New Opportunities for Criminal Growth

Forecasting Cyber-Crime during the IPv6 Transition

Barry Raveendran Greene

bgreene@isc.org

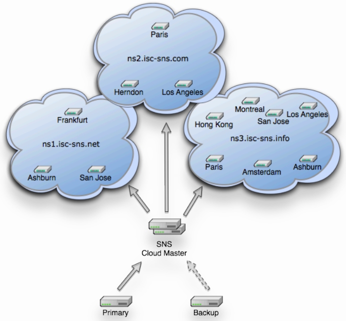
Version 1.1

Context

- The Internet Systems Consortium (ISC) is a strong driver for IPv6 adoption.
- The information contained in this presentation is an effort to empower organizations to deploy IPv6 to take extra effort to be mindful of their security risk.
- Risk can be mitigated if a clear understanding of the risk exist.
- It takes one big “IPv6 back doors a network” *Press Cycle* to shake the confidence of CIOs around the World – slowing down IPv6 deployment.

ISC and IPv6

Yes! IPv6 is running natively at my desk, on our wireless, our services, our software, our services, and VPN tunneled from home.

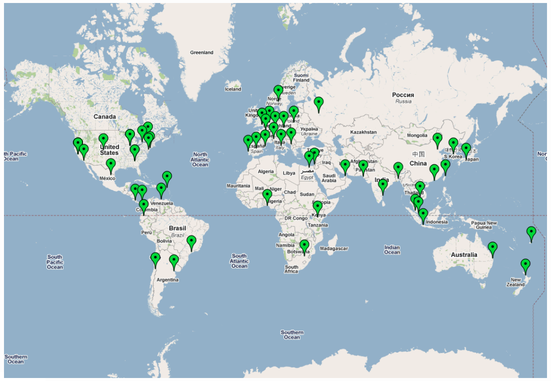


Secondary DNS Services

Open Source Software that are the “Gears” of the Net

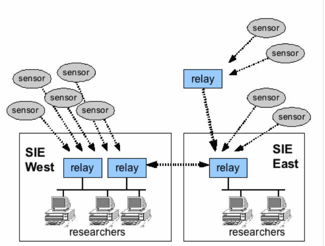
BIND
AFTR
RPKI

DHCP
PCP
(TBA)



DNS F-Root

SIE pDNS



Hosted @ w/ Open Source Community and Others

Internet Systems Consortium, Inc. (ISC) is a non-profit 501(c)(3) public benefit corporation dedicated to supporting the *infrastructure of the universal connected self-organizing Internet*—and the autonomy of its participants—by developing and maintaining core production quality software, protocols, and operations.

Logistics

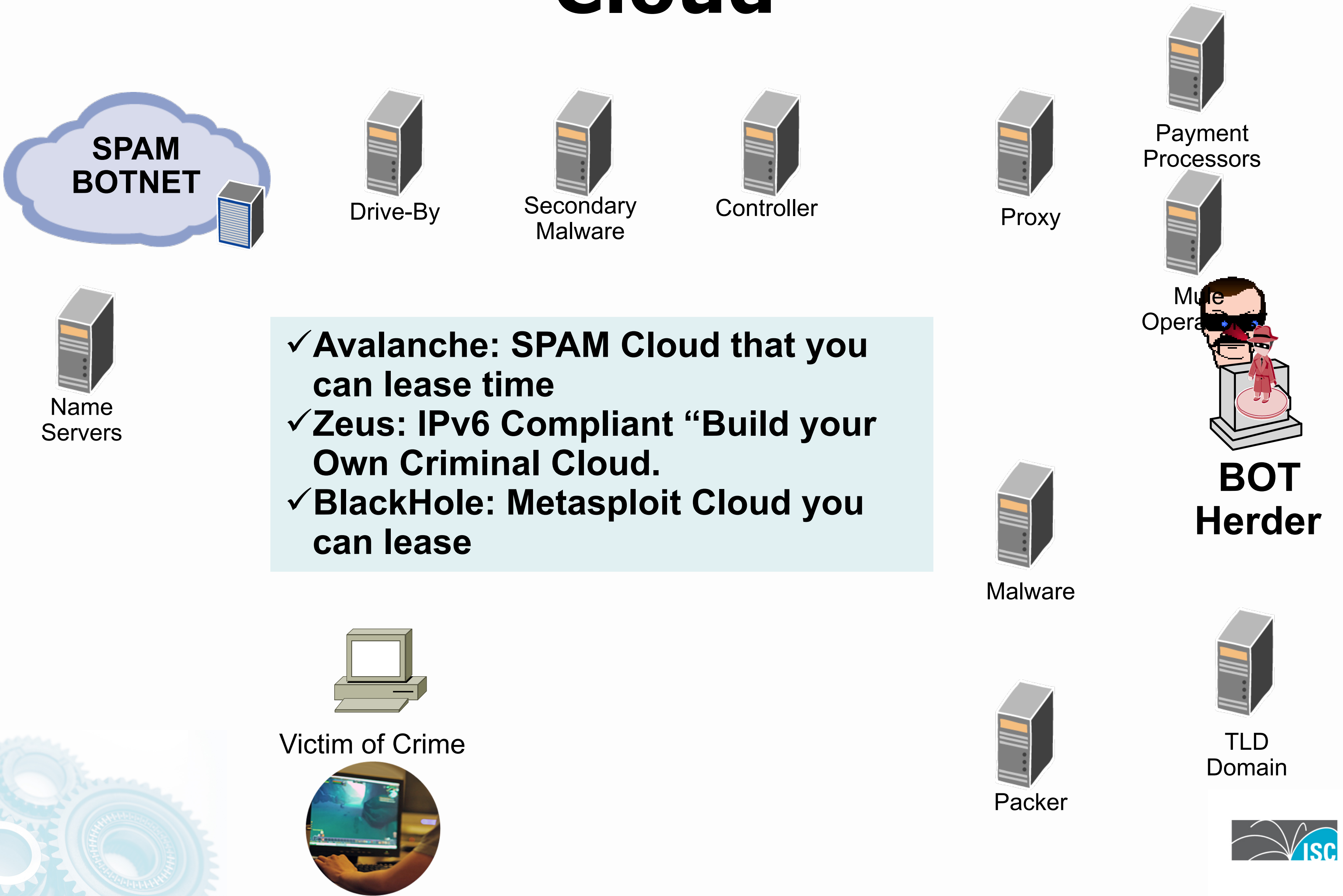
- This presentation can be downloaded from the Webinar recording and from ISC’s Knowledge Base: http://deepthought.isc.org
- ISC updates, presentations, and materials can be followed on:
  - Facebook - http://www.facebook.com/InternetSystemsConsortium
  - Twitter - ISCdotORG
  - Linkedin - http://www.linkedin.com/company/internet-systems-consortium
  - RSS via our Website

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?

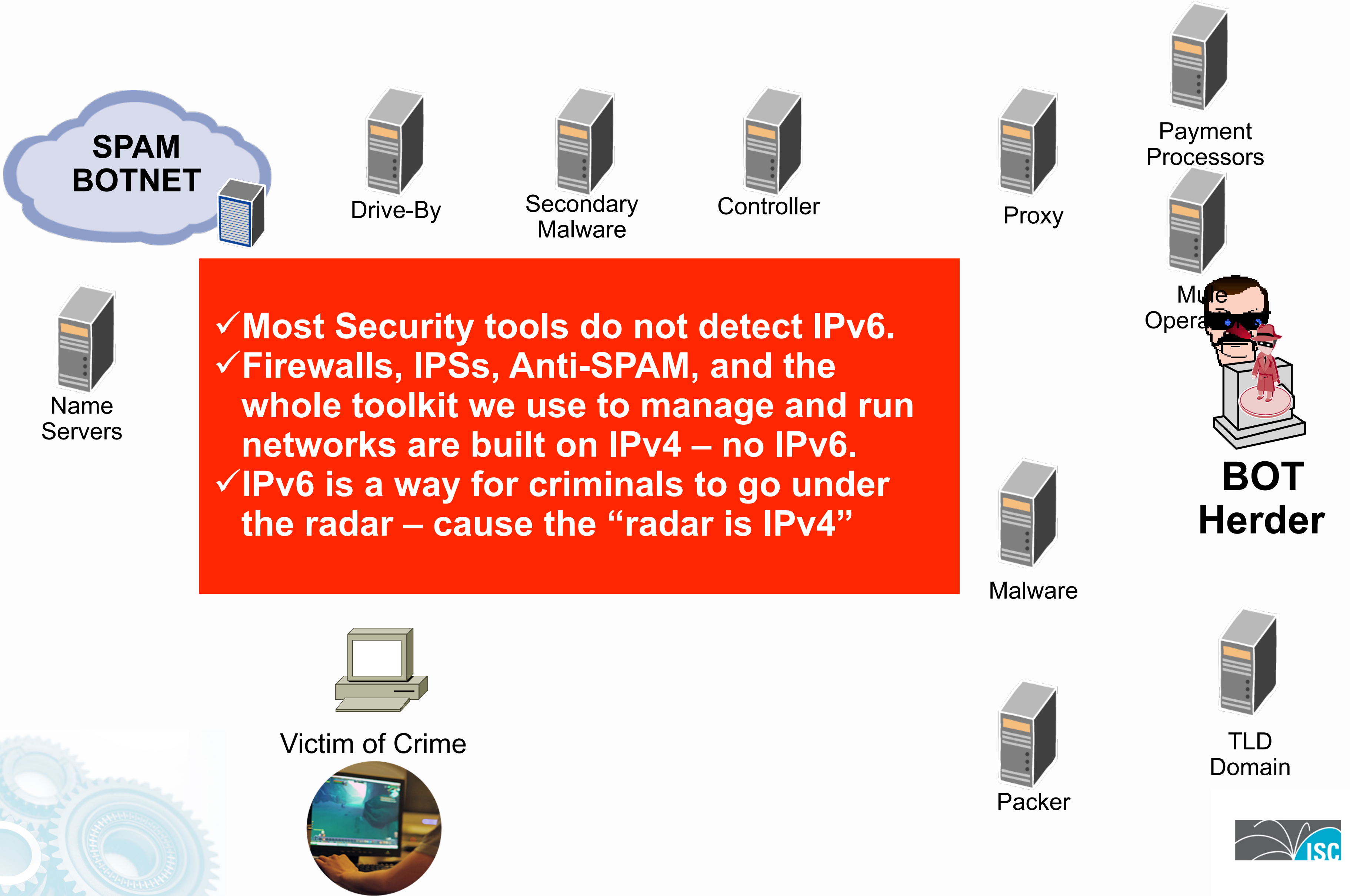
Cyber Criminal Toolkit that is the foundation for the *Criminal Cloud*

Components of the Criminal Cloud



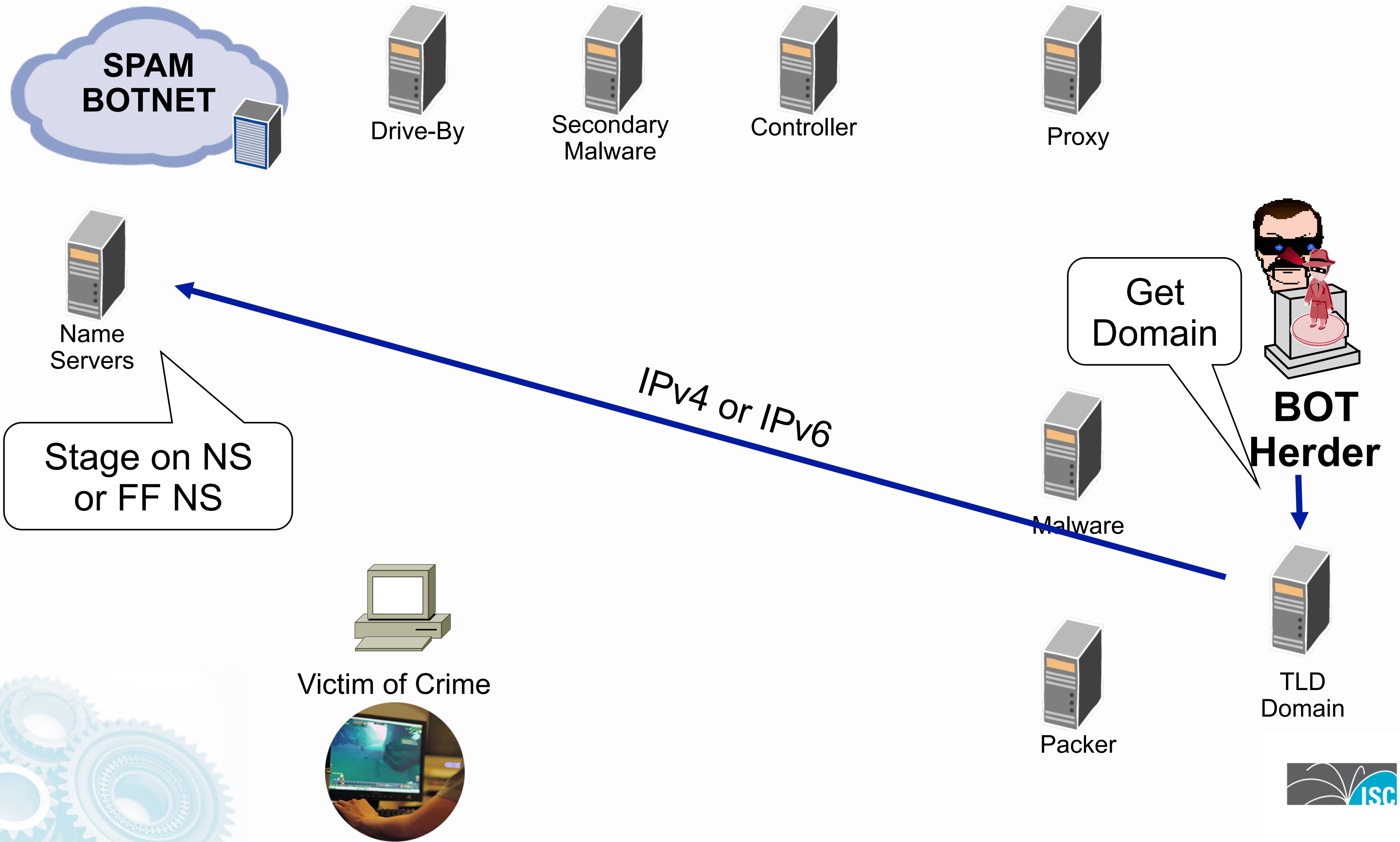
- ✓Avalanche: SPAM Cloud that you can lease time
- ✓Zeus: IPv6 Compliant “Build your Own Criminal Cloud.
- ✓BlackHole: Metasploit Cloud you can lease

Why not use a IPv6 Criminal Cloud?



- ✓Most Security tools do not detect IPv6.
- ✓Firewalls, IPSs, Anti-SPAM, and the whole toolkit we use to manage and run networks are built on IPv4 – no IPv6.
- ✓IPv6 is a way for criminals to go under the radar – cause the "radar is IPv4"

Stage Domain Name



SPAM BOTNET

Drive-By

Secondary Malware

Controller

Proxy

Name Servers

Stage on NS or FF NS

IPv4 or IPv6

Get Domain

BOT Herder

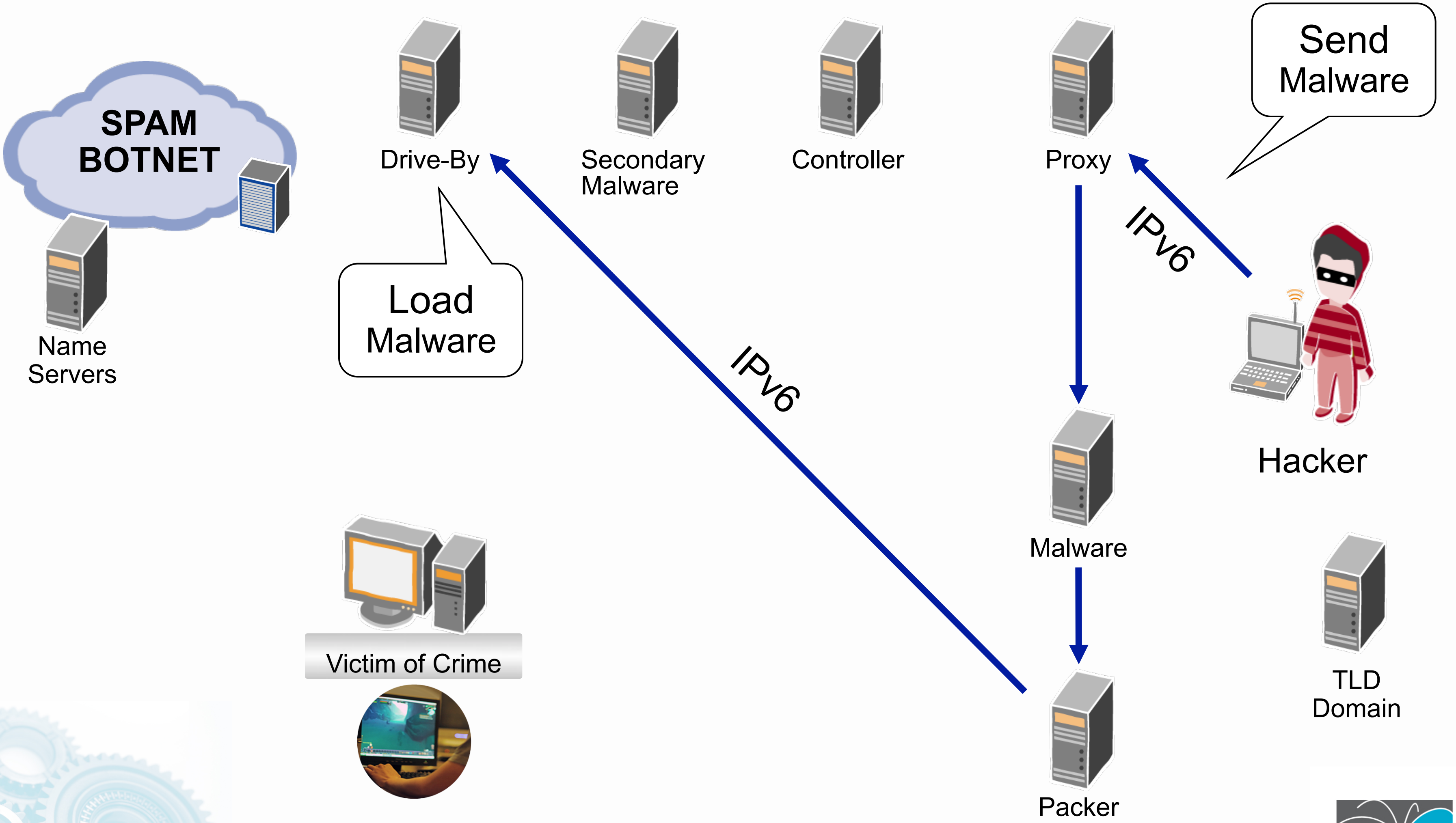
Malware

TLD Domain

Packer

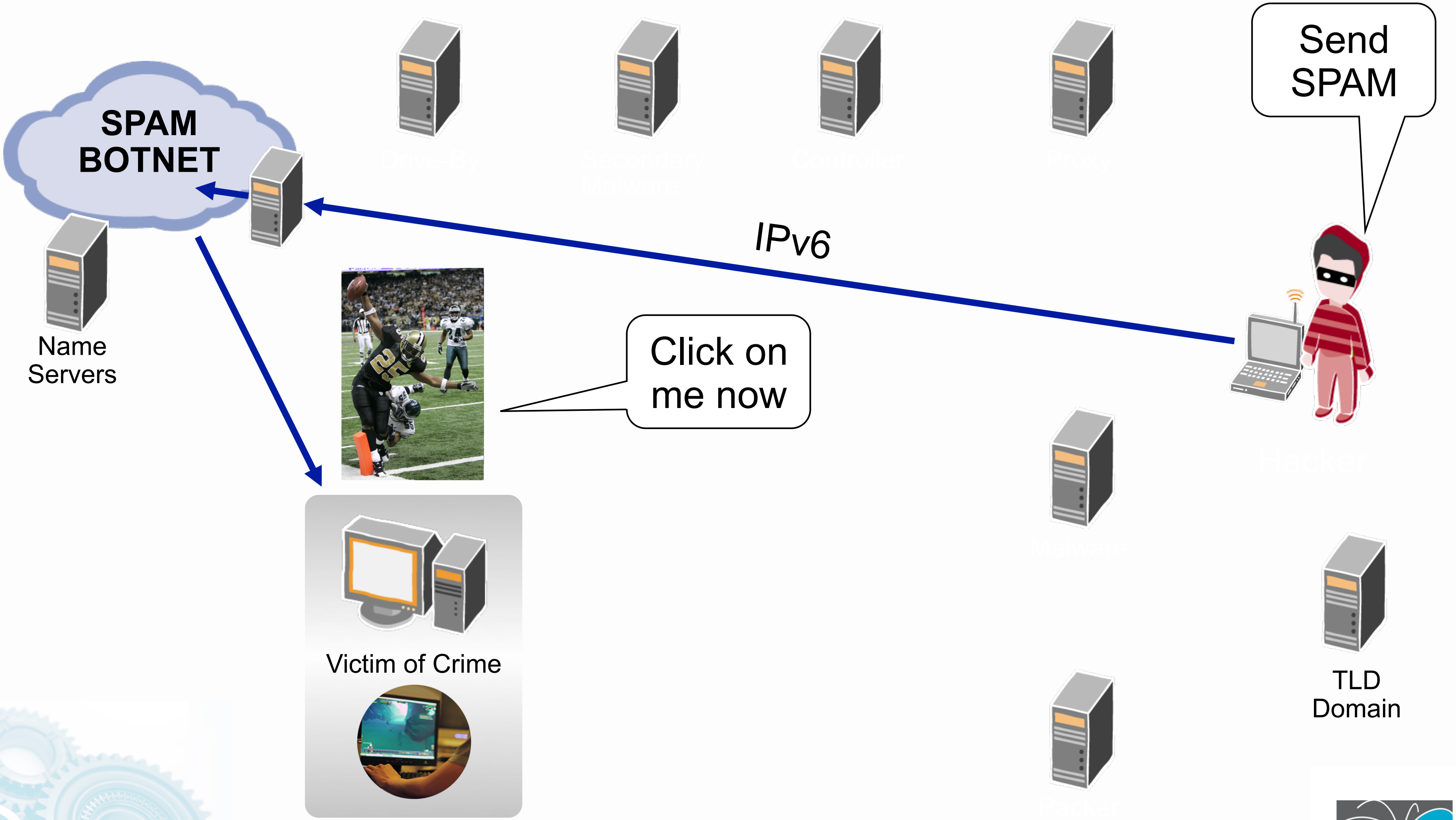
Victim of Crime

Prepare Drive-By

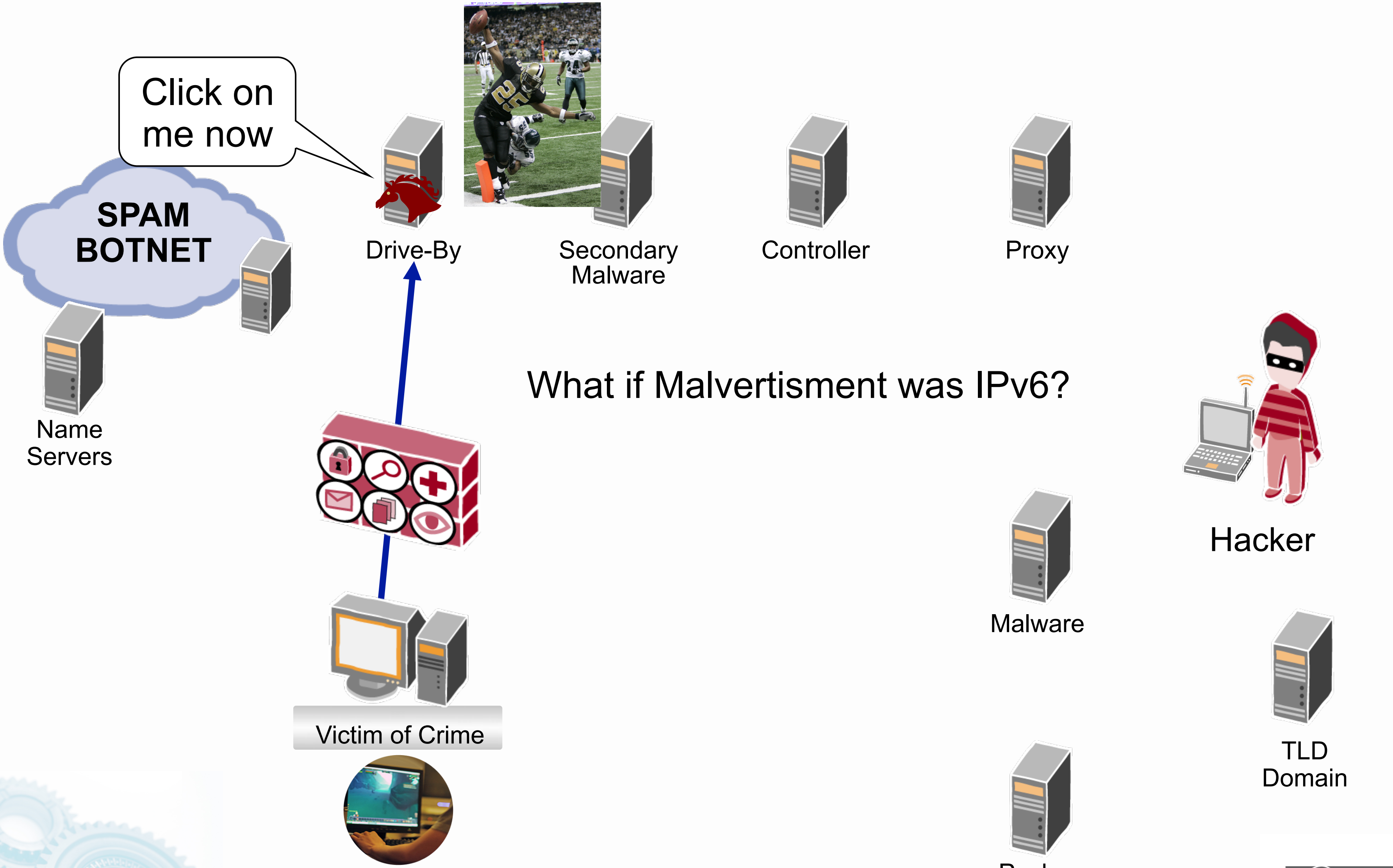


Social Engineered SPAM to Get People to Click

(Spear Phishing)

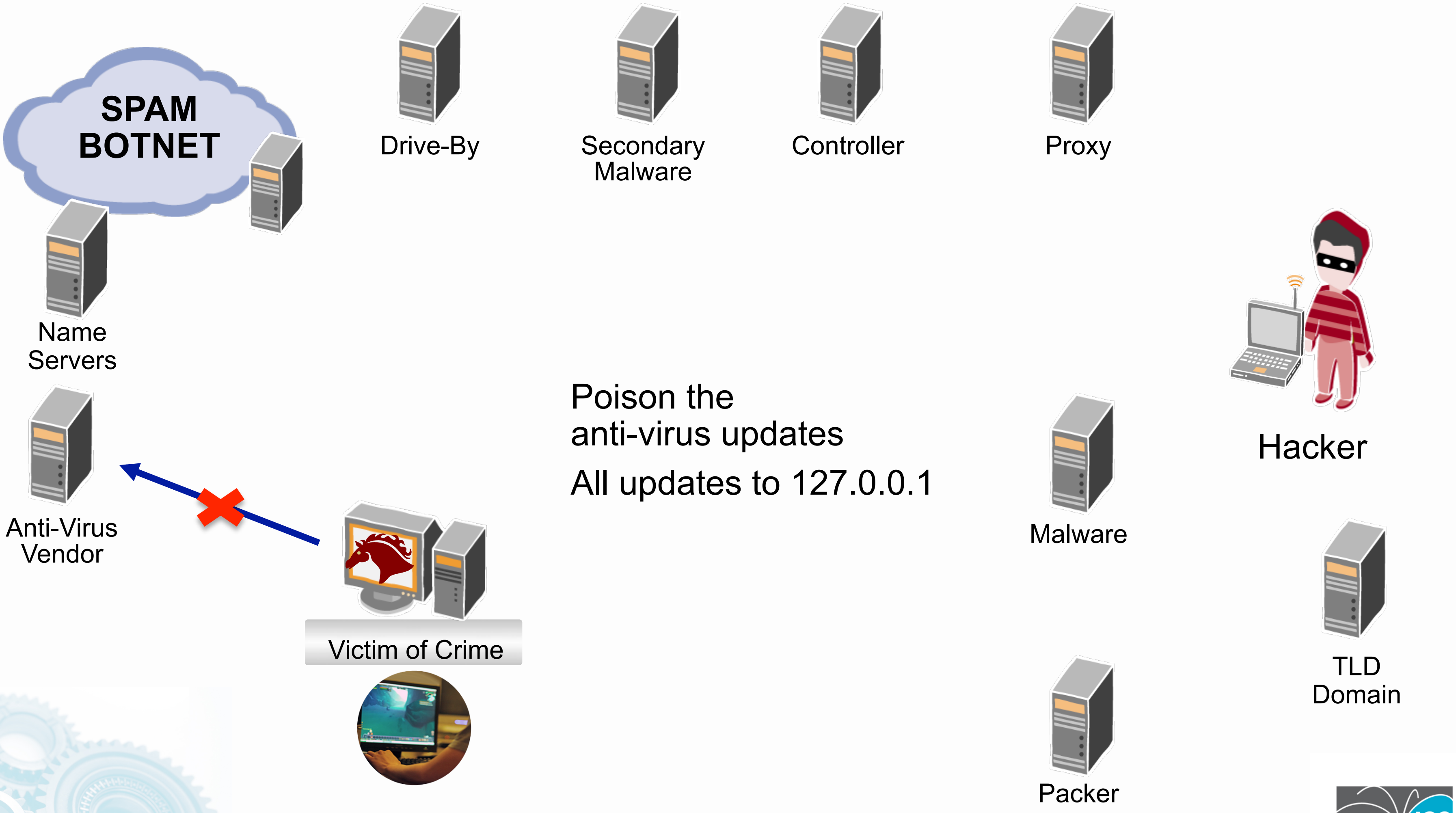


Drive-By Violation



What if Malvertisment was IPv6?

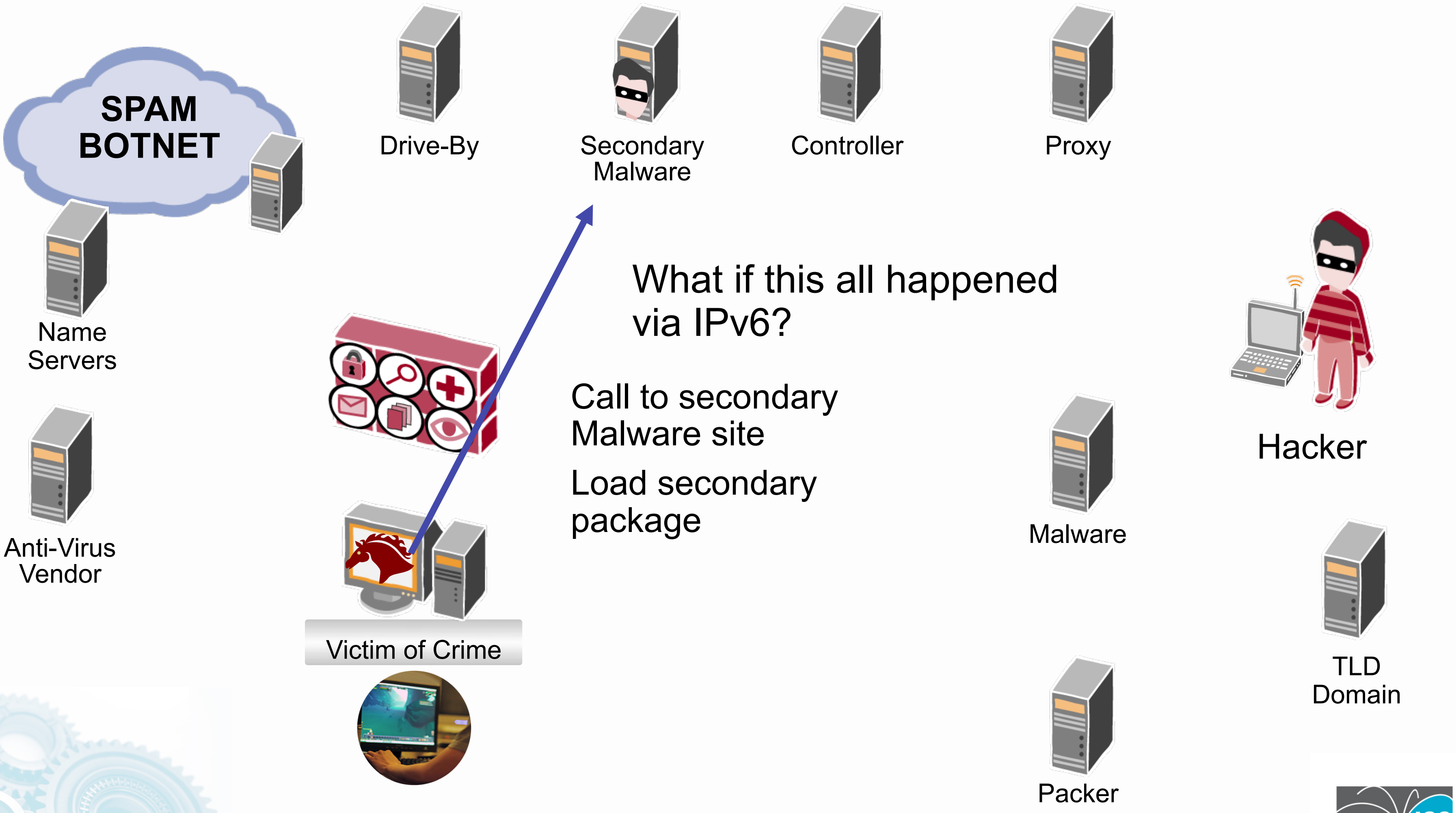
Poison Anti-Virus Updates



Poison the
anti-virus updates

All updates to 127.0.0.1

Prepare Violated Computer

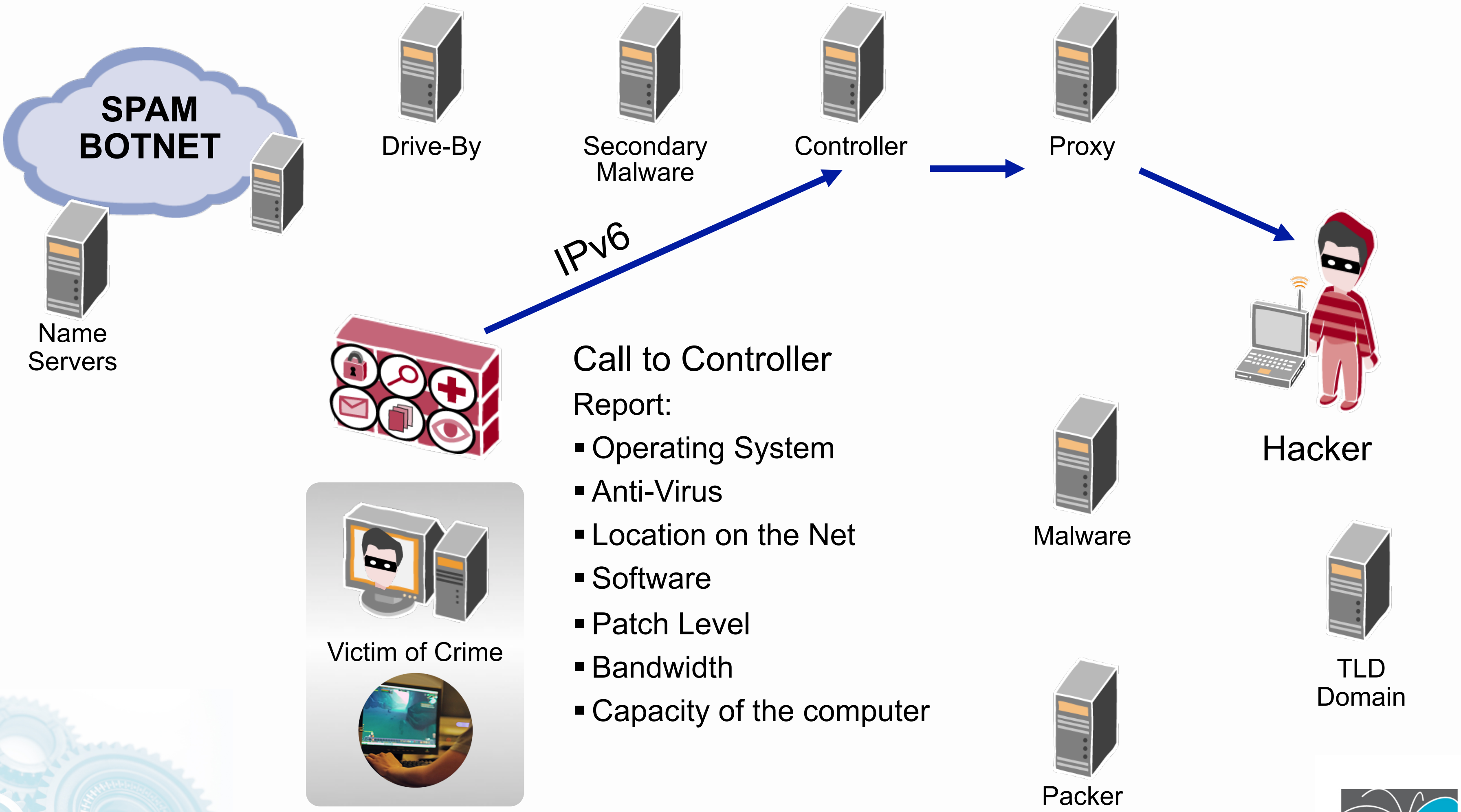


What if this all happened via IPv6?

Call to secondary Malware site

Load secondary package

Call Home

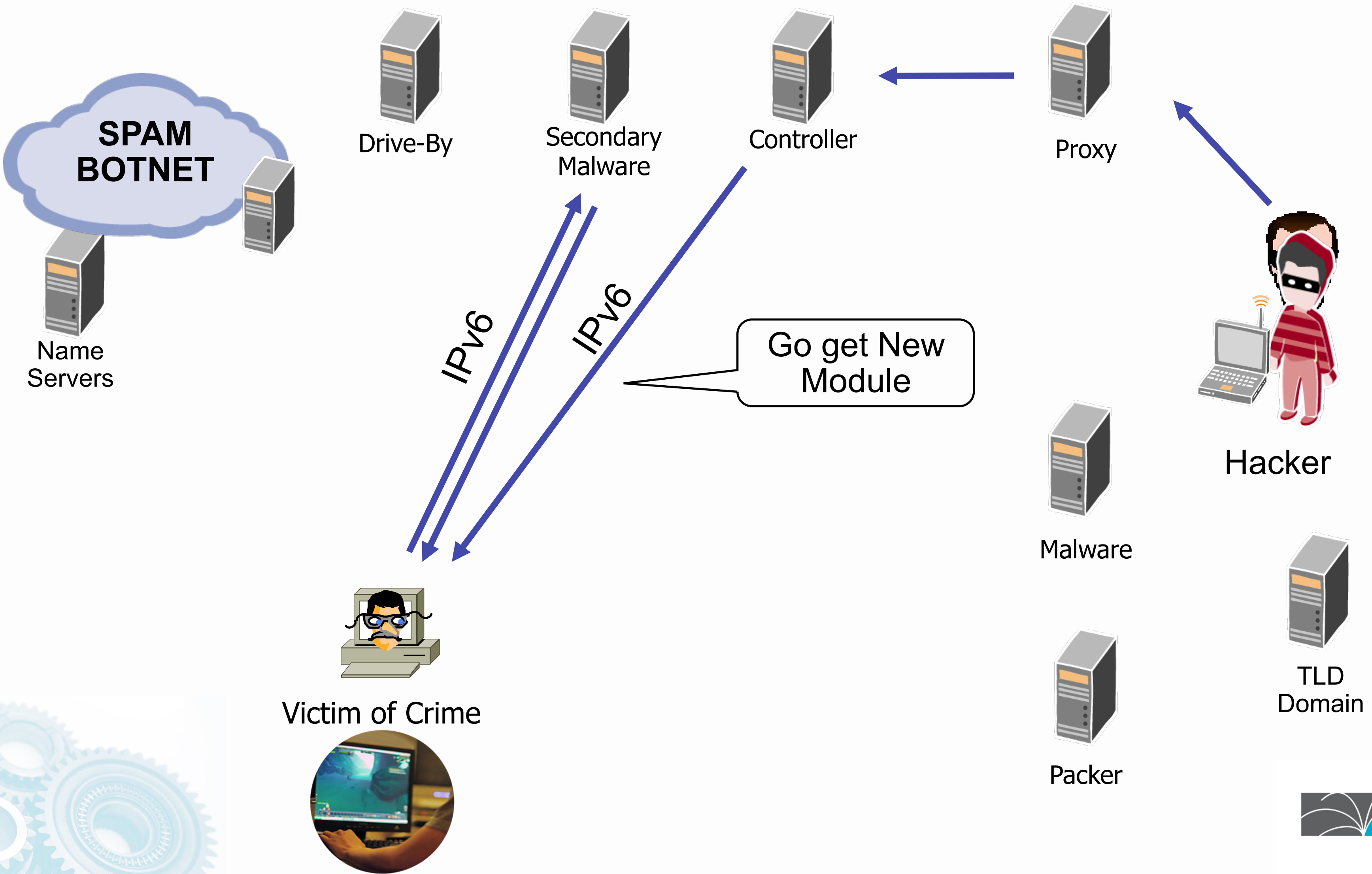


Call to Controller

Report:

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

Load Custom Malware



SPAM BOTNET

Name Servers

Drive-By

Secondary Malware

Controller

Proxy

IPv6

IPv6

Go get New Module

Hacker

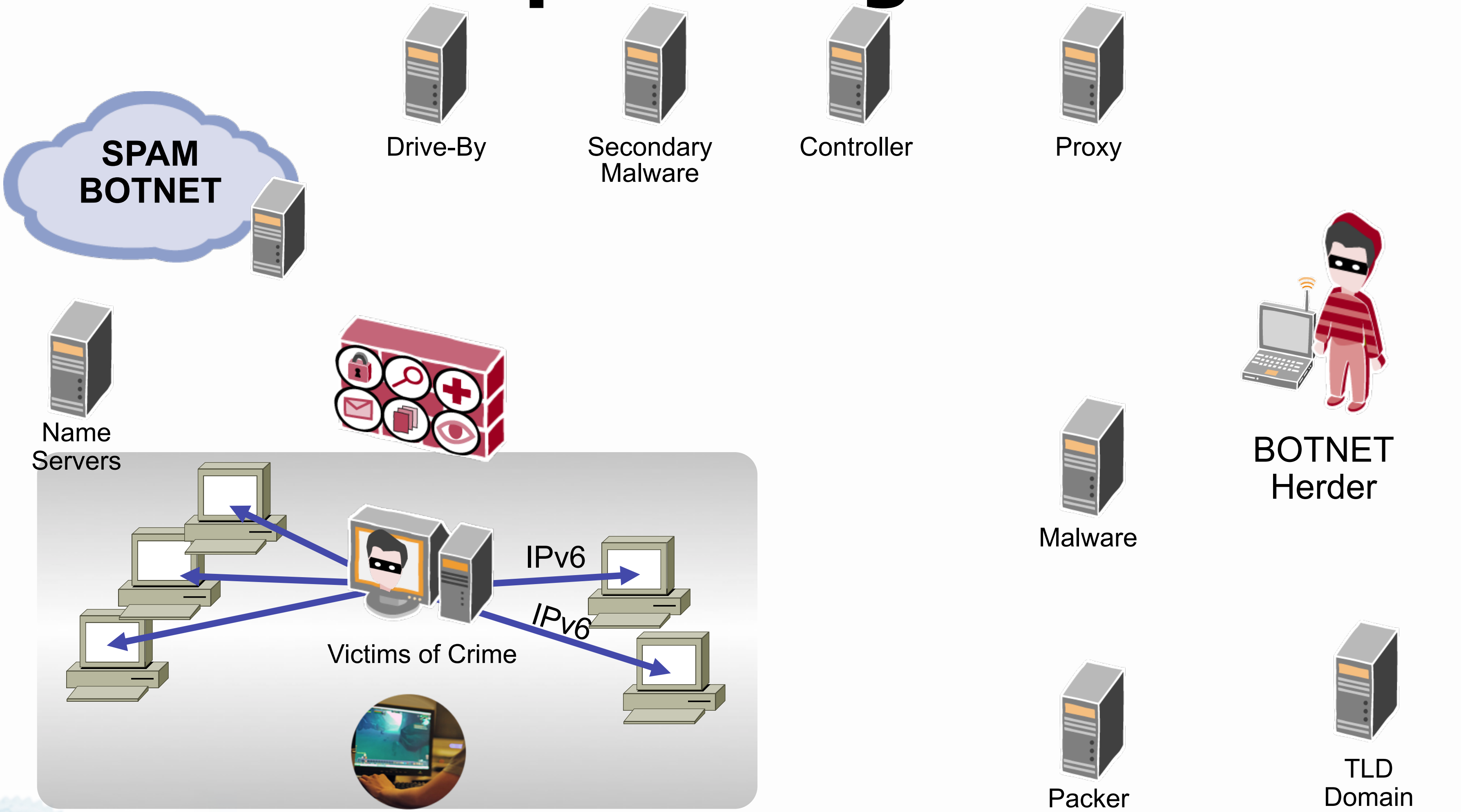
Malware

TLD Domain

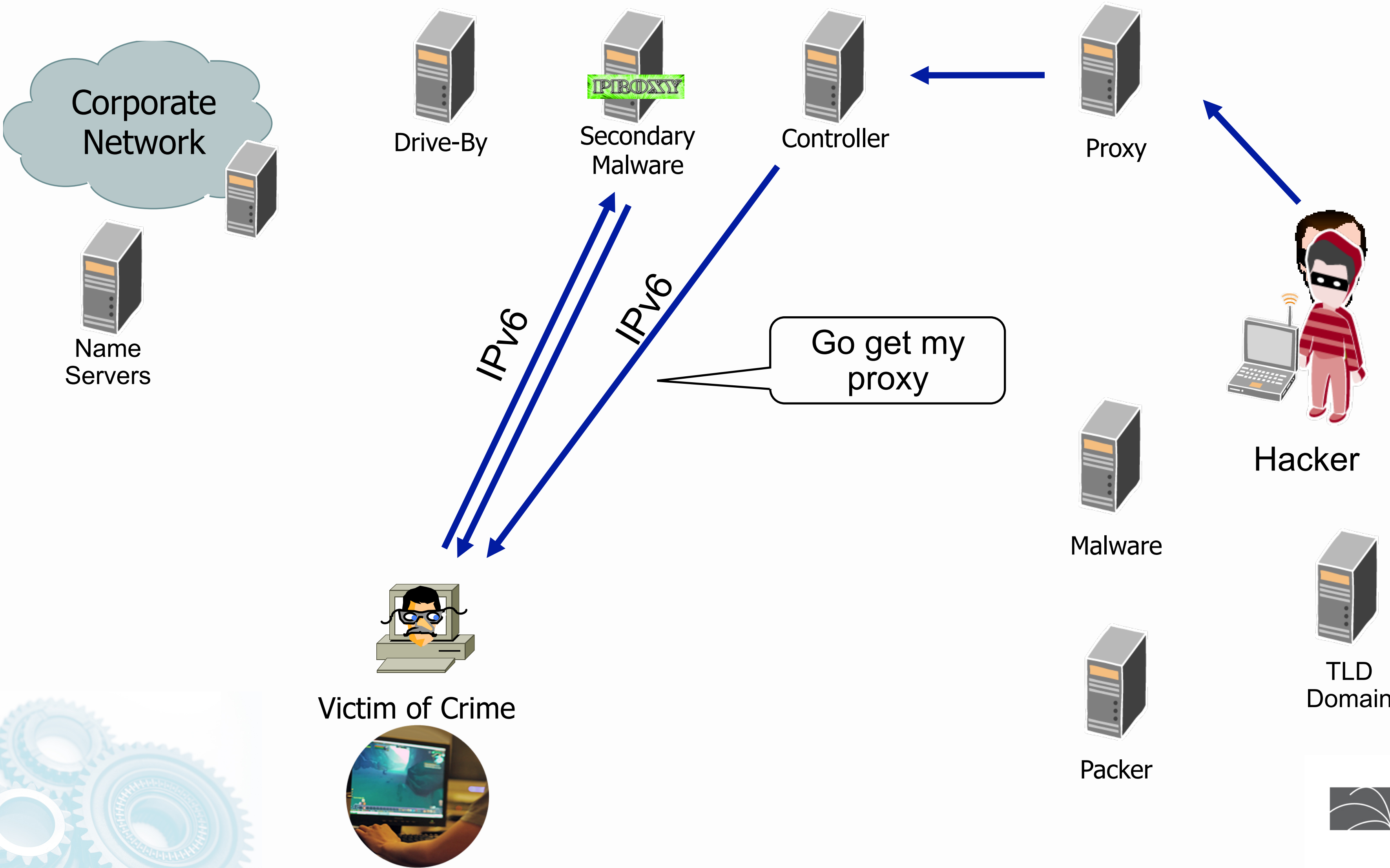
Packer

Victim of Crime

Start Worming, Scanning, & Spreading



Load a Proxy with Trigger



Corporate Network

Drive-By

Secondary Malware

Controller

Proxy

Name Servers

IPv6

IPv6

Go get my proxy

Hacker

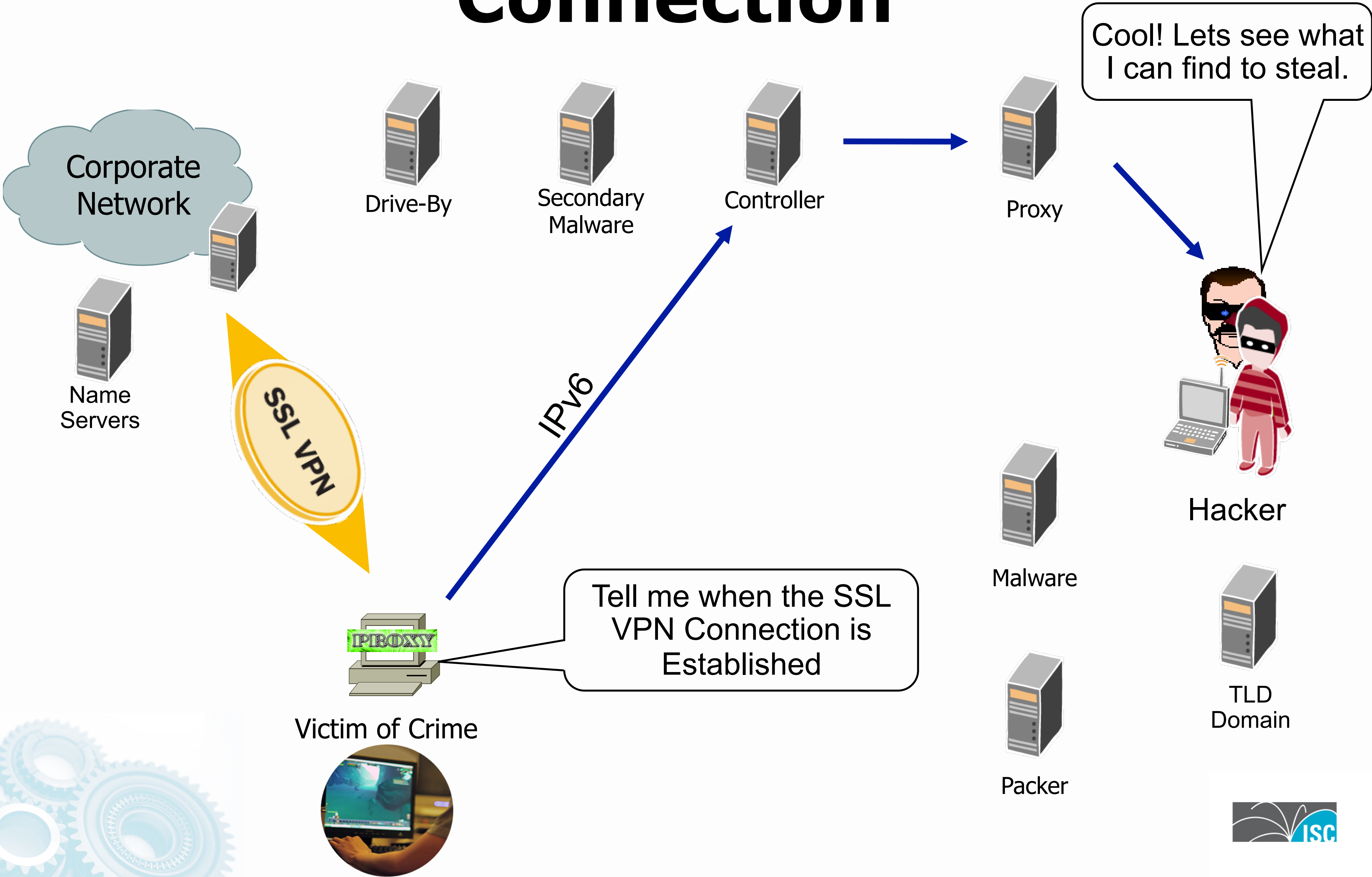
Malware

TLD Domain

Packer

Victim of Crime

Watch for the SSL VPN Connection



Corporate Network

Name Servers

Drive-By

Secondary Malware

Controller

Proxy

Cool! Lets see what I can find to steal.

Hacker

SSL VPN

IPv6

PROXY

Victim of Crime

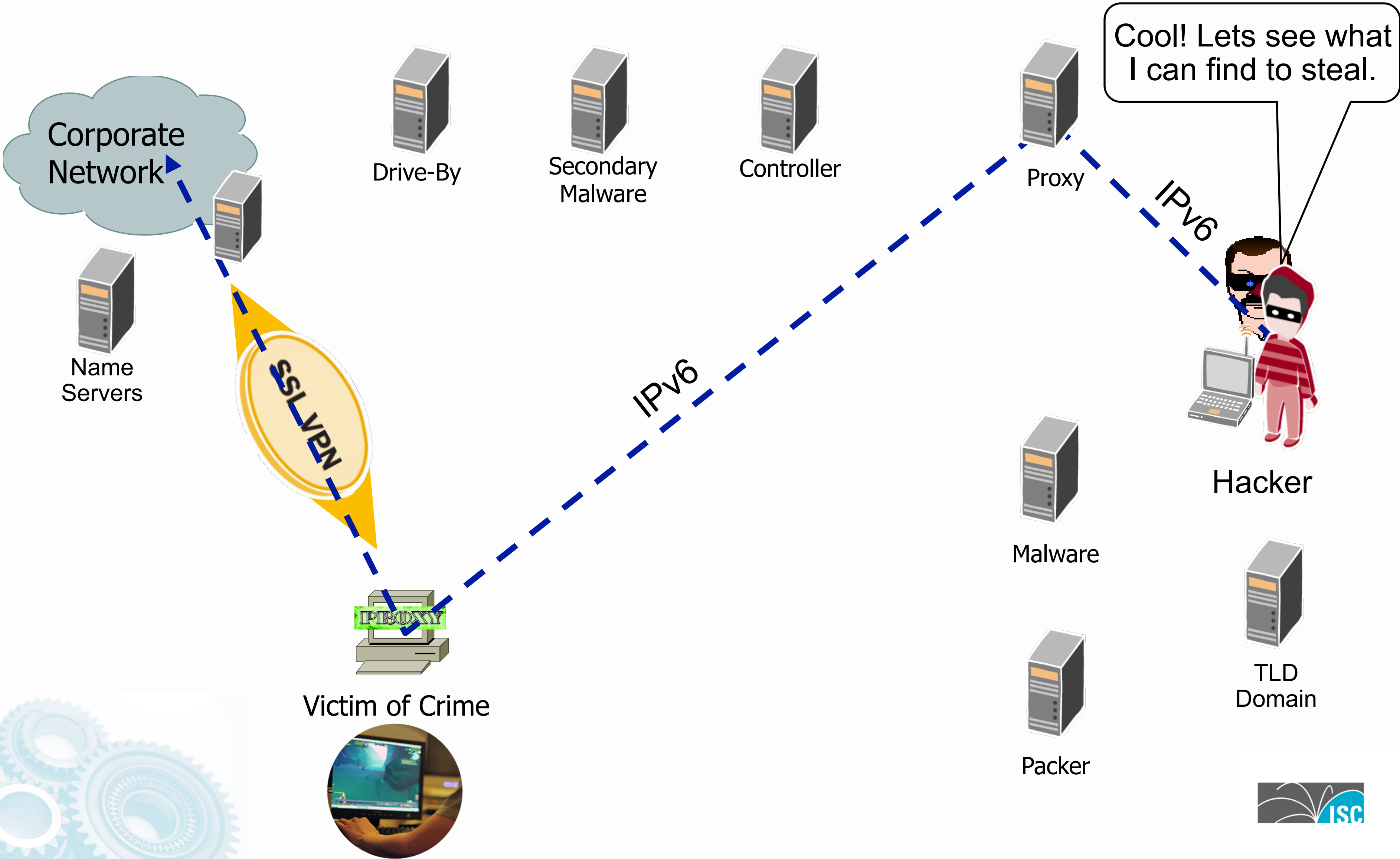
Tell me when the SSL VPN Connection is Established

Malware

Packer

TLD Domain

Set up the Proxy Tunnel



Corporate Network

Name Servers

SSL VPN

Drive-By

Secondary Malware

Controller

Proxy

Cool! Lets see what I can find to steal.

IPv6

IPv6

PROXY

Victim of Crime

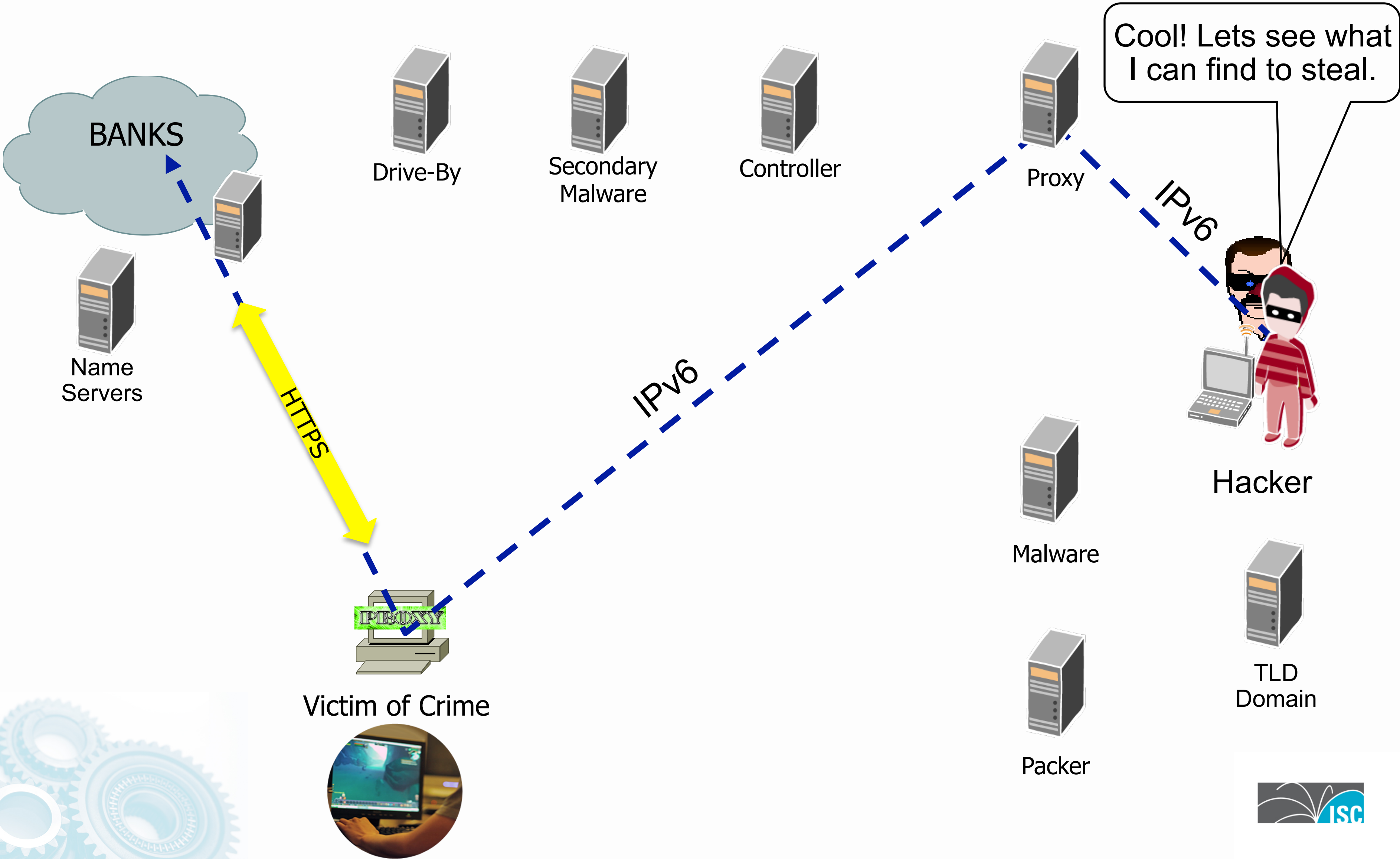
Hacker

Malware

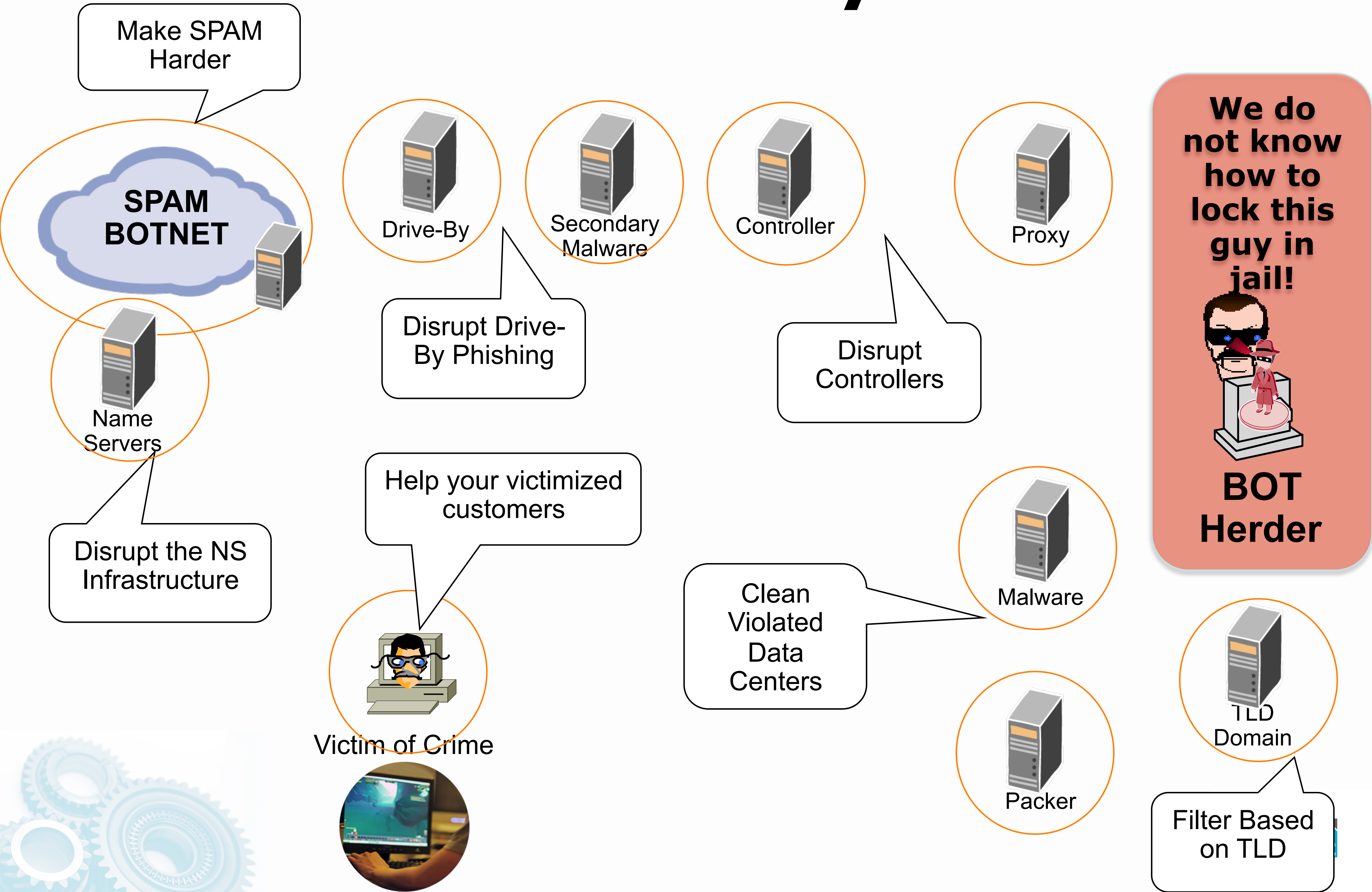
TLD Domain

Packer

Proxy Behind the Bank Login



OPSEC Community’s Action



Make SPAM Harder

SPAM BOTNET

Drive-By

Secondary Malware

Controller

Proxy

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

BOT Herder

Name Servers

Disrupt Drive-By Phishing

Disrupt Controllers

Help your victimized customers

Disrupt the NS Infrastructure

Malware

Clean Violated Data Centers

Victim of Crime

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.

Touch Point

- Are you looking for miscreant activities on your network?
- If you have IPv6 turned on – are you watching?
- Are you looking for v6 in v4 tunnels?
- Recommendation – Views from your Network & from the Outside World:
  - Free Server from www.shawdowserver.org

Get Reports On Your Network

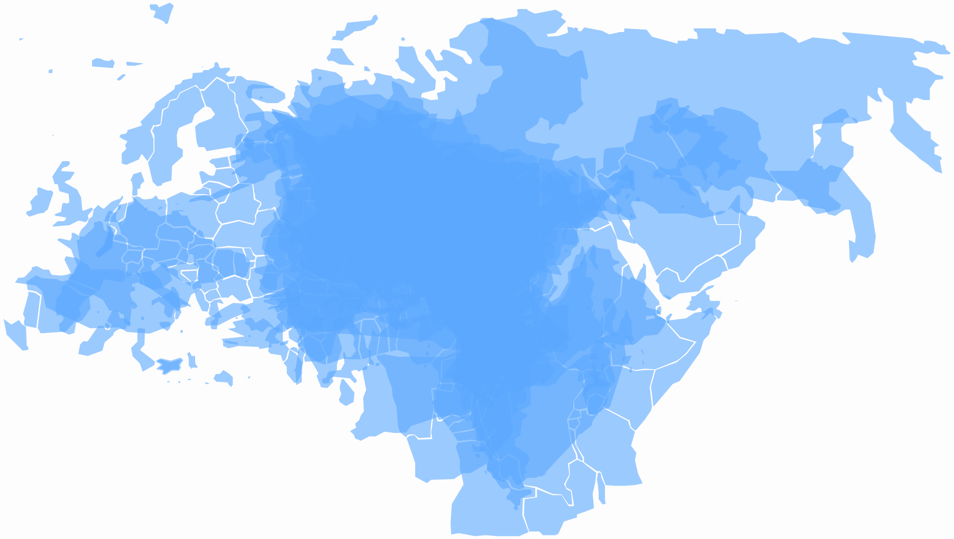
Shadowserver - ASN & Netblock Alerting & Reporting Service

The Shadowserver Foundation is pleased to announce the formal rollout of

Understanding Today's Cyber-Criminal Behavior Drivers

Our Traditional View of the World

The Reality of the Internet
No Borders



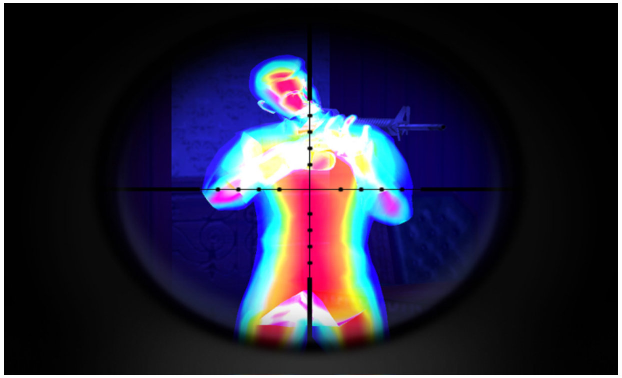
How to project civic society and the rule of law where there is no way to enforce the law?

The Good Guys are part of the the Security Problem

- The “White Hat” Security Community fixates on the mechanics – rushing to blog details of how the malware works and how the botnet is built.
- *It is like the US Drug Enforcement Agency approaching the Meth epidemic with this approach:*
  - *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.*
- *What about the Meth criminal eco-system? What about the gangs? What about the victims?*

The Good Guys are part of the 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.

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)

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?

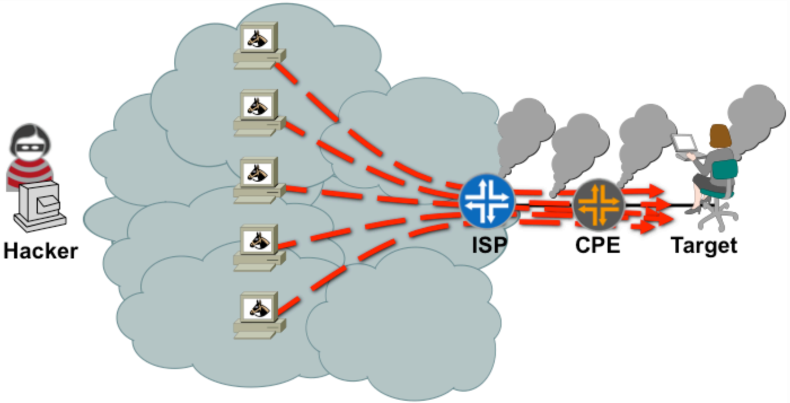
Why Use DNS “Noisy” Poisoning when it is easier to violate a ccTLD?

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

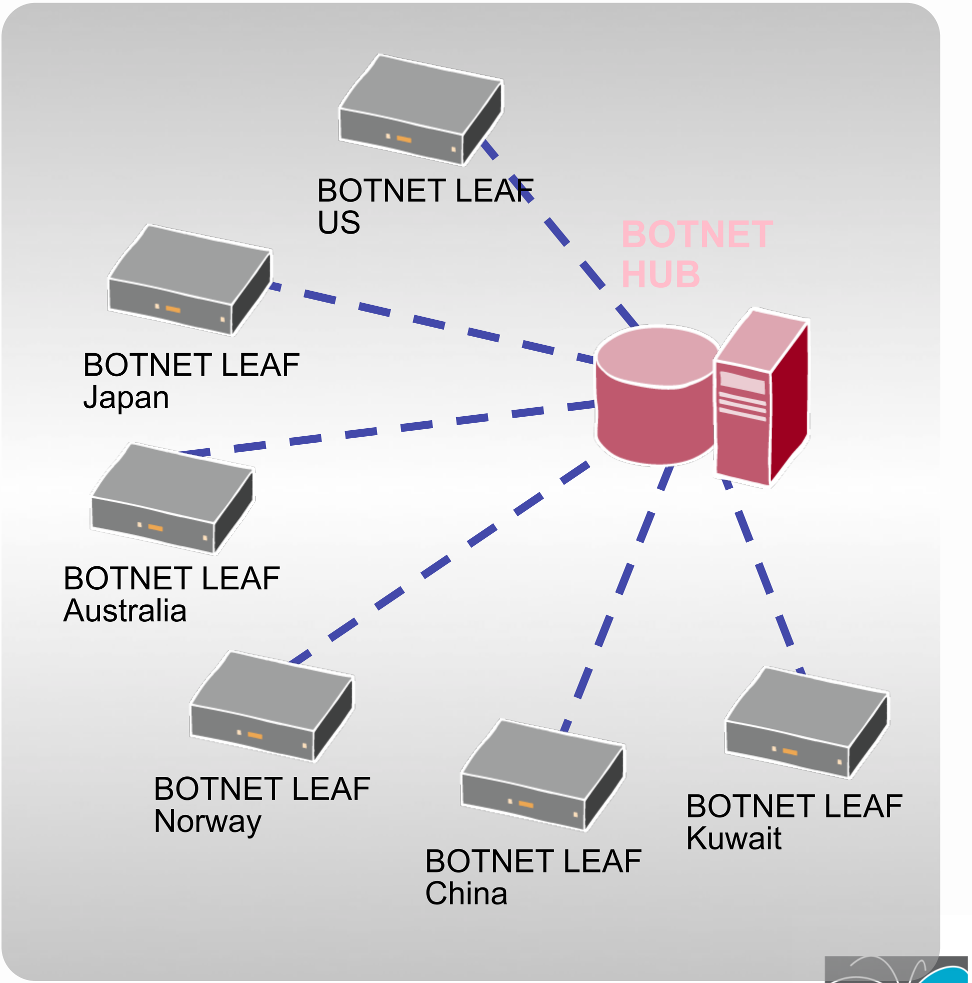
Principle 4: If You Cannot Take Out The Target…

- 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

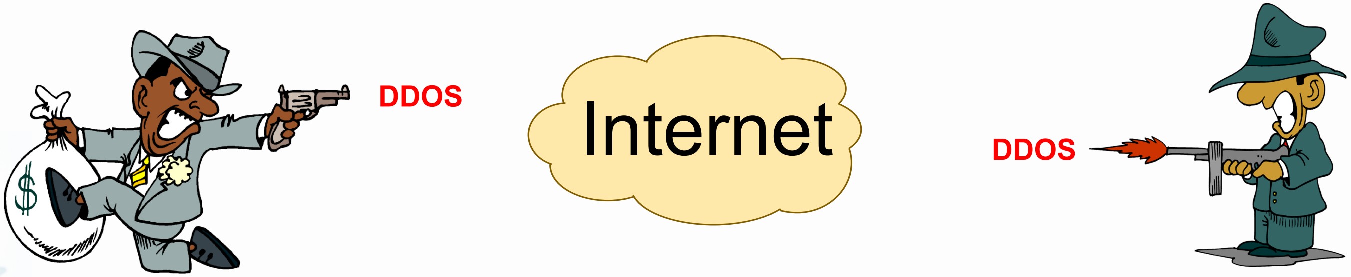
- If your activity is something that would not want everyone around you to know about, then you are a miscreant target
- Why? Cause when you become a victim, you are not motivated to call the authorities
- Examples:
  - Someone addicted to gambling is targeted via a Phishing site
  - Someone addicted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

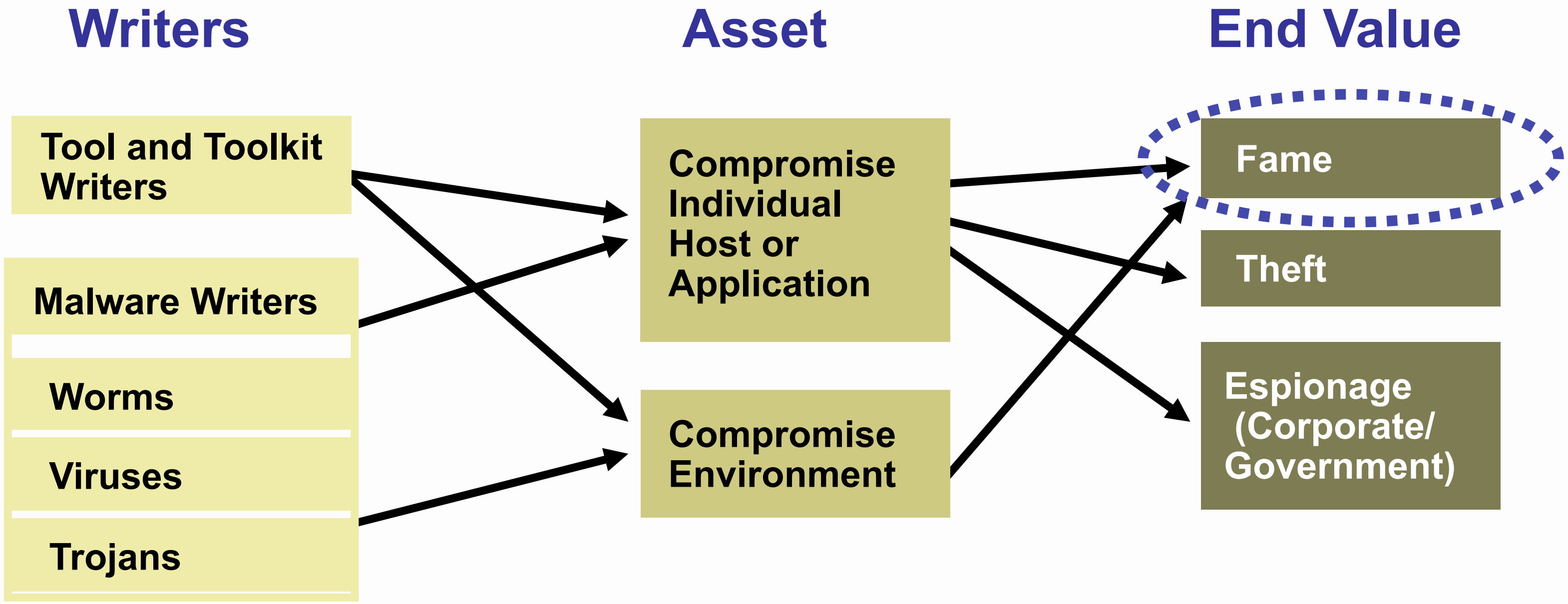
Enduring Financial Opportunities

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



Writers

Tool and Toolkit Writers

Malware Writers

Worms

Viruses

Trojans

Asset

Compromise Individual Host or Application

Compromise Environment

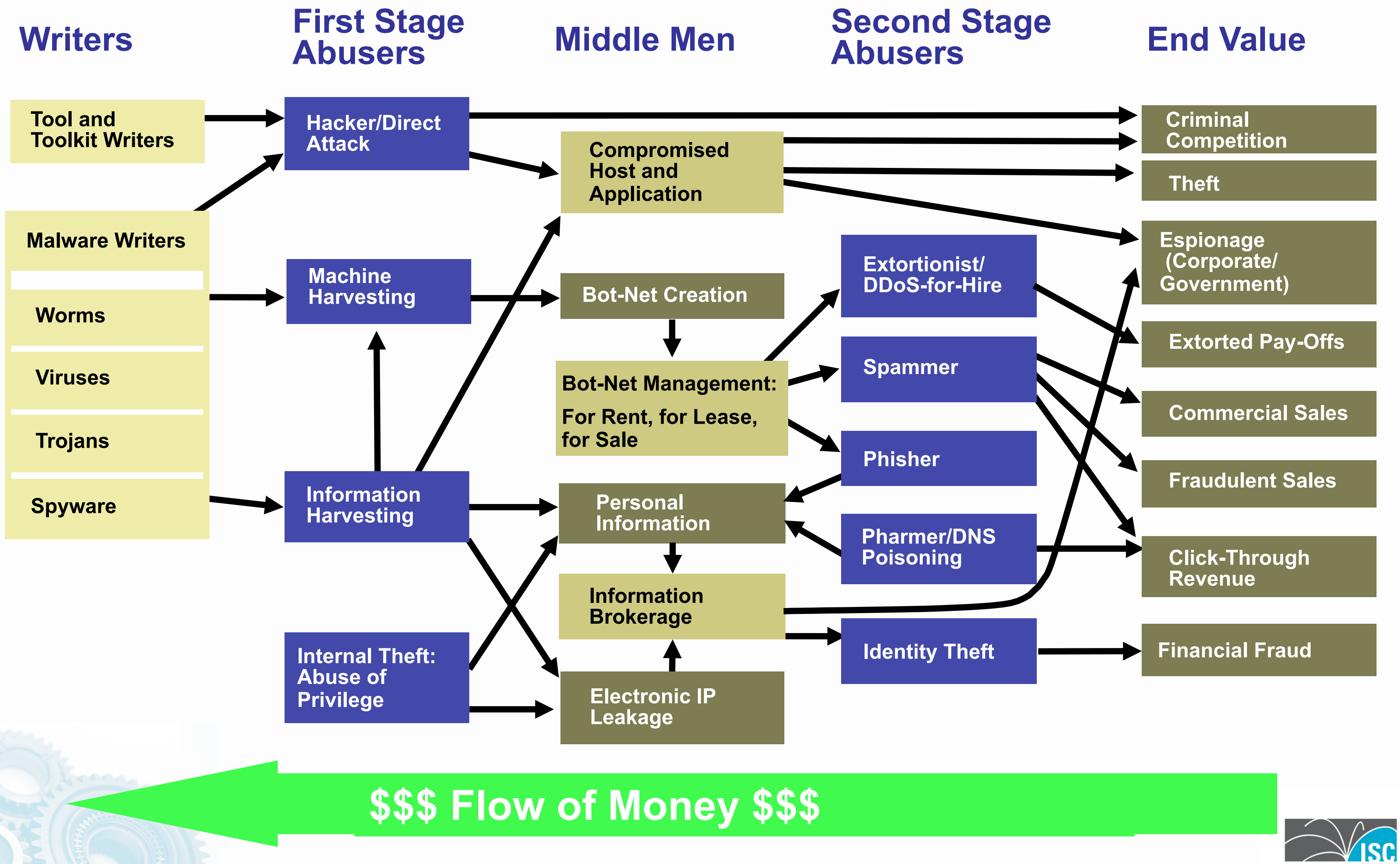
End Value

Fame

Theft

Espionage (Corporate/ Government)

Threat Economy: Today



Writers

First Stage Abusers

Middle Men

Second Stage Abusers

End Value

Tool and Toolkit Writers

Malware Writers

Worms

Viruses

Trojans

Spyware

Hacker/Direct Attack

Machine Harvesting

Information Harvesting

Internal Theft: Abuse of Privilege

Compromised Host and Application

Bot-Net Creation

Bot-Net Management:

For Rent, for Lease, for Sale

Personal Information

Information Brokerage

Electronic IP Leakage

Extortionist/ DDoS-for-Hire

Spammer

Phisher

Pharmer/DNS Poisoning

Identity Theft

Criminal Competition

Theft

Espionage (Corporate/ Government)

Extorted Pay-Offs

Commercial Sales

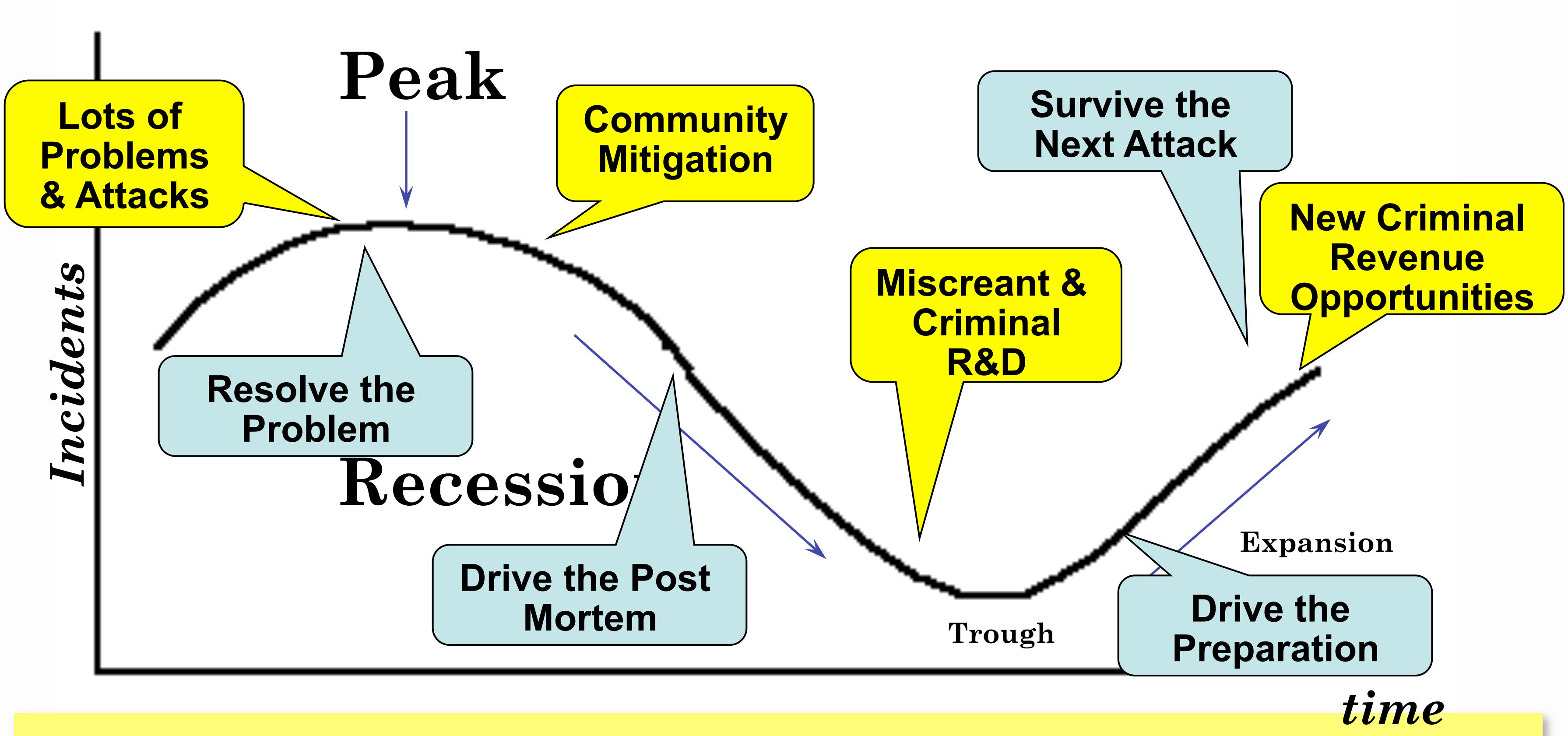
Fraudulent Sales

Click-Through Revenue

Financial Fraud

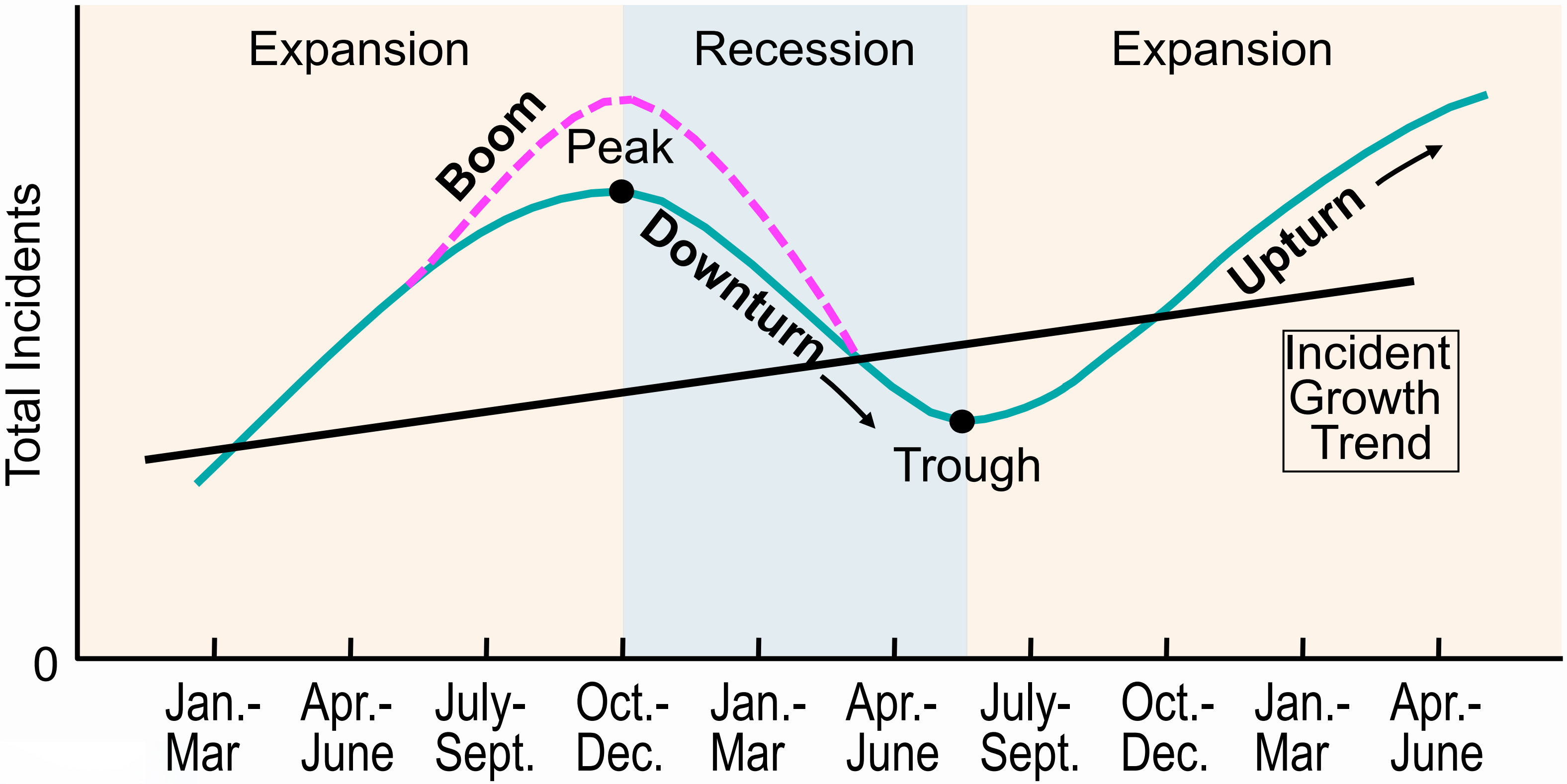
$$$ Flow of Money $$$

Miscreant - Incident Economic Cycles

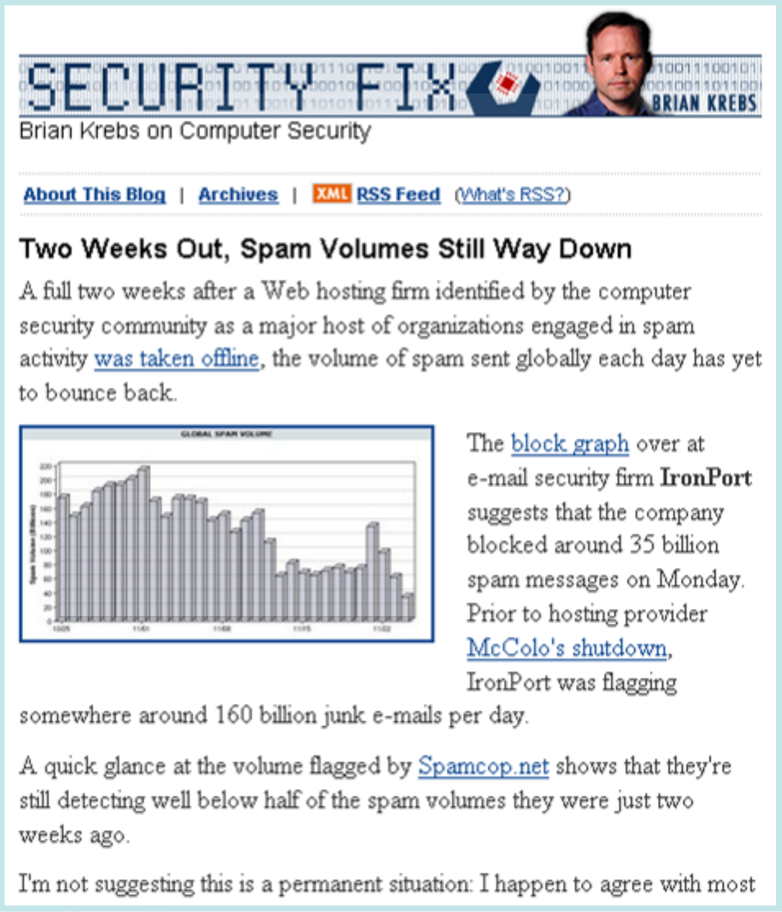


These Cycles Repeat

Miscreant Economic Cycles



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?)

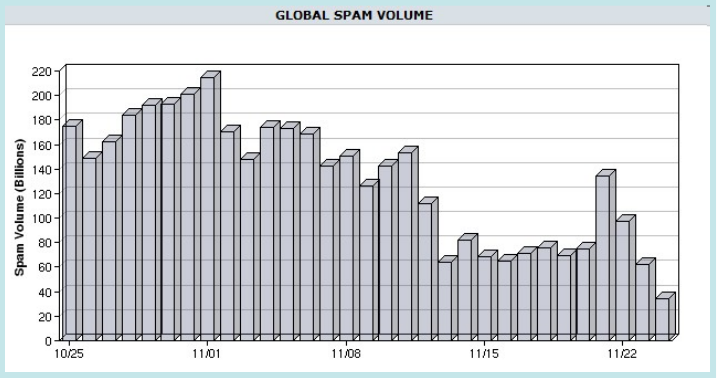
Two Weeks Out, Spam Volumes Still Way Down

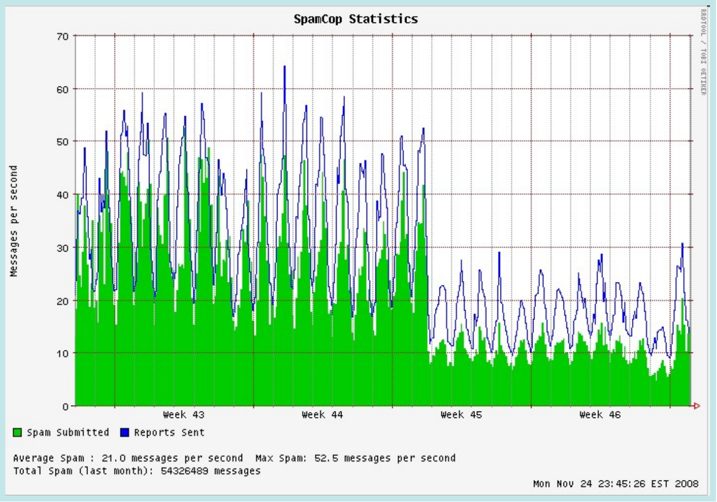
A full two weeks after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline, the volume of spam sent globally each day has yet to bounce back.

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



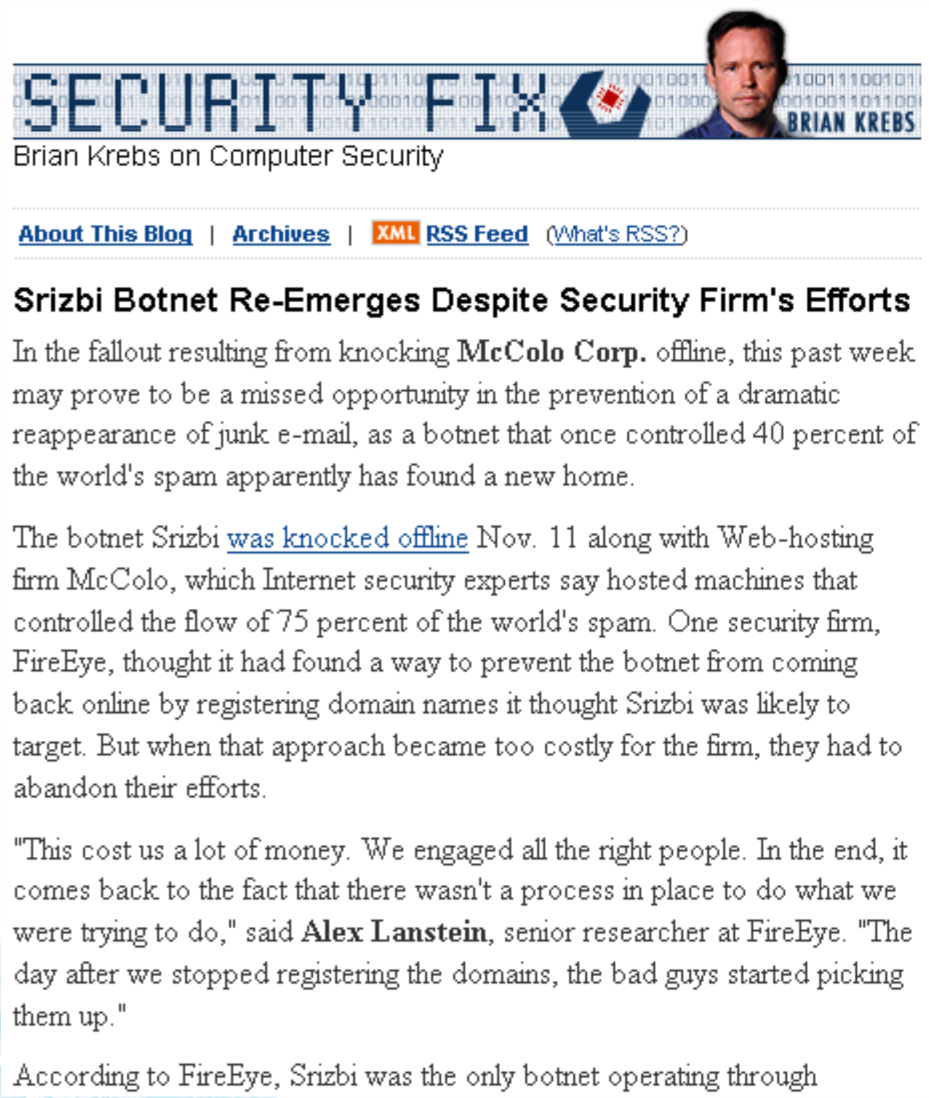


Average Spam : 21.0 messages per second Max Spam: 52.5 messages per second
Total Spam (last month): 54326489 messages

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?)

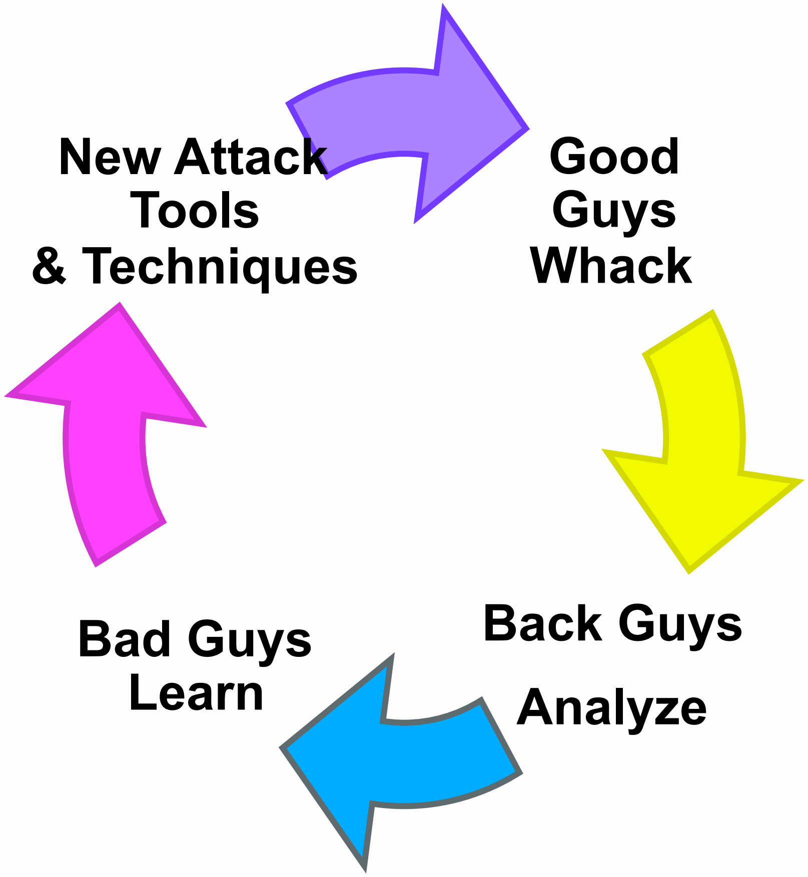
Srizbi Botnet Re-Emerges Despite Security Firm's Efforts

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.

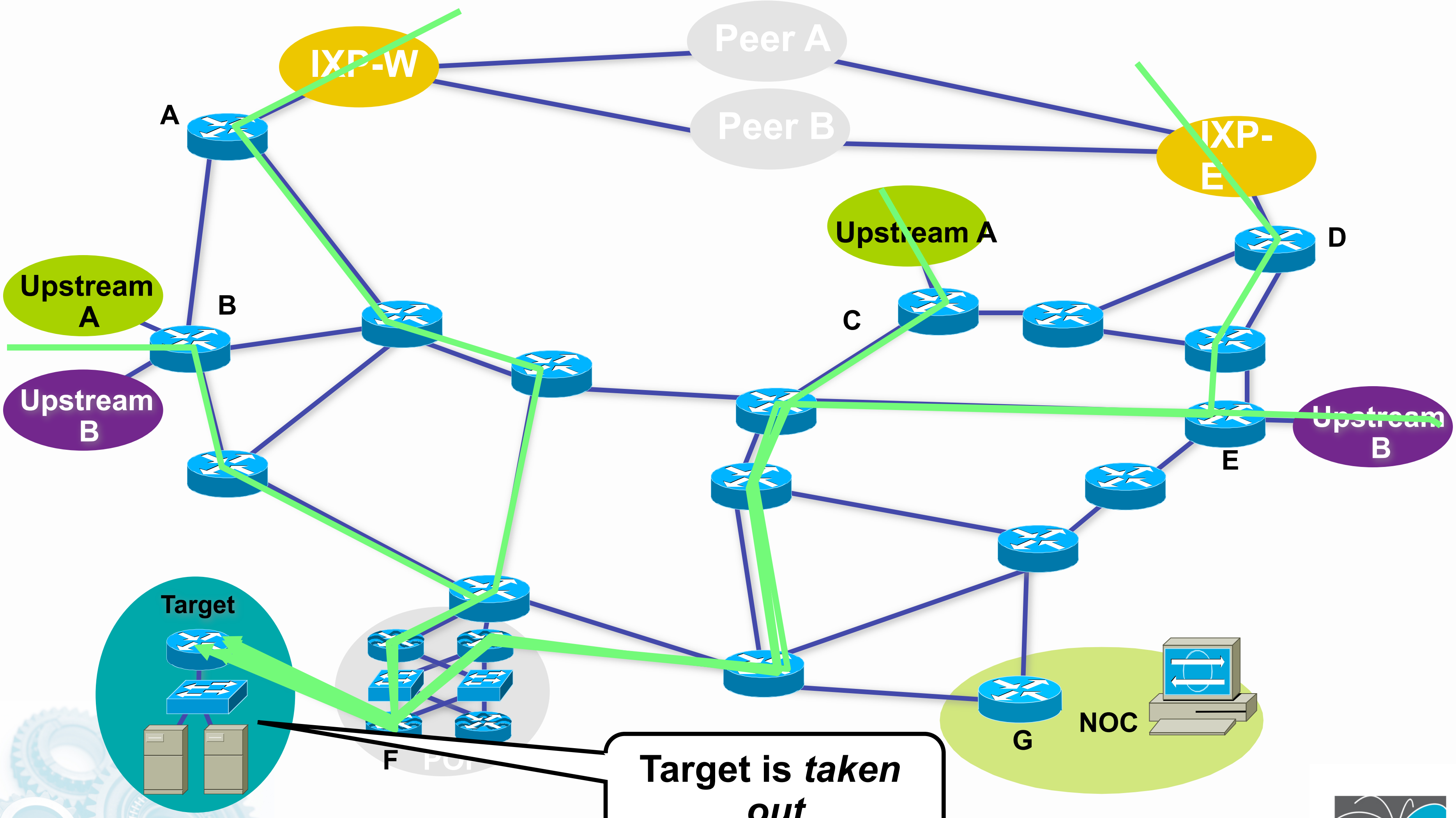
Cyber Warfare

- 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.

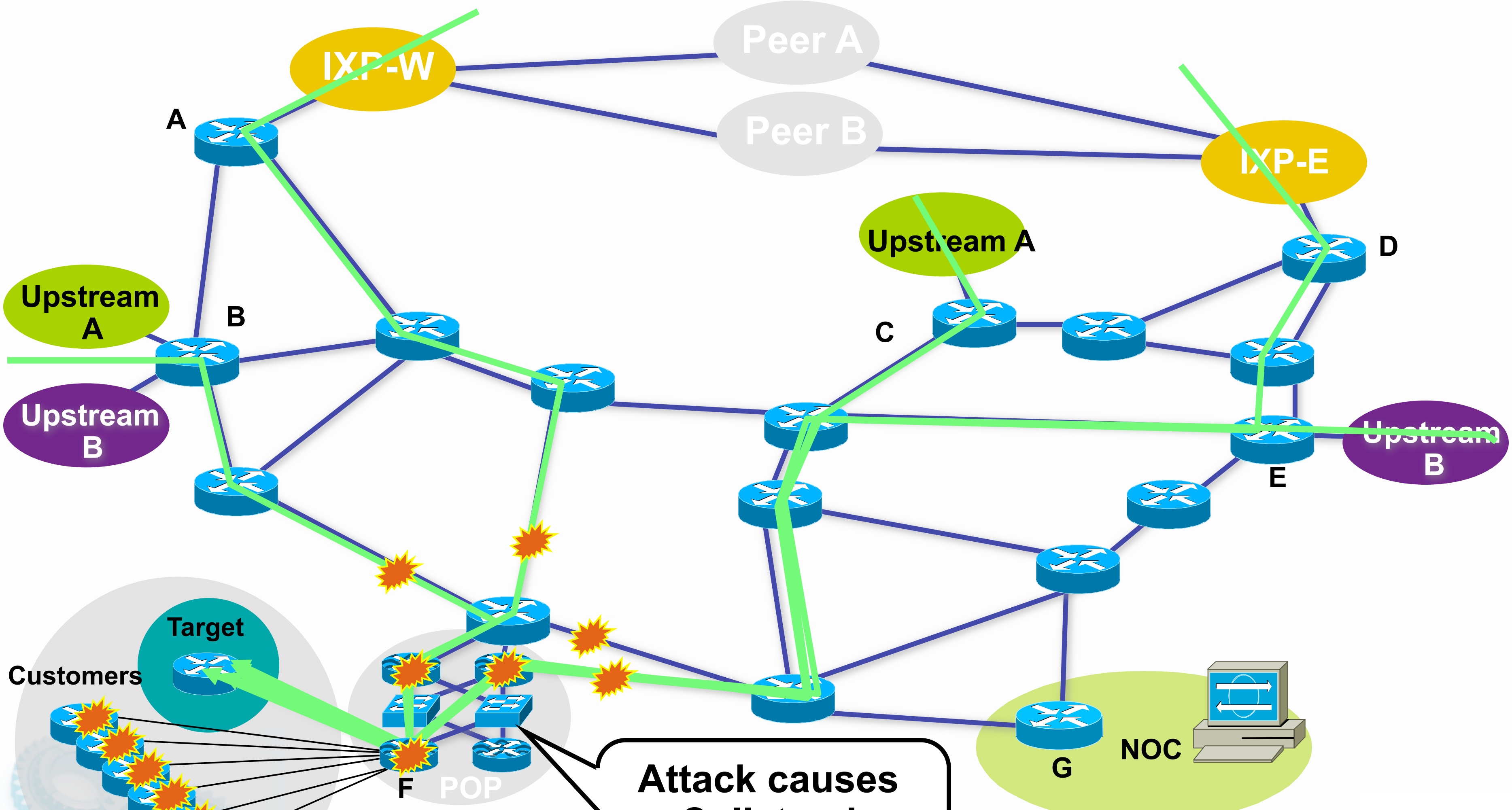
Michael Falco / The New York Times / Redux

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

谢谢理解和支持！记住随

During the attack, You may want to try the following links if

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

Touch Point

- Do you use “behavior” as a tool to help you evaluate risk?

Now What?

What can you do?

1. This security problem is happening now – with IPv4. Gain control over it now.
   - Use the IPv4 knowledge to map what you really need for dual stack.
   - Use Open Source Security tools (Bothunter, Netflow Tools, IDP/IDS tools, etc). Open source gives you experience before the big capital investment.
2. Understand that you might have a IPv6 “security problems” right now.
   - Security people inside a organization need to be pushing for strategic IPv6 deployment to gain situational awareness of the IPv6 in their network.

What can you do?

3. An IPv6 VISIBILITY plan is needed as part of your IPv6 deployment.
   - Given the criminal economic incentives behind the threat, all organizations need to have visibility tools as an integral part of their IPv6 plan.
   - Passive DNS, Open Source Netflow, IPv6 Sinkholes, Network management, logging (compatible with IPv6).
5. Yes, you will need a IPv6 Security Plan.
   - Know how you security team is going to cope with IPv6.

No Excuses!

- An organization cannot use the dynamics & threat of the cyber criminal ecosystem to not deploy IPv6.
- The pace if IPv6 migration is not in the control of the end-user. Moving from “zero” to “100” is a crowd dynamic.
- That “crowd” can move the industry faster than anyone expects.
- The criminals will follow the crowd – following their potential markets.

Plug into the Operational Security Community

- Step 1: Get the Operational and Security Contacts for each of your peering and transit networks.
  - Get their phone numbers, Chat IDs, and E-mails.
  - Find out what tools they have deployed to help you "work an attack" and "work a criminal investigation."
  - Find out what other civic self-defense groups they belong to.
- Step 2: Join open "security communities" which allow you to work with others to defend each other.
  - CERTs
  - ISACs
  - Others.
- Step 3: Act! Do Something! Fight Back!
  - Investigate – pursue – take legal action
  - Call Law Enforcement – pull in the police – file a case
  - International Laws only change through action

What can you do?

- Join the Security Information Exchange Forum (SIE@ISC).
  - Forum only briefings on the threat and tools used to change the battle against the threat.
  - Connect you and your organizations to the most appropriate operational security communities – building the sphere of trust with peers
  - Funding the tools the Operational Security Community need to track the threats, disrupt the threat, and put the community into a position to arrest the threat.
  - Gain insight into how “collective defense” protects everyone. everyone.

+
+
= SIE@ISC
Security
Trust
Information

Send E-mail to info@sie.isc.org

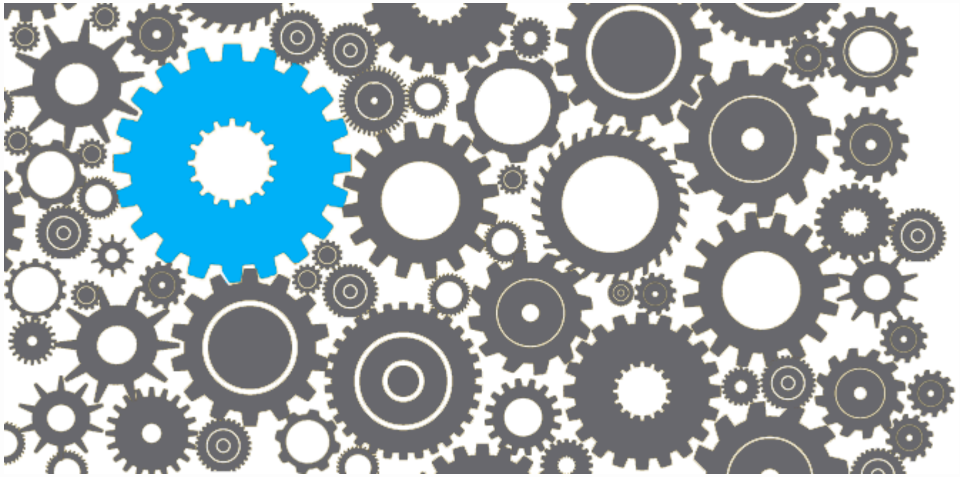
Summary and Questions

Internet Systems Consortium (ISC)

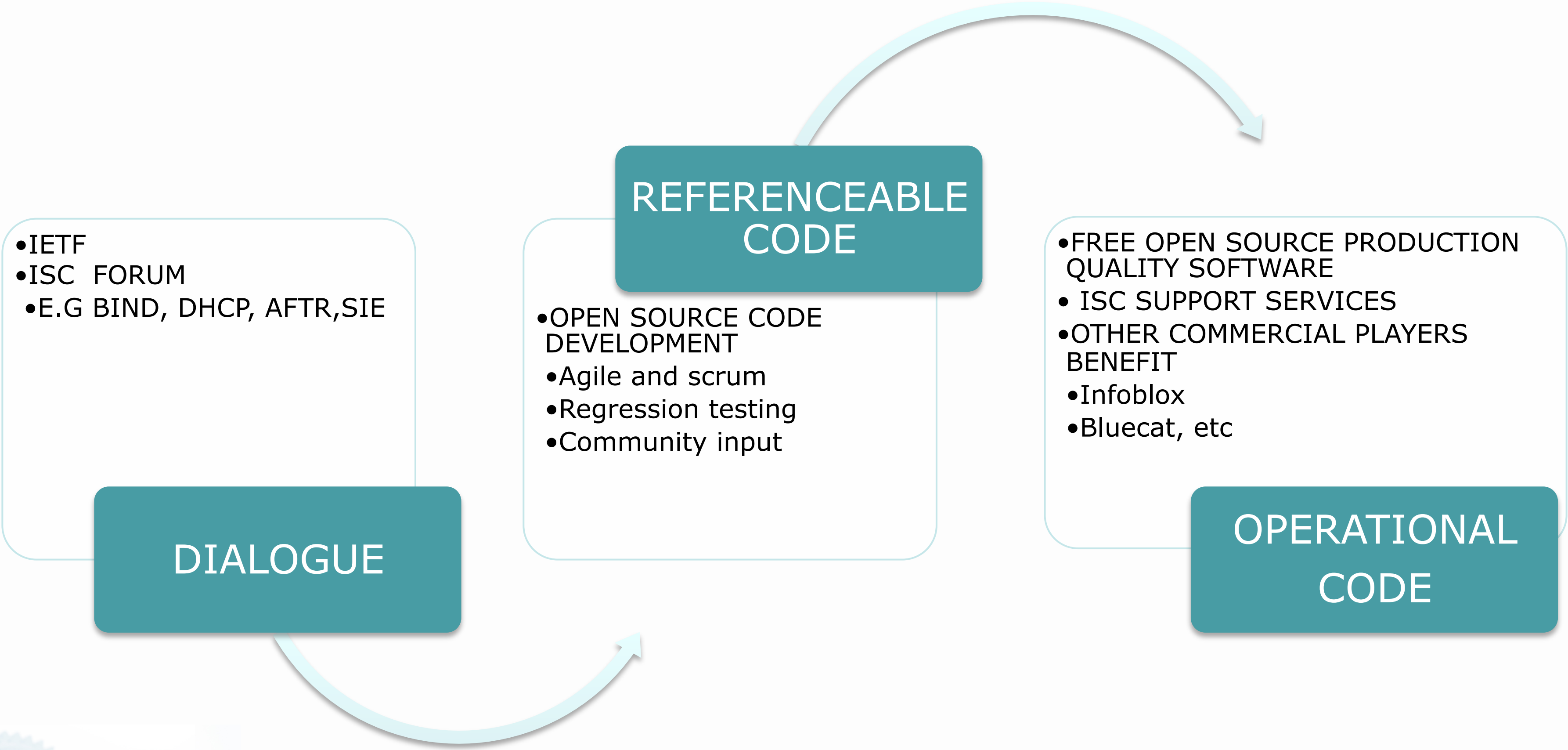
How we can help your IPv6 Journey

Who Builds the Cogs?

- The Internet's "Guts" require someone to build the cogs which keep the Internet moving.
- These "cogs" need to be open and accessible to anyone who wants to connect to the Internet.
- Standards need to be open so that anyone can build.
- Enter the Internet Systems Consortium (ISC)



Technology Leadership for the Common Good



DIALOGUE

- IETF
- ISC FORUM
  - E.G BIND, DHCP, AFTR,SIE

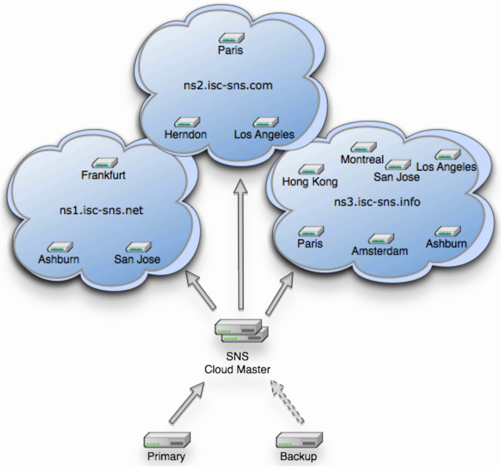
REFERENCEABLE CODE

- OPEN SOURCE CODE DEVELOPMENT
  - Agile and scrum
  - Regression testing
  - Community input

OPERATIONAL CODE

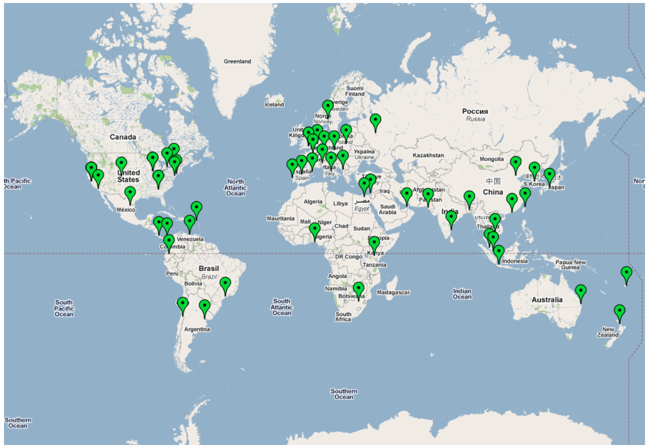
- FREE OPEN SOURCE PRODUCTION QUALITY SOFTWARE
- ISC SUPPORT SERVICES
- OTHER COMMERCIAL PLAYERS BENEFIT
  - Infoblox
  - Bluecat, etc

More "Common Good" Activities



Secondary DNS
Services

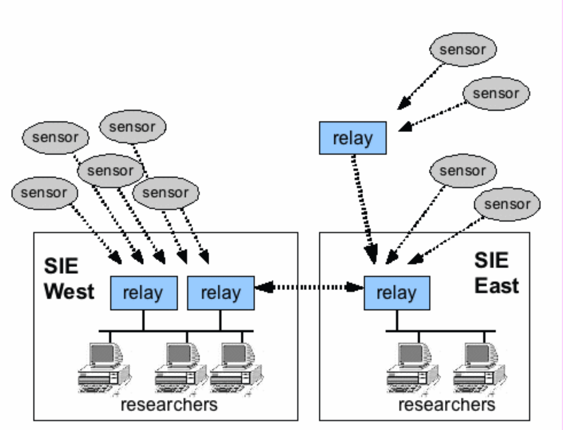
DNS Everywhere
IPv6
DNSSEC
OPS-SEC



DNS F-Root

Hosted @ w/ Open Source Community and Others

free the lizard! mozilla.org
OpenLDAP
FreeBSD
openBSD
NetBSD
PC-BSD
nic MX
nic at the austrian registry
registro.br
DENIC de
CNNIC 中国互联网络信息中心 China Internet Network Information Center
NIC CHILE
creative commons
Keio University
INTERNET ARCHIVE
PLoS PUBLIC LIBRARY of SCIENCE



Security Data Peering

Sustainability while Serving Community

- Professional Services
  - Software Support
  - Training
  - Consulting
- Custom Software Development
  - Usability features
  - Operation Improvements
  - Private branches
  - Proto types
  - Integration/APIs

New from ISC

Open Source Routing Forum

Security + Trust + Information = SIE@ISC

ISC In a Nutshell

Forum

- BIND
- BIND 10 Working Group
- DHCP
- AFTR/PCP
- SIE
- Open Source Routing

RPKI (Securing BGP) and more to come … first reference, standards based code.

Professional Services

- Consulting
- Training
- Software Support Services
- Custom Software Development
- F-root Corporate Node
- DNS SNS-Com
- Full version The Domain Survey

Public Benefit Services

- DNS “F-ROOT”
- DNS Secondary Server Resiliency (SNS) PB
- Hosted@ - hosting a range of open source code)
- Free Domain Survey Report
- ISC assistance at IETF, ICANN, ARIN, ISOC RIPE WG, UKNOF, etc

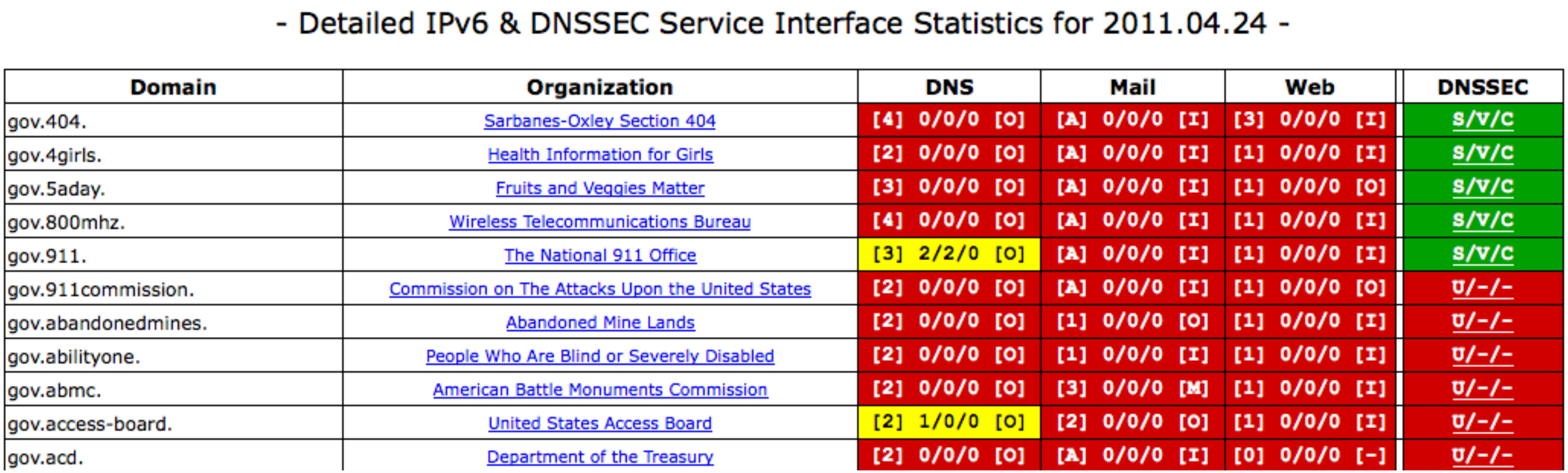
Empowerment

- Standards drivers – with first implementation of standards based code.
- Policy Meetings – Empowering Spheres of Influence
- Operational Security – Pioneering new approaches to safe guard the Internet (OPSEC-Trust).
- Operations Meeting Empowerment (APRICOT, AFNOG, NANOG, etc)
- Research (DNS OARC)

How can ISC Help?

(Keeping it Simple)

1. Check your Ipv6 Health @ http://usgv6-deploymon.antd.nist.gov/



- Detailed IPv6 & DNSSEC Service Interface Statistics for 2011.04.24 -

Domain	Organization	DNS	Mail	Web	DNSSEC
gov.404.	Sarbanes-Oxley Section 404	[4] 0/0/0 [O]	[A] 0/0/0 [I]	[3] 0/0/0 [I]	S/V/C
gov.4girls.	Health Information for Girls	[2] 0/0/0 [O]	[A] 0/0/0 [I]	[1] 0/0/0 [I]	S/V/C
gov.5aday.	Fruits and Veggies Matter	[3] 0/0/0 [O]	[A] 0/0/0 [I]	[1] 0/0/0 [O]	S/V/C
gov.800mhz.	Wireless Telecommunications Bureau	[4] 0/0/0 [O]	[A] 0/0/0 [I]	[1] 0/0/0 [I]	S/V/C
gov.911.	The National 911 Office	[3] 2/2/0 [O]	[A] 0/0/0 [I]	[1] 0/0/0 [I]	S/V/C
gov.911commission.	Commission on The Attacks Upon the United States	[2] 0/0/0 [O]	[A] 0/0/0 [I]	[1] 0/0/0 [O]	U/-/-
gov.abandonedmines.	Abandoned Mine Lands	[2] 0/0/0 [O]	[1] 0/0/0 [O]	[1] 0/0/0 [I]	U/-/-
gov.abilityone.	People Who Are Blind or Severely Disabled	[2] 0/0/0 [O]	[1] 0/0/0 [I]	[1] 0/0/0 [I]	U/-/-
gov.abmc.	American Battle Monuments Commission	[2] 0/0/0 [O]	[3] 0/0/0 [M]	[1] 0/0/0 [I]	U/-/-
gov.access-board.	United States Access Board	[2] 1/0/0 [O]	[2] 0/0/0 [O]	[1] 0/0/0 [I]	U/-/-
gov.acd.	Department of the Treasury	[2] 0/0/0 [O]	[A] 0/0/0 [I]	[0] 0/0/0 [-]	U/-/-

2. If your DNS or DNSSEC is RED (i.e. not IPv6 dual stack), contact ISC for help. Everyone needs to be GREEN.
3. Send an E-mail to info@isc.org to start the conversation.