MESSAGING MALWARE MOBILE

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

Barry Raveendran Greene, bgreene@senki.org

October 22, 2012, Baltimore, Maryland, USA

M^{3}AAWG
MESSAGING MALWARE MOBILE

M^{3}AAWG Training Video Series

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

(more than 2.25 hours of training)

This is Segment 3 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)**

M³AAWG
MESSAGING MALWARE MOBILE

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

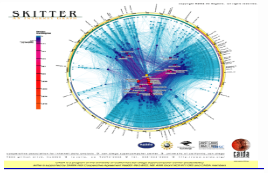
M3AAWG
MESSAGING MALWARE MOBILE

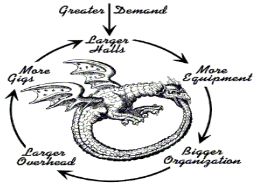
Barry Greene has over 30 years industry experience including having served as president of the ISC (Internet Systems Consortium). He is a pioneer in service provider security and operational security reaction teams.

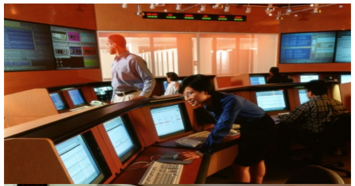
Barry is currently a participant on the U.S. Federal Communications Commission's (FCC's) Communications Security, Reliability and Interoperability Council (CSRIC).

Understanding the Threat

A Typical Cyber-Criminal’s Work Day







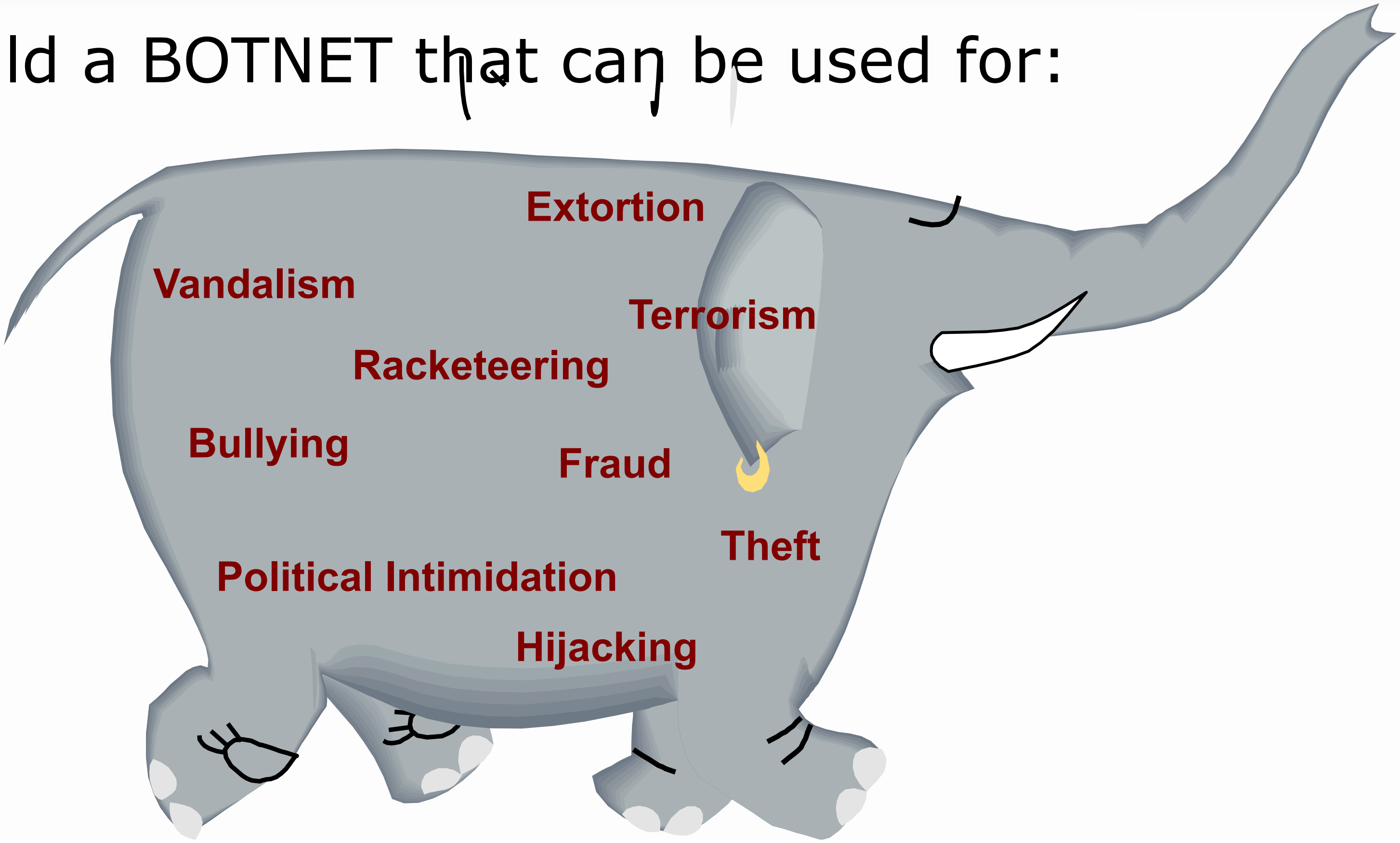
Agenda

- 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:



Extortion

Vandalism

Terrorism

Racketeering

Bullying

Fraud

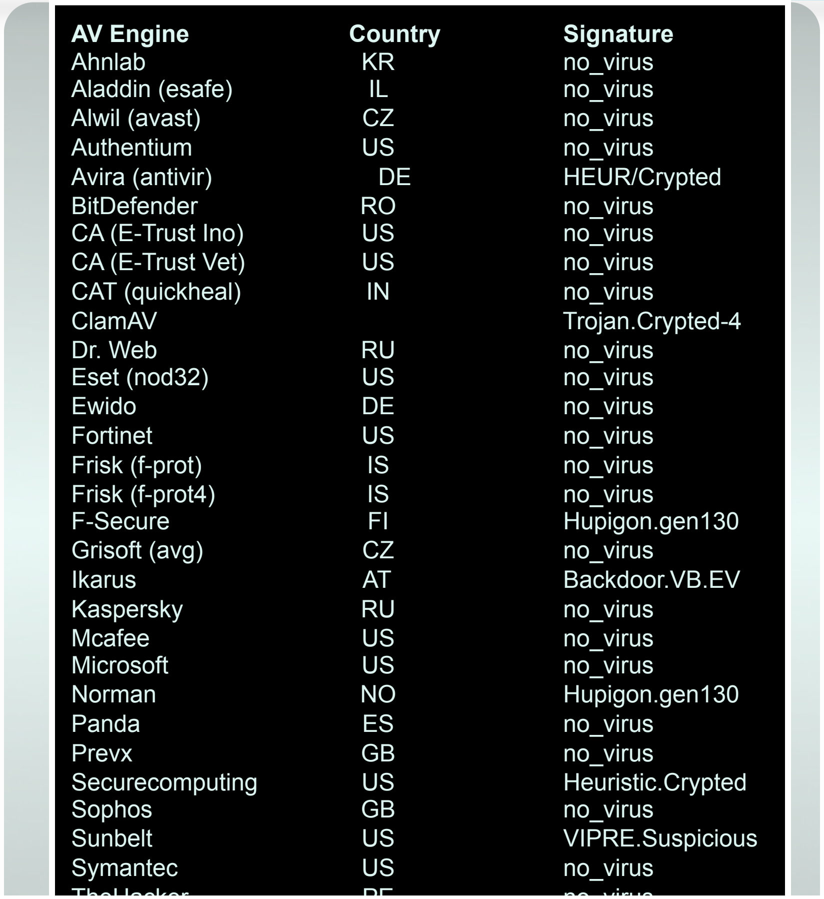
Theft

Political Intimidation

Hijacking

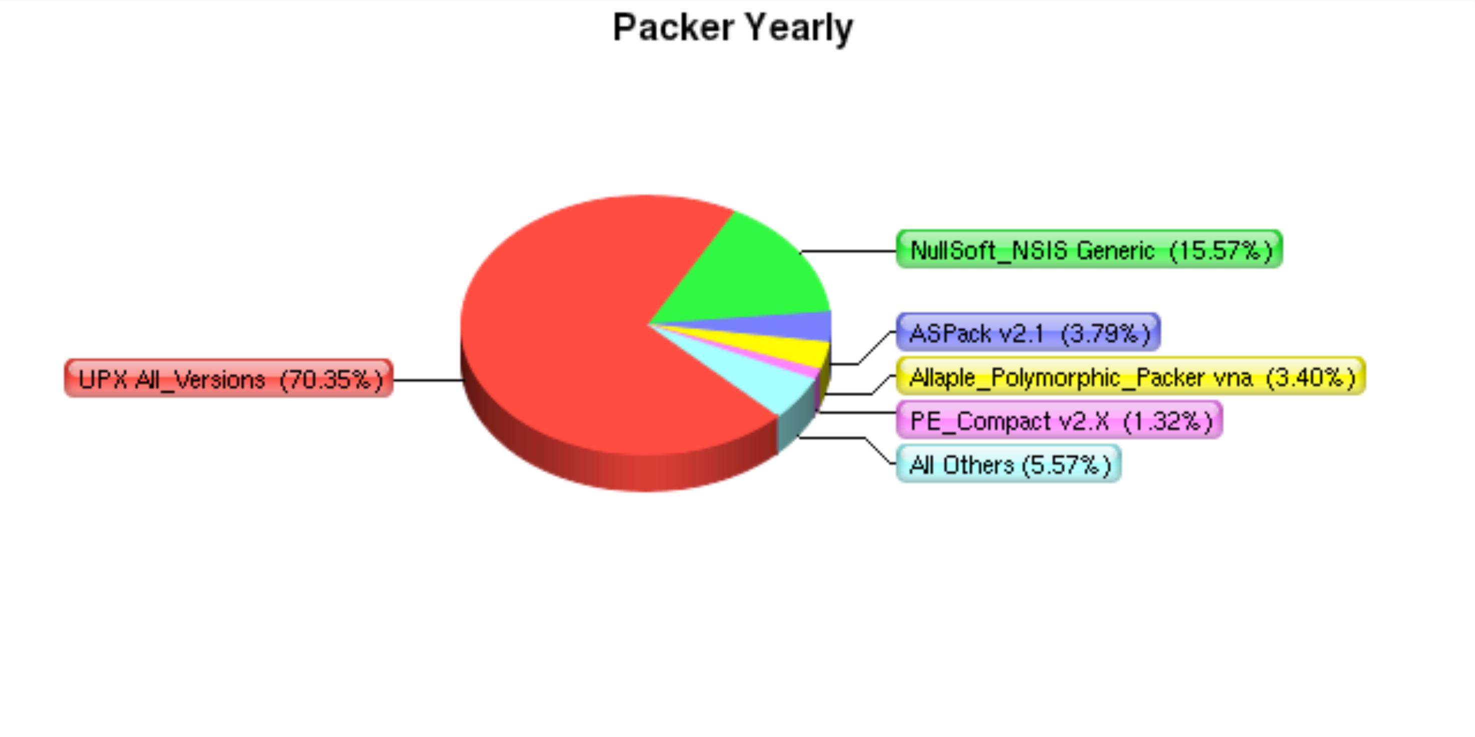
But What About Anti Virus?

- 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
TheHacker	PE	no_virus

What Packers Are Used?

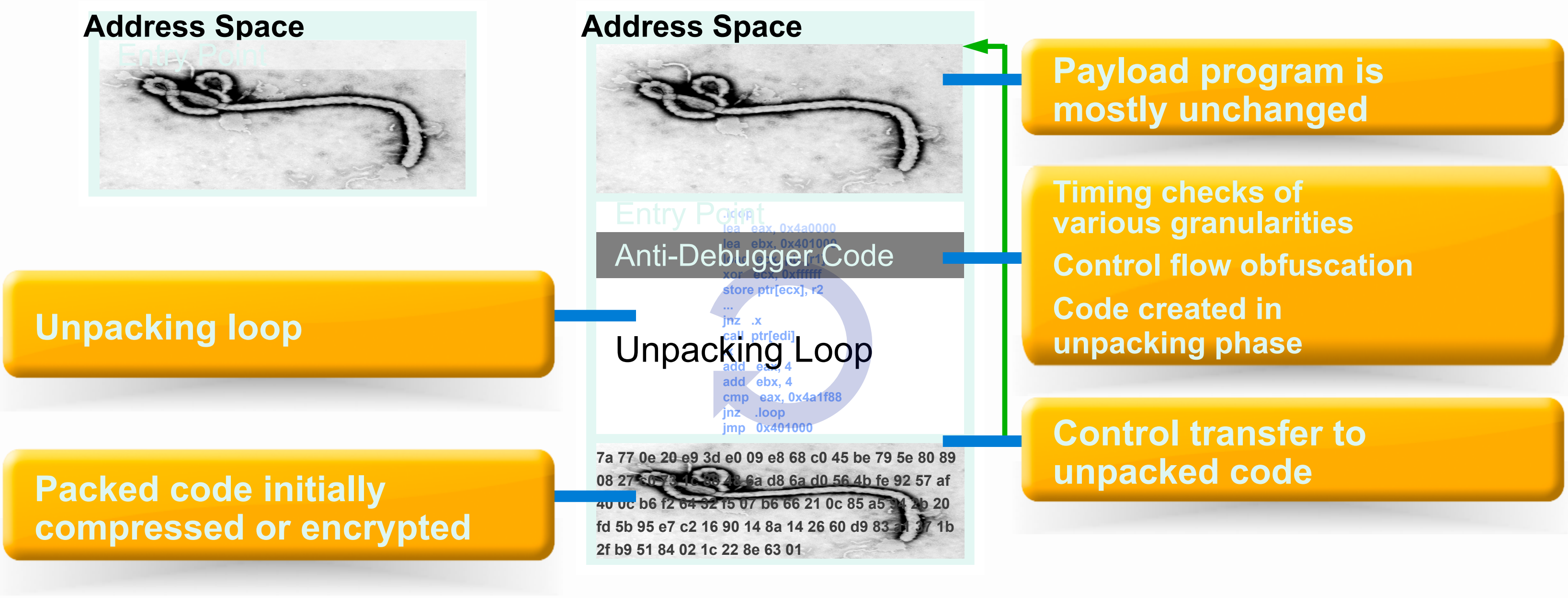


http://www.shadowserver.org/wiki/pmwiki.php/Stats/PackerStatistics

A Packed Malware Binary

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

Original Binary **Packed Binary**



```
.loop
lea   eax, 0x4a0000
lea   ebx, 0x401000
load  ecx, ptr[r1]
xor   ecx, 0xffffff
store ptr[ecx], r2
...
jnz   .x
call  ptr[edi]
.x
add   eax, 4
add   ebx, 4
cmp   eax, 0x4a1f88
jnz   .loop
jmp   0x401000
```

```
7a 77 0e 20 e9 3d e0 09 e8 68 c0 45 be 79 5e 80 89
08 27 c0 73 1c 88 48 6a d8 6a d0 56 4b fe 92 57 af
40 0c b6 f2 64 32 f5 07 b6 66 21 0c 85 a5 94 2b 20
fd 5b 95 e7 c2 16 90 14 8a 14 26 60 d9 83 a1 37 1b
2f b9 51 84 02 1c 22 8e 63 01
```

Payload program is mostly unchanged

Timing checks of various granularities

Control flow obfuscation

Code created in unpacking phase

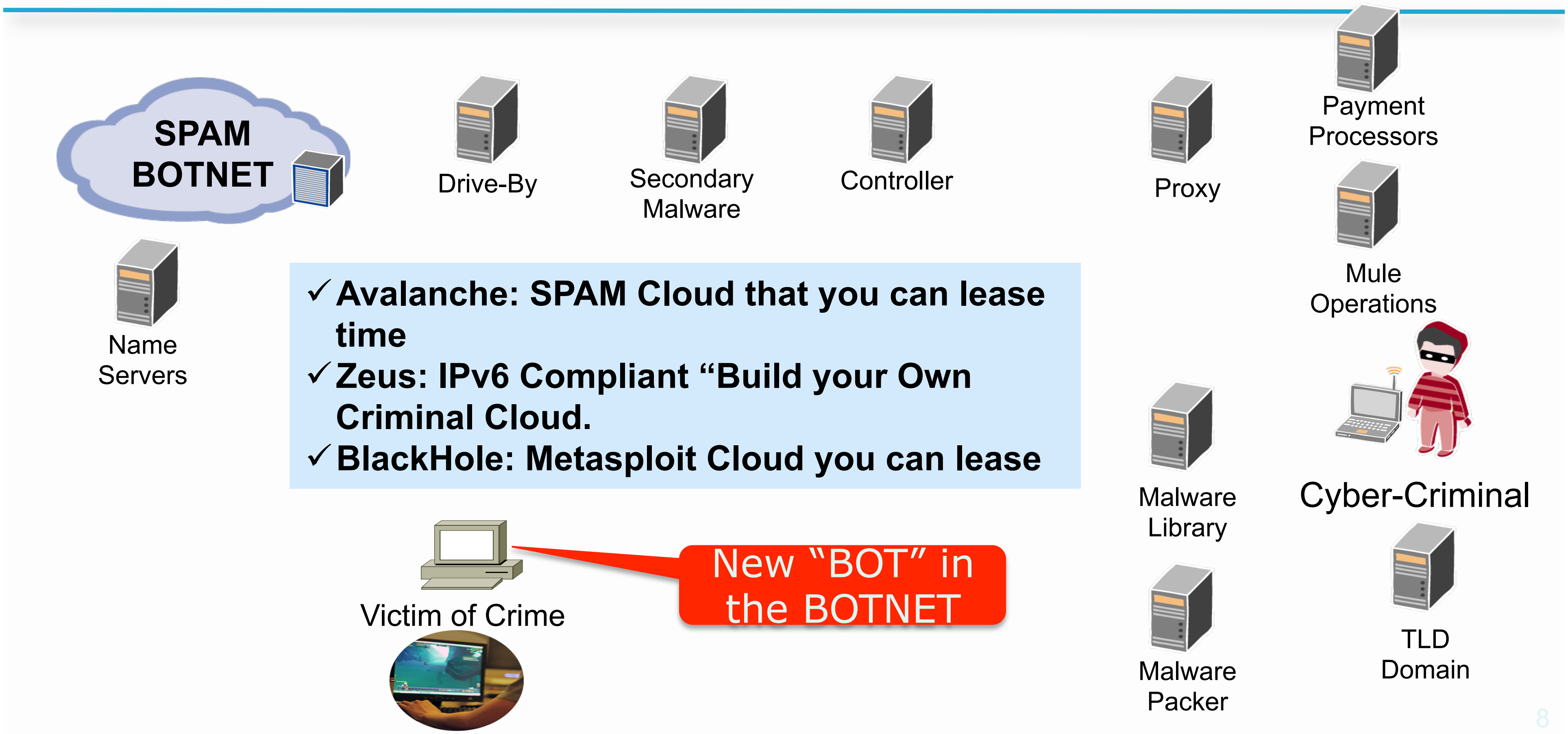
Control transfer to unpacked code

Unpacking loop

Packed code initially compressed or encrypted

Courtesy of Kevin Roundy (Paradyn Project)

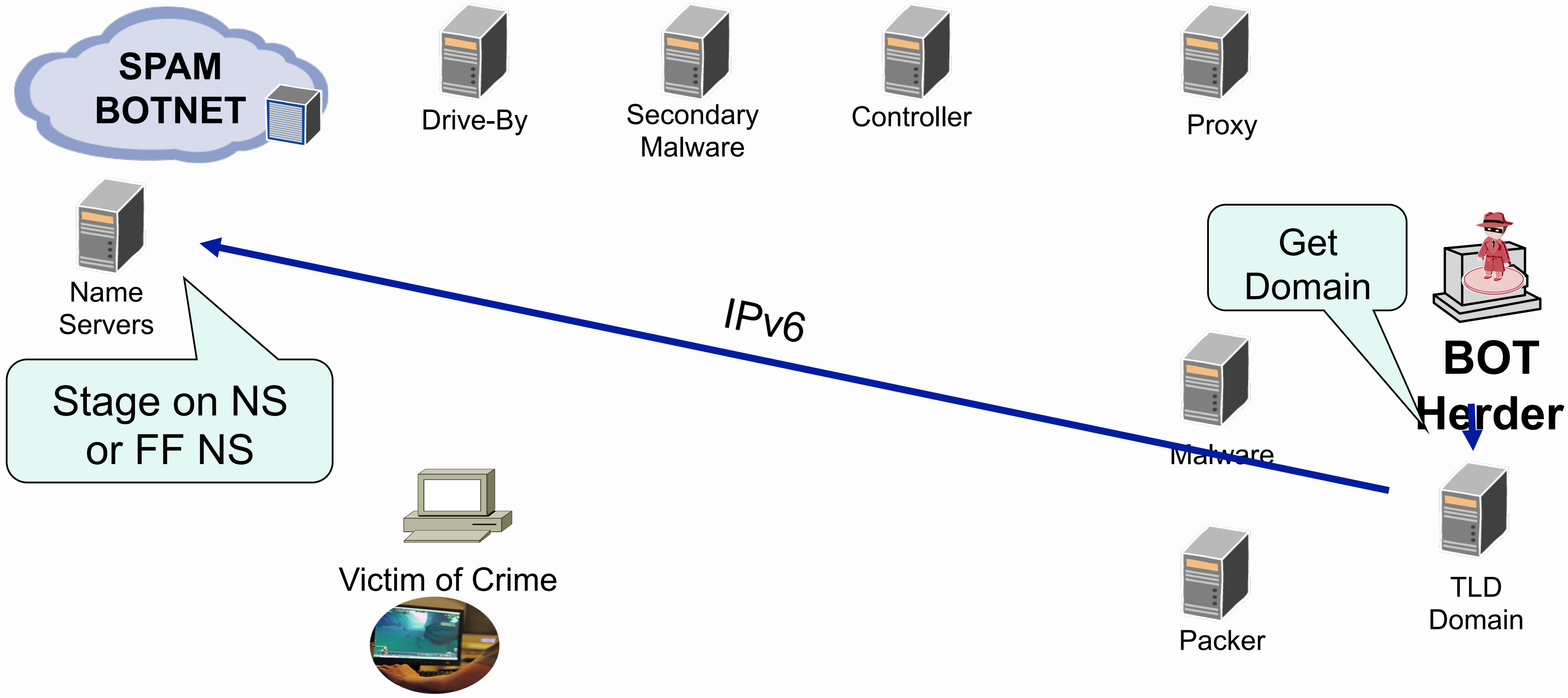
Components of the Criminal Cloud



- ✓ **Avalanche: SPAM Cloud that you can lease time**
- ✓ **Zeus: IPv6 Compliant “Build your Own Criminal Cloud.**
- ✓ **BlackHole: Metasploit Cloud you can lease**

New “BOT” in the BOTNET

Stage Domain Name



SPAM BOTNET

Drive-By

Secondary Malware

Controller

Proxy

Name Servers

Stage on NS or FF NS

IPv6

Get Domain

BOT Herder

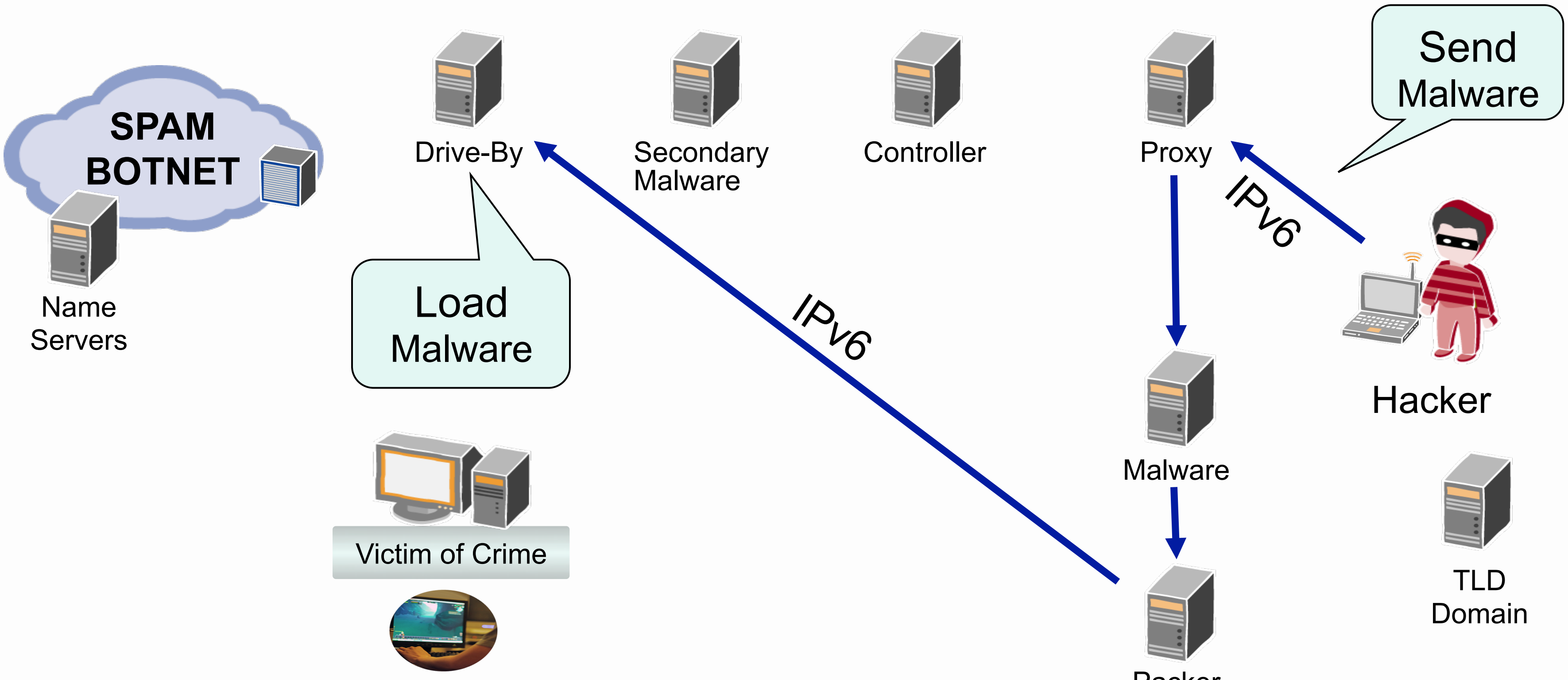
Malware

Victim of Crime

Packer

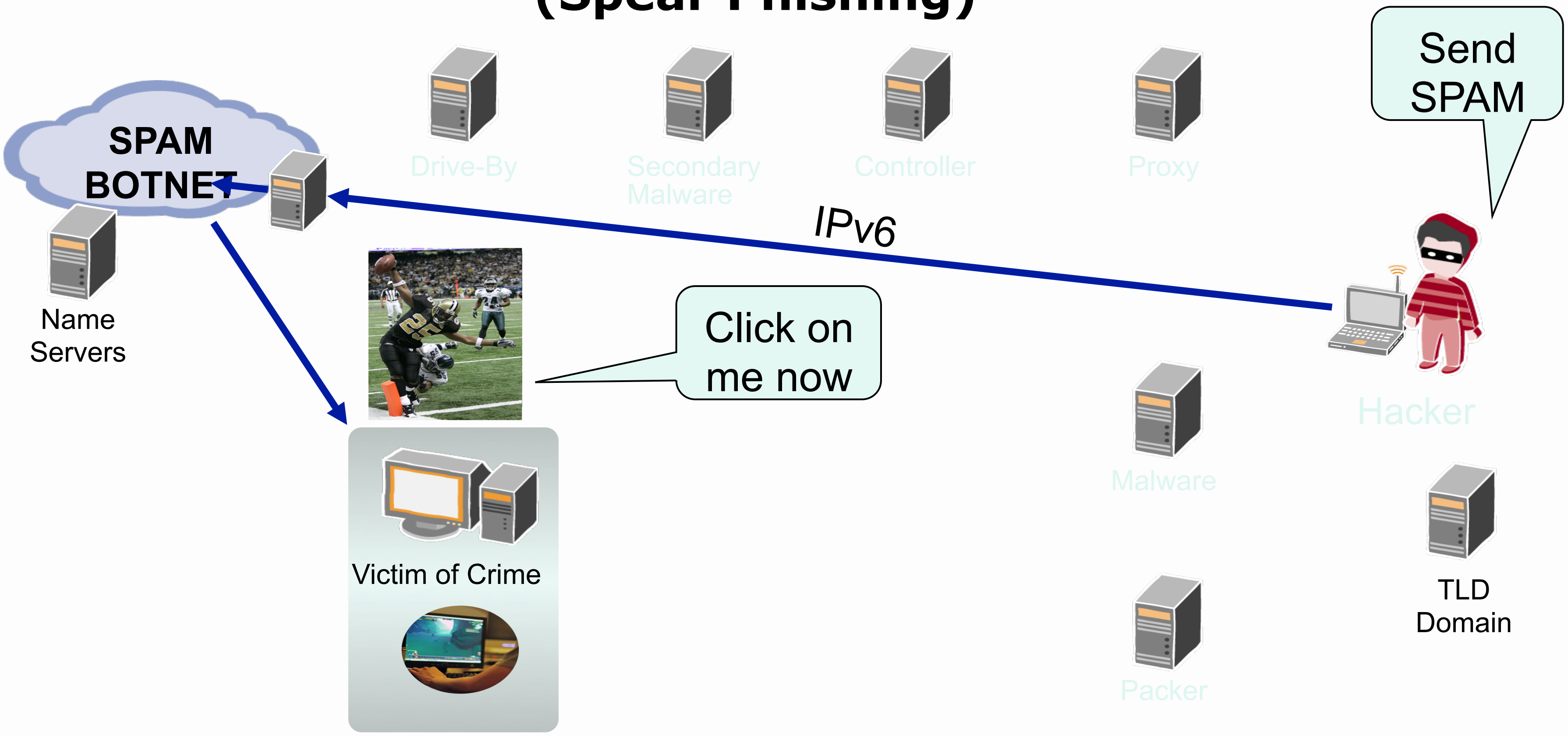
TLD Domain

Prepare Drive-By



Social Engineered SPAM to Get People to Click

(Spear Phishing)



Send SPAM

SPAM BOTNET

Name Servers

Drive-By

Secondary Malware

Controller

Proxy

IPv6

Click on me now

Hacker

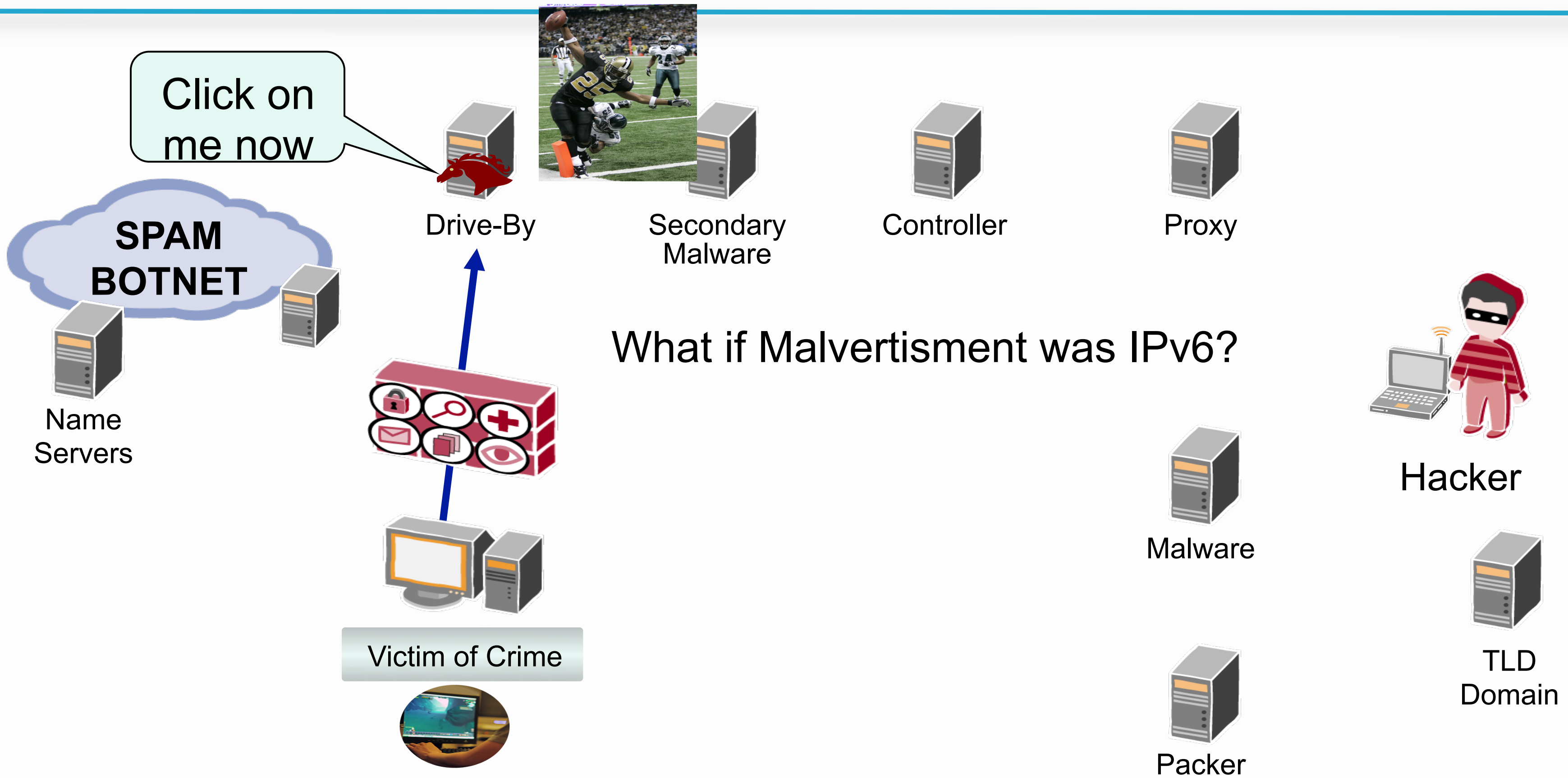
Victim of Crime

Malware

TLD Domain

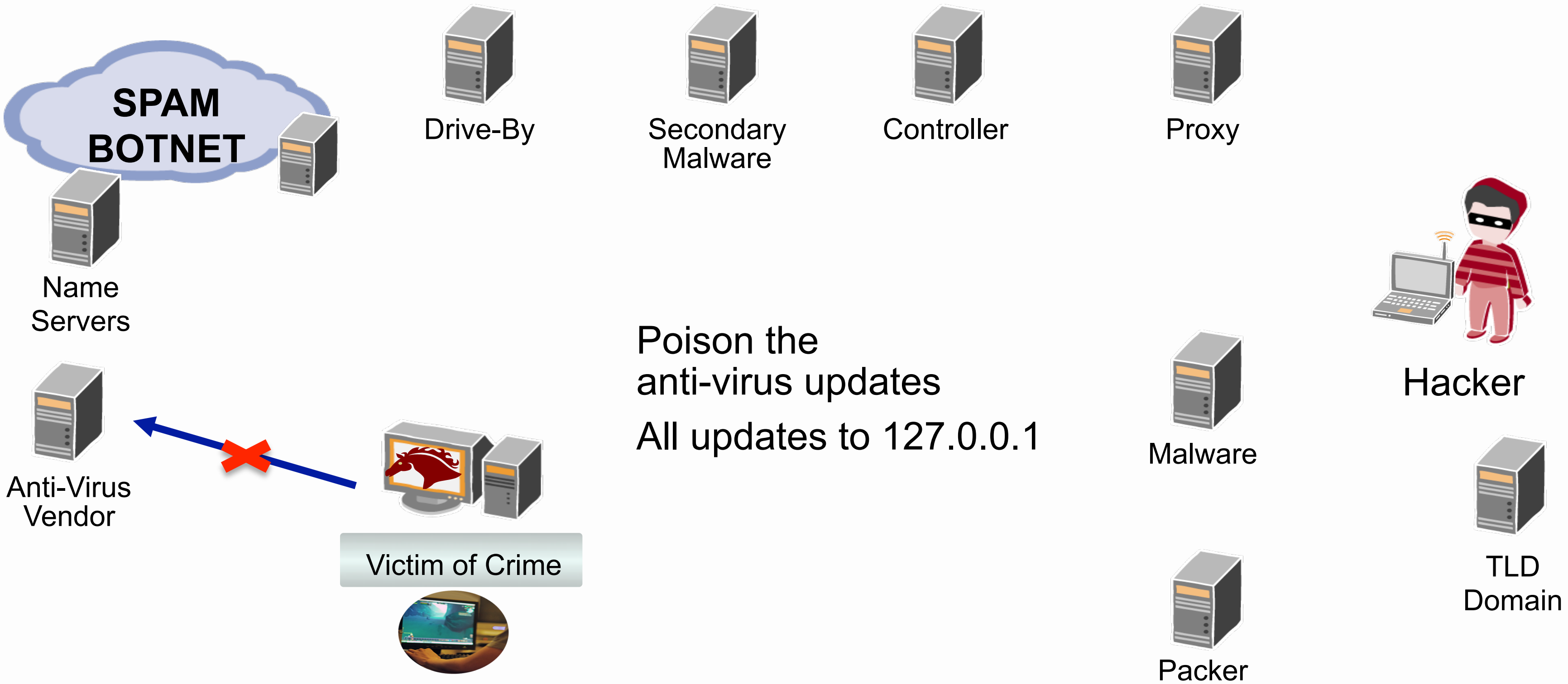
Packer

Drive-By Violation



What if Malvertisment was IPv6?

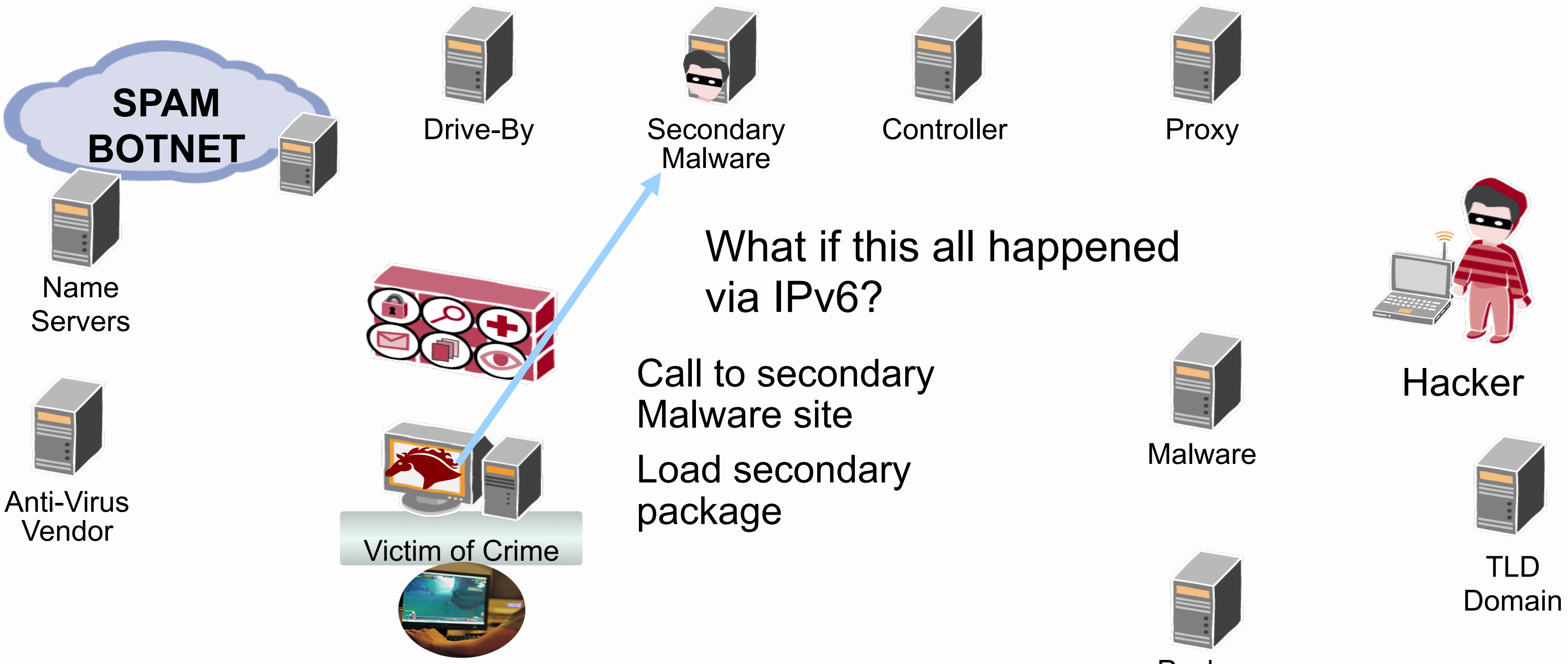
Poison Anti-Virus Updates



Poison the
anti-virus updates

All updates to 127.0.0.1

Prepare Violated Computer

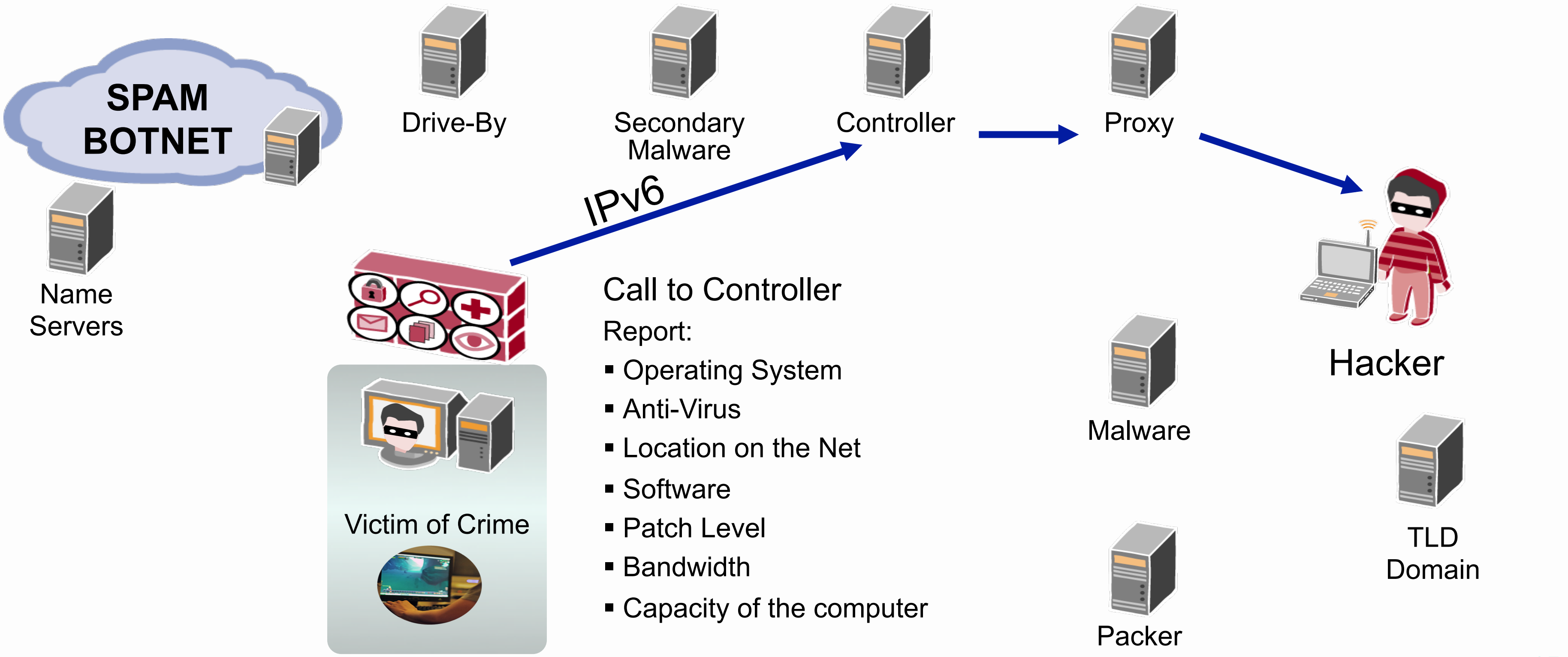


What if this all happened via IPv6?

Call to secondary Malware site

Load secondary package

Call Home

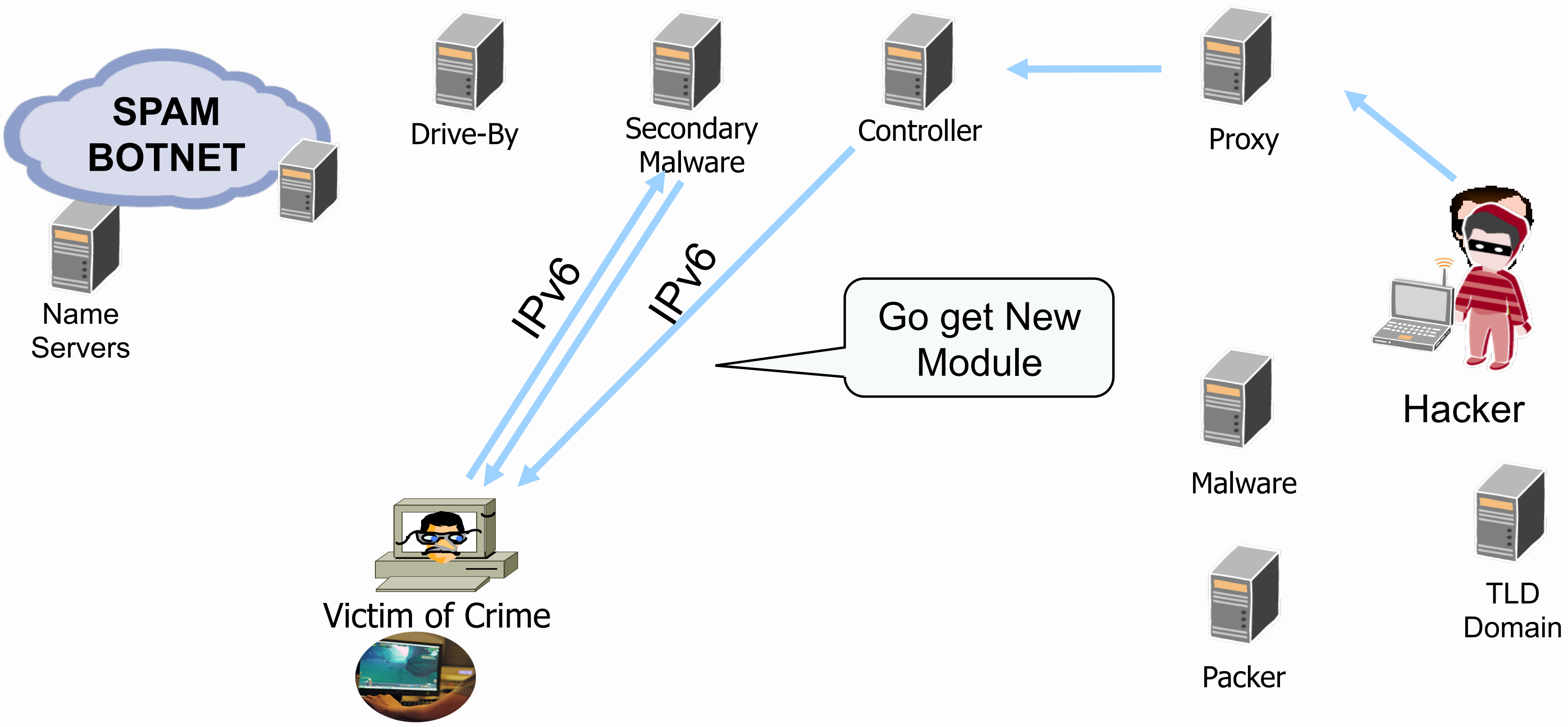


Call to Controller

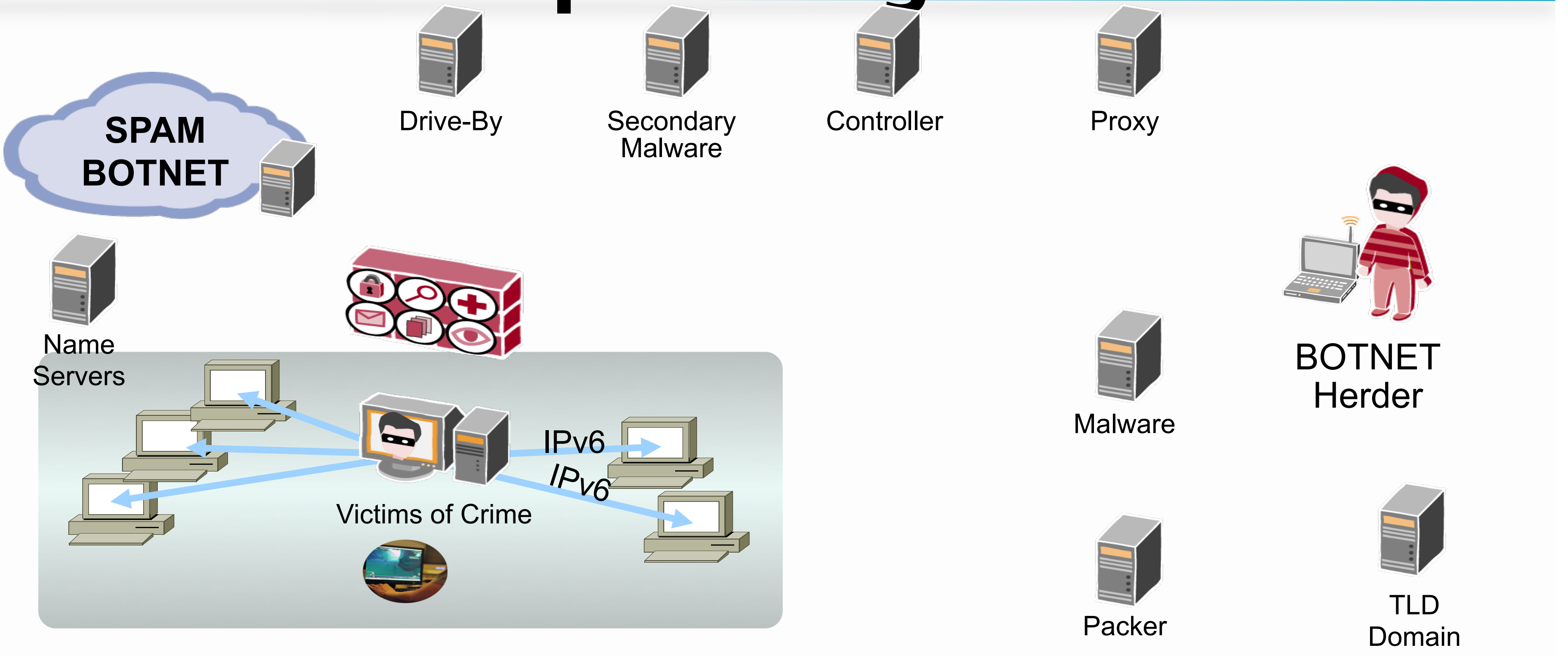
Report:

- Operating System
- Anti-Virus
- Location on the Net
- Software
- Patch Level
- Bandwidth
- Capacity of the computer

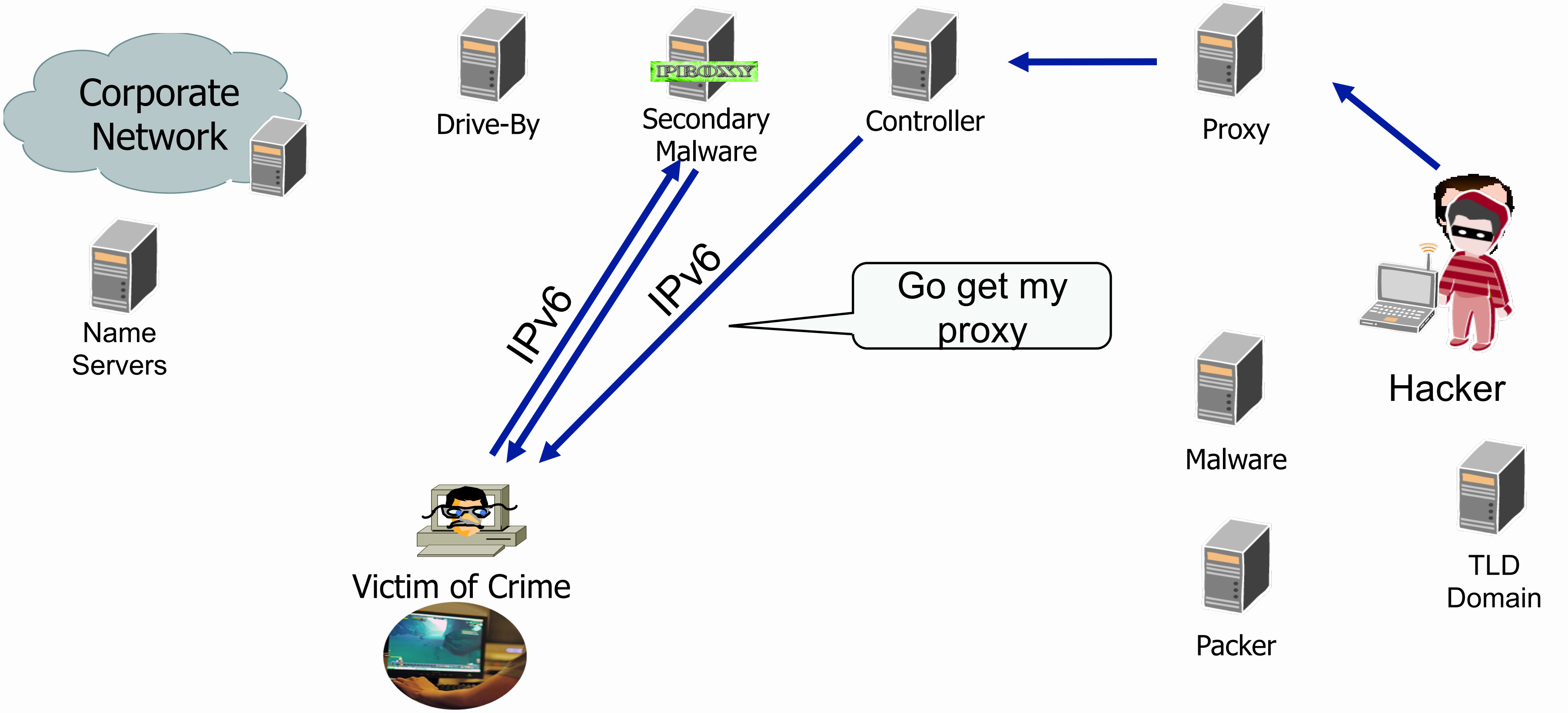
Load Custom Malware



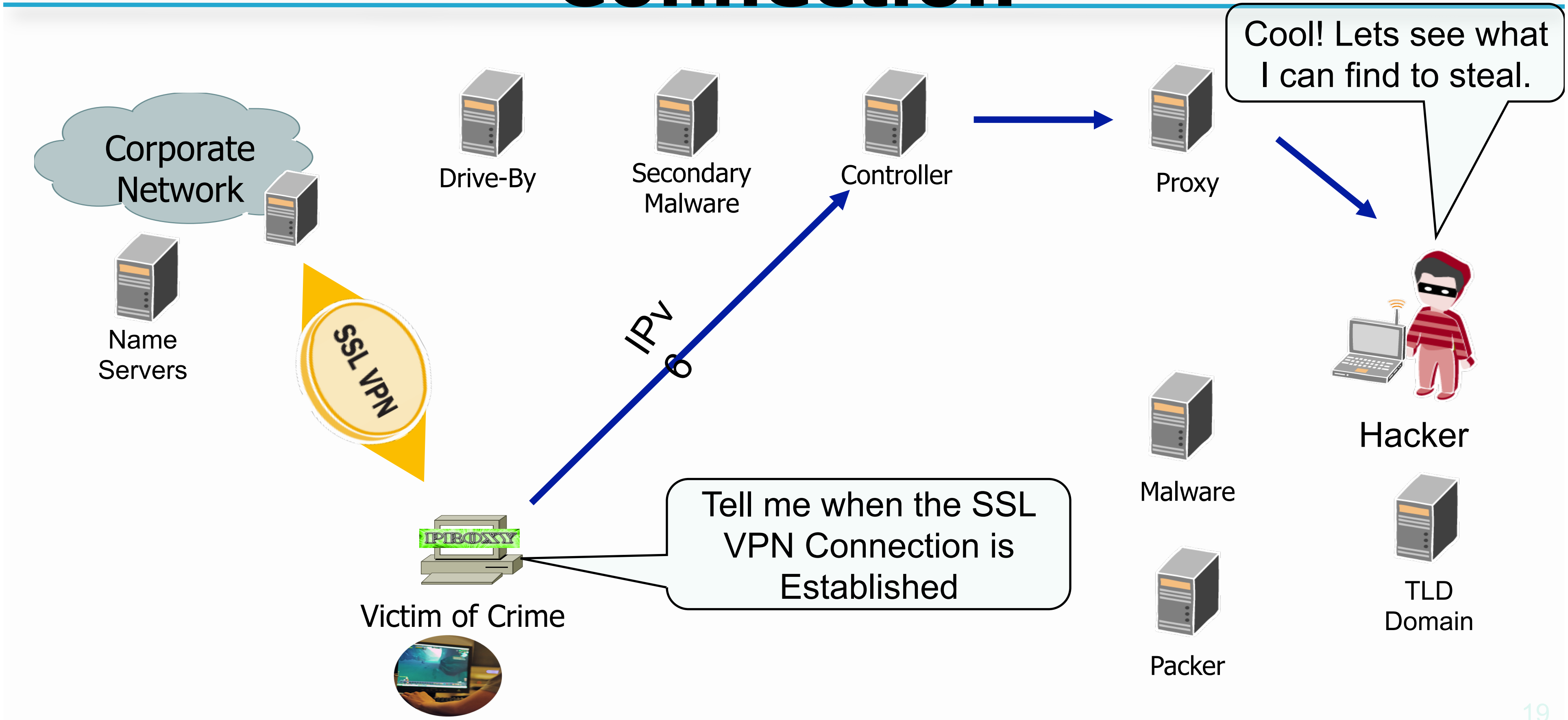
Start Worming, Scanning, & Spreading



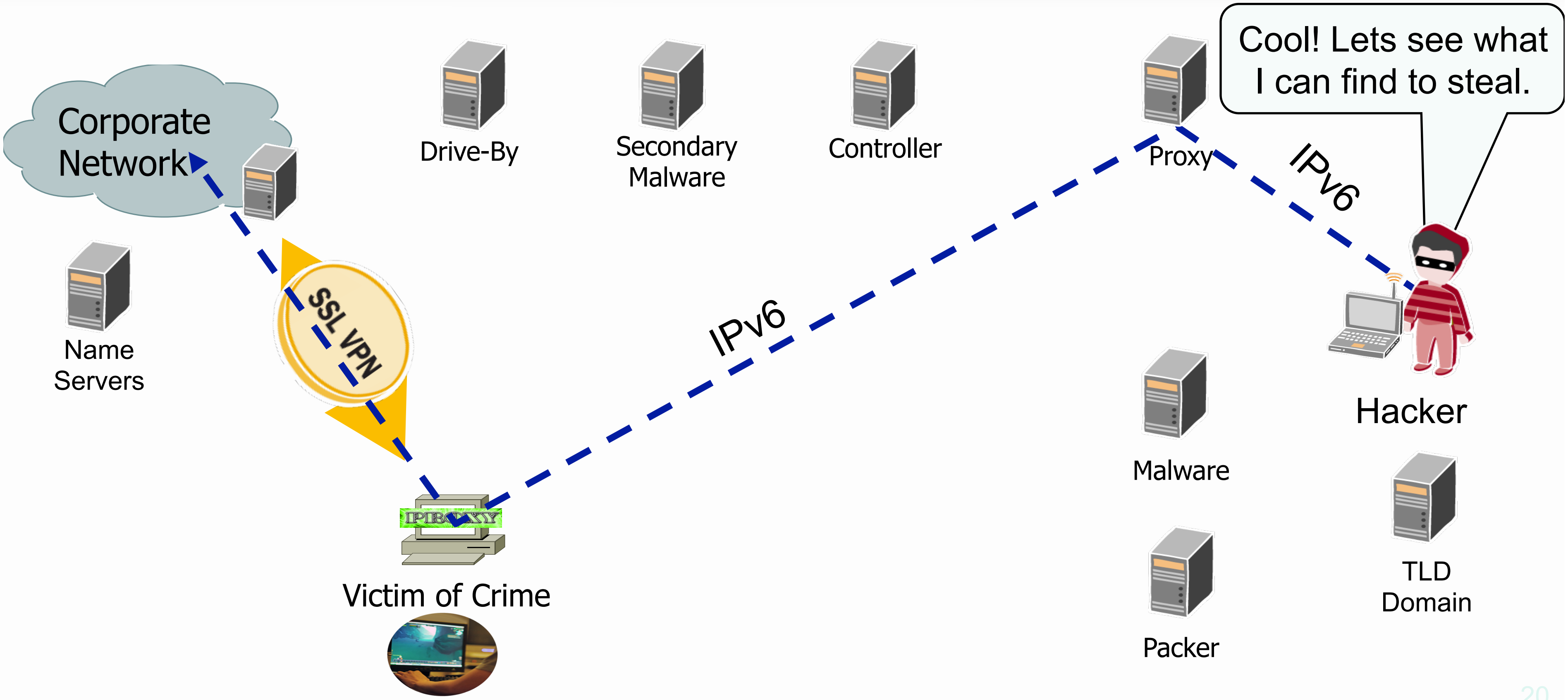
Load a Proxy with Trigger



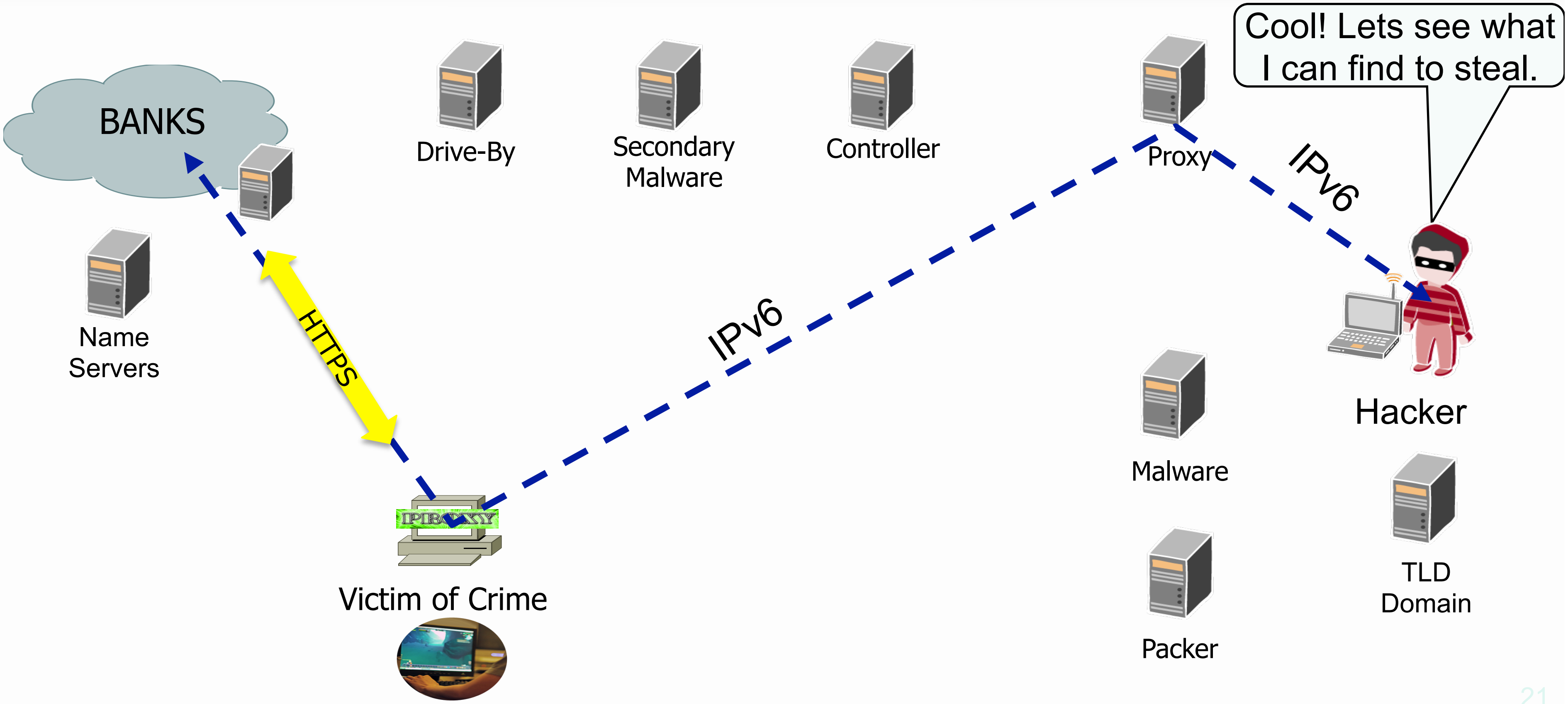
Watch for the SSL VPN Connection



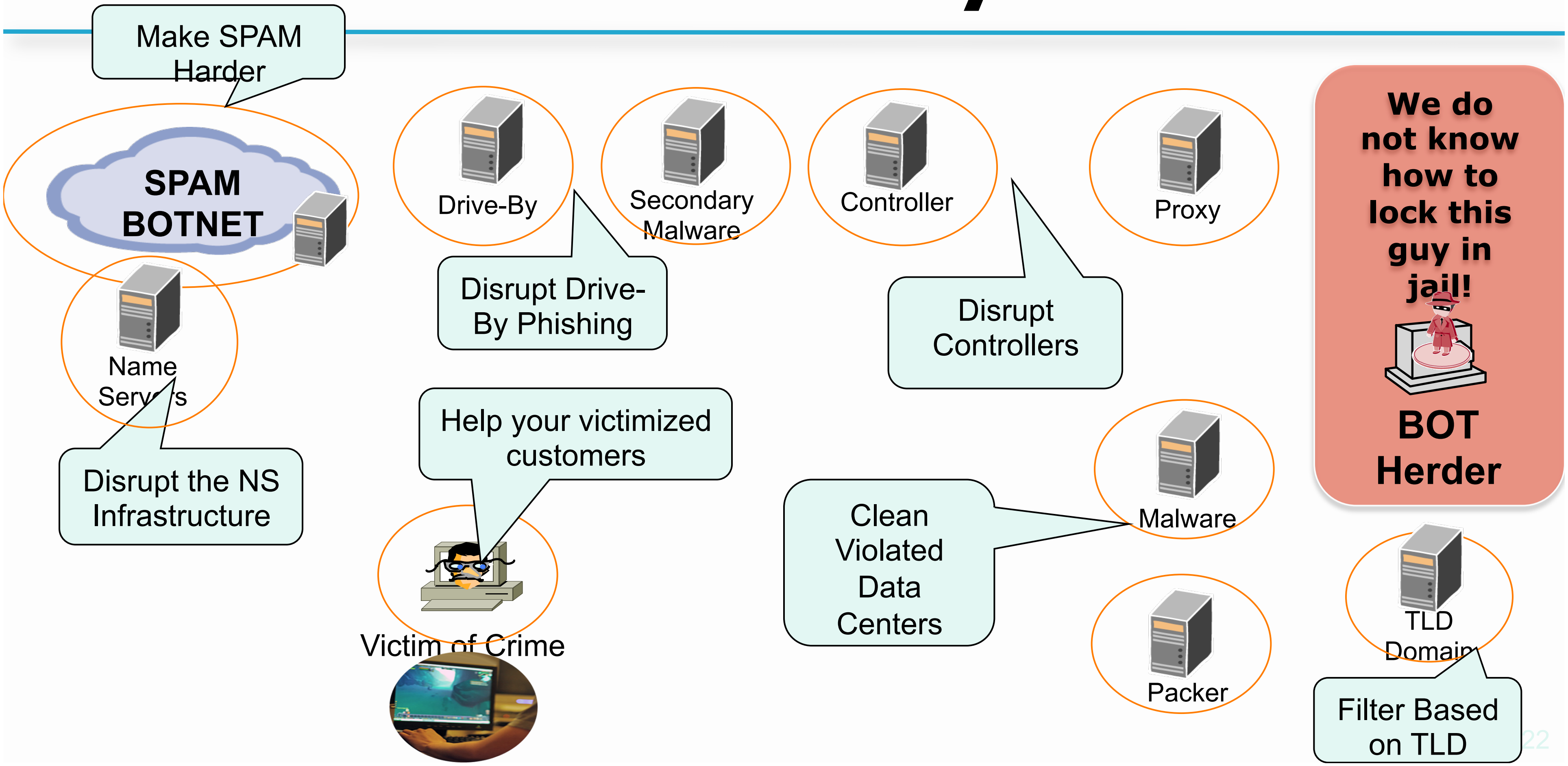
Set up the Proxy Tunnel



Proxy Behind the Bank Login



OPSEC Community’s Action



Make SPAM Harder

SPAM BOTNET

Name Servers

Drive-By

Secondary Malware

Controller

Proxy

We do not know how to lock this guy in jail!

BOT Herder

Disrupt Drive-By Phishing

Disrupt Controllers

Disrupt the NS Infrastructure

Help your victimized customers

Victim of Crime

Clean Violated Data Centers

Malware

Packer

TLD Domain

Filter Based on TLD

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

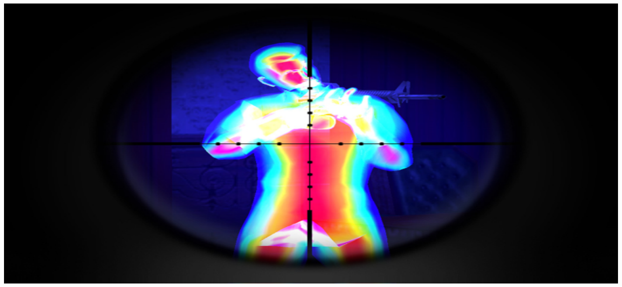
Key Take Away – The Good Guys are the Big Part of the Security Problem

- 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

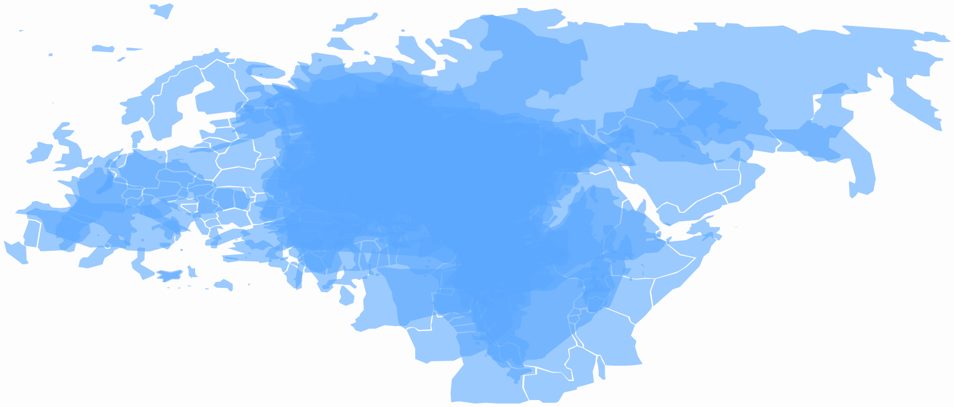


This is nice to know

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?

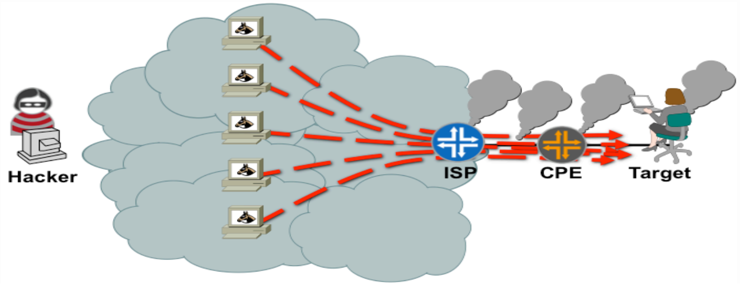
Why Use DNS "Noisy" Poisoning when it is easier to violate a ccTLD?

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

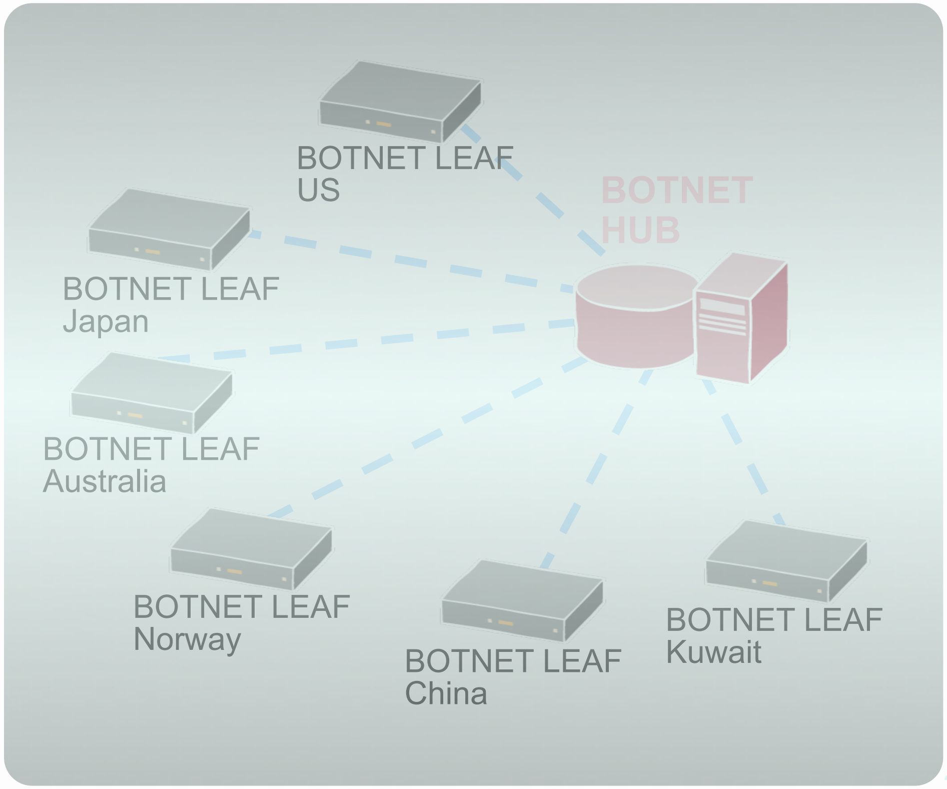
Principle 4: If You Cannot Take Out The Target…

- 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

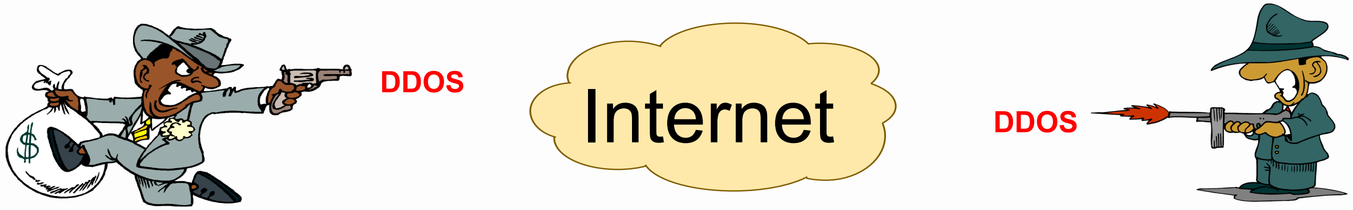
- If your activity is something that would not want everyone around you to know about, then you are a miscreant target
- Why? Cause when you become a victim, you are not motivated to call the authorities
- Examples:
  - Someone addicted to gambling is targeted via a Phishing site
  - Someone addicted 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.

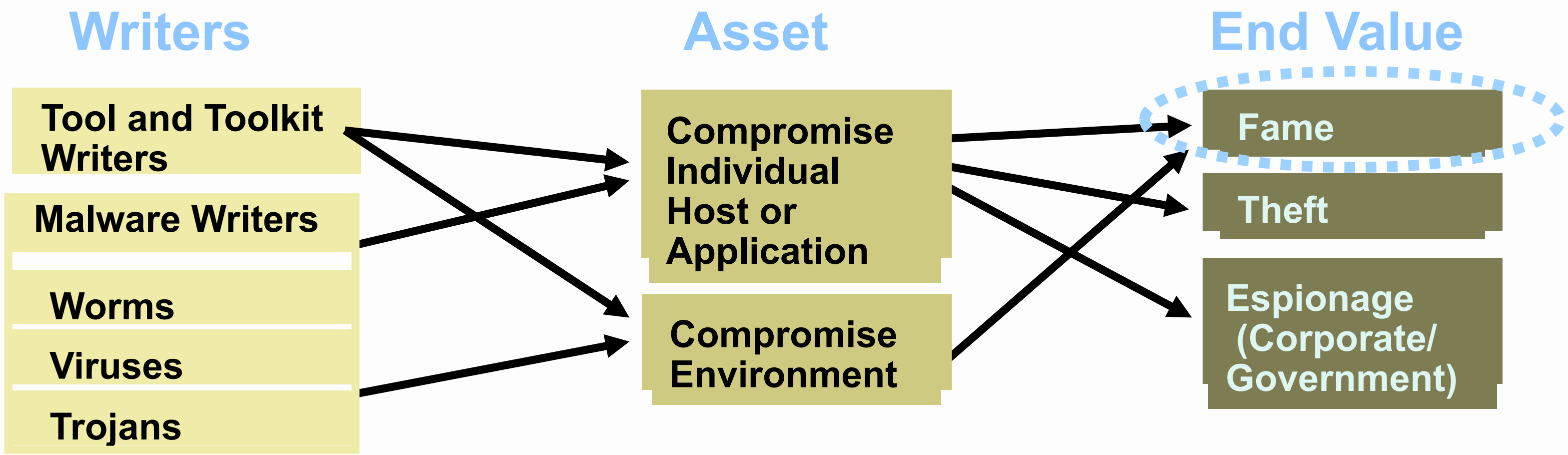
Enduring Financial Opportunities

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

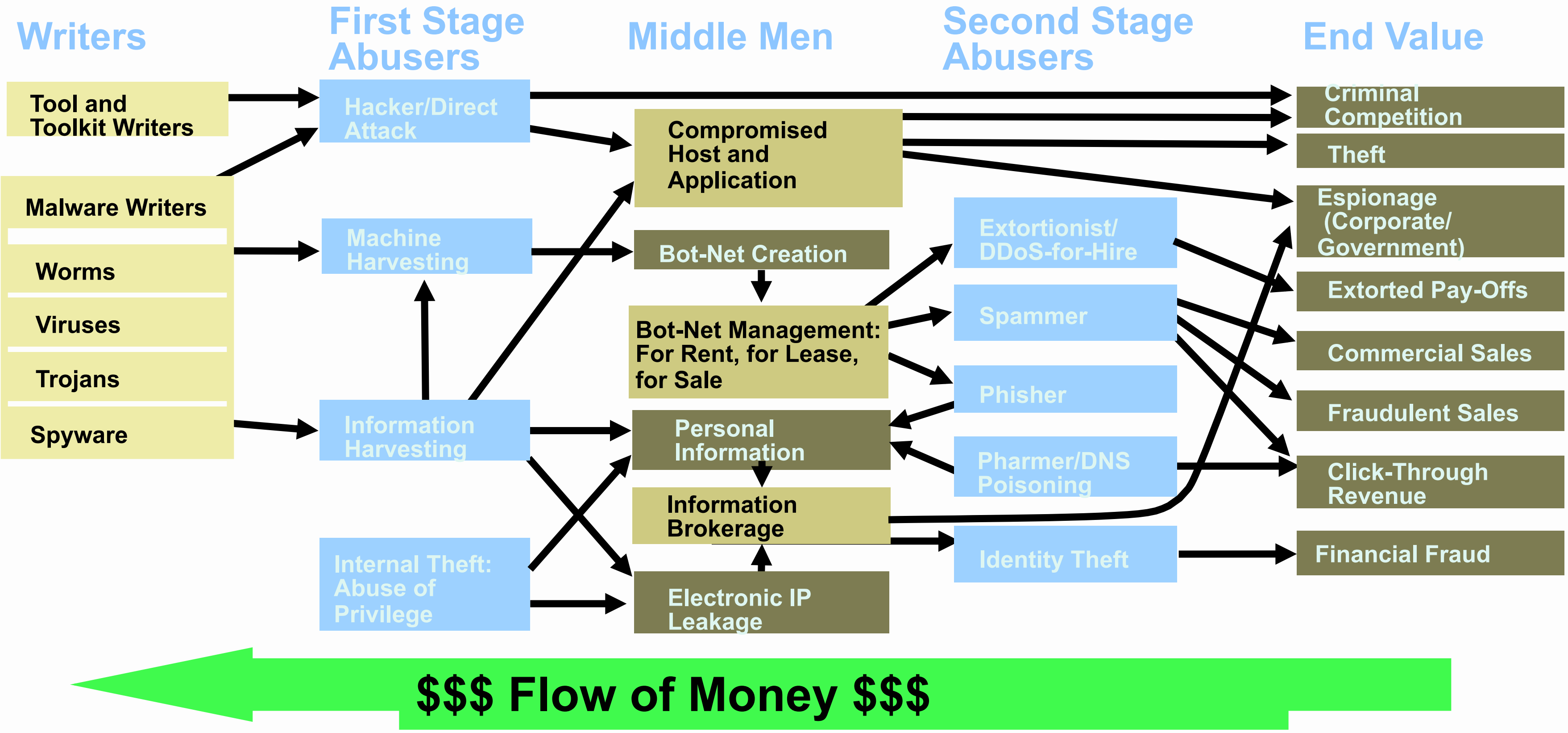
Enduring *criminal* financial opportunities:

- 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



Writers

- Tool and Toolkit Writers
- Malware Writers
- Worms
- Viruses
- Trojans
- Spyware

First Stage Abusers

- Hacker/Direct Attack
- Machine Harvesting
- Information Harvesting
- Internal Theft: Abuse of Privilege

Middle Men

- Compromised Host and Application
- Bot-Net Creation
- Bot-Net Management: For Rent, for Lease, for Sale
- Personal Information
- Information Brokerage
- Electronic IP Leakage

Second Stage Abusers

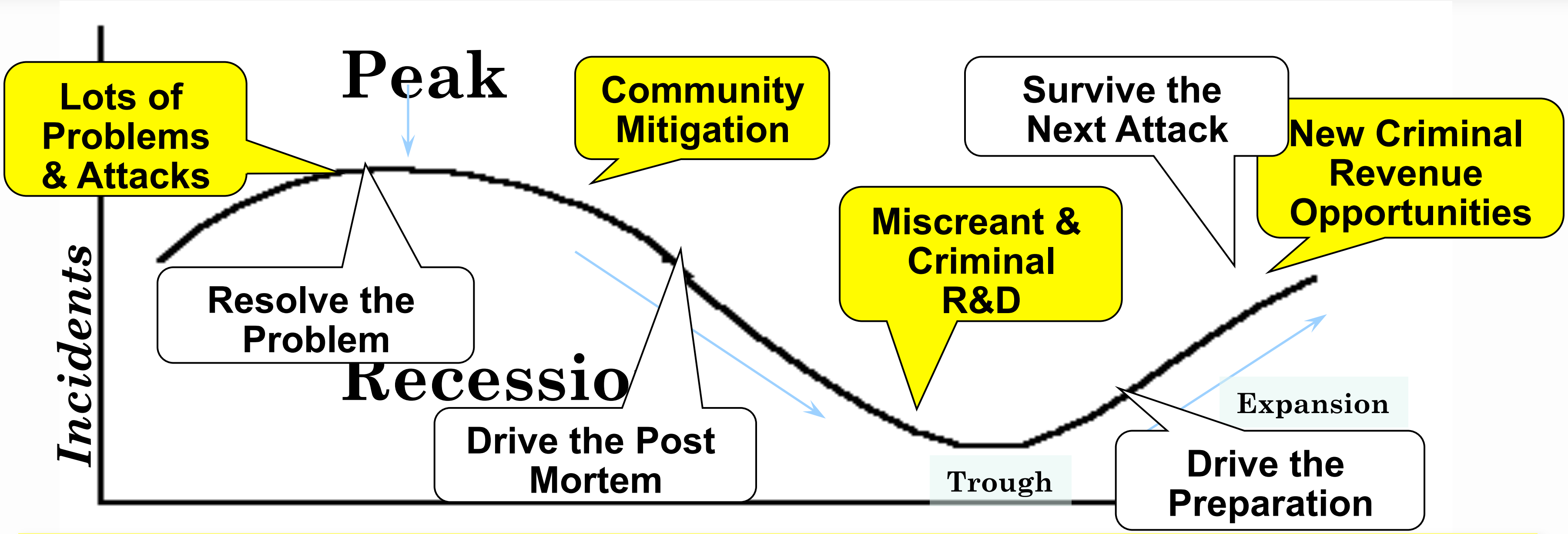
- Extortionist/ DDoS-for-Hire
- Spammer
- Phisher
- Pharmer/DNS Poisoning
- Identity Theft

End Value

- Criminal Competition
- Theft
- Espionage (Corporate/ Government)
- Extorted Pay-Offs
- Commercial Sales
- Fraudulent Sales
- Click-Through Revenue
- Financial Fraud

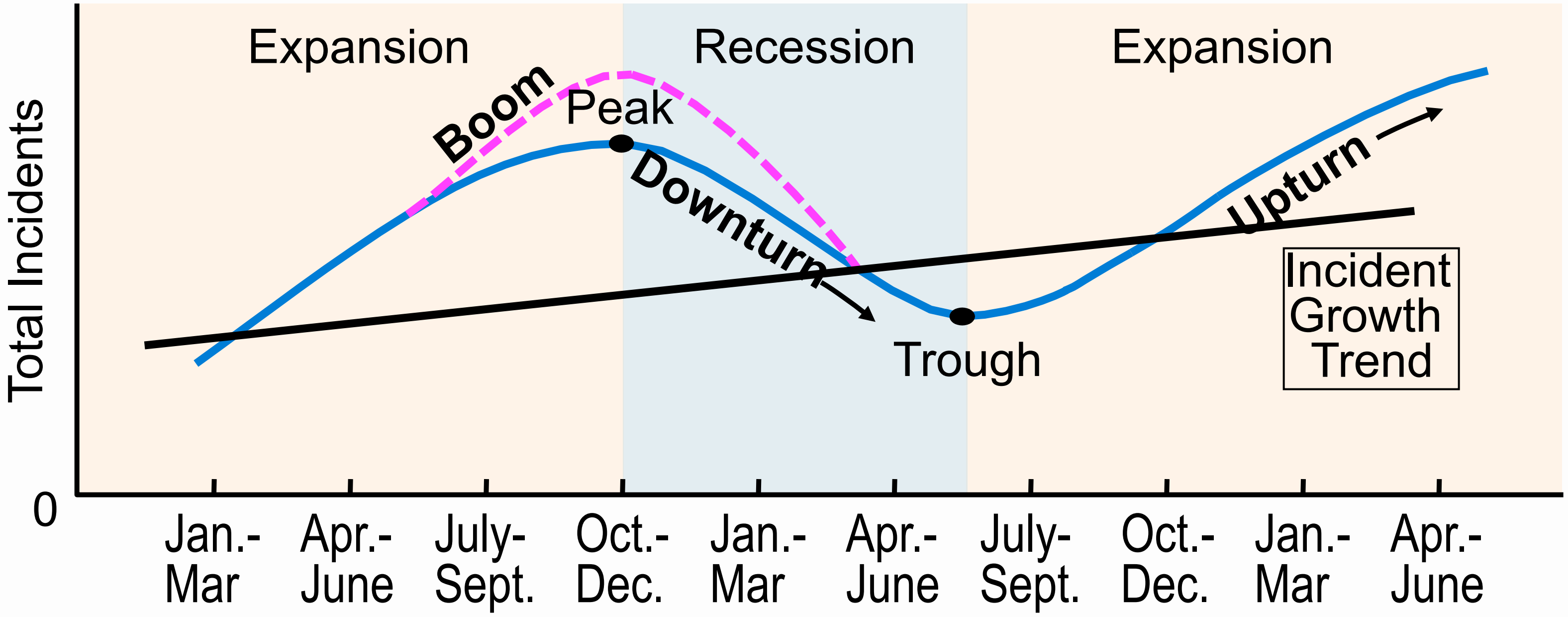
$$$ Flow of Money $$$

Miscreant - Incident Economic Cycles

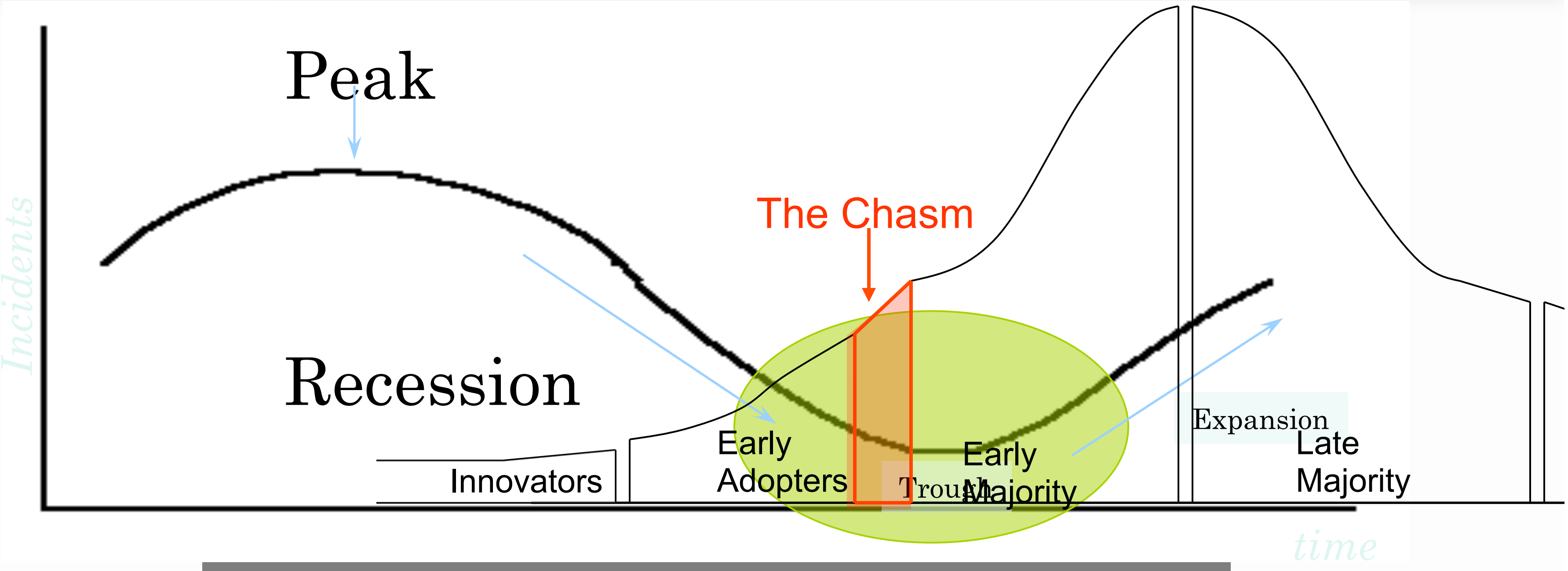


These Cycles Repeat

Miscreant Economic Cycles



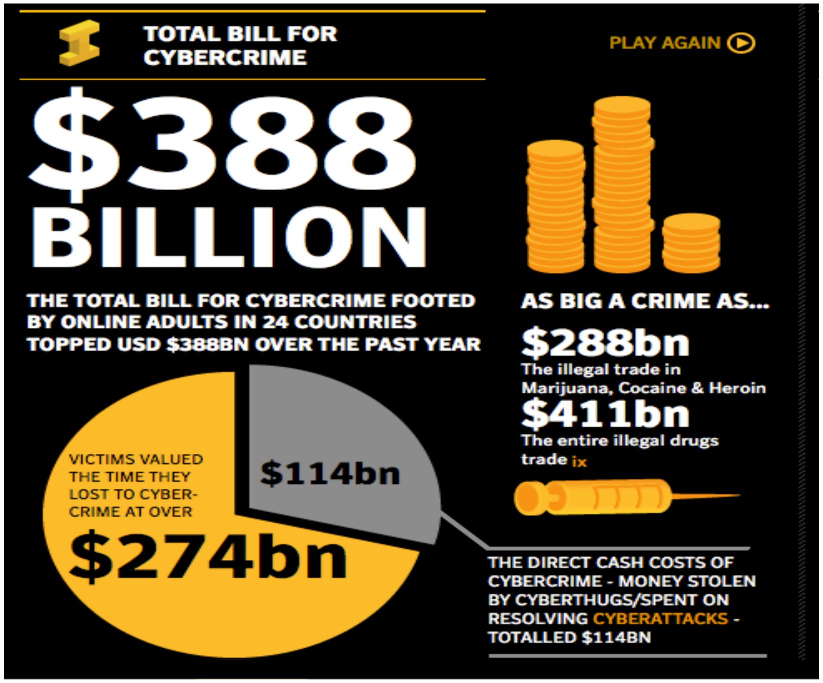
The dire trap – the *Chasm* of in action



No Pain
No Business Justification for Action

Cyber Crime Cost are Huge!

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



THE TOTAL BILL FOR CYBERCRIME FOOTED BY ONLINE ADULTS IN 24 COUNTRIES TOPPED USD $388BN OVER THE PAST YEAR

AS BIG A CRIME AS...

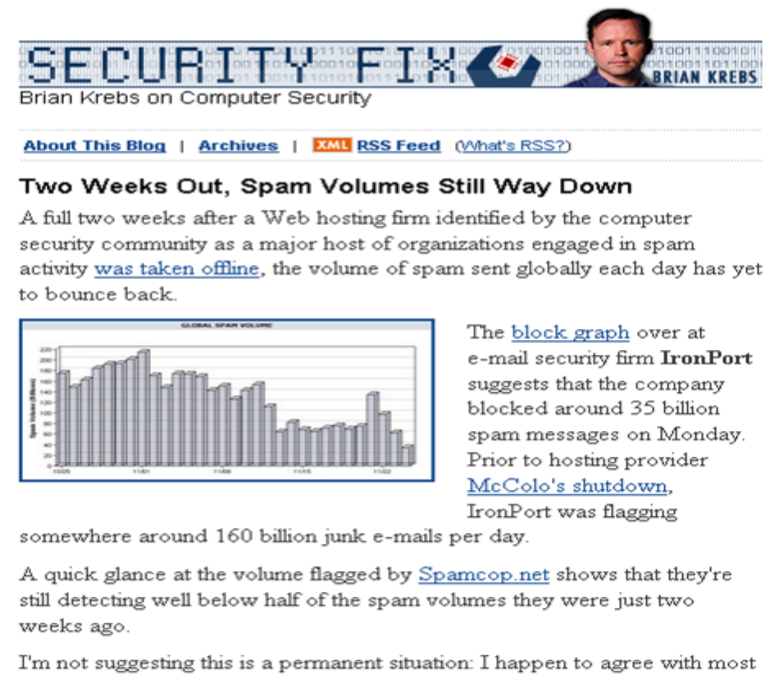
$288bn The illegal trade in Marijuana, Cocaine & Heroin

$411bn The entire illegal drugs trade ix

VICTIMS VALUED THE TIME THEY LOST TO CYBER-CRIME AT OVER $274bn

THE DIRECT CASH COSTS OF CYBERCRIME - MONEY STOLEN BY CYBERTHUGS/SPENT ON RESOLVING CYBERATTACKS - TOTALLED $114BN

Community Action Can Have an Impact



SECURITY FIX BRIAN KREBS

Brian Krebs on Computer Security

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

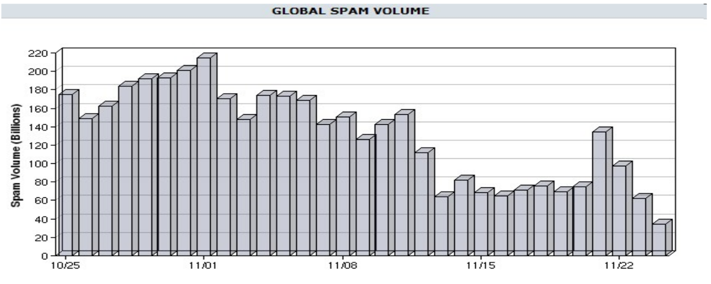
Two Weeks Out, Spam Volumes Still Way Down

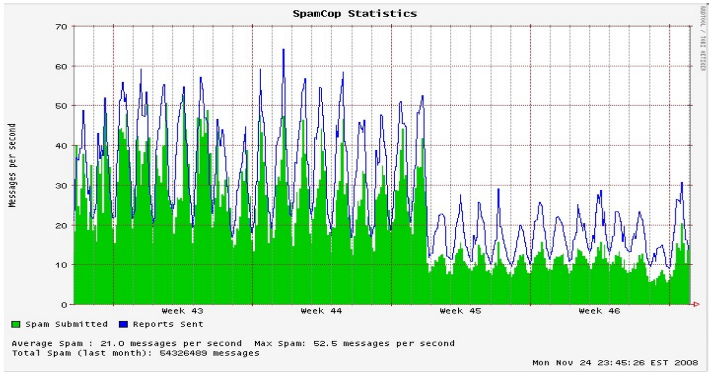
A full two weeks after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline, the volume of spam sent globally each day has yet to bounce back.

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



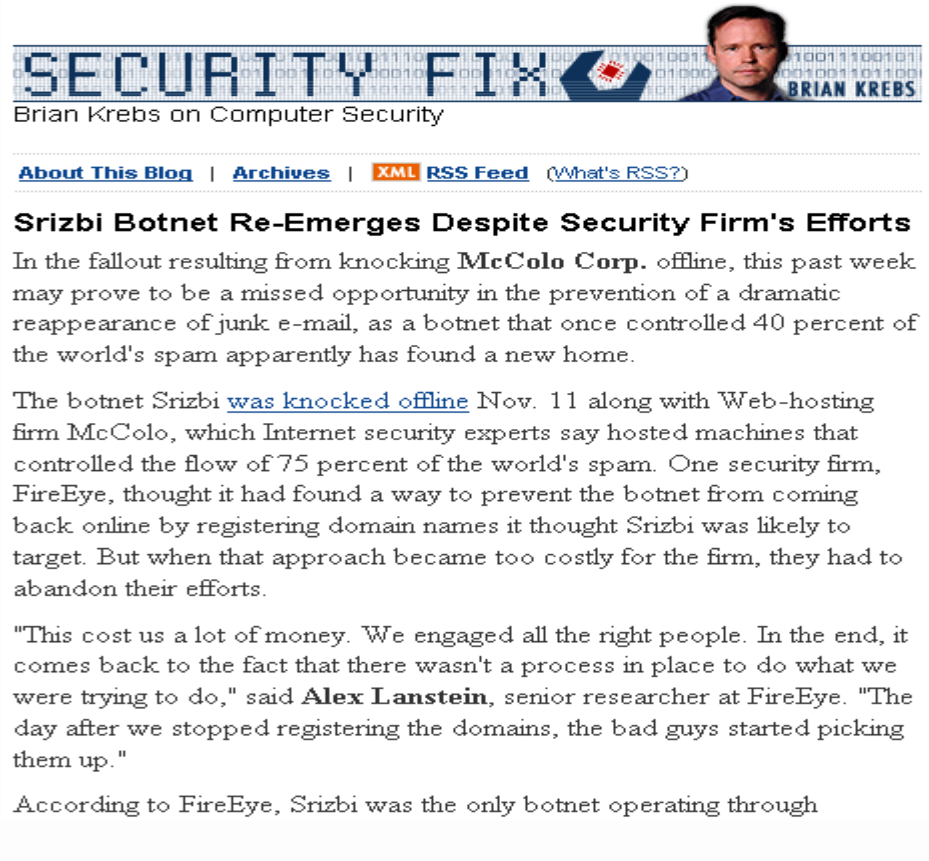


Average Spam : 21.0 messages per second Max Spam: 52.5 messages per second
Total Spam (last month): 54326489 messages

Mon Nov 24 23:45:26 EST 2008

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

But for how long .....



SECURITY FIX
BRIAN KREBS
Brian Krebs on Computer Security

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

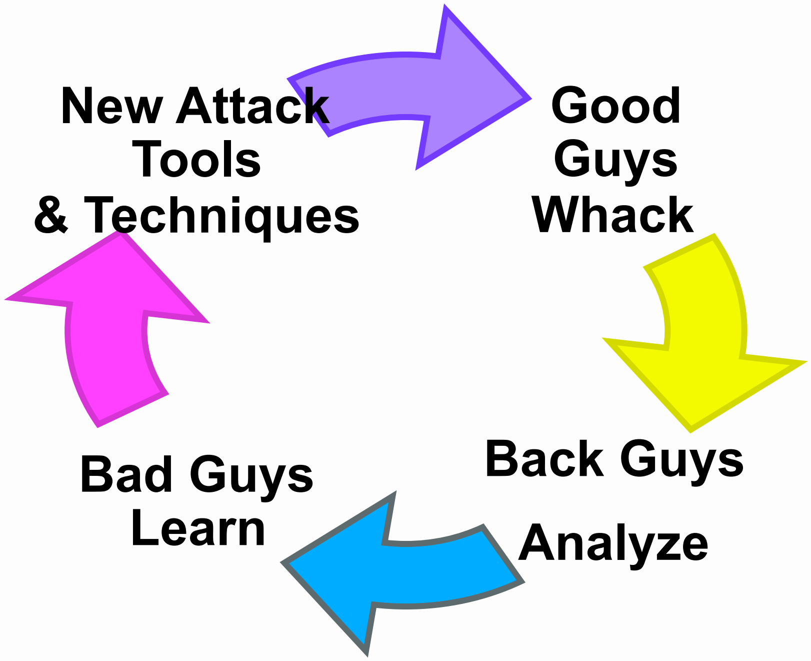
Srizbi Botnet Re-Emerges Despite Security Firm's Efforts

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



New Attack Tools & Techniques

Good Guys Whack

Back Guys Analyze

Bad Guys Learn

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 to 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.

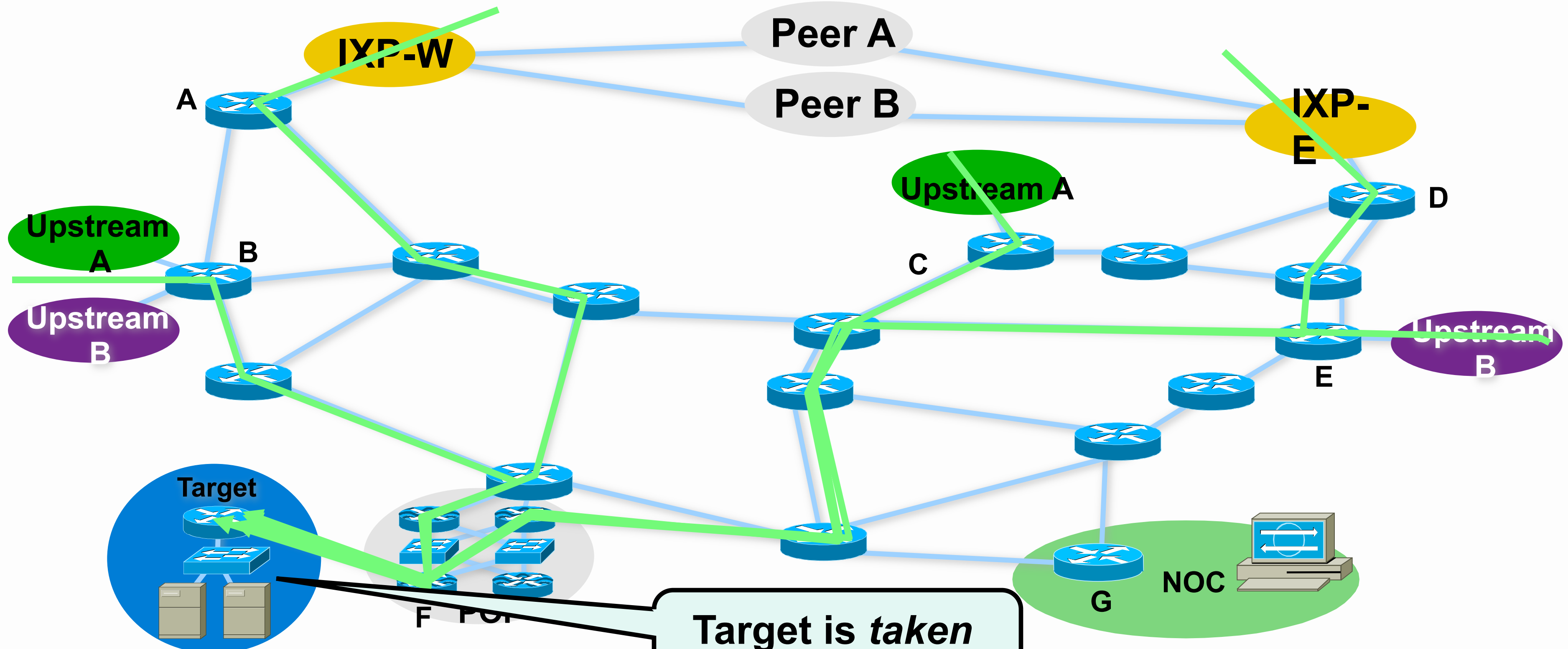
Cyber Warfare

- 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.

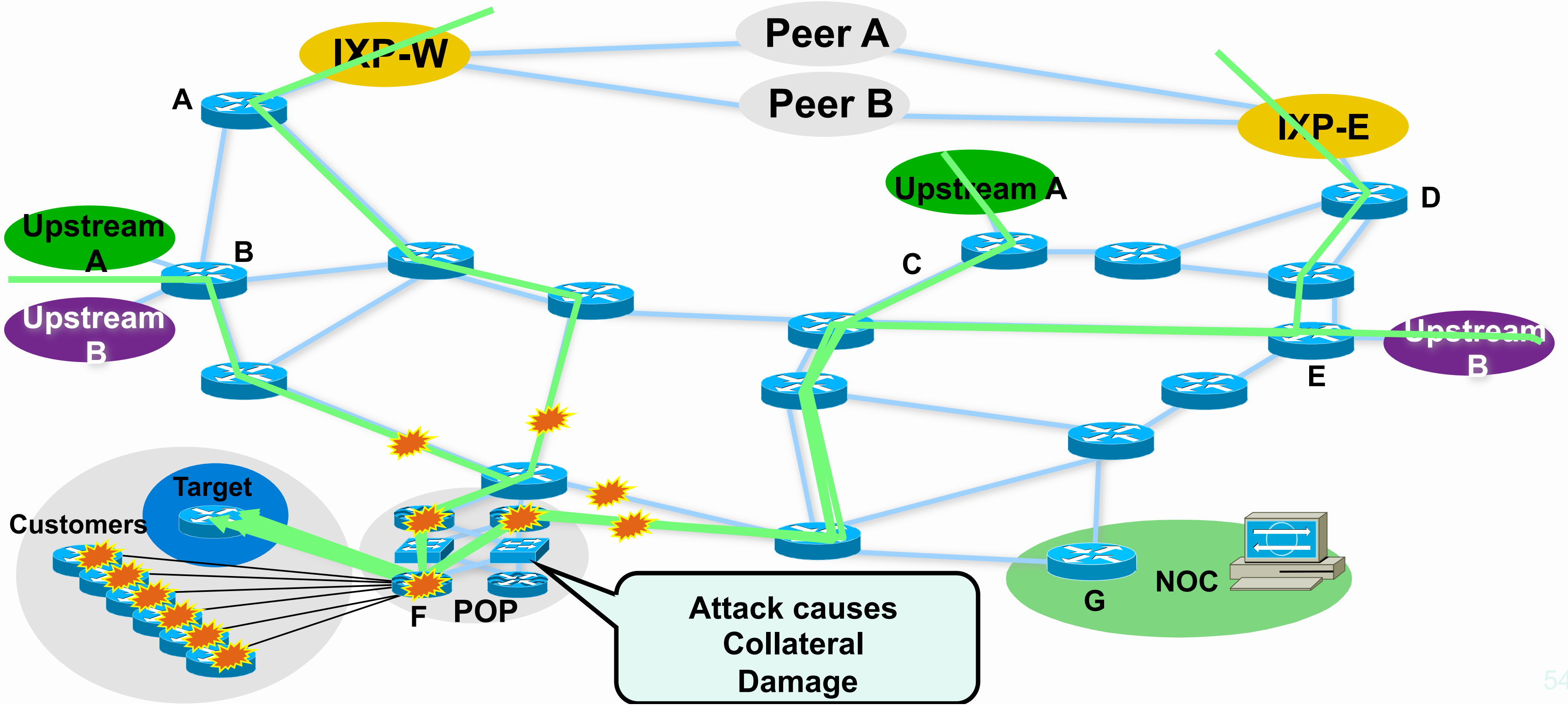
Michael Falco / The New York Times / Redux

Cyber Warfare’s Consequences …



Target is *taken out*

… Extend beyond the perceived "Battle Space."



Attack causes Collateral Damage

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.”

博讯正被攻击，请点击这里
谢谢理解和支持！记住随时

During the attack, You may want to try the following links if the
www.boxun.com
http://news.boxun.com
www.peacehall.com

欢迎

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

MESSAGING MALWARE MOBILE

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 M^{3}AAWG website at:
https://www.m3aawg.org/activities/maawg-training-series-videos

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

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

For information about M^{3}AAWG:
www.m3aawg.org
www.facebook.com/maawg
www.twitter.com/maawg
www.youtube.com/maawg

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