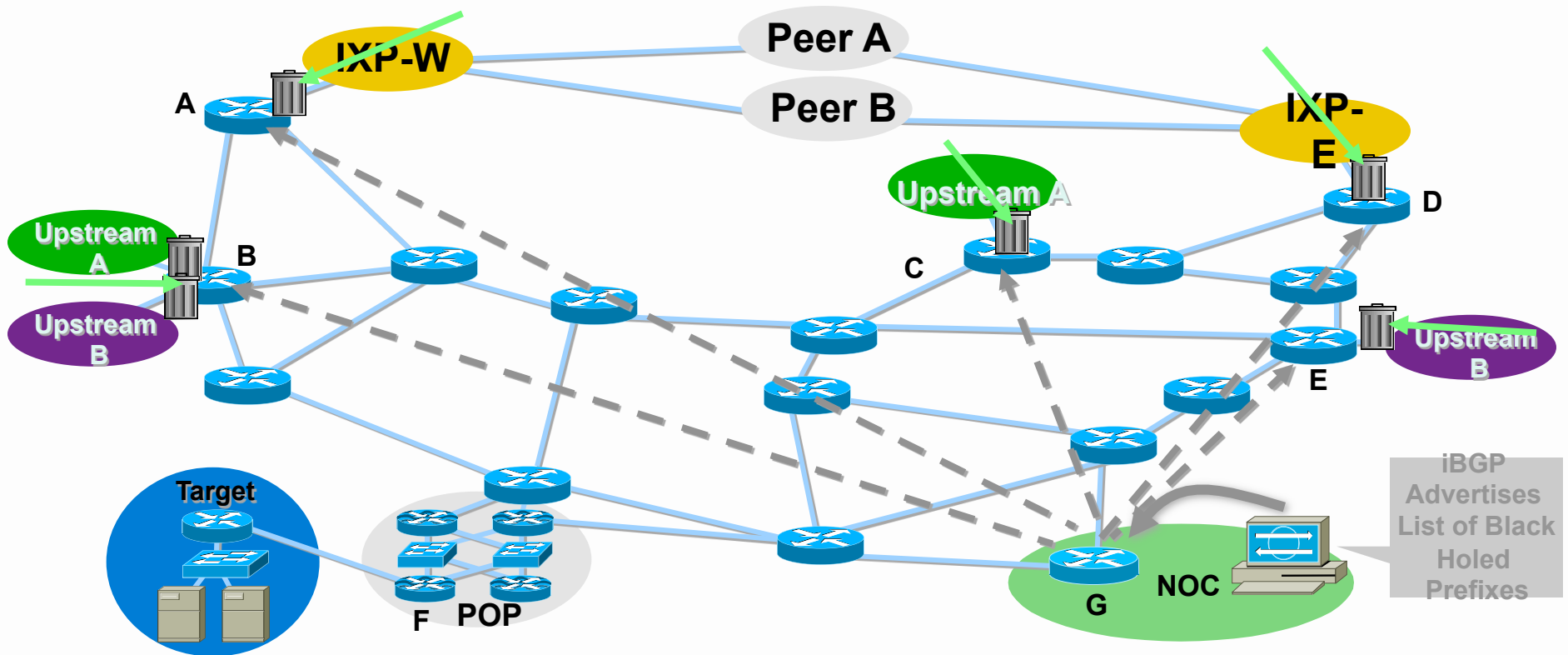


Edge Protection

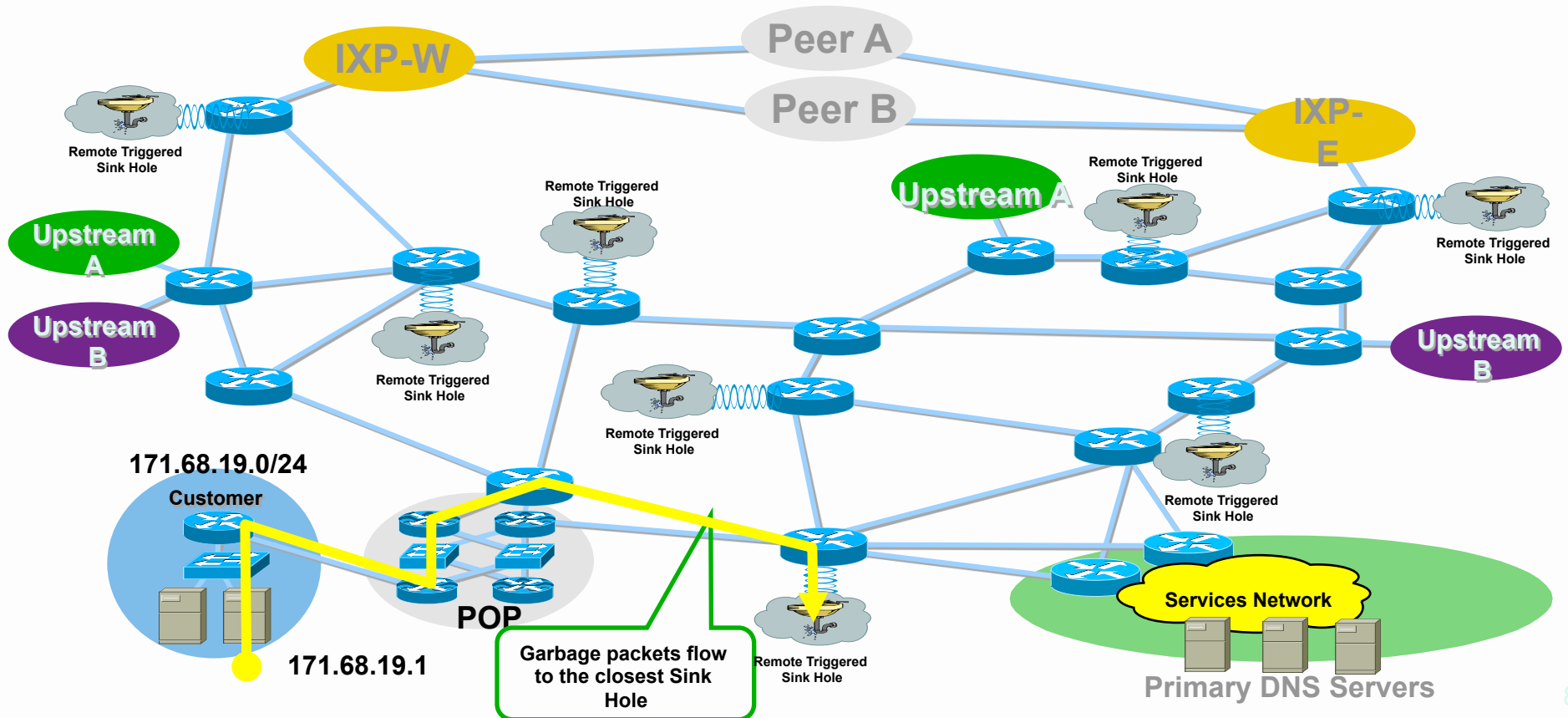


- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside

Destination Based RTBH



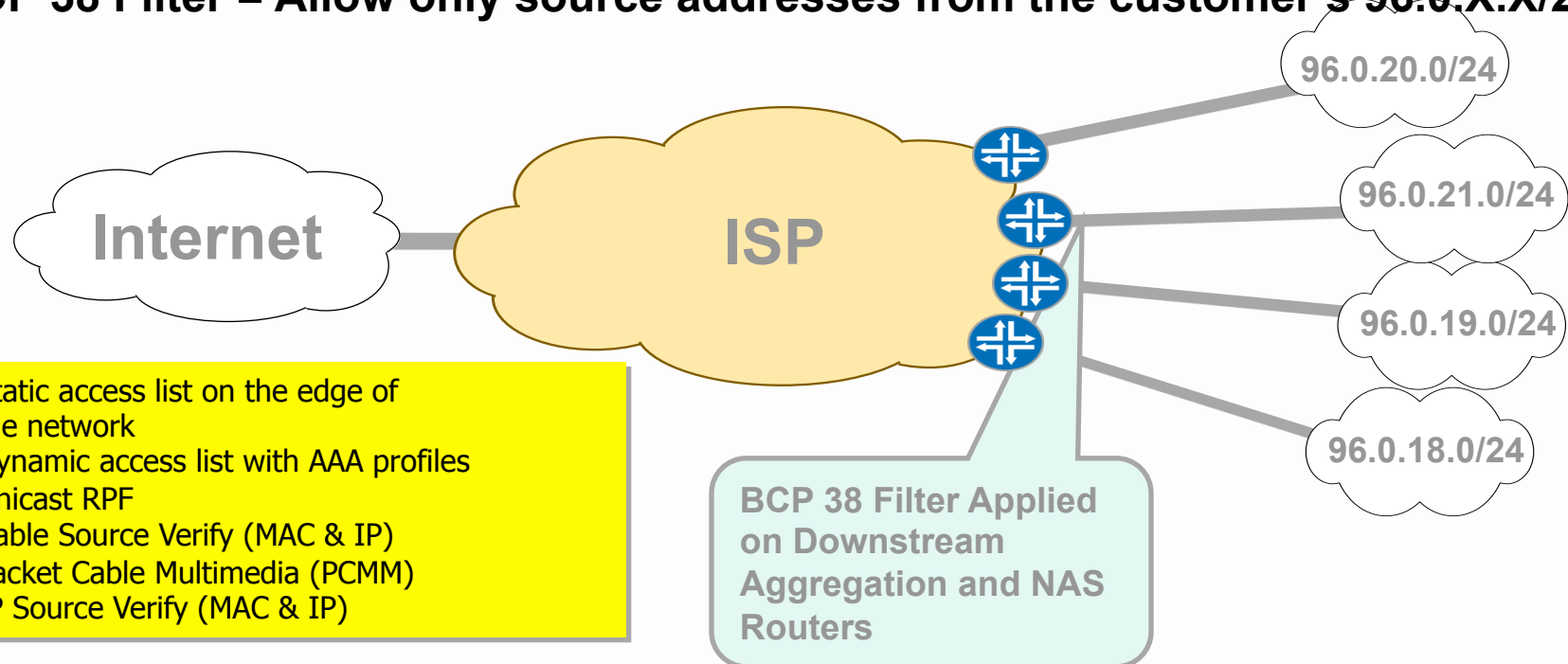
Sink Holes



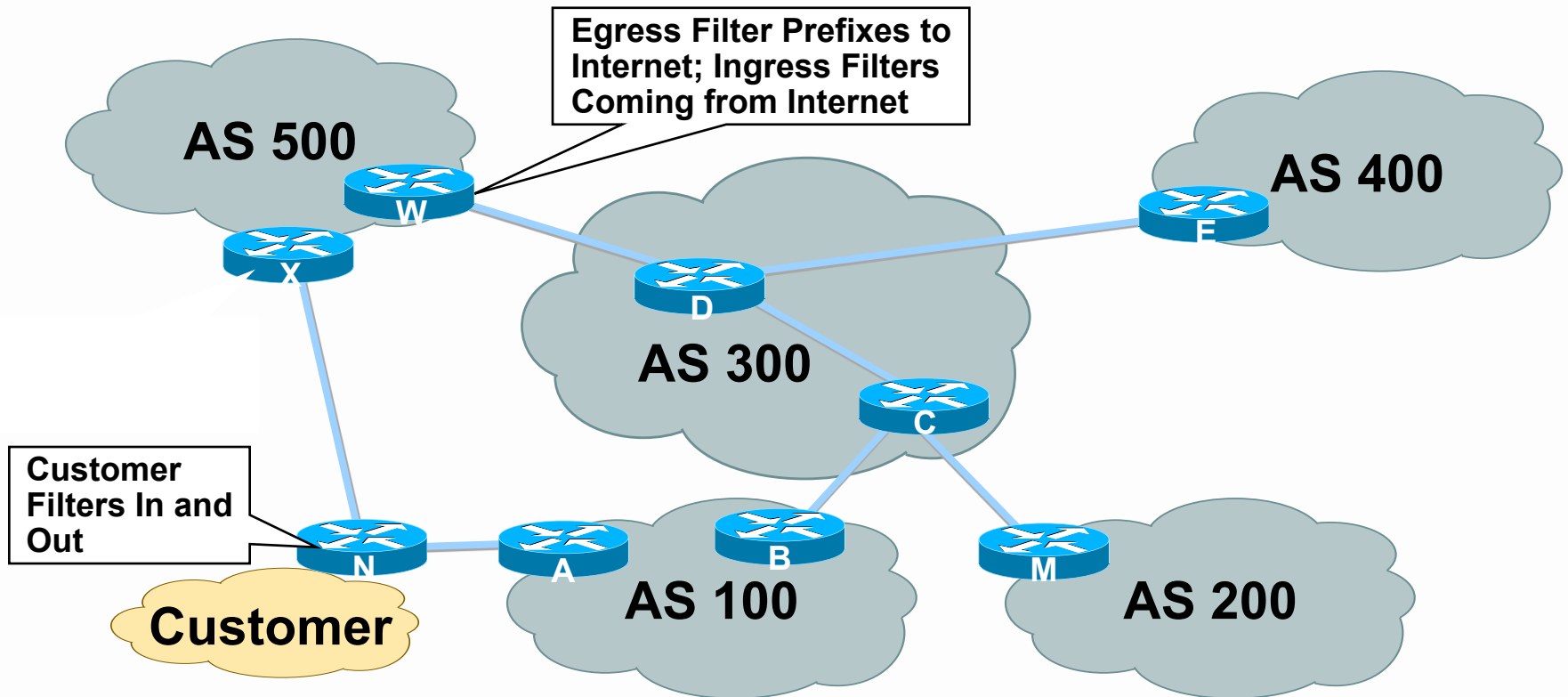
BCP 38 Ingress Packet Filtering

ISP's Customer Allocation Block: 96.0.0.0/19

BCP 38 Filter = Allow only source addresses from the customer's 96.0.X.X/24

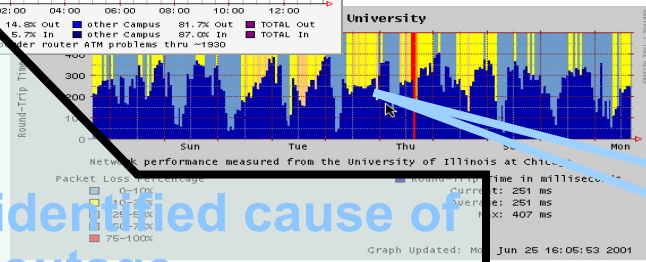
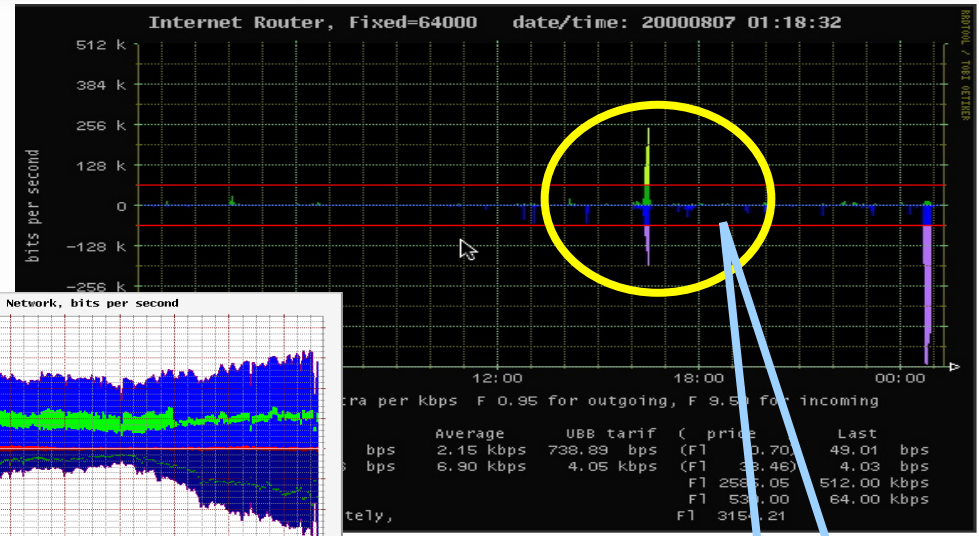
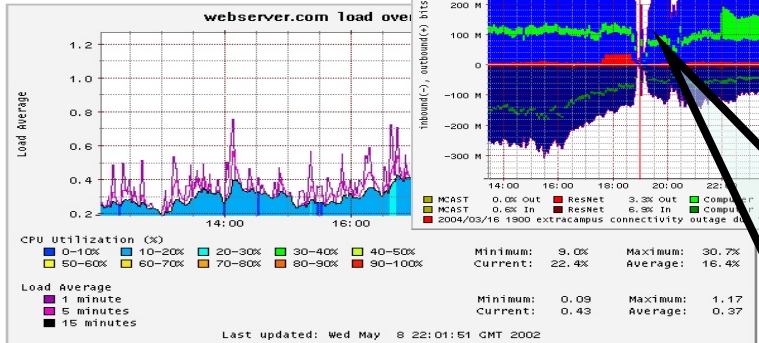
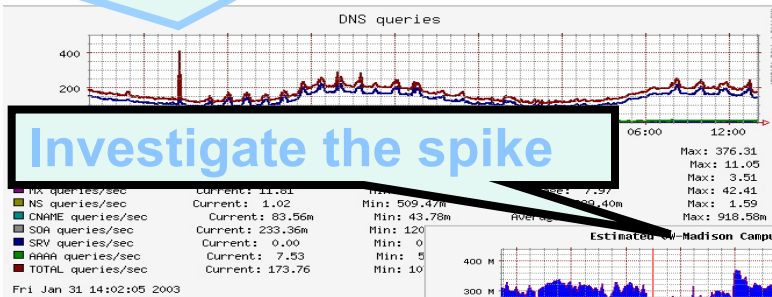


BGP Prefix Filtering



Total Visibility

Anomaly for DNS Queries

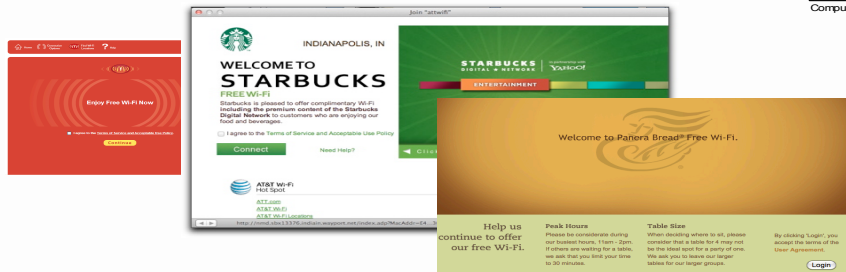
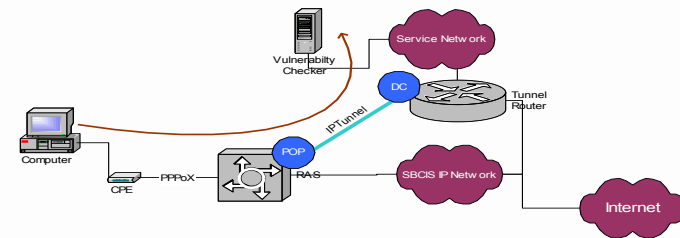
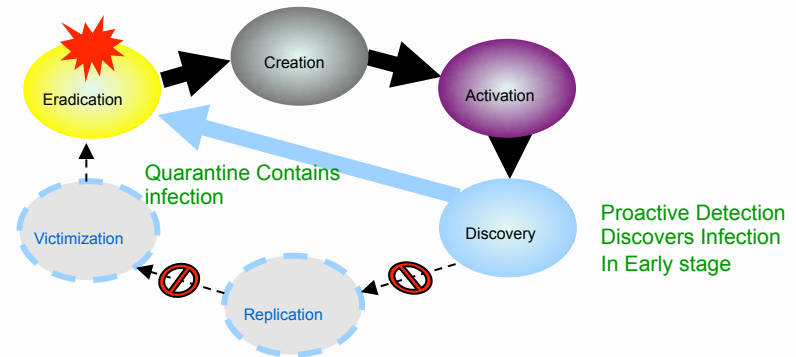


An identified cause of the outage

Source: <http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>

Remediating Violated Customers

- We have enough experience in the industry to move remediation of violated customers to a normal part of the business.
- Leaving violated customers on your network puts your whole operation at risk.



Bot Mitigation for ISPs – Link to Materials

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



This has been the second 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

© slide PDF files and video copyrighted by the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)



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](https://www.m3aawg.org/contact_form)



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

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 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 3 of 6

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

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

Understanding the Threat:

A Cyber-Criminal's Work Day & Cyber-Criminal Behavior Drivers

Segment 3 of 6

Barry Raveendran Greene, bgreene@senki.org

October 22, 2012, Baltimore, Maryland, USA



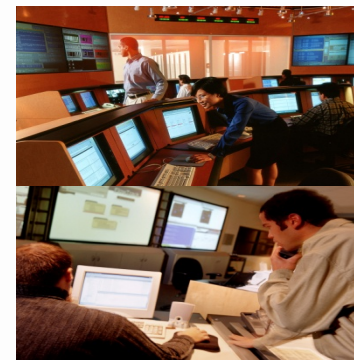
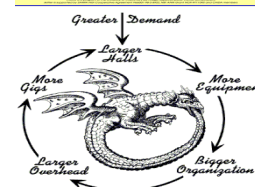
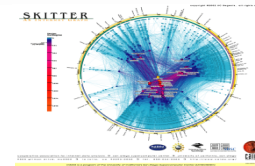


Barry Greene has over 30 years industry experience including having served as president of the ISC (Internet Systems Consortium). He is a pioneer in service provider security and operational security reaction teams.

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

Understanding the Threat

A Typical Cyber-Criminal's Work Day



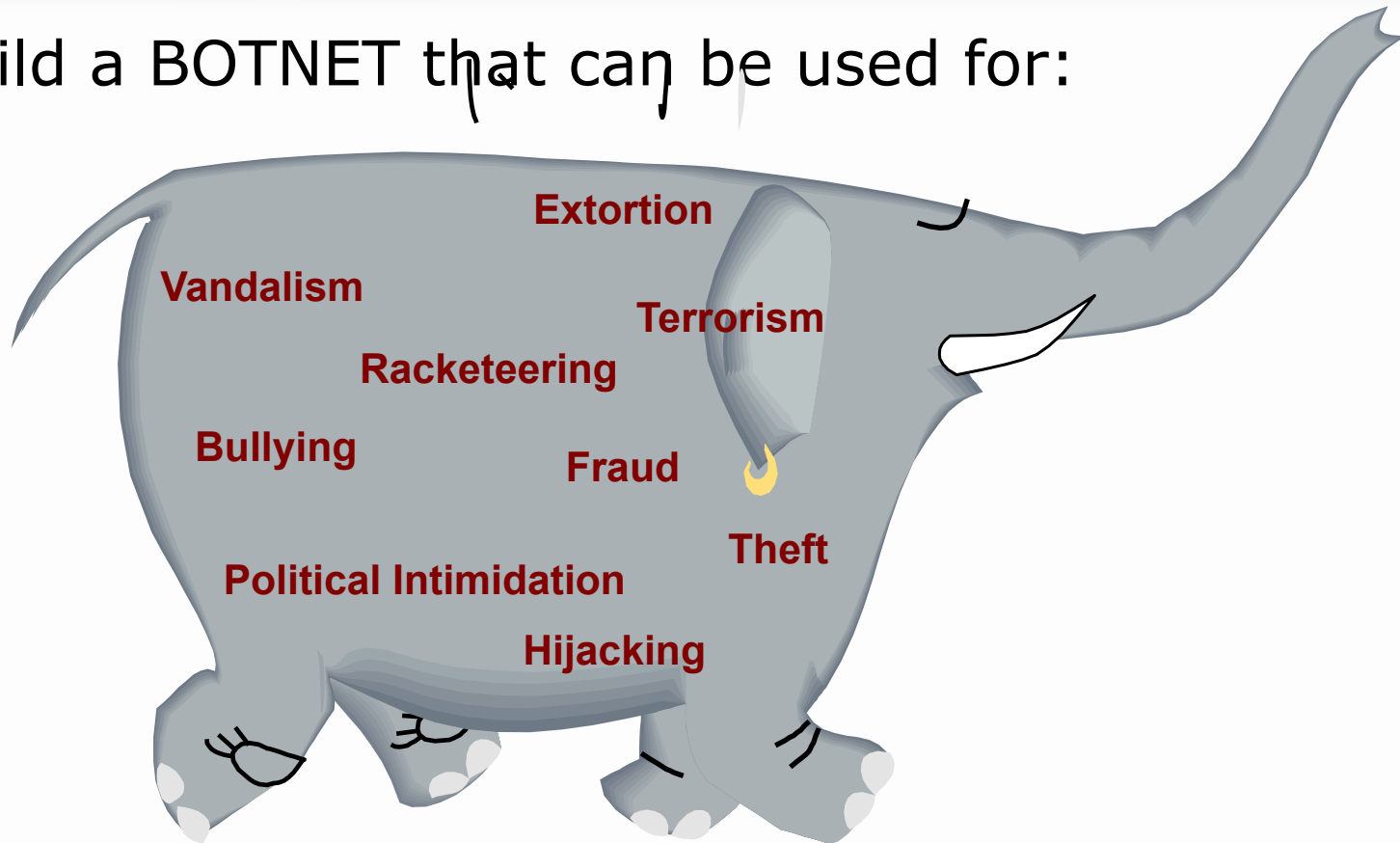
Agenda

- Today's Cybercriminal Toolkit – The Criminal Cloud ... what how IPv6 will Enhance that "Cloud"
- Understanding Today's Cyber-Criminal Behavior Drivers
- Now What? What do I need to do to deploy IPv6?

Cyber Criminal Toolkit
that is the foundation
for the *Criminal Cloud*

Cyber Criminal's Goal

- Build a BOTNET that can be used for:



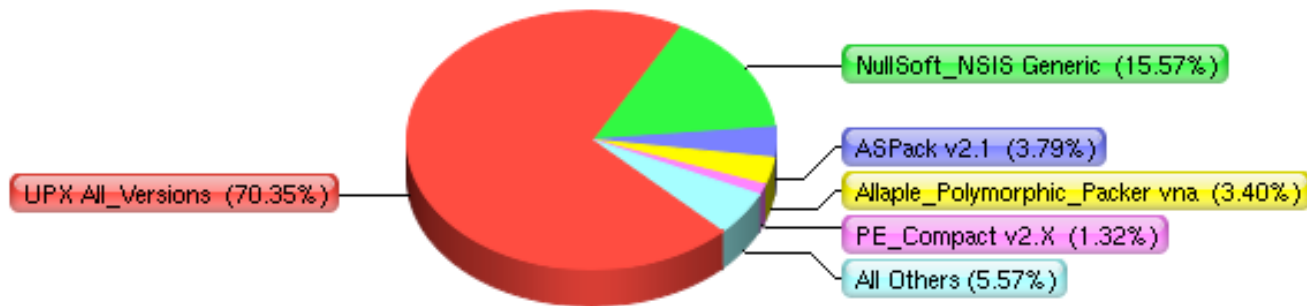
But What About Anti Virus?

- Packing Tools allow the Cyber-Criminal to change the signature of the malware every hour on the hour
- This bypasses the anti-virus software

AV Engine	Country	Signature
Ahnlab	KR	no_virus
Aladdin (esafe)	IL	no_virus
Alwil (avast)	CZ	no_virus
Authentium	US	no_virus
Avira (antivir)	DE	HEUR/Crypted
BitDefender	RO	no_virus
CA (E-Trust Ino)	US	no_virus
CA (E-Trust Vet)	US	no_virus
CAT (quickheal)	IN	no_virus
ClamAV		Trojan.Crypted-4
Dr. Web	RU	no_virus
Eset (nod32)	US	no_virus
Ewido	DE	no_virus
Fortinet	US	no_virus
Frisk (f-prot)	IS	no_virus
Frisk (f-prot4)	IS	no_virus
F-Secure	FI	Hupigon.gen130
Grisoft (avg)	CZ	no_virus
Ikarus	AT	Backdoor.VB.EV
Kaspersky	RU	no_virus
Mcafee	US	no_virus
Microsoft	US	no_virus
Norman	NO	Hupigon.gen130
Panda	ES	no_virus
Prevx	GB	no_virus
Securecomputing	US	Heuristic.Crypted
Sophos	GB	no_virus
Sunbelt	US	VIPRE.Suspicious
Symantec	US	no_virus
The Hacker	DE	no_virus

What Packers Are Used?

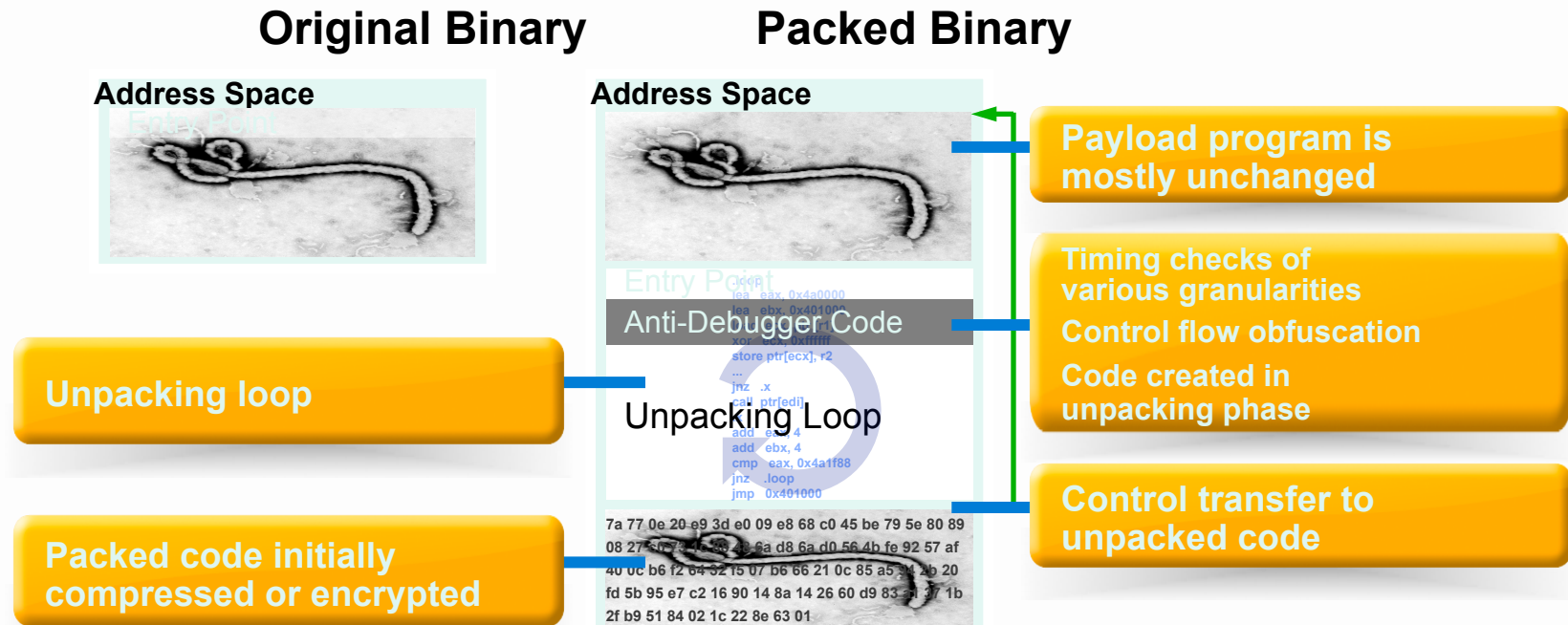
Packer Yearly



<http://www.shadowserver.org/wiki/pmwiki.php/Stats/PackerStatistics>

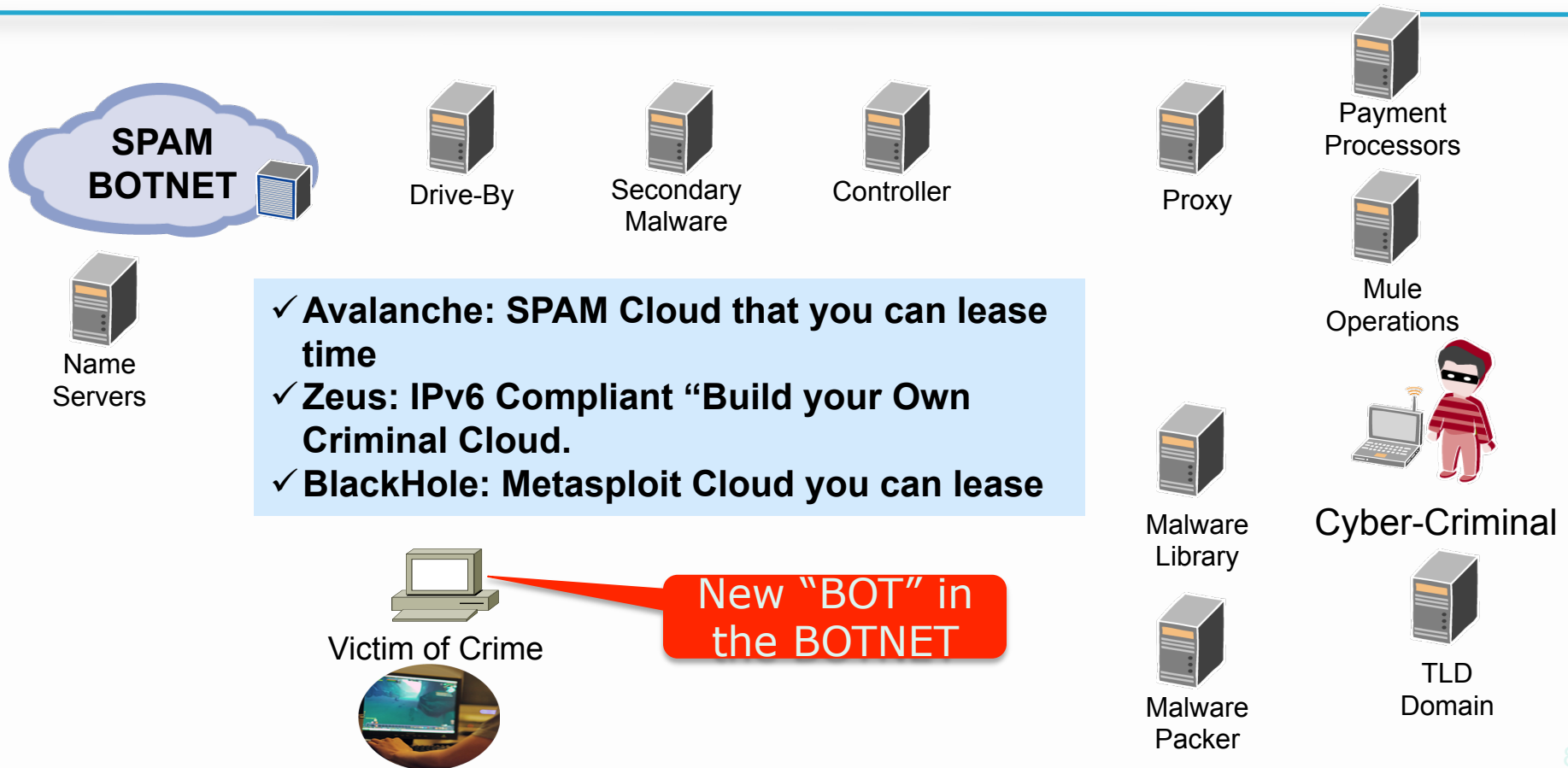
A Packed Malware Binary

A binary is *packed* if some portion of its code is not present until runtime

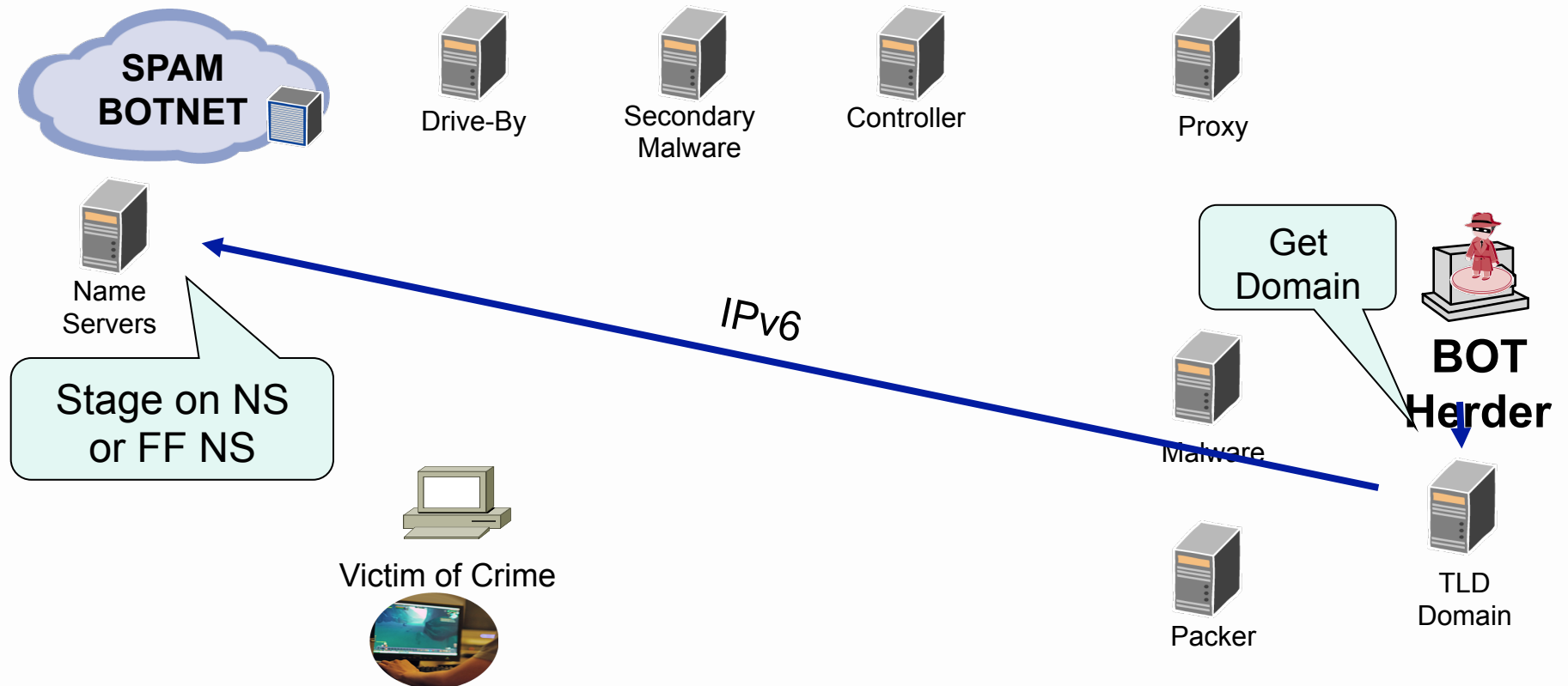


Courtesy of Kevin Roundy (Paradyn Project)

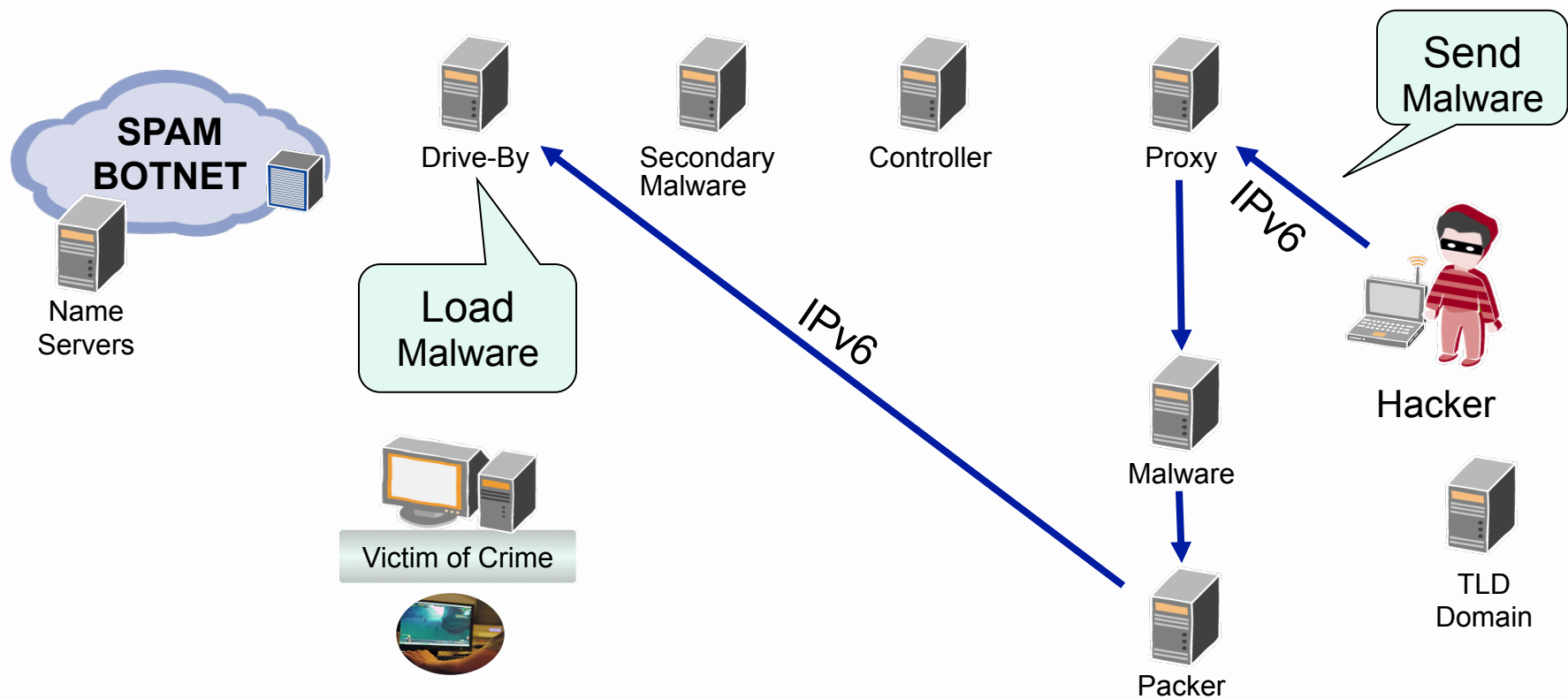
Components of the Criminal Cloud



Stage Domain Name



Prepare Drive-By

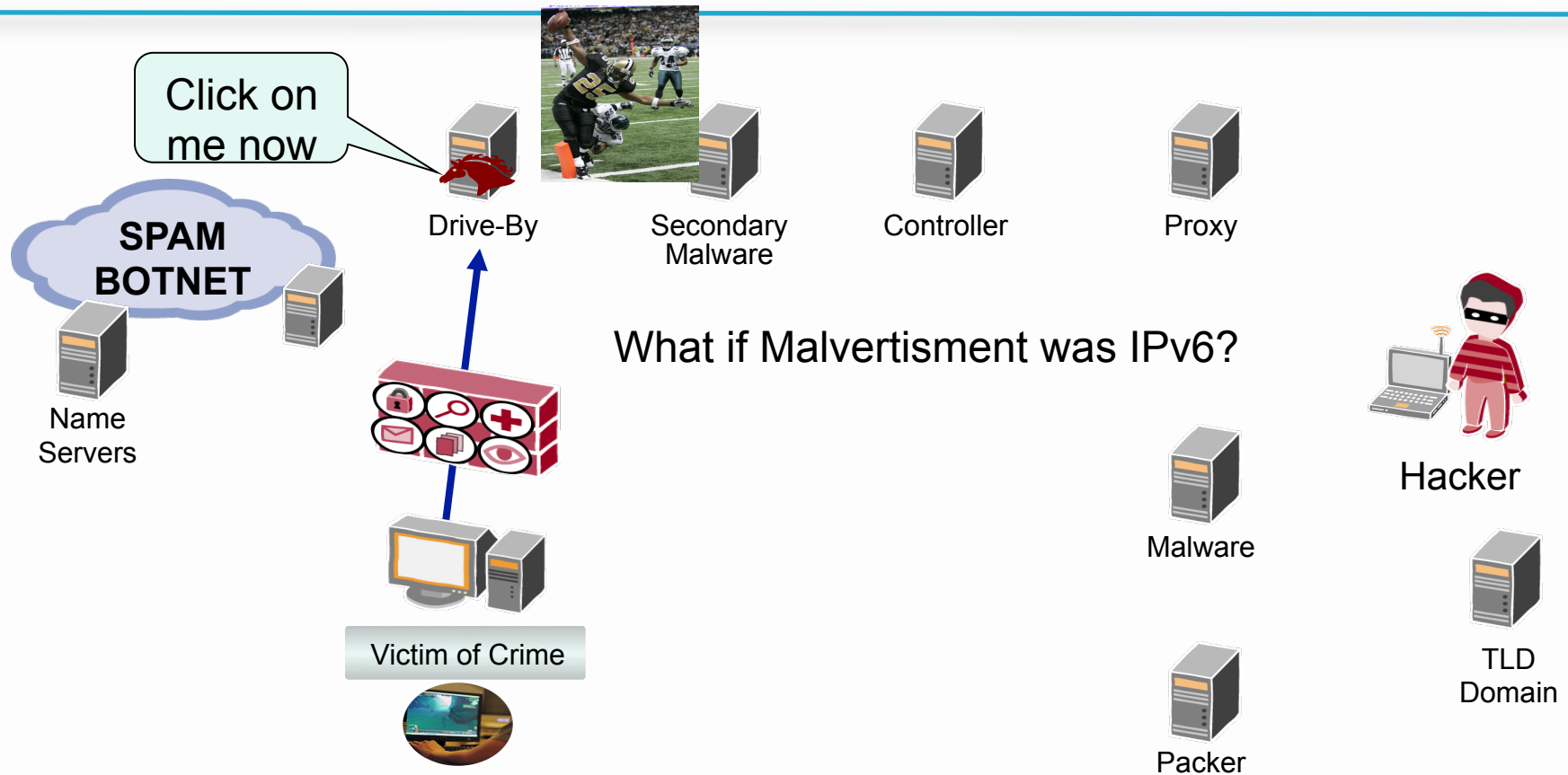


Social Engineered SPAM to Get People to Click

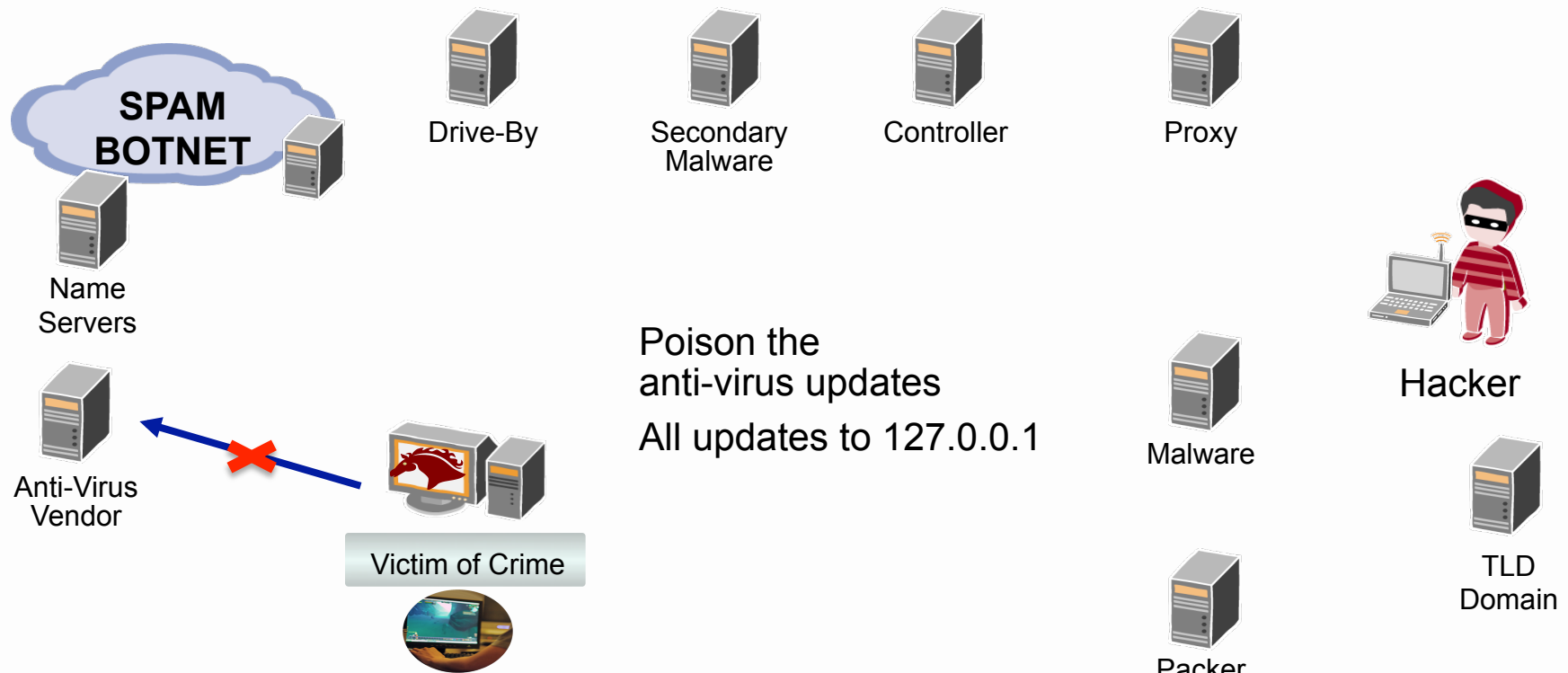
(Spear Phishing)



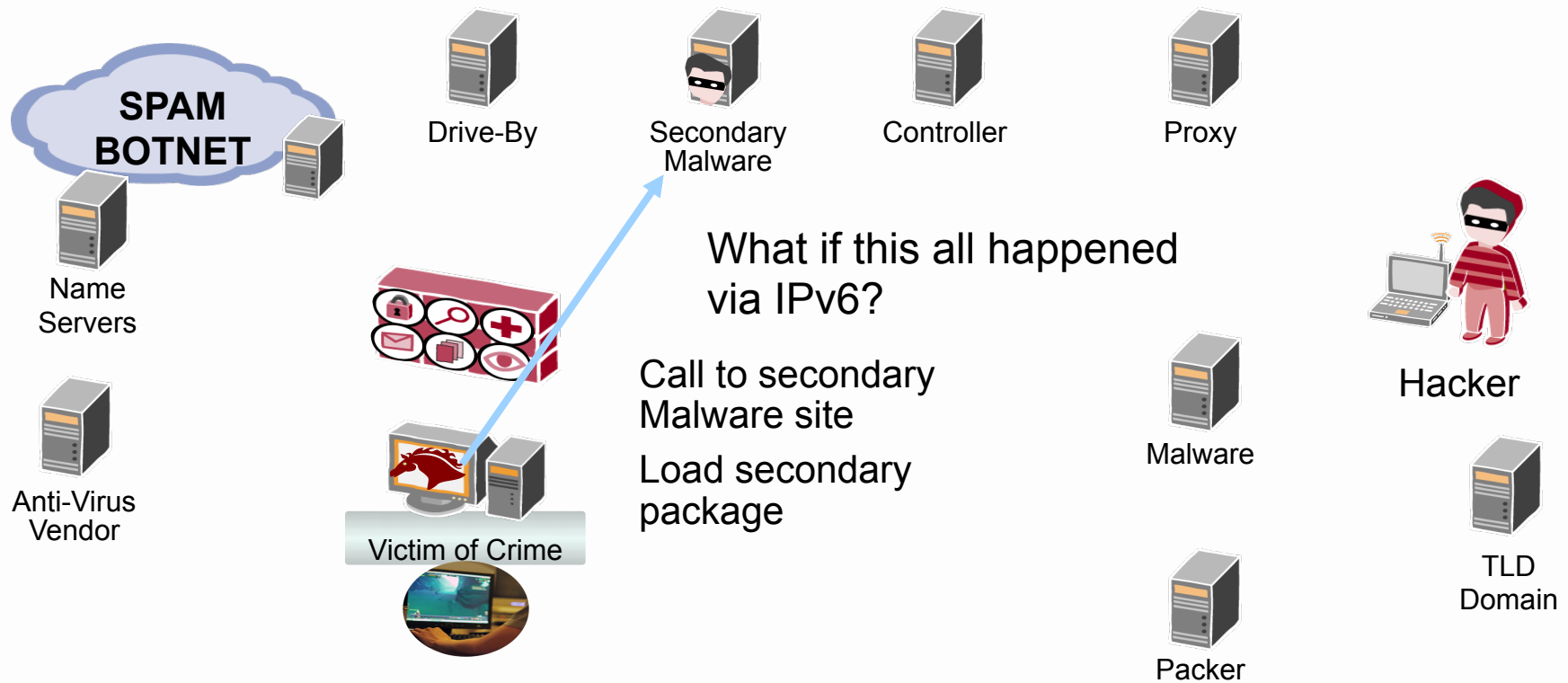
Drive-By Violation



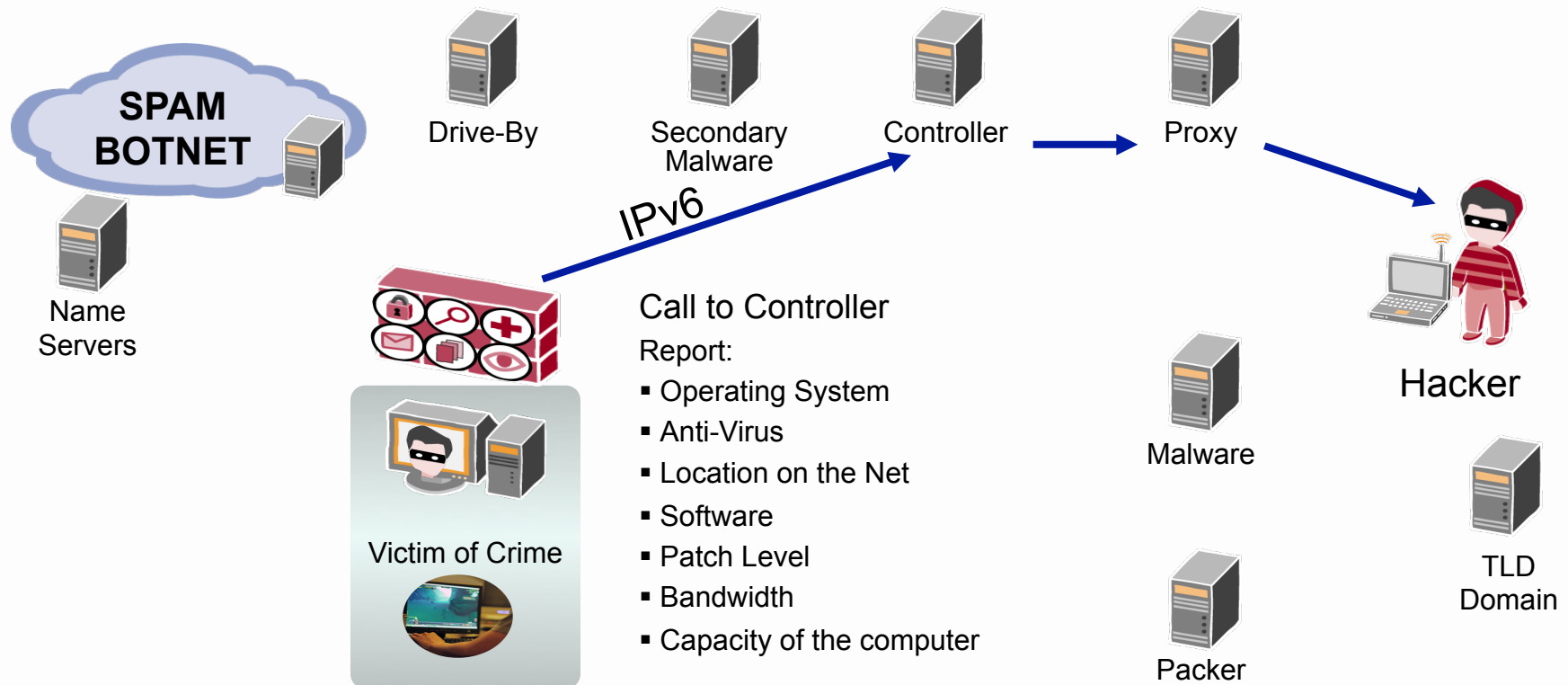
Poison Anti-Virus Updates



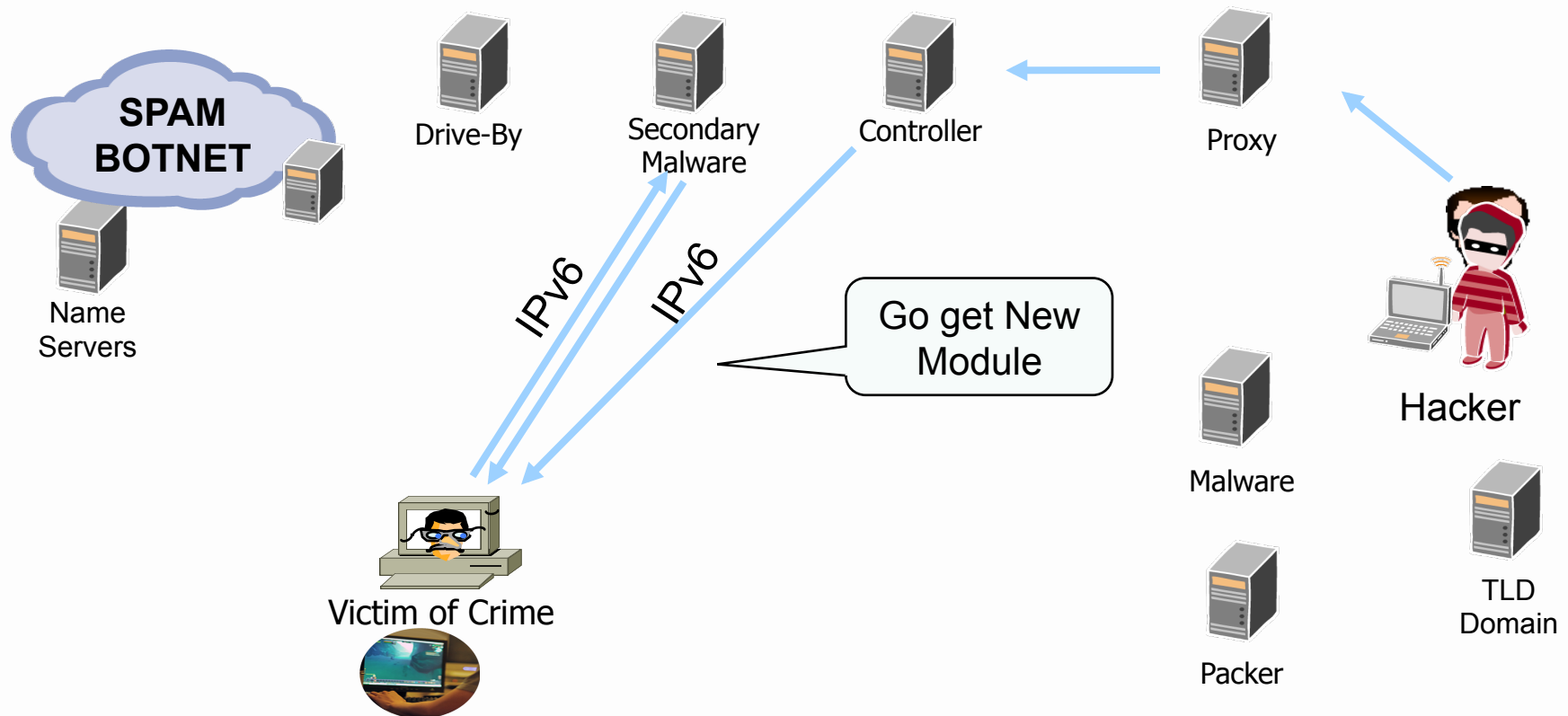
Prepare Violated Computer



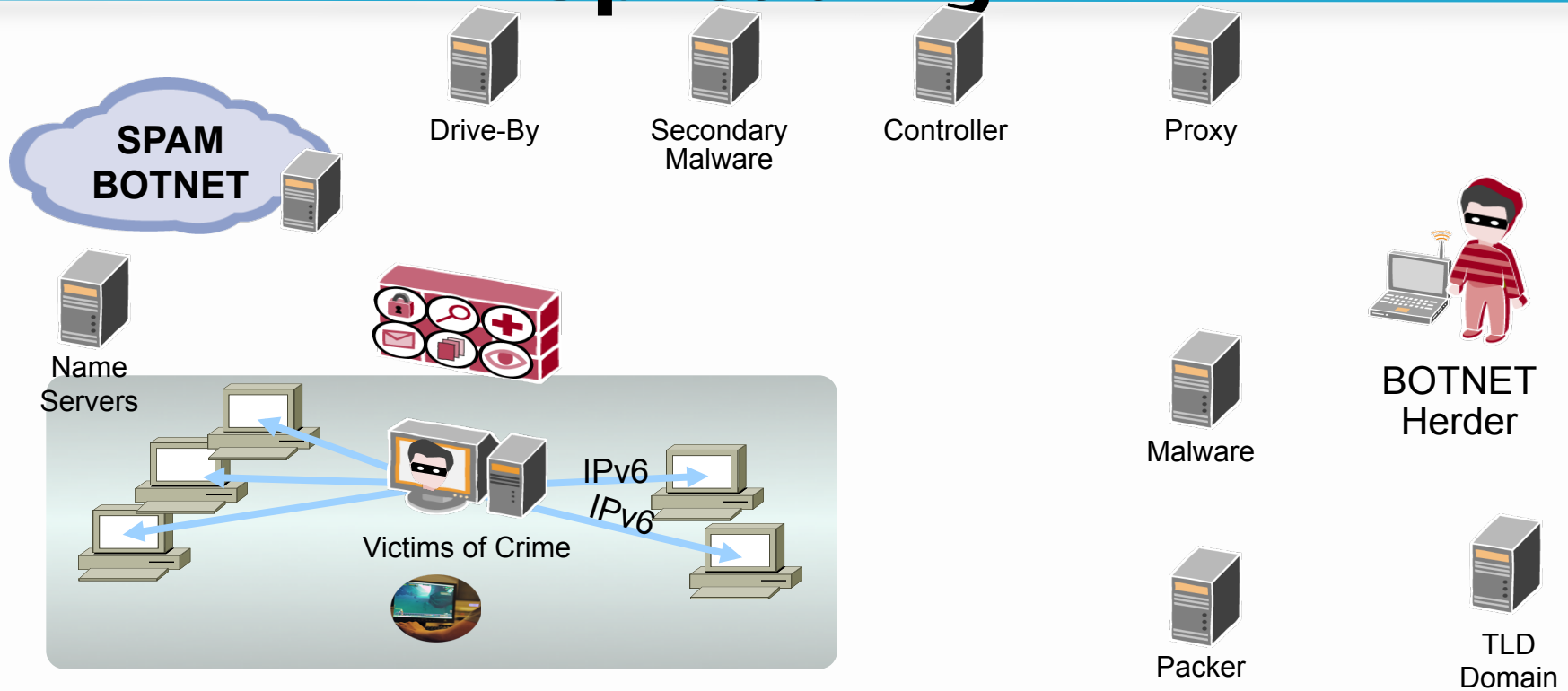
Call Home



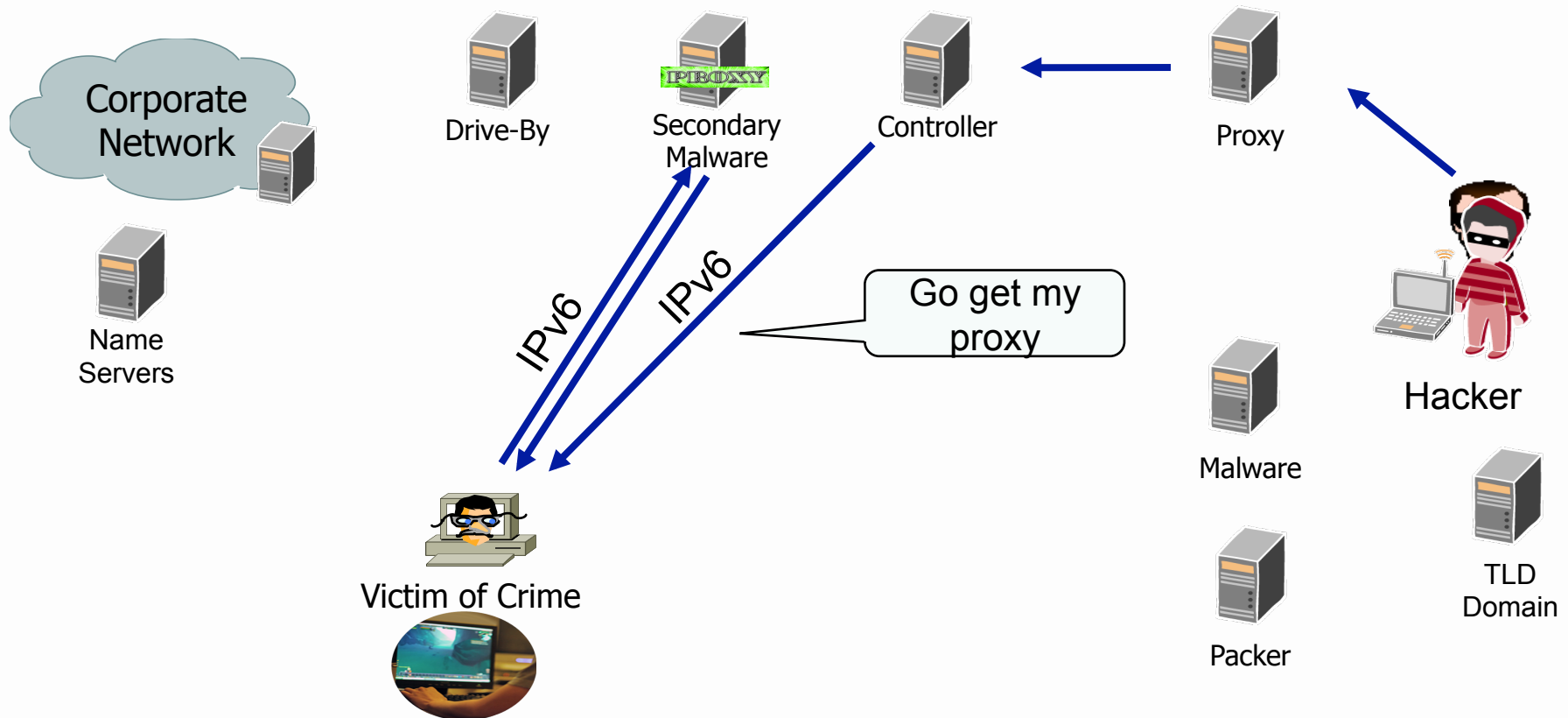
Load Custom Malware



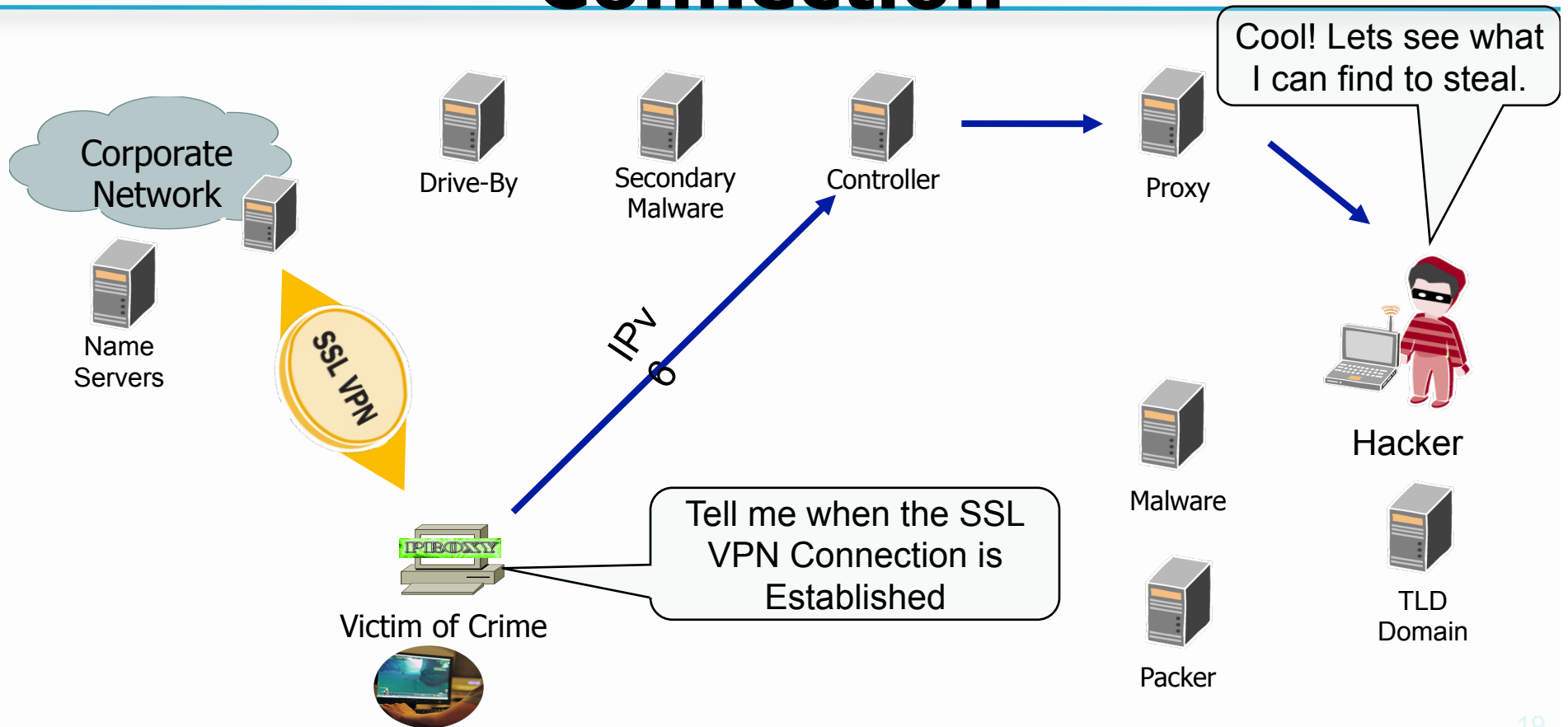
Start Worming, Scanning, & Spreading



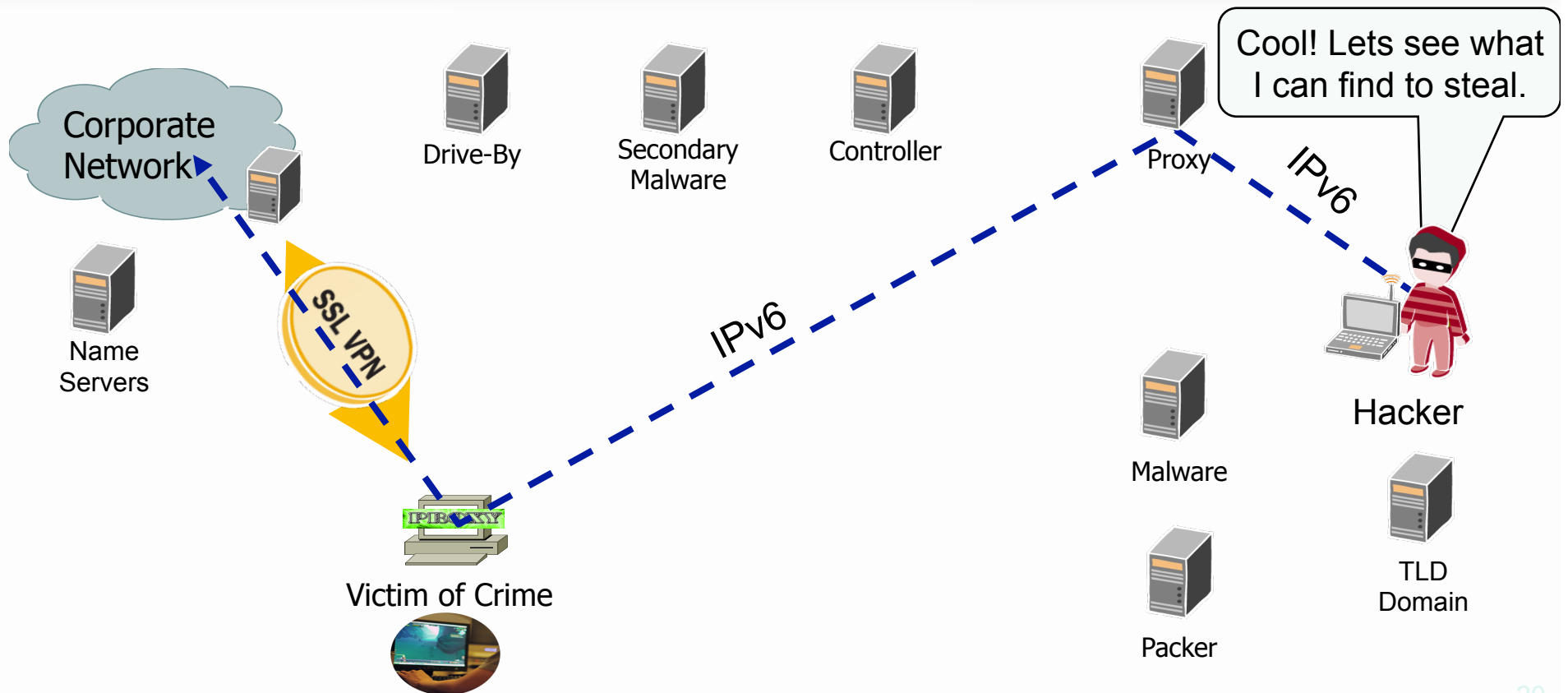
Load a Proxy with Trigger



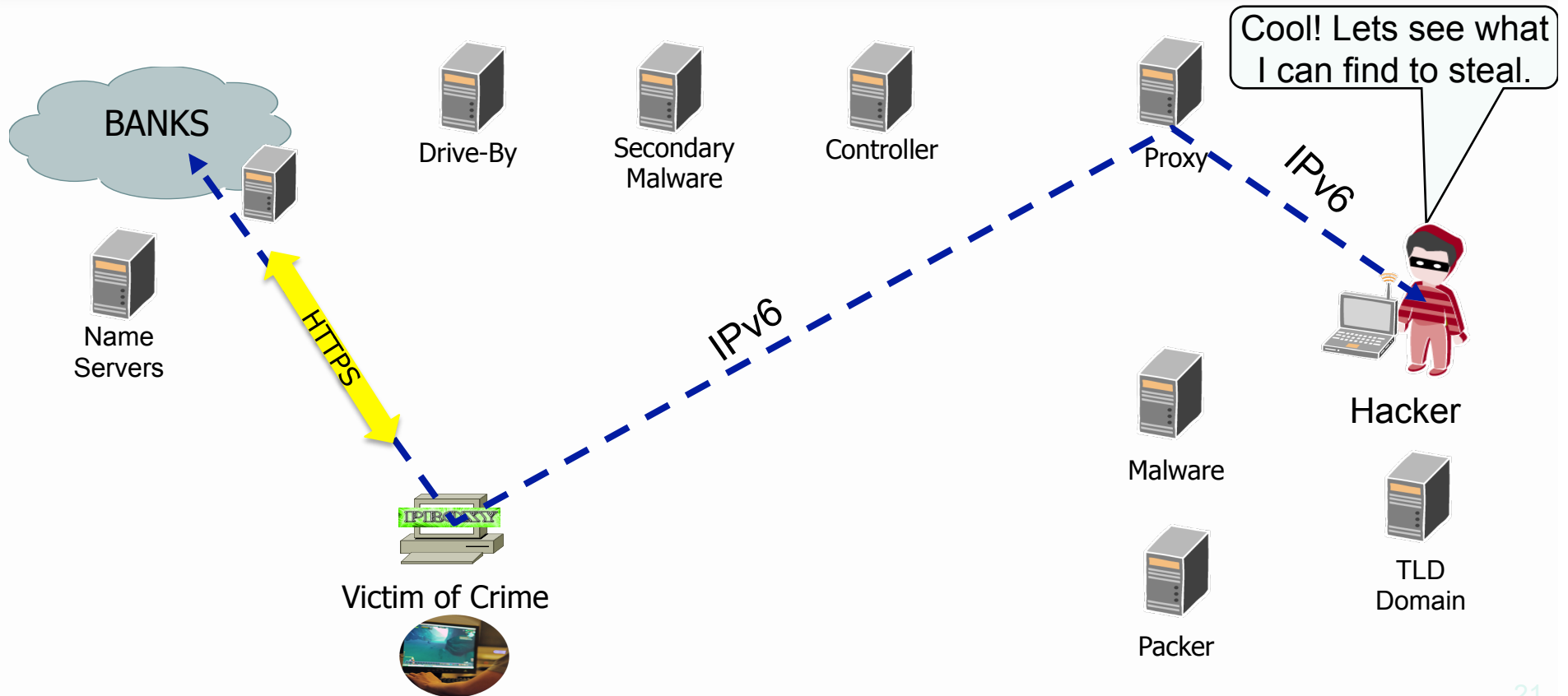
Watch for the SSL VPN Connection



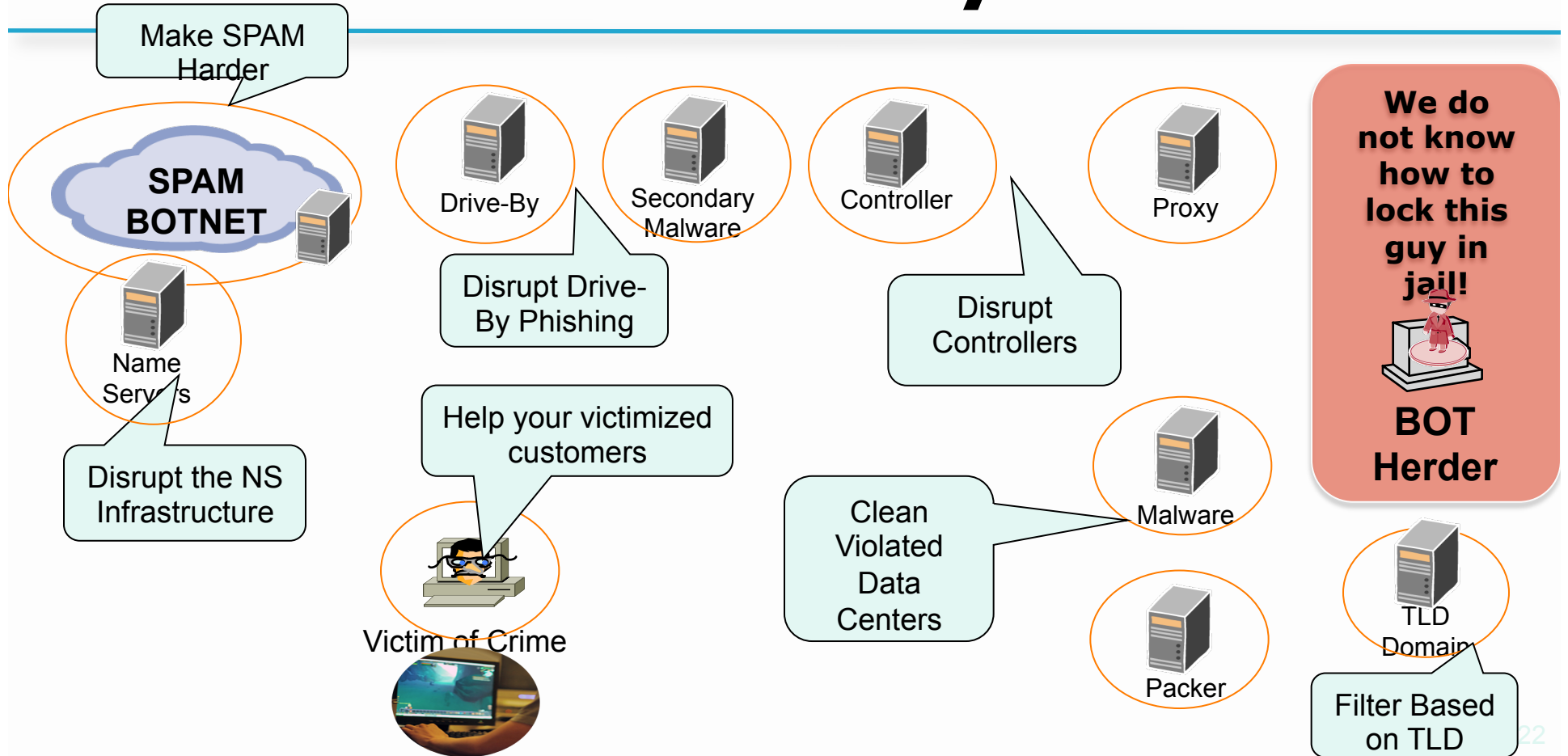
Set up the Proxy Tunnel



Proxy Behind the Bank Login



OPSEC Community's Action



Scary Consequences (B4 IPv6)

1. Building "Secure" Operating Systems with "Security Development Lifecycles" and aggressive testing are not delivering to expectations.
2. Host Security Tools (anti-virus) are not delivering to expectations.
3. Application Security is not delivering and becoming more complicated.
4. Network Security tools (firewalls, IDP/IPS, etc) are not delivering as expected.
5. Defense in Depth are not delivering as expected.
6. Malware Remediation is not working (i.e. how to clean up infections).
7. The Bad Guys follow economic equilibrium patterns – finding optimization thresholds.
8. Law Enforcement is not in a position to act on International Crime – where the laws are not in place.
9. The "eco-system" of the "security industry" is locked in a symbiotic relationship.

Now What?

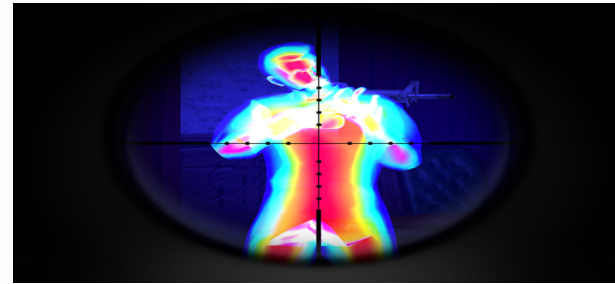
Understanding Today's Cyber-Criminal Behavior Drivers

Key Take Away – The Good Guys are the Big Part of the Security Problem

- What is the “White Hat” Security Community really doing to solve the problem?
- *We’re trying to solve the methamphetamine drug abuse problem by funding studies and pontificating on the chemical make up of methamphetamine, processes for producing methamphetamine, and variations for new methamphetamine mixes.*

Key Take Away – The Good Guys are the Big Part of the Security Problem

Who we need to Target



This is nice to know

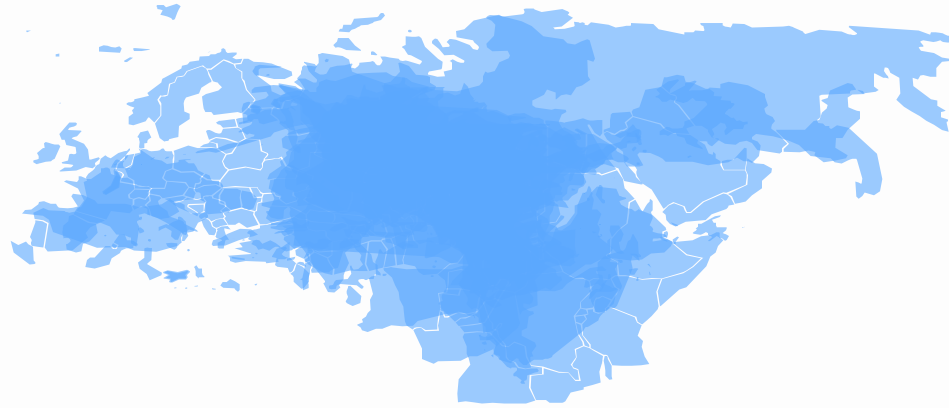


Not understanding that our problem is a human problem leads to “security solutions” which get bought, deployed, and never used.

Our Traditional View of the World



The Reality of the Internet No Borders



How to project civic society and the rule of law
where there is no way to enforce the law?

Three Major Threat Vectors

- Critical Infrastructure has three major threat drivers:
 - Community #1 Criminal Threat
 - Criminal who use critical infrastructure as a tools to commit crime. Their motivation is money.
 - Community #2 War Fighting, Espionage and Terrorist Threat
 - What most people think of when talking about threats to critical infrastructure.
 - Community #3 P3 (Patriotic, Passion, & Principle) Threat
 - Larges group of people motivated by cause – be it national pride (i.e. Estonia & China) or a passion (i.e. Globalization is Wrong) aka Anonymous

Essential Criminal Principles

- There are key essential principles to a successful miscreant (i.e. cyber criminal)
- These principles need to be understood by all Security Professionals
- Understanding allows one to cut to the core concerns during security incidents
- Attacking the **dynamics** behind these principles are the core ways we have to attempt a **disruption** of the Miscreant Economy

Principles of Successful Cybercriminals

1. Don't Get Caught
2. Don't work too hard
3. Follow the money
4. If you cannot take out the target, move the attack to a coupled dependency of the target
5. Always build cross jurisdictional attack vectors
6. Attack people who will not prosecute
7. Stay below the pain threshold

Principle 1: Do Not Get Caught!

- The first principle is the most important – it is no fun getting caught, prosecuted, and thrown in jail
 - (or in organized crime – getting killed)
- All threat vectors used by a miscreant will have an element of un-traceability to the source
- If a criminate activity can be traced, it is one of three things:
 1. A violated computer/network resources used by the miscreant
 2. A distraction to the real action
 3. A really dumb newbie



Principle 2: Do Not Work Too Hard!

- Use the easiest attack/penetration vector available in the toolkit to achieve the job's objective
- Example: If your job is to take out a company's Internet access the day of the quarterly number's announcement, would you:
 1. Penetrate the Site and Delete files?
 2. Build a custom worm to create havoc in the company?
 3. DOS the Internet connection?
 4. DOS the SP supporting the connection?

Why Use DNS "Noisy" Poisoning when it is easier to violate a ccTLD?



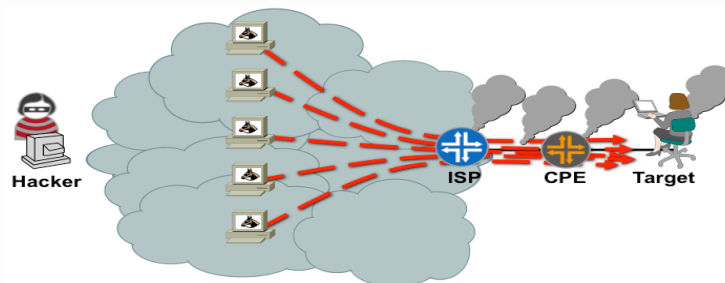
Principle 3: Follow the Money

- *If there is no money in the crime then it is not worth the effort.*
- *Follow the money* is the flow of money or exchanged value as one miscreant transfers value to another miscreant (or the victim transfers value to the criminal)
- A **Cyber-Criminal Threat Vector** opens when the miscreant finds a way to **move 'stored value' from the victim through the economy**
- It is worse if the cyber 'stored value' can cross over to normal economic exchange



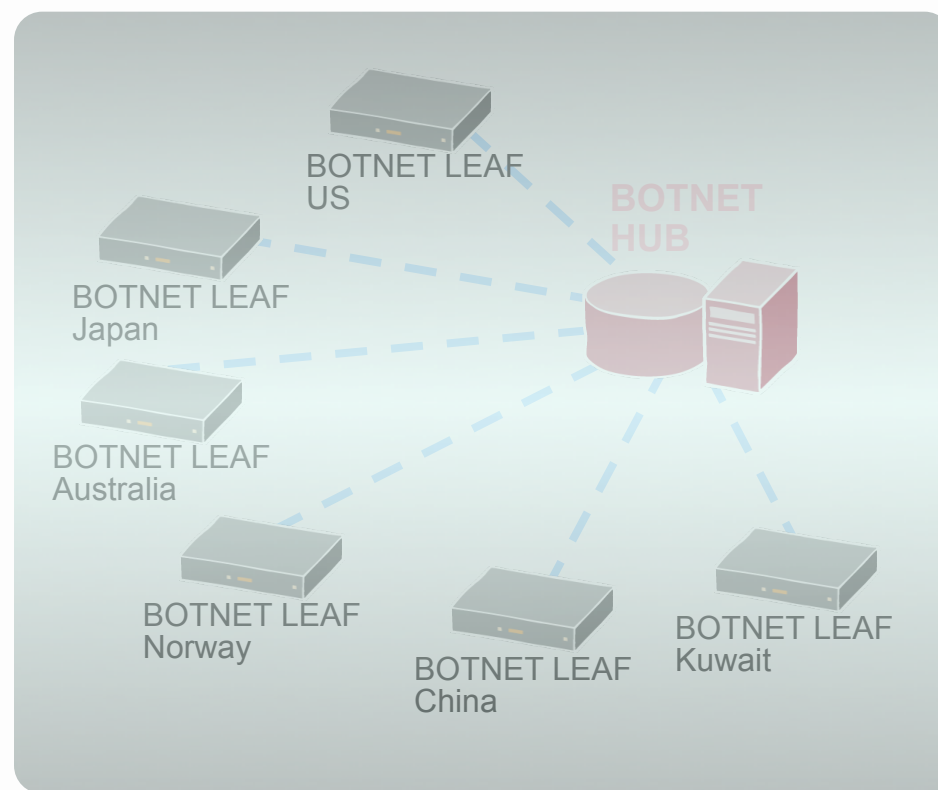
Principle 4: If You Cannot Take Out The Target...

- If you cannot take out the target, move the attack to a coupled dependency of the target
- There are lots of coupled dependencies in a system:
 - The target's supporting PE router
 - Control Plane
 - DNS Servers
 - State Devices (Firewalls, IPS, Load Balancers)
- Collateral Damage!



Principle 5: Always Build Cross Jurisdictional Attack Vectors

- Remember – Don't get caught! Do make sure ever thing you do is cross jurisdictional.
- Even better – cross the law systems (Constitutional, Tort, Statutory, Islamic, etc.)
- Even Better – Make sure your "gang" is multi-national – making it harder for Law Enforcement



Principle 6: Attack People Who Will NOT Prosecute

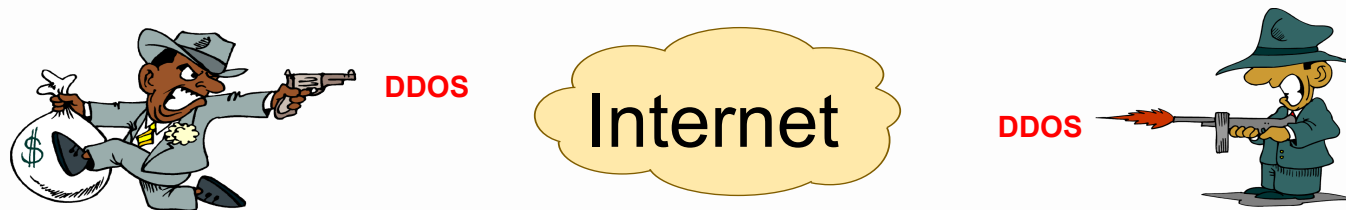
- If your activity is something that would not want everyone around you to know about, then you are a miscreant target
- Why? Cause when you become a victim, you are not motivated to call the authorities
- Examples:
 - Someone addicted to gambling is targeted via a Phishing site
 - Someone addicted to porn is targeted to get botted
 - Someone addicted to chat is targeted to get botted
 - Someone new to the Net is targeted and abused on the physical world
 - Government, Finance, and Defense, Employees – who lose face when they have to call INFOSEC

Principle 7: Stay below the Pain Threshold

- The *Pain Threshold* is the point where an SP or Law Enforcement would pay attention
- If you are below the pain threshold – where you do not impact an SP's business, then the SP's Executive Management do not care to act
- If you are below the pain threshold – where you do not have a lot of people calling the police, then the Law Enforcement and Elected Official do not care to act
- The Pain Threshold is a matter of QOS, Resource Management, and picking targets which will not trigger action

Criminal Trust

- Miscreants will guardedly trust each other
- They can be competitors
- They can be collaborators
- But when there is money on the table, criminal human behavior and greed take over.
- Cybercriminal cannibalize each other's infrastructure.
- Cybercriminals attack each other's infrastructure.



Dire Consequences

- The Miscreant Economy is not a joke. It is not a game. It is not something to play with.
 - **PEOPLE DIE**
- Once organized crime enter the world of the Miscreant Economy, the days of *fun* were over.
- Now that Cyber-Criminals will use any resource on the net to commit their crime, they don't worry about the collateral damage done.
 - Think of computer resources at a hospital, power plant, or oil refinery – infected and used to commit phishing and card jacking.
 - What happens if someone gets mad at the phishing site, attacks it in retaliation, unintentionally knocking out a key system.

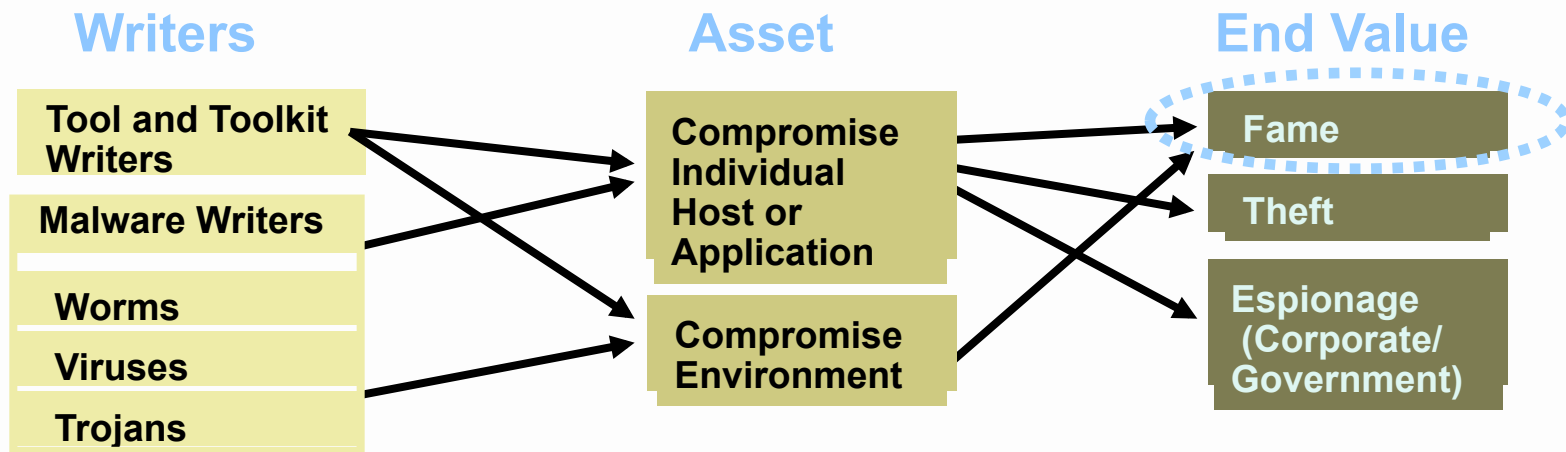
Enduring Financial Opportunities

Postulate: Strong, Enduring Criminal Financial Opportunities Will Motivate Participants in the Threat Economy to Innovate to Overcome New Technology Barriers Placed in Their Way

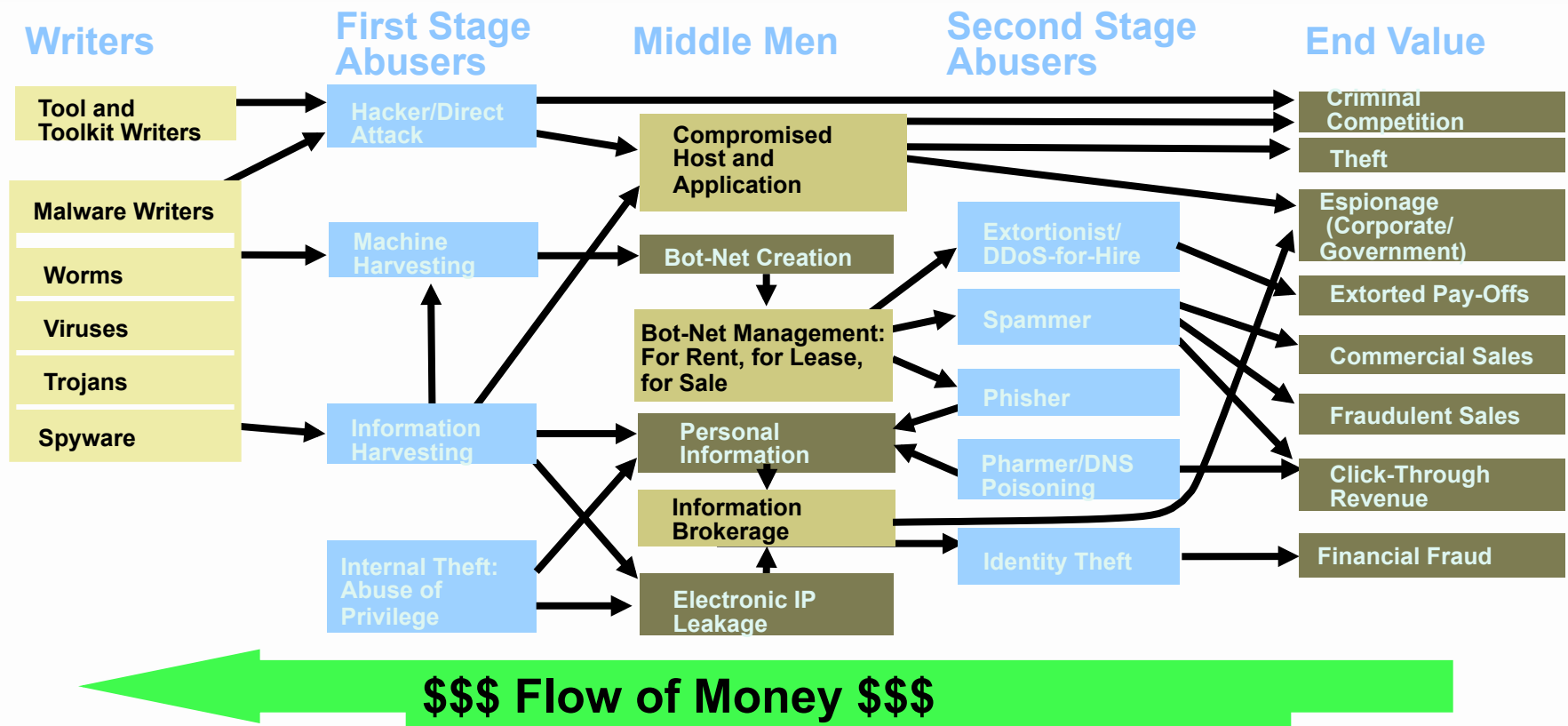
Enduring *criminal* financial opportunities:

- Extortion
- Advertising
- Fraudulent sales
- Identity theft and financial fraud
- Theft of goods/services
- Espionage/theft of information

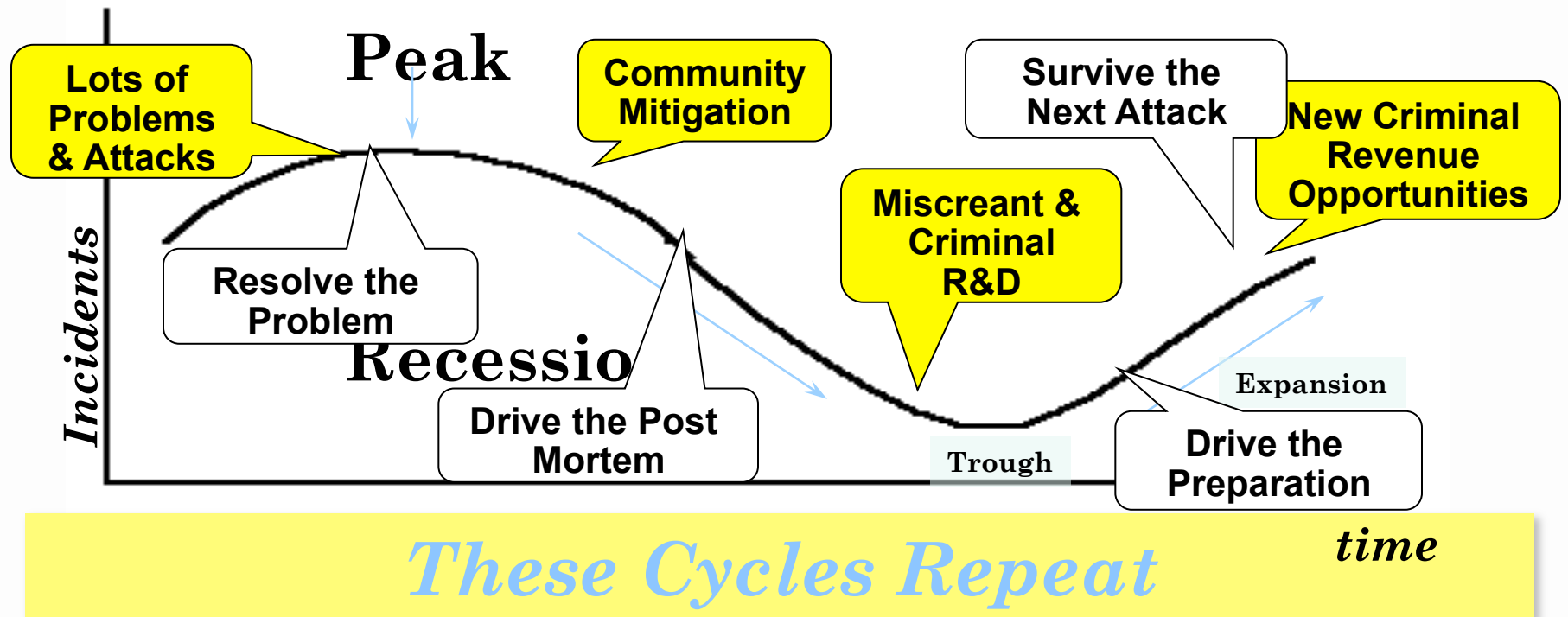
Threat Economy: In the Past



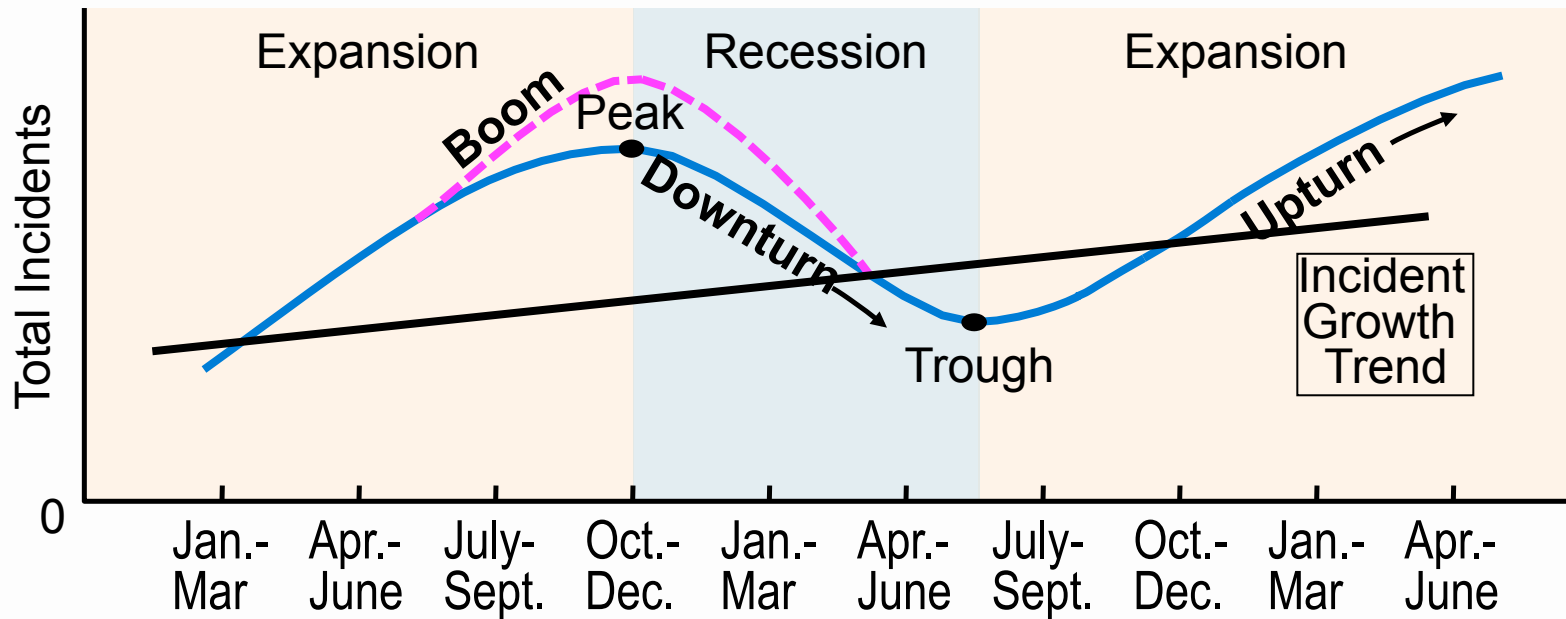
Threat Economy: Today



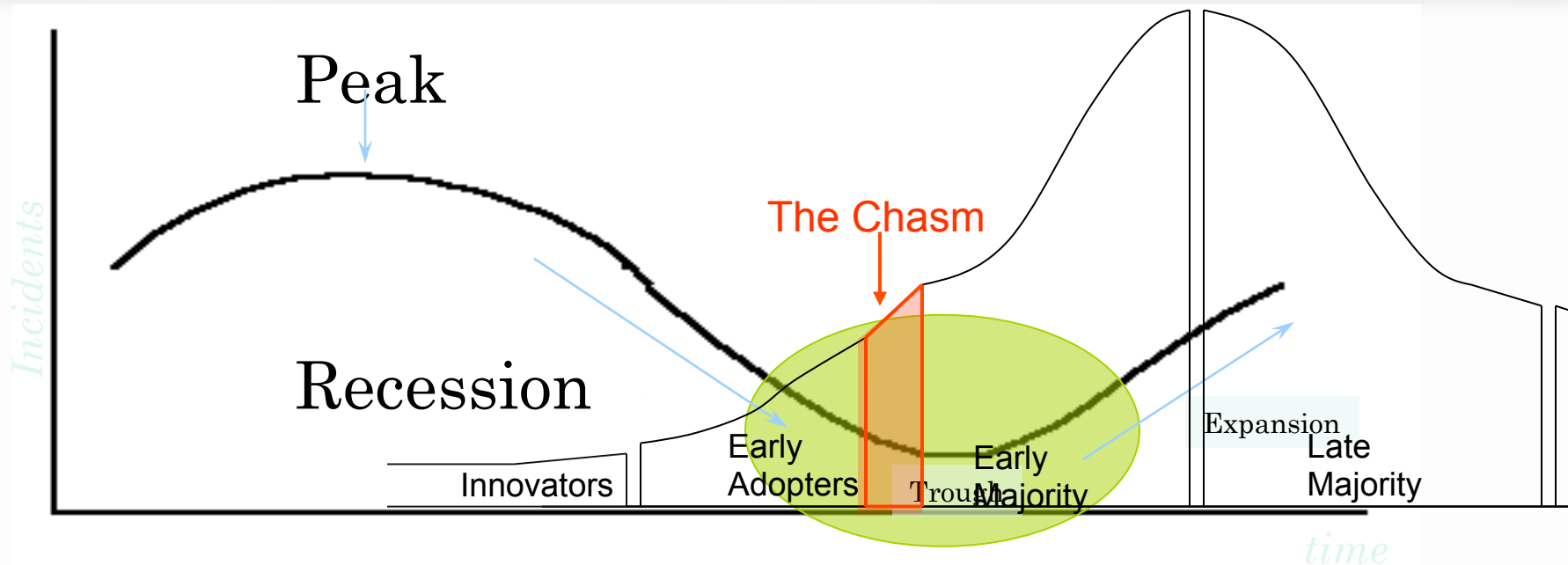
Miscreant - Incident Economic Cycles



Miscrime Economic Cycles



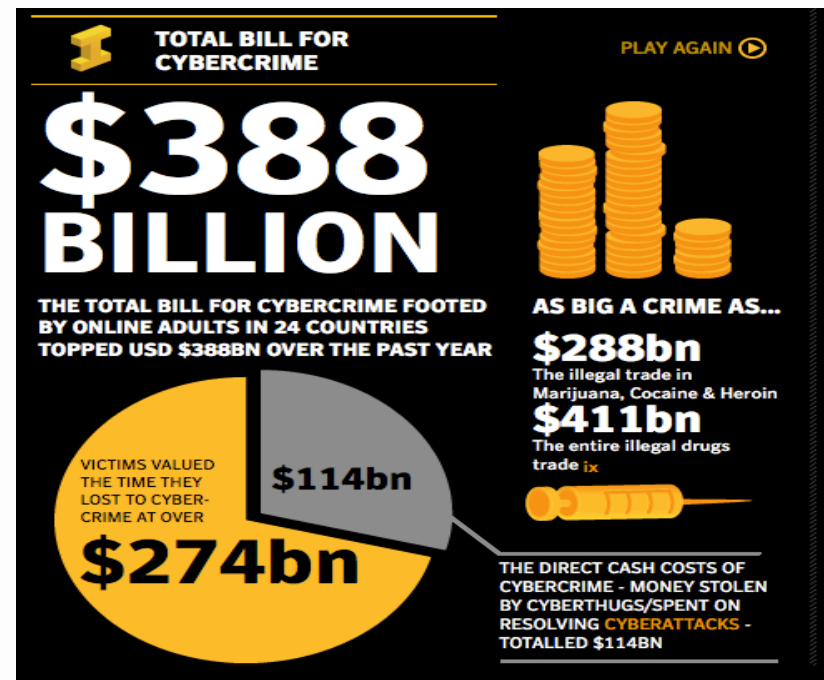
The dire trap – the *Chasm* of in action



No Pain
No Business Justification for Action

Cyber Crime Cost are Huge!

- Bigger than the illegal drug trade!
- Bigger than human trafficking trade!



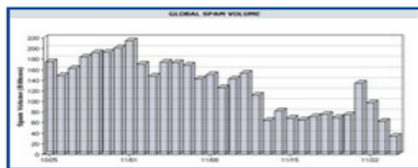
Community Action Can Have an Impact



[About This Blog](#) | [Archives](#) | [XML](#) [RSS Feed](#) ([What's RSS?](#))

Two Weeks Out, Spam Volumes Still Way Down

A full two weeks after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity [was taken offline](#), the volume of spam sent globally each day has yet to bounce back.

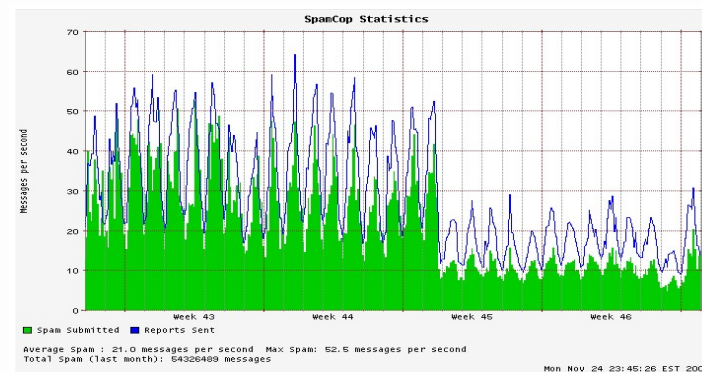
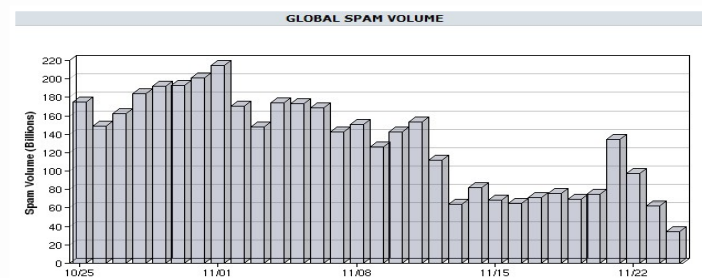


The [block graph](#) over at e-mail security firm **IronPort** suggests that the company blocked around 35 billion spam messages on Monday. Prior to hosting provider [McColo's shutdown](#), IronPort was flagging

somewhere around 160 billion junk e-mails per day.

A quick glance at the volume flagged by [Spamcop.net](#) shows that they're still detecting well below half of the spam volumes they were just two weeks ago.

I'm not suggesting this is a permanent situation: I happen to agree with most



Source: http://voices.washingtonpost.com/securityfix/2008/11/64_69_65_73_70_61_6d_64_69_65.html

But for how long



[About This Blog](#) | [Archives](#) | [XML](#) [RSS Feed](#) (What's RSS?)

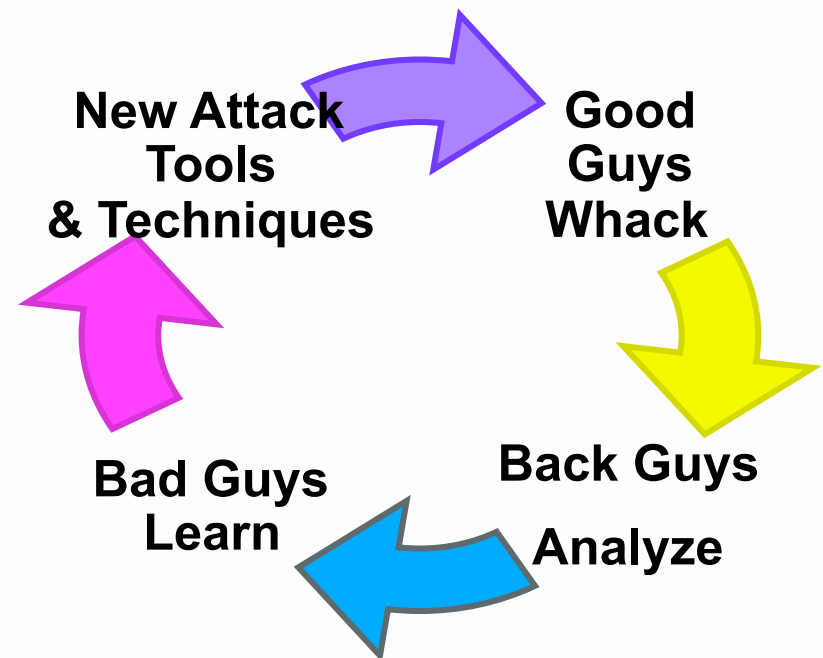
Srizbi Botnet Re-Emerges Despite Security Firm's Efforts

In the fallout resulting from knocking **McColo Corp.** offline, this past week may prove to be a missed opportunity in the prevention of a dramatic reappearance of junk e-mail, as a botnet that once controlled 40 percent of the world's spam apparently has found a new home.

The botnet **Srizbi** was knocked offline Nov. 11 along with Web-hosting firm **McColo**, which Internet security experts say hosted machines that controlled the flow of 75 percent of the world's spam. One security firm, **FireEye**, thought it had found a way to prevent the botnet from coming back online by registering domain names it thought **Srizbi** was likely to target. But when that approach became too costly for the firm, they had to abandon their efforts.

"This cost us a lot of money. We engaged all the right people. In the end, it comes back to the fact that there wasn't a process in place to do what we were trying to do," said **Alex Lanstein**, senior researcher at **FireEye**. "The day after we stopped registering the domains, the bad guys started picking them up."

According to **FireEye**, **Srizbi** was the only botnet operating through



This virtuous cycle drives cyber-criminal IPv6 innovations.

What will we do when the Cyber-Criminals ...

- Retaliate! Historically, Organized Crime will retaliate against civic society to impose their will and influence on civic society.
 - What will the today's organized crime do in a cyber equivalent world?
- How will the world respond when:
 - We cannot as a global society investigate and prosecute International crime?
 - Too much dependence on "security vendors" for protection.
- Global Telecom's *Civic Society* has to step forward – work with each other collectively to protect their interest.

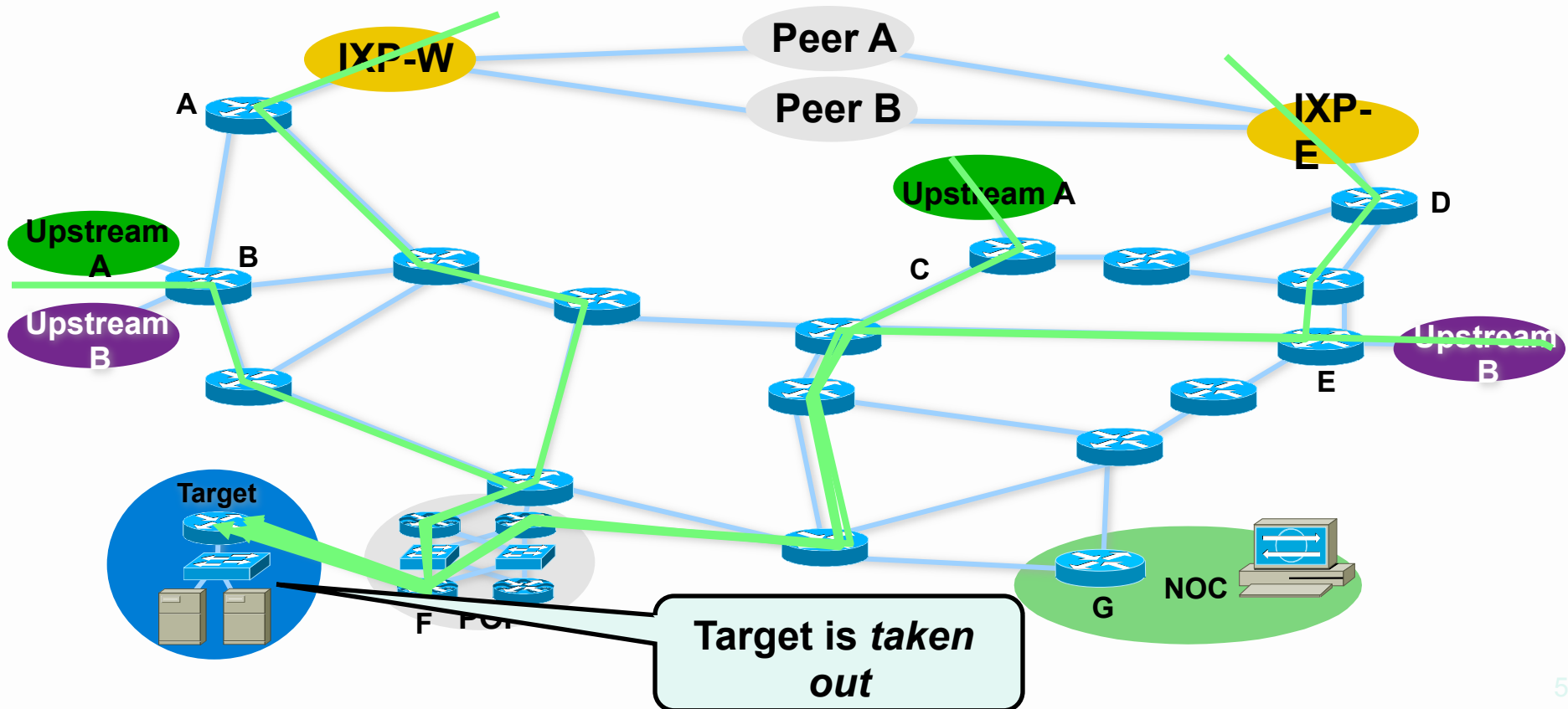
Cyber Warfare

- Of the three threat vectors, cyber-warfare is a “constrained” threat.
- All cyber warfare is a constrained with in State Actors and Actions.
 - There are Generals who are in charge giving orders.
 - There are Government officials who are providing state policy.
- Espionage is part of state policy, a persistent threat, but not “warfare.”
- New State actors can make mistakes – unintentionally creating collateral consequence.

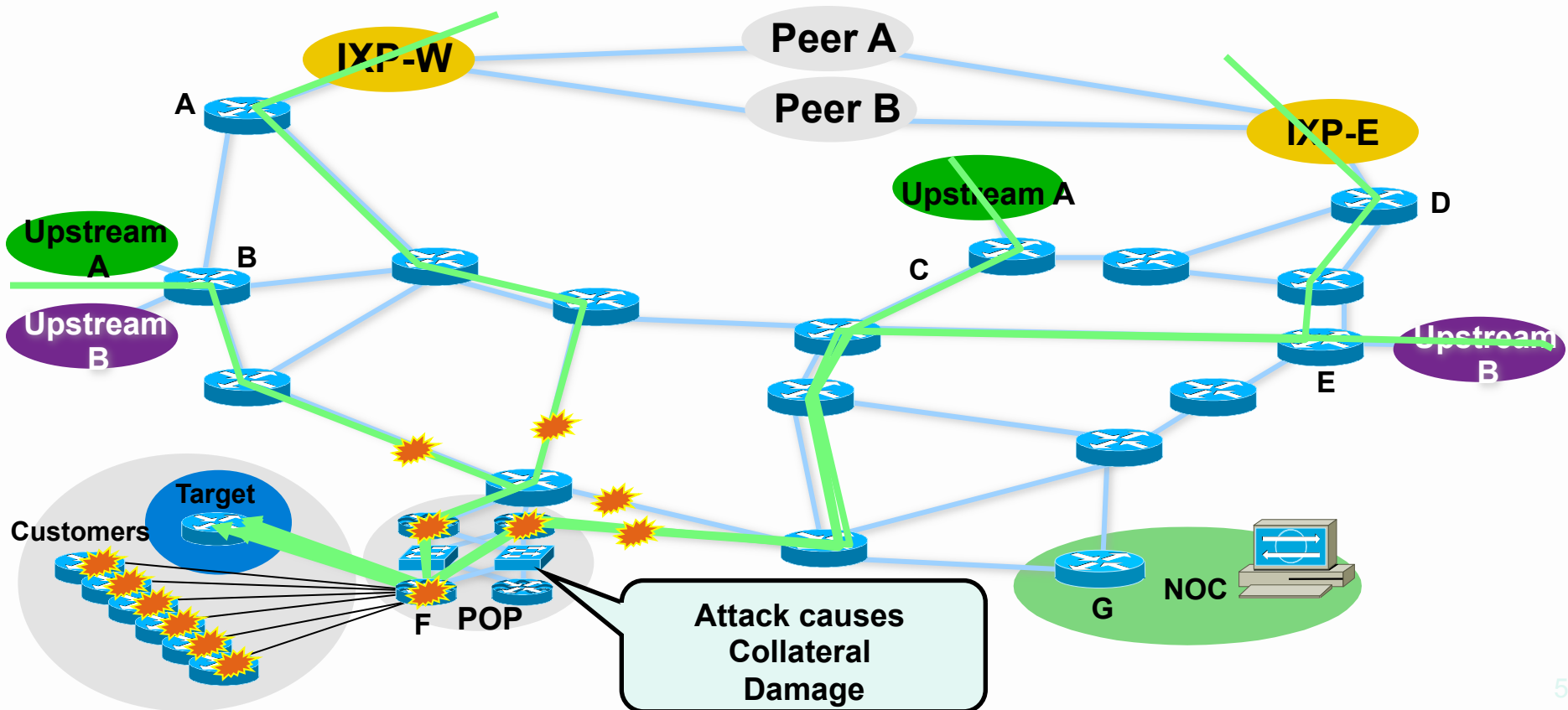


Michael Falco / The New York Times / Redux

Cyber Warfare's Consequences ...



... Extend beyond the perceived "Battle Space."



Cyber Warfare's Reality

- Cyber Warfare is a threat to business, but not the threat to spend hours and money to protect.
- Protecting against Cyber-Crime and the P3 threat will mitigate many of the cyber warfare threats.

P3 Threat – the Big Change

- The Dramatic Change over the past year has been the increasing security threat from individuals and groups that are not “constrained.”
- These groups are driven by motivations that are not “money driven.” They are not given “orders.” They do it based on self motivation.

- **Patriotic** – They believe they have a right to stand up for their country, cause, or crusade.
- **Passionate** – They attach to a cause and will work long hours to further that cause.
- **“Principled”** – The base their actions on principles they passionately believe and will perform actions that they feel is within their “Internet Rights.”



Patriotic, Passion, & Principle Drivers



"The post-90 generation teens that run 2009.90admin.com, wrote on their website, "We are not Internet attackers, we are just a group of computer fans; we are not mentally handicapped kids, we are the real patriotic youth. We'll target anti-China websites across the nation and send it as a birthday gift to our country."

"The 500-word statement appeared over a red and black background decorated with a flying national flag. Zhang Yiwu, a professor at Peking University and a literary critic, said although many believe young people are not as patriotic as previous generations, there are exceptions. "The post-90s generation is undoubtedly passionate and patriotic, but their lifestyle and attitude is varied. The campaign of attacking anti-China websites shows their unstable and immature nature," Zhang said. "Although their behavior is not worthy of praise, the unfair reports about China coming from many foreign media will encourage the youngsters to fight back."

- <http://news.alibaba.com/article/detail/technology/100168523-1-teen-hackers-vow-prove-patriotism.html>

Are you part of the new “Civic Society?”

- Are you sitting back and trusting your “security vendors?”
- Or, are you stepping forward, working with all others with like interest in Global Telecom’s Civic Society to go after and shutdown the miscreants?
- Two Recommendations for SCADA Organizations to get started:
 - DSHIELD
 - SCADASEC-L

Bot Mitigation for ISPs – Link to Materials

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



This has been the third 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

© slide PDF files and video copyrighted by the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)



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](https://www.m3aawg.org/contact_form)

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 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>

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

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 “public – private partnership”.
- There **are effective Private Industry “Operational Security” Communities** that specialize and succeed.
- 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 facilitate the flexibility of private industry to collaborate 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 grasp 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

bgreene@senki.org ([logout](#))

Main Ops-Trust Group
([change](#)) Ω

[Home](#)

[List member airports](#)

[Nominate new member](#)

[Vouching control panel](#)

[CIDRs of Interest](#)

[AutSys' of Interest](#)

[Domains of Interest](#)

[View mailing lists](#)

[Download PGP key ring](#)


[Visit the Wiki](#)
(Your WikiName must be set)

[Confluence](#) (Experimental)

[Edit contact info](#)

[Change password](#)

Member Information for: bgreene@senki.org

Full name: Barry Raveendran Greene 

Affiliation: @senki.org

PGP Key: [16BF45F3](#)

Entered: 2008-10-11 03:00:04 UTC

Last Activity: 2010-09-01 10:38:38 UTC

Inactive for: 00:00:00

Status: *active*

Timezone info: US Westcoast

SMS info: +1.408.218.4669

I.M. info:

Phone info: +1 408 218 4669

Postal info:

WikiName: BarryRGreene

Home Airport: SFO

Biography: <http://www.linkedin.com/in/barryrgreene>
0x16BF45F3

Has vouched For:

[jose@arbor.net](#)
2010-08-27 21:13:11
[Delete](#) Know, trust, and work with w

[ddugal@juniper.net](#)
2010-08-20 16:58:52
[Delete](#) I've worked with Dave for ov
has been part of Juniper's S
investigator.

[derrick.scholl@sun.com](#)
2010-05-24 16:50:24
[Delete](#) Know and worked with Derrick's first activities. CSIRT work and other industry security issues. Know

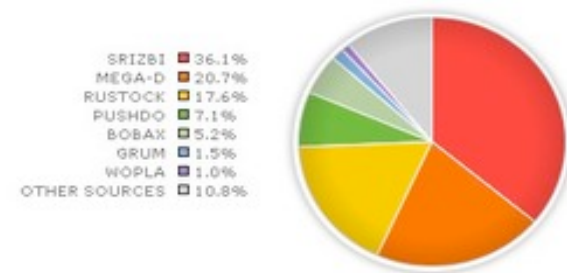
In 2012, we will have the tools for the good guy to organize and effectively take action (taking lessons from OPSEC Trust's successes)

Cyber Strategy of Action

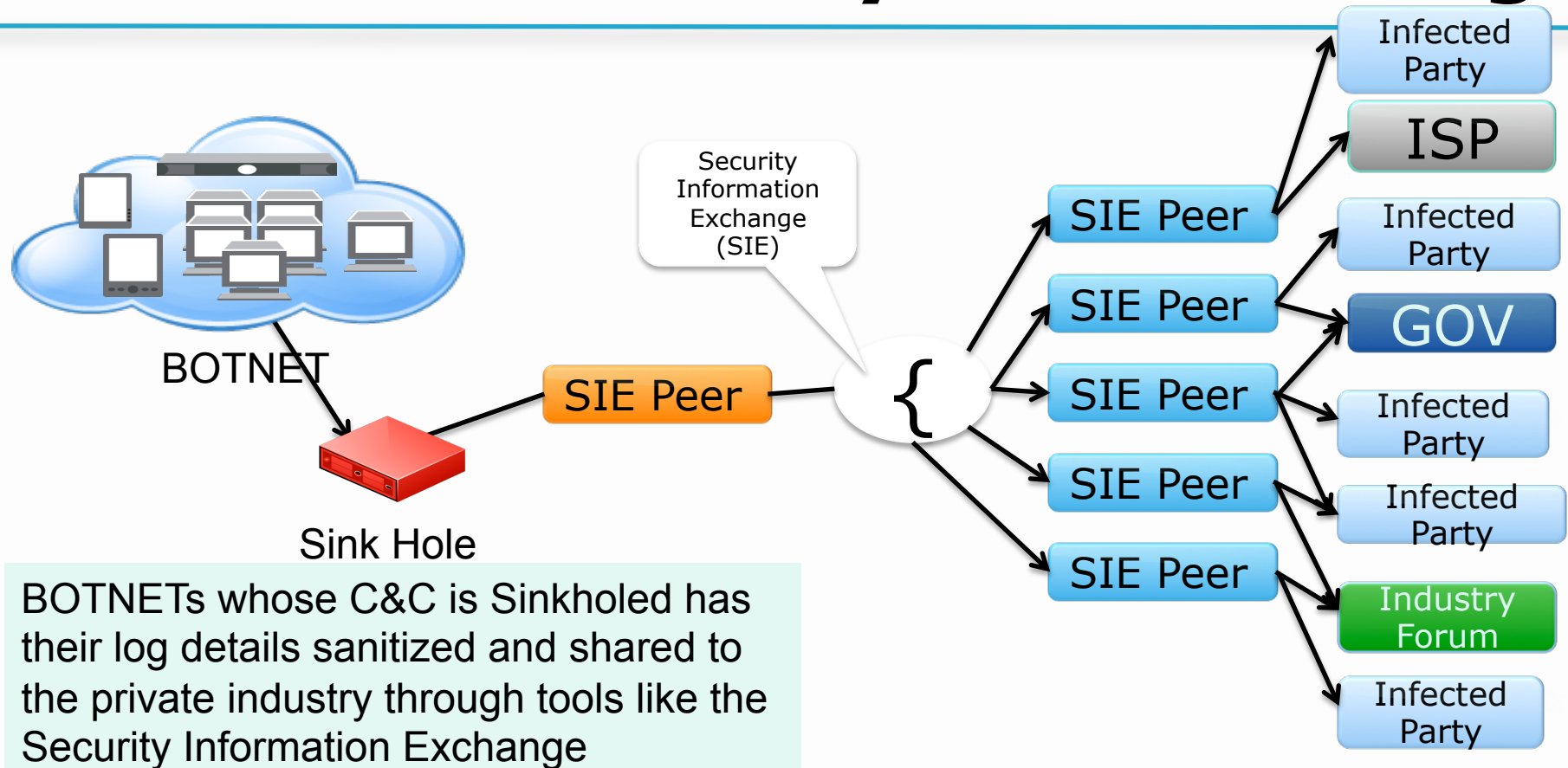
- **Exercise the Court with Criminal and Civil Action. Laws are driven by cases in the court.** We are consistently working on criminal action, but that is one side of the legal system. Civil action is as important as the criminal action. As seen by Microsoft, damages to a company can be used as a bases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

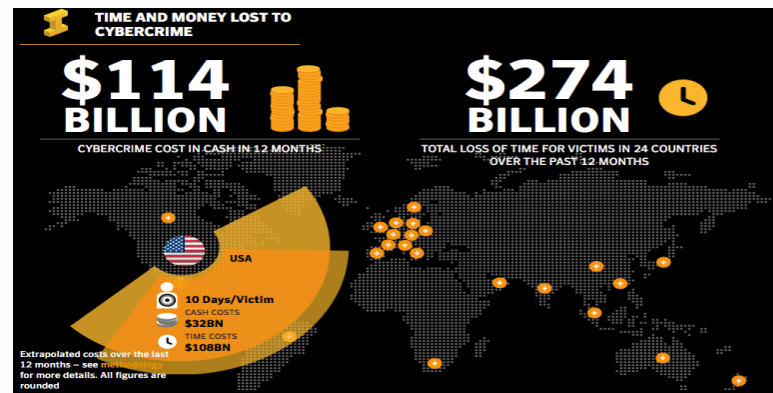


Real Time Security Data Sharing



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

last seen	2010-11-25 09:52:03 -0000
oquyclyedi.com.	A 213.55.114.132
balliwick	com.
first seen	2010-11-15 02:47:01 -0000
last seen	2010-11-26 02:07:10 -0000
first seen in zone file	2010-11-15 17:09:22 -0000
last seen in zone file	2010-11-24 17:09:28 -0000
oquyclyedi.com.	NS ns1.gvhhi.ru.
oquyclyedi.com.	NS ns2.justecosy.com.
balliwick	com.
first seen in zone file	2010-11-14 17:09:22 -0000
last seen in zone file	2010-11-14 17:09:22 -0000
oquyclyedi.com.	NS ns3.lerelaisinternet.com.
oquyclyedi.com.	NS ns4.lerelaisinternet.com.
balliwick	oquyclyedi.com.
first seen	2010-11-16 02:24:21 -0000
last seen	2010-11-25 12:16:08 -0000
oquyclyedi.com.	NS ns1.oquyclyedi.com.
oquyclyedi.com.	NS ns2.oquyclyedi.com.

balliwick	gvnni.ru.
first seen	2010-11-18 15:54:49 -0000
last seen	2010-11-22 03:31:24 -0000
ns1.gvhhi.ru.	A 190.86.101.171
balliwick	gvhhi.ru.
first seen	2010-11-11 03:12:45 -0000
last seen	2010-11-18 15:42:32 -0000
ns1.gvhhi.ru.	A 201.147.145.254
balliwick	gvhhi.ru.
first seen	2010-11-23 13:53:07 -0000
last seen	2010-11-25 11:12:16 -0000
ns1.gvhhi.ru.	A 218.67.78.181

03:43:04 -0000
13:44:15 -0000
03.66

Rdata results for ANY/218.67.78.181

Found 4700 RRs in 1.12 seconds.

ns2.tabletspilldrug.net.	A	218.67.78.181
apy.ru.	A	218.67.78.181
atlanticmedrx.net.	A	218.67.78.181
enclavedirect.com.	A	218.67.78.181
grandrxpills.com.	A	218.67.78.181
justecosy.com.	A	218.67.78.181
locutionsite.com.	A	218.67.78.181
mail.c3o.ru.	A	218.67.78.181
mail.usualworld.com.	A	218.67.78.181
maternitybuydirect.com.	A	218.67.78.181
medrxpills.net.	A	218.67.78.181
ns1.alternativehealthrx.net.	A	218.67.78.181
ns1.badsquide.com.	A	218.67.78.181
ns1.bafac.ru.	A	218.67.78.181
ns1.bafad.ru.	A	218.67.78.181
ns1.bafaf.ru.	A	218.67.78.181
ns1.bafag.ru.	A	218.67.78.181
ns1.bafaj.ru.	A	218.67.78.181
ns1.bafal.ru.	A	218.67.78.181
ns1.bafap.ru.	A	218.67.78.181
ns1.bafar.ru.	A	218.67.78.181
ns1.bafaw.ru.	A	218.67.78.181

Rdata results for ANY/213.55.114.132

Found 10000 RRs in 1.65 seconds.

01jwahwdje.curibeudo.com.	A	213.55.114.132
0ok37mtnfw.hattytysl.com.	A	213.55.114.132
0dm106xfr.drinksage.com.	A	213.55.114.132
0dst3uw24r.cyzsoekfo.com.	A	213.55.114.132
0gtnu.mas.bayhealthmedicine.ru.	A	213.55.114.132
0hfvvthw23.curibeudo.com.	A	213.55.114.132
0pt7yqdrop.edfasawen.com.	A	213.55.114.132
0q2ufc10tx.curibeudo.com.	A	213.55.114.132
0q1foqogpva.drinksage.com.	A	213.55.114.132
0ftbtkkt9.hattytysl.com.	A	213.55.114.132
0xaiuej10t.synpaybs.com.	A	213.55.114.132
0zu54eln0n.aneznauka.com.	A	213.55.114.132
10004.buvaisklo.com.	A	213.55.114.132
10004.lekpoeha.com.	A	213.55.114.132
10005.nrukixbya.com.	A	213.55.114.132
10006hop.myralfiab.com.	A	213.55.114.132
1001ahop.myralfiab.com.	A	213.55.114.132
1003ahop.myralfiab.com.	A	213.55.114.132
10061.psyatlin.com.	A	213.55.114.132
10064.adevrecos.com.	A	213.55.114.132
100675.drugeshop.com.	A	213.55.114.132
10089.kleobdoie.com.	A	213.55.114.132
1009.suryqesli.com.	A	213.55.114.132

Criminal Domain Names found via the bad A Record

Criminal Domain Names found via the bad Name Server

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

[Home](#) [News](#) [Checkup](#) [Cleanup](#) [Victim Rights](#) [For ISPs](#) [About/Contact](#)

What is the DNS Changer Malware?

On November 8, the FBI, the NASA-OIG and Estonian police arrested several cyber criminals in "Operation Ghost Click". The criminals operated under the company name "Rove Digital", and distributed DNS changing viruses, variously known as TDSS, Alureon, TidServ and TDL4 viruses. You can read more about the arrest of the Rove Digital principals [here](#), and in the [FBI Press Release](#).

What does the DNS Changer Malware do?

The botnet operated by Rove Digital altered user DNS settings, pointing victims to malicious DNS in data centers in Estonia, New York, and Chicago. The malicious DNS servers would give fake, malicious answers, altering user searches, and promoting fake and dangerous products. Because every web search starts with DNS, the malware showed users an altered version of the Internet.

How Can I Protect Myself?

This page describes how you can determine if you are infected, and how you can clean infected machines. To check if you're infected, [Click Here](#). If you believe you are infected, [here are instructions](#) on how to clean your computer.

DCWG.ORG

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

© slide PDF files and video copyrighted by the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)



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](https://www.m3aawg.org/contact_form)

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 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>

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

Remediating Violated Customers

Segment 5 of 6

Barry Raveendran Greene, bgreene@senki.org

October 22, 2012, Baltimore, Maryland, USA

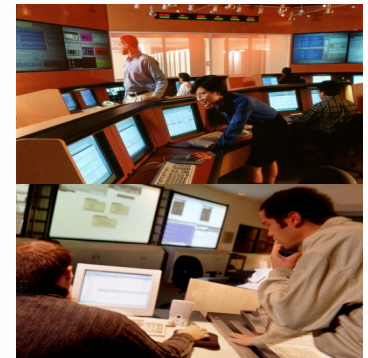
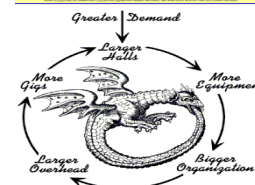
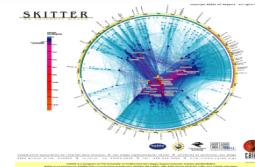




Barry Greene has over 30 years industry experience including having served as president of the ISC (Internet Systems Consortium). He is a pioneer in service provider security and operational security reaction teams.

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



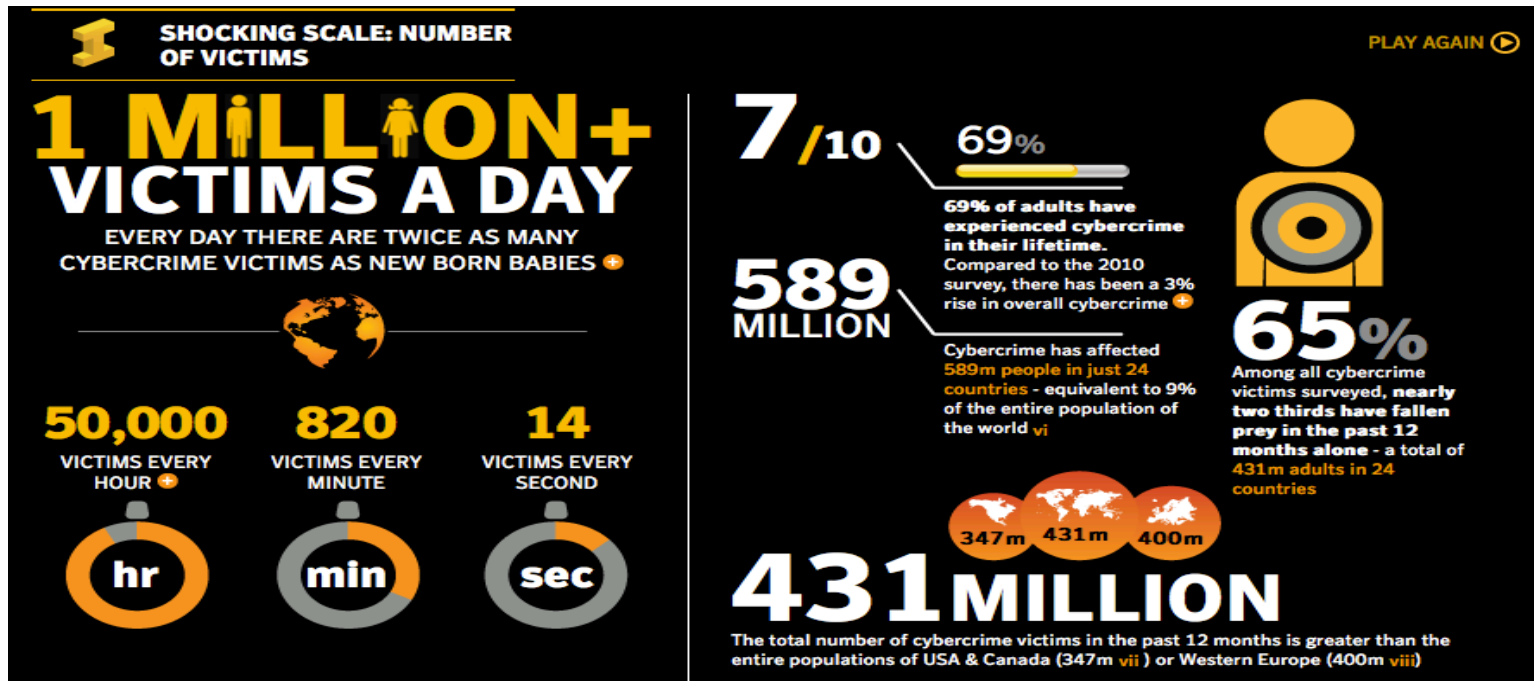
Time for Remediation Action

- 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!

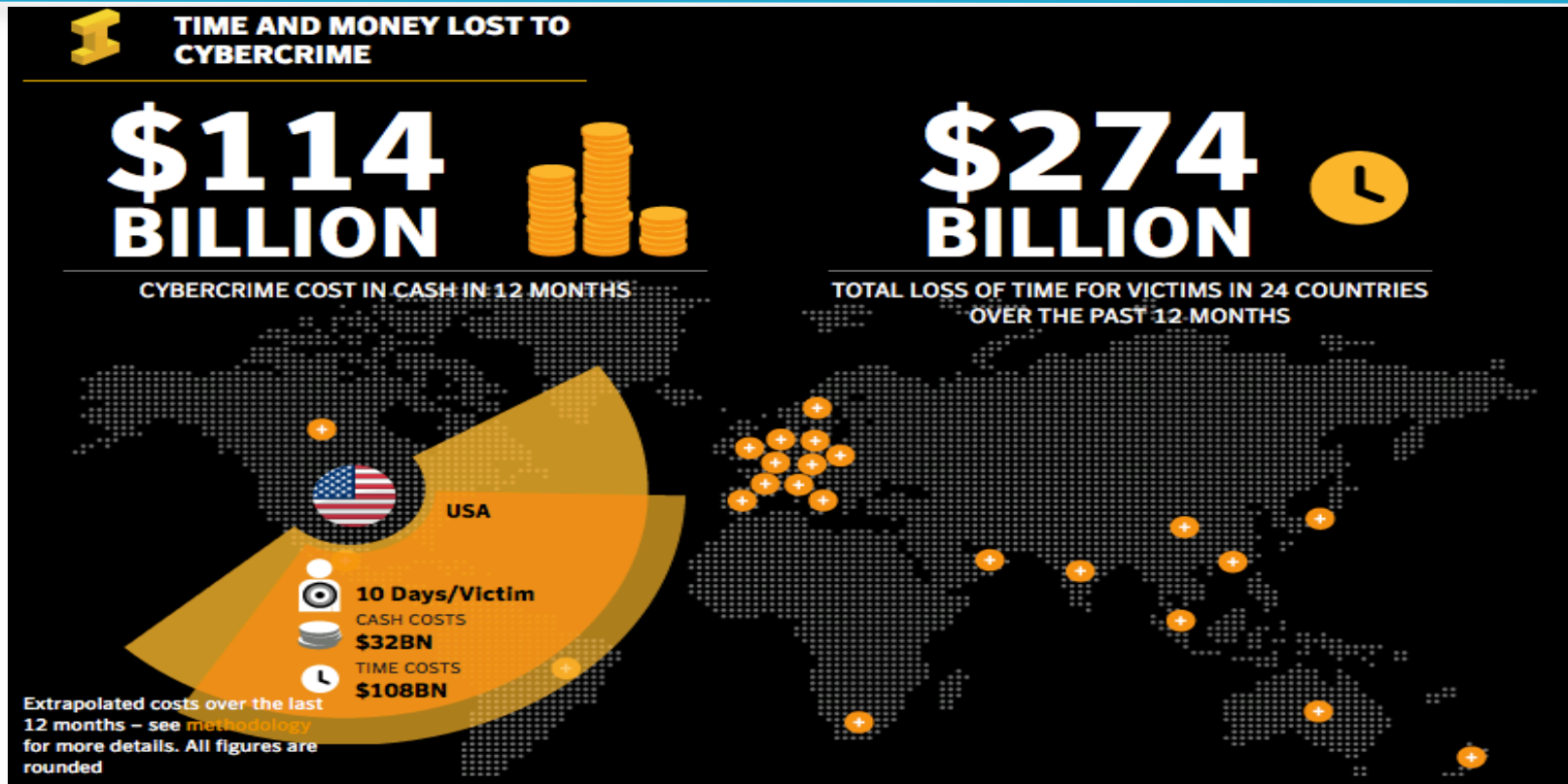
- There was a time where “users” and “customers” were blamed for doing dumb things to get their systems infected.
- When users who have up to date hardware, operating systems, software, anti-virus, anti-malware, and is mindfully doing the right think still getting infected, then we have to consider that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

This is your Network!



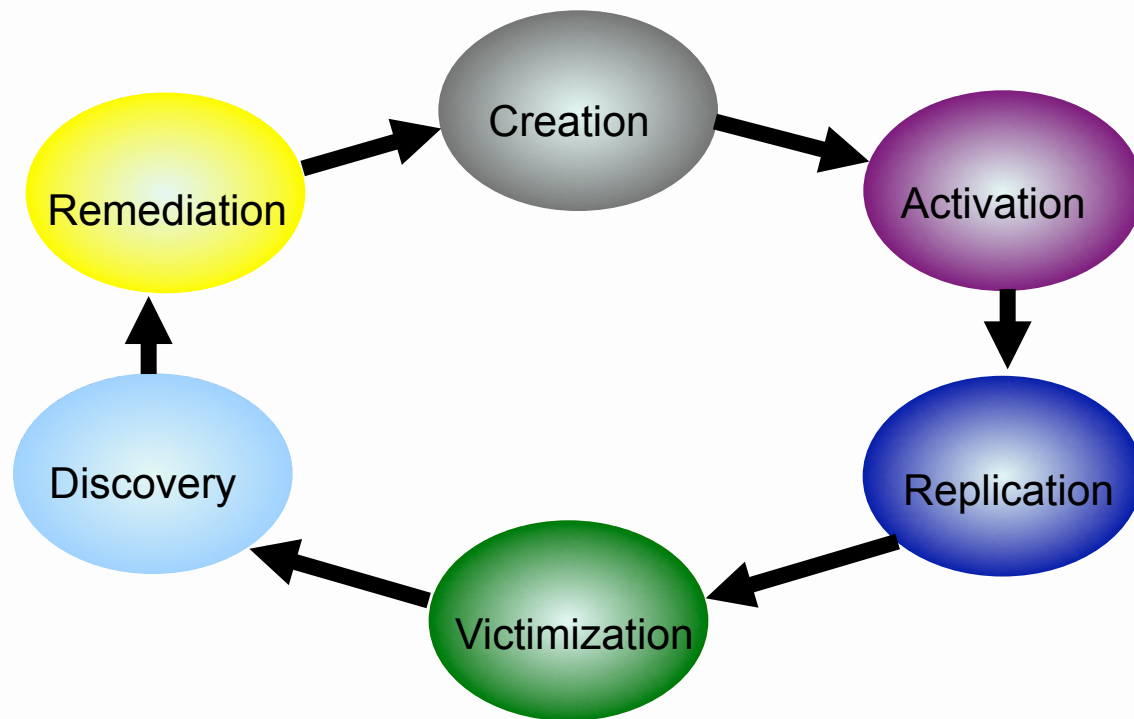
See <http://norton.com/cybercrimereport>.

Victimization Cost

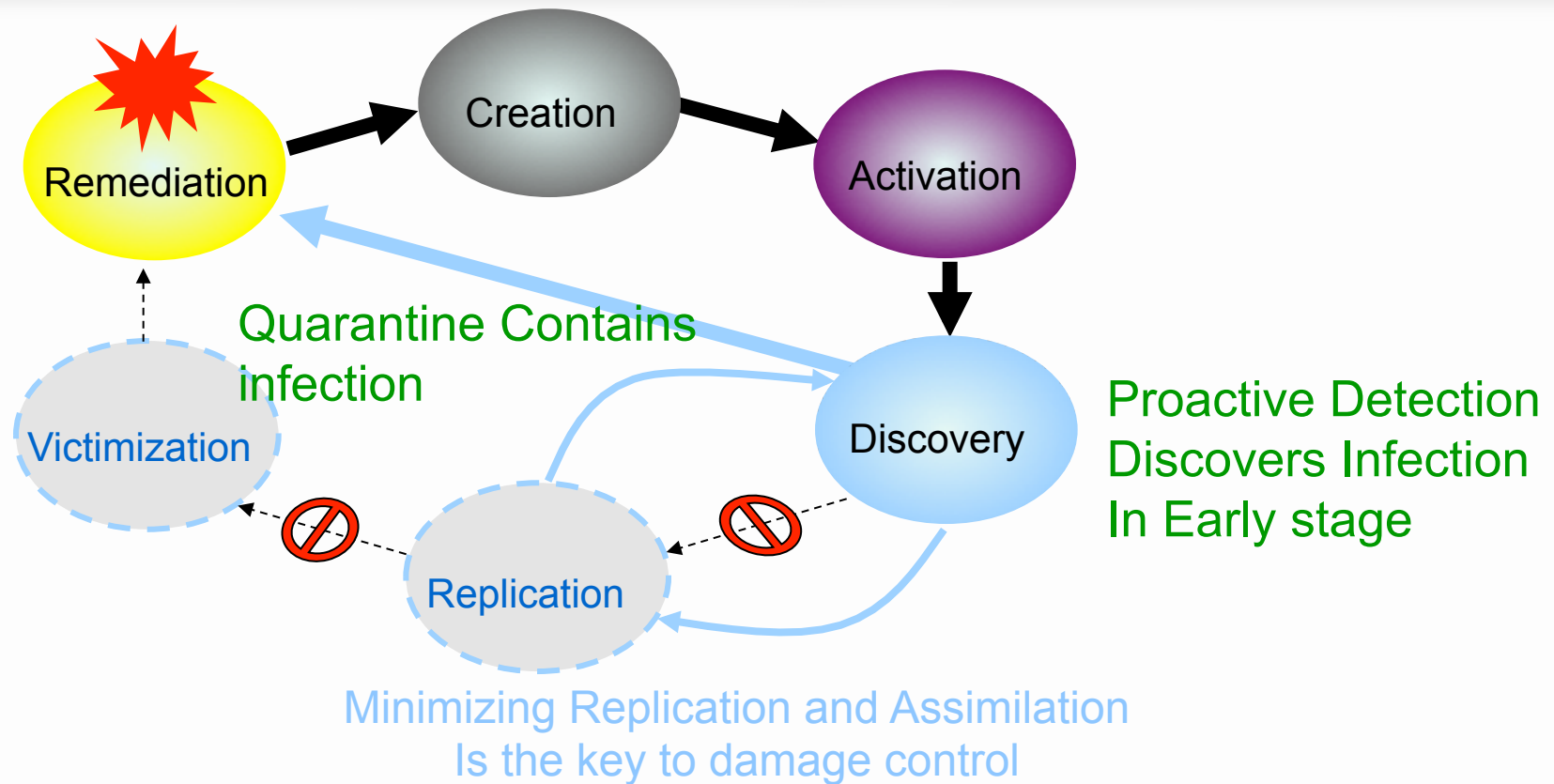


See <http://norton.com/cybercrimereport>.

Normal Malware Cycle



Remediation Shortens the Cycle



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 Remediation

- 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

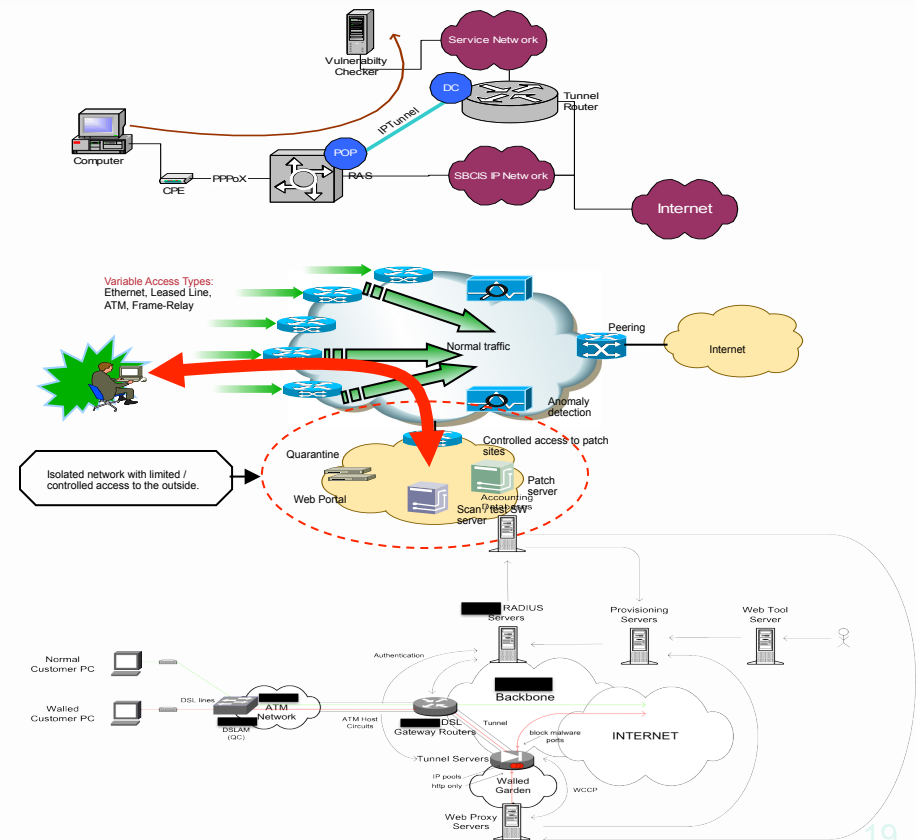
- **Notification to Public Access Points.** Alerting violated customers that are tracked from a public WIFI point may or may not be the best time to notify. A coffee shop would not be a good place to try to recover your system from a malware infection.
- **Shared IP addresses.** Many residence and businesses 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 solar 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 1/2 a decade of experience with production walled garden/quarantine systems.
- These systems work, they have not turned 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.



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 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

© slide PDF files and video copyrighted by the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)



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](https://www.m3aawg.org/contact_form)

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 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>

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

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





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).



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

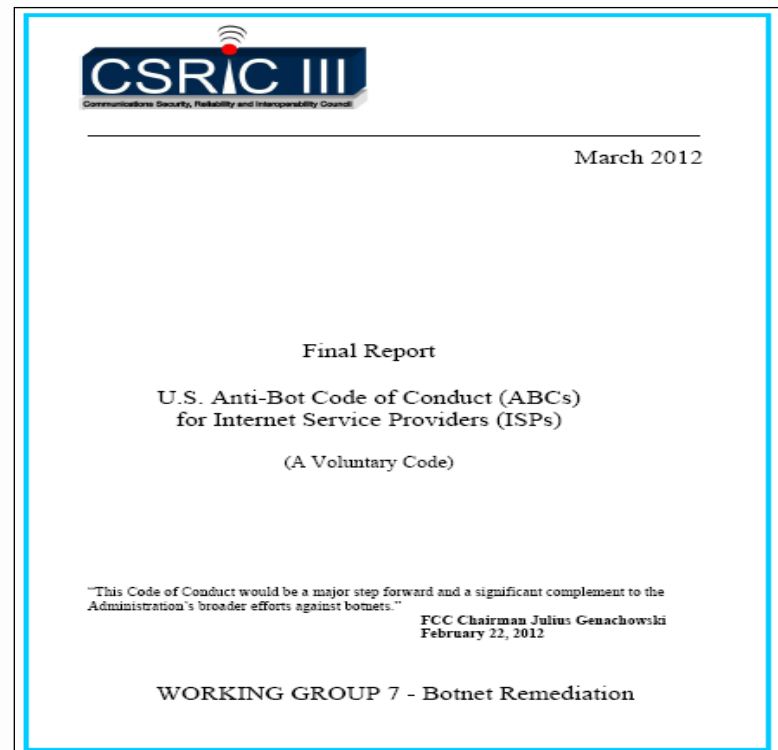
- CSRIC III is covering these areas:
 - WG 1: NG 9-1-1
 - WG 2: Next Generation Alerting
 - WG 3: E9-1-1 Location Accuracy
 - WG 4: Network Security Best Practices
 - WG 5: DNSSEC Implementation Practices for ISPs
 - WG 6: Secure BGP Deployment
 - **WG 7: Botnet Remediation**
 - WG 8: E9-1-1 Best Practices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



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>



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 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

© slide PDF files and video copyrighted by the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)



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](https://www.m3aawg.org/contact_form)