ccTLD Security

Understanding the Anxiety and Consequences

Barry Raveendran Greene

bgreene@isc.org

Version 1.1

Agenda

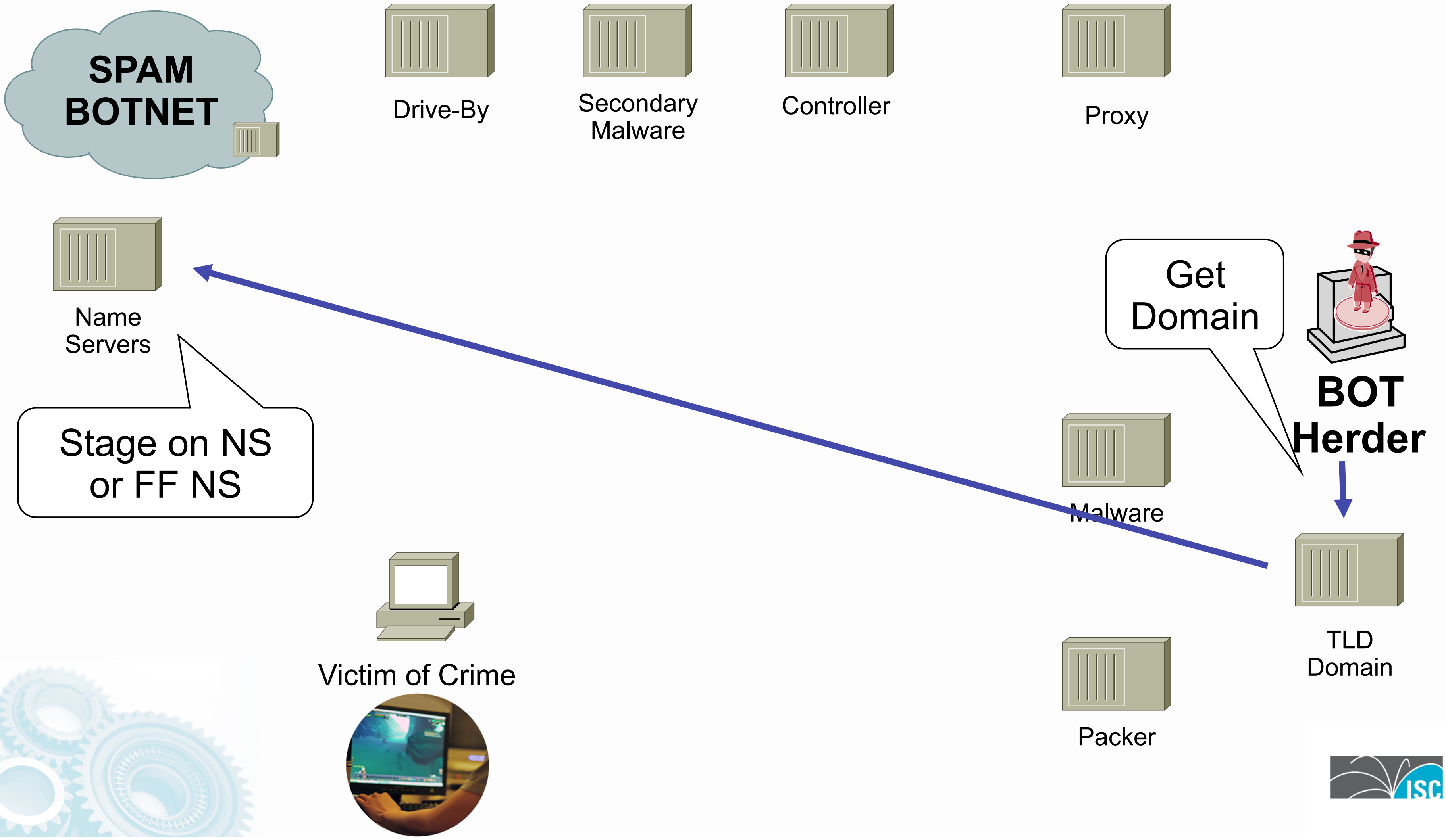
- ccTLD Security is not “new”
- Cybercriminal Toolkit
- Understanding why security people are irritated might help to provide context.
- Criminal Complicity, Internet Embargo, Chain of Consequence
- What can a ccTLD do now?

ccTLD Security is not “New”

- ICANN - Security and Stability Advisory Committee (SSAC)
- ICANN - Attack and Contingency Response Planning (ACRP)
- APTLD Guidelines for Operation of DNS Infrastructure by ccTLDs
- DNS-OARC Guidelines
- Lots of presentations:
  - ICANN and DNS Security, Stability and Resiliency Activities by Greg Rattray
  - Best Practices of a ccTLD Registry by Adrian Kinderis
  - Introducing ICANN Security, Stability and Resiliency Activities - DNS Security Training – by Yurie Ito
  - ccTLD Best Practices by Michuki Mwangi
  - ccTLD Best Practices & Considerations by John Crain
  - ccTLD Best Practices & Considerations by Kim Davies

Cyber Criminal Toolkit

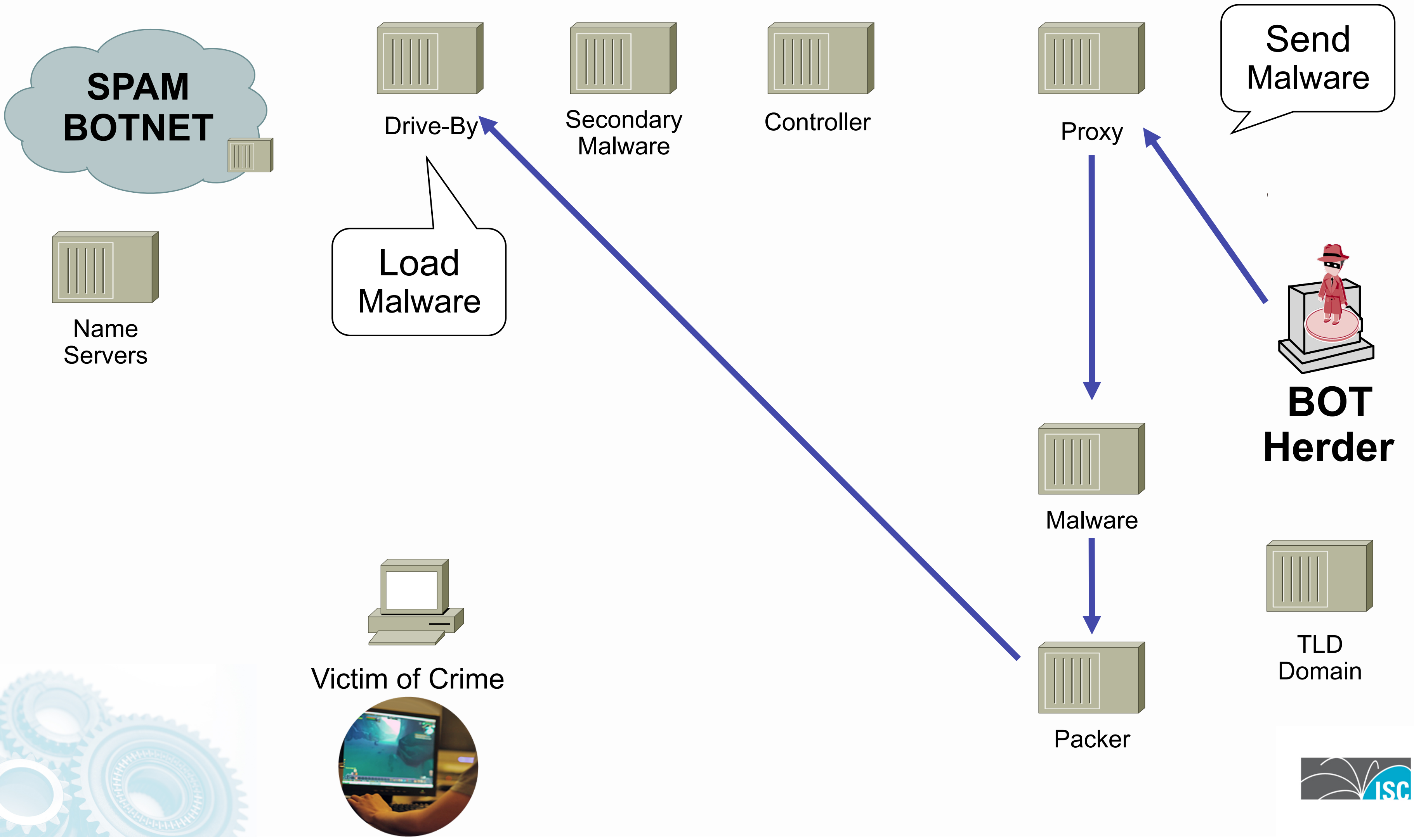
Stage Domain Name



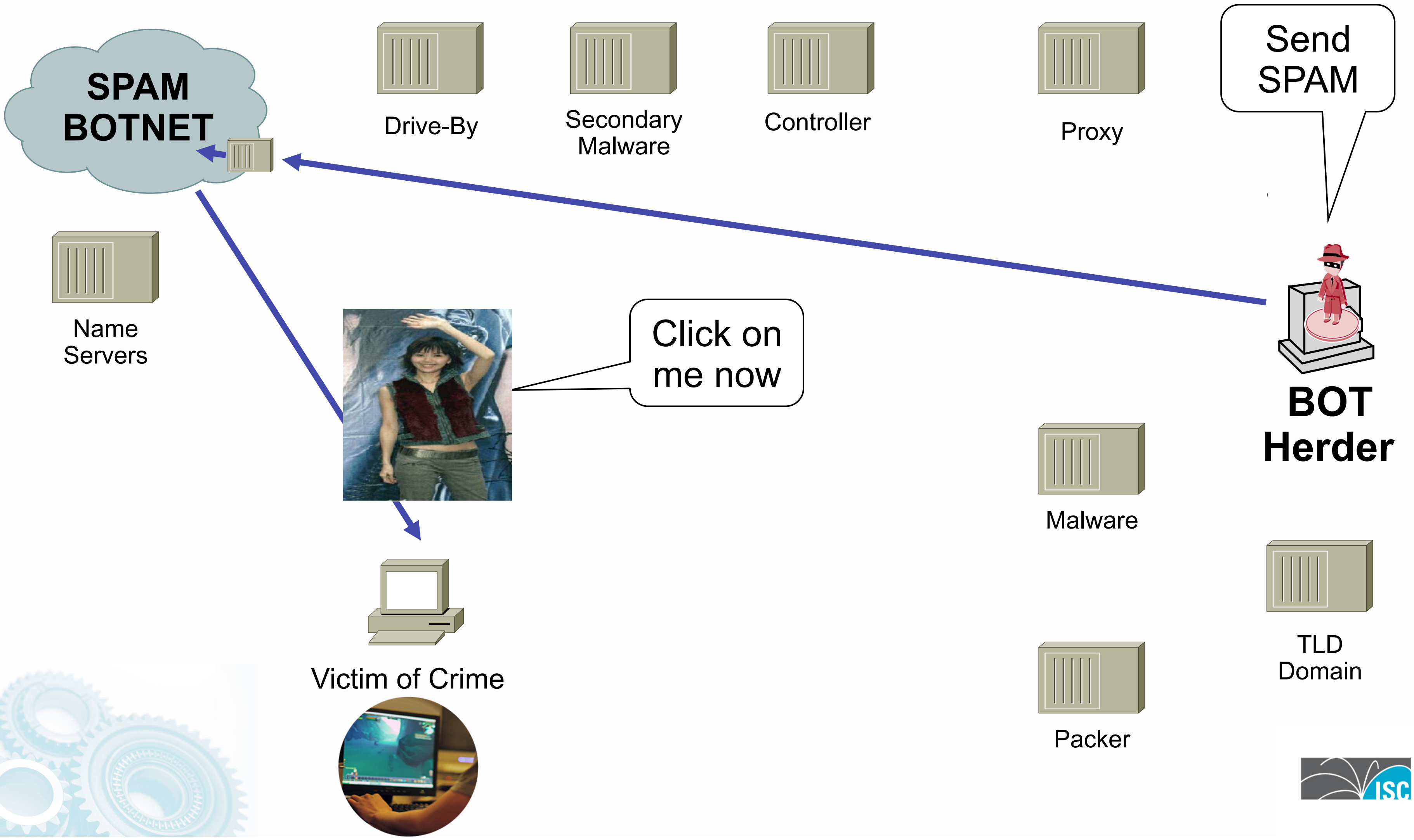
Get Domain

Stage on NS or FF NS

Prepare Drive-by



Send SPAM to get People To Click



SPAM BOTNET

Drive-By

Secondary Malware

Controller

Proxy

Send SPAM

Name Servers

Click on me now

BOT Herder

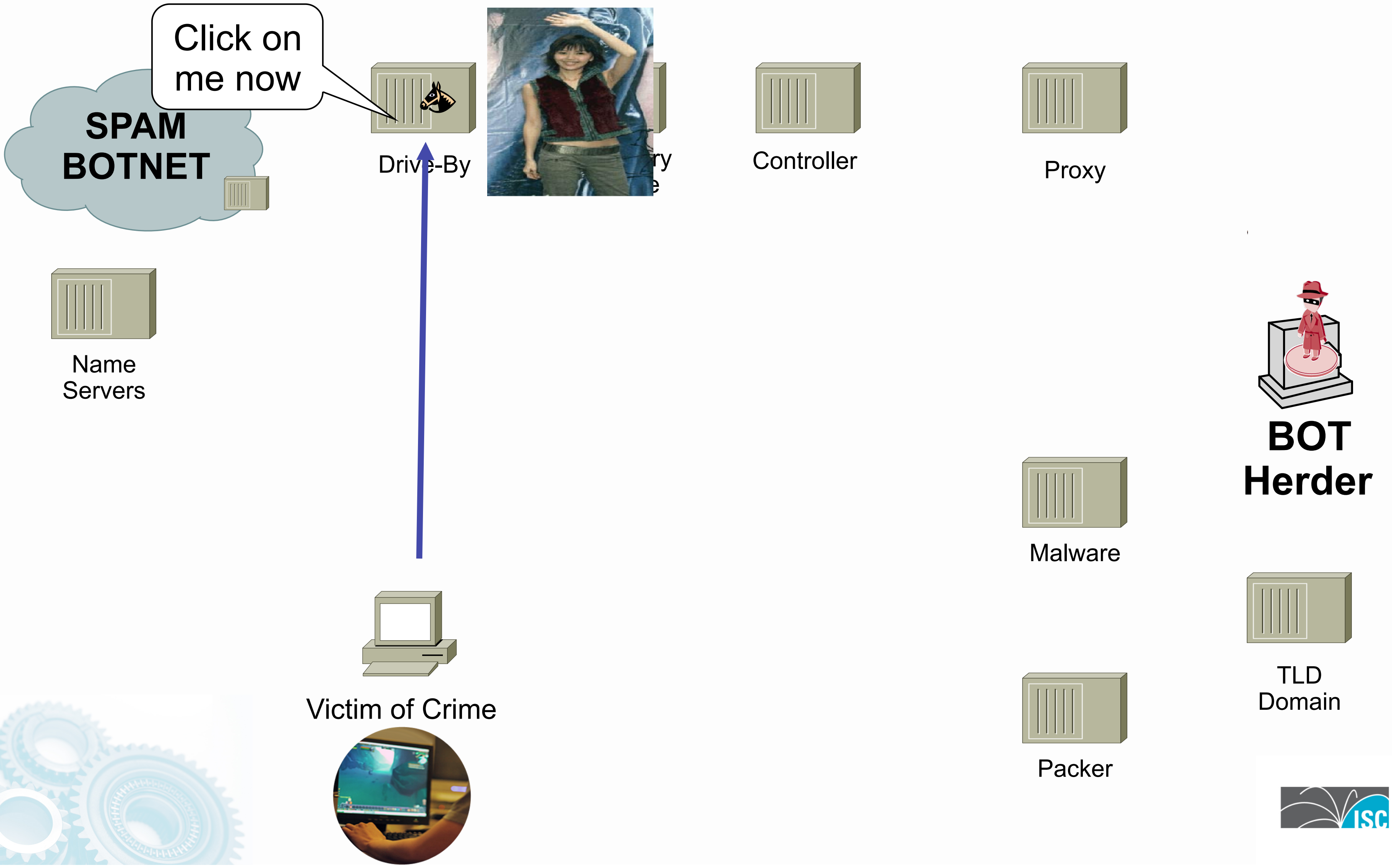
Malware

TLD Domain

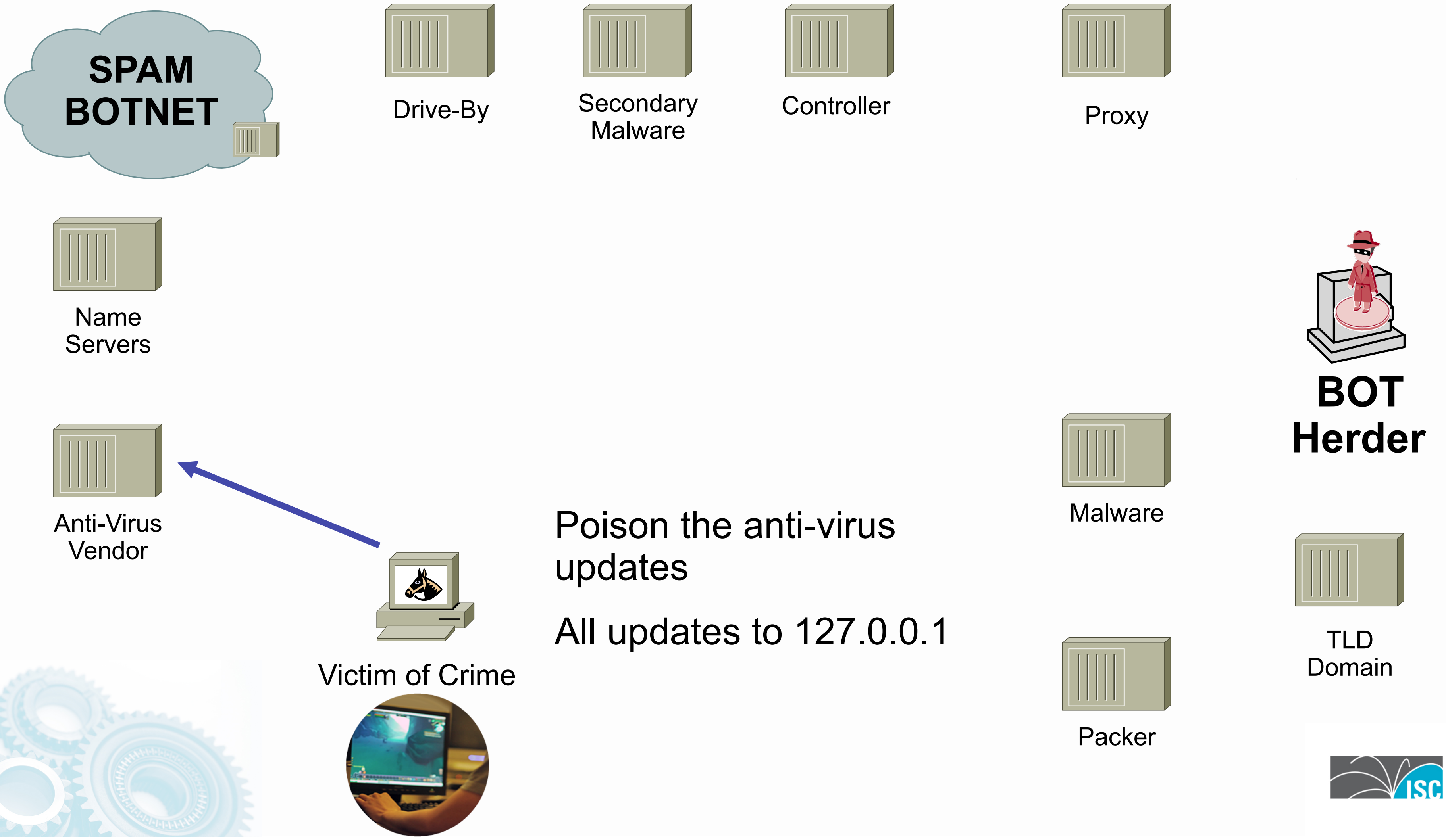
Victim of Crime

Packer

Drive By Violation



Poison Anti-Virus Updates



SPAM BOTNET

Drive-By

Secondary Malware

Controller

Proxy

Name Servers

BOT Herder

Anti-Virus Vendor

Malware

Victim of Crime

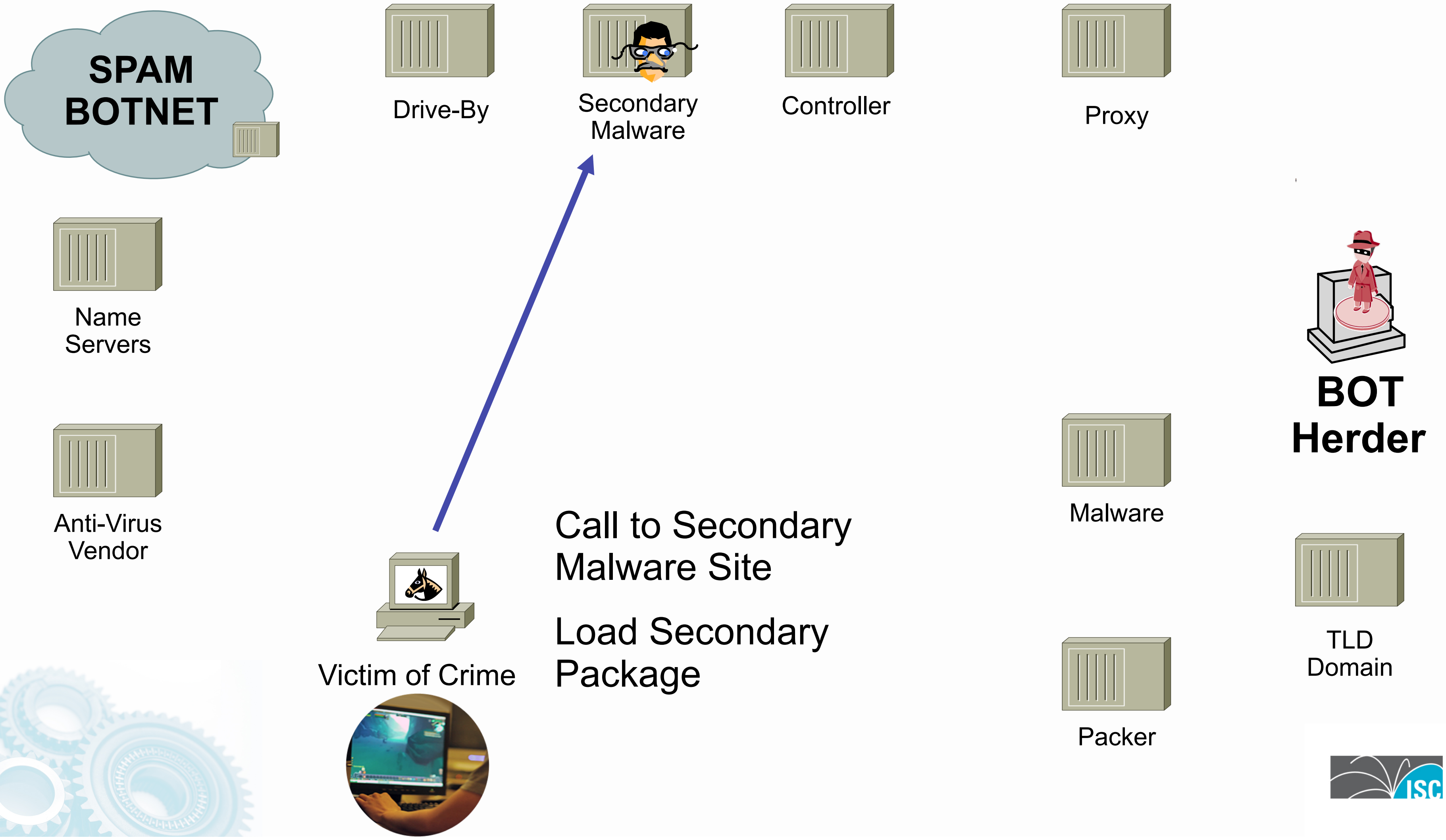
TLD Domain

Packer

Poison the anti-virus updates

All updates to 127.0.0.1

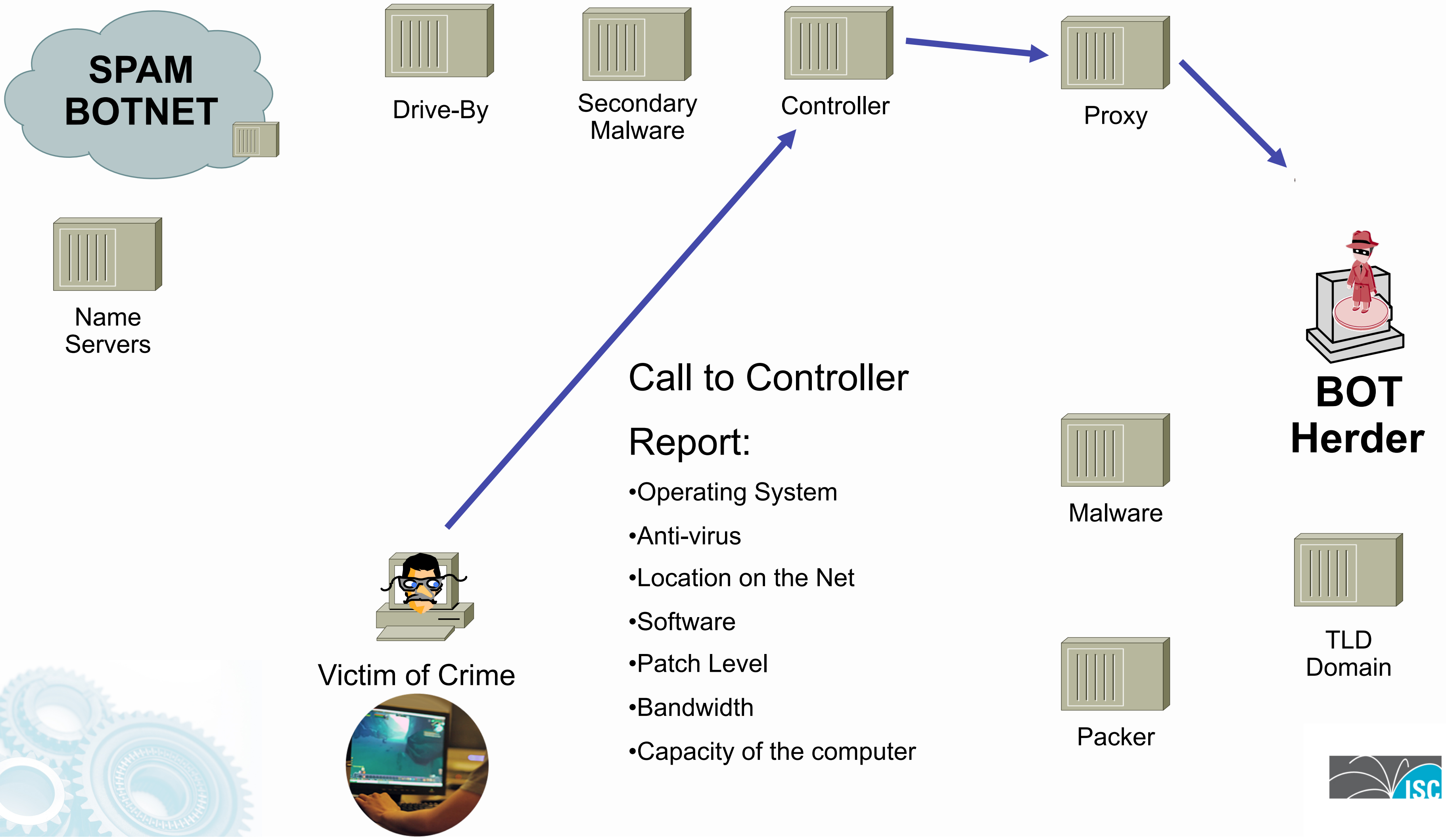
Prepare Violated Computer



Call to Secondary Malware Site

Load Secondary Package

Call Home

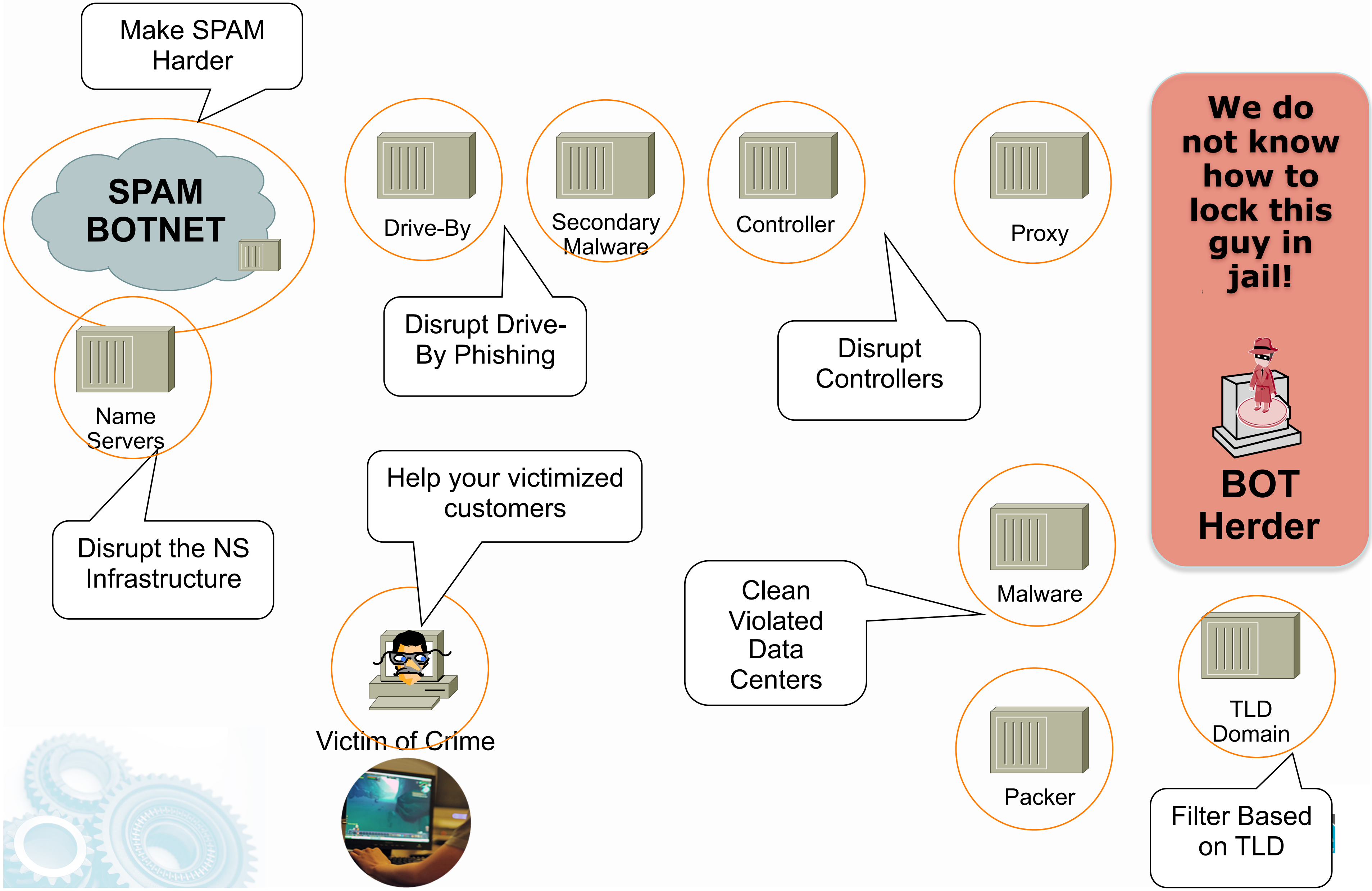


Call to Controller

Report:

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

What can an ANS do?



Make SPAM Harder

SPAM BOTNET

Name Servers

Disrupt the NS Infrastructure

Drive-By

Secondary Malware

Disrupt Drive-By Phishing

Controller

Disrupt Controllers

Proxy

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

BOT Herder

Help your victimized customers

Victim of Crime

Clean Violated Data Centers

Malware

Packer

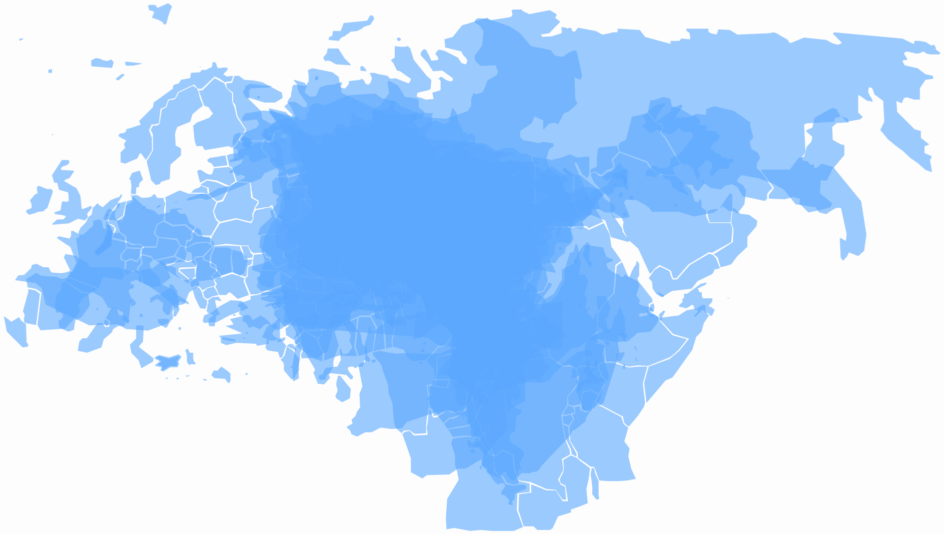
TLD Domain

Filter Based on TLD

Why Cyber-Crime is Institutionalized?

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)

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?

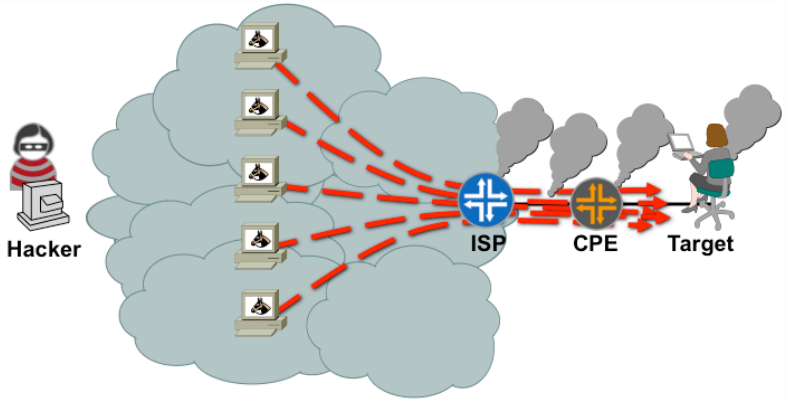
Why Use DNS “Noisy” Poisoning when it is easier to violate a ccTLD?

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

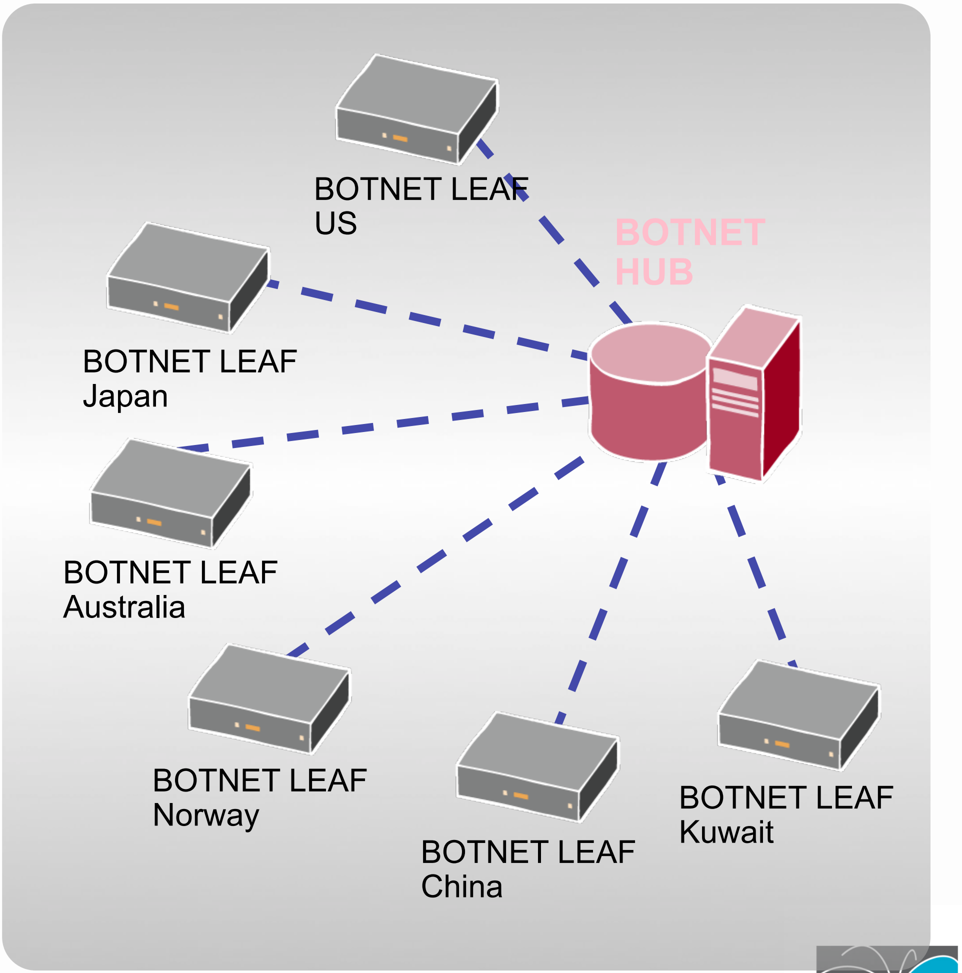
Principle 4: If You Cannot Take Out The Target…

- 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

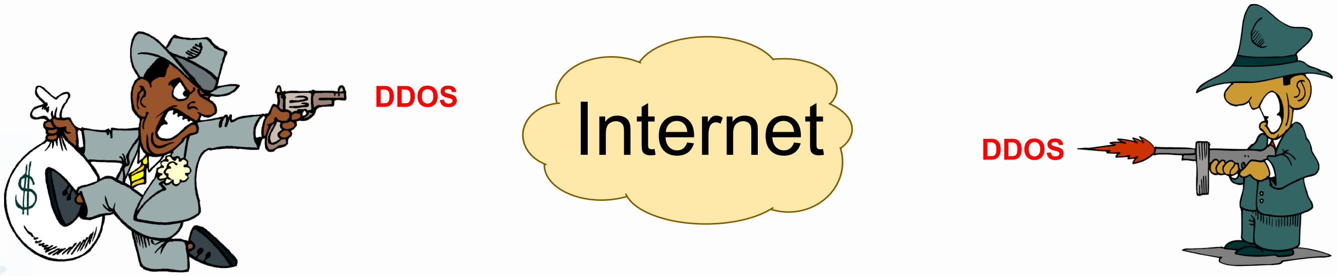
- If your activity is something that would not want everyone around you to know about, then you are a miscreant target
- Why? Cause when you become a victim, you are not motivated to call the authorities
- Examples:
  - Someone addicted to gambling is targeted via a Phishing site
  - Someone addicted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



DDOS

Internet

DDOS

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.

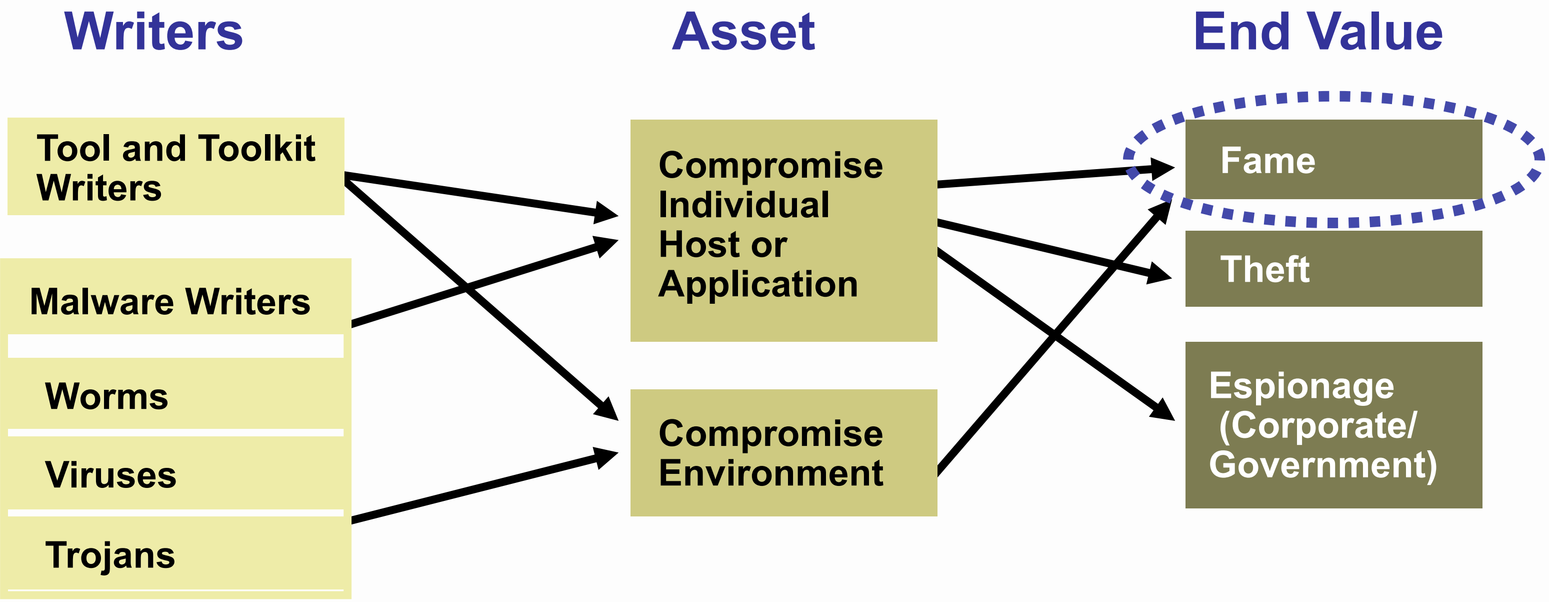
Enduring Financial Opportunities

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

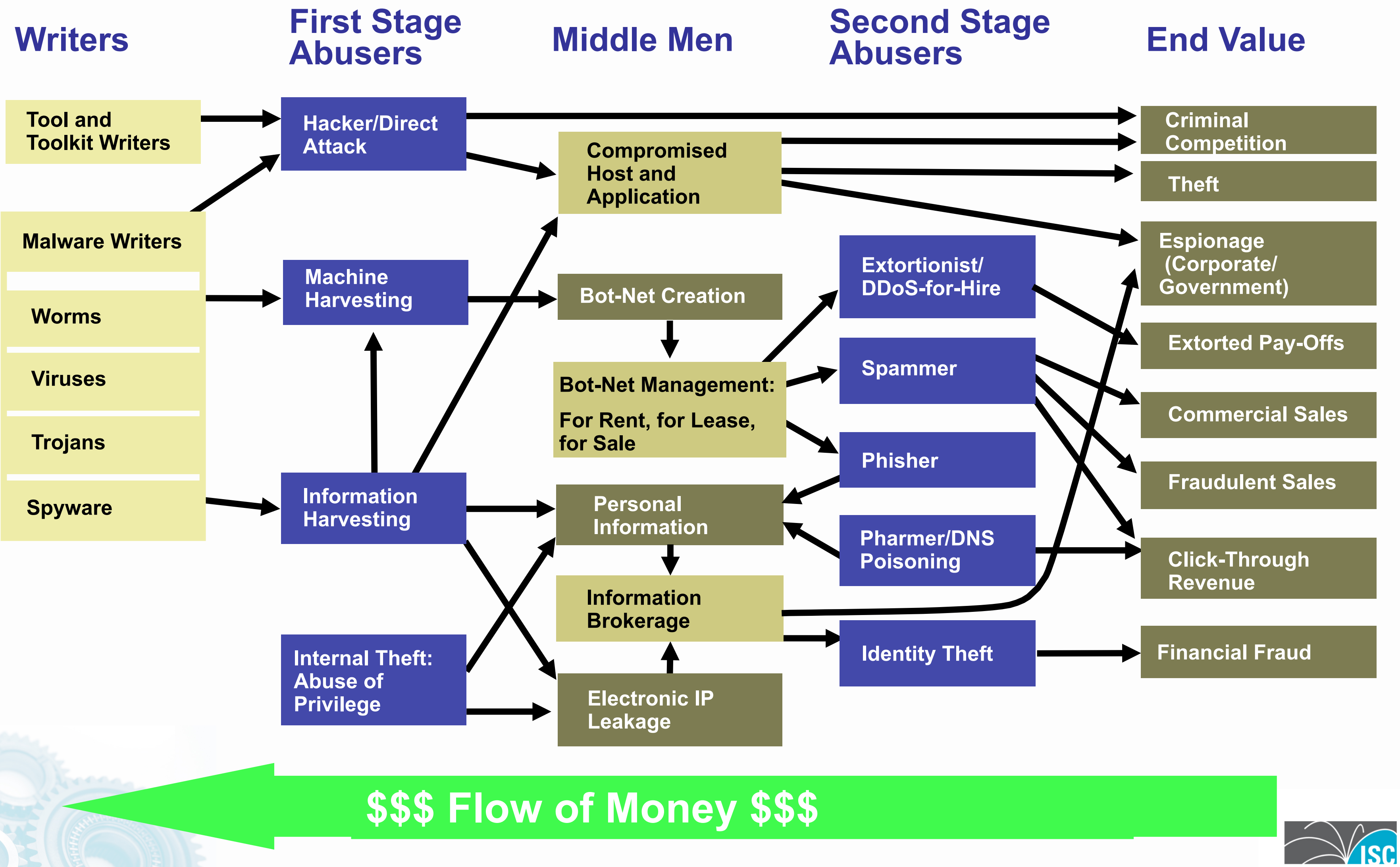
Enduring *criminal* financial opportunities:

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

Threat Economy: In the Past



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

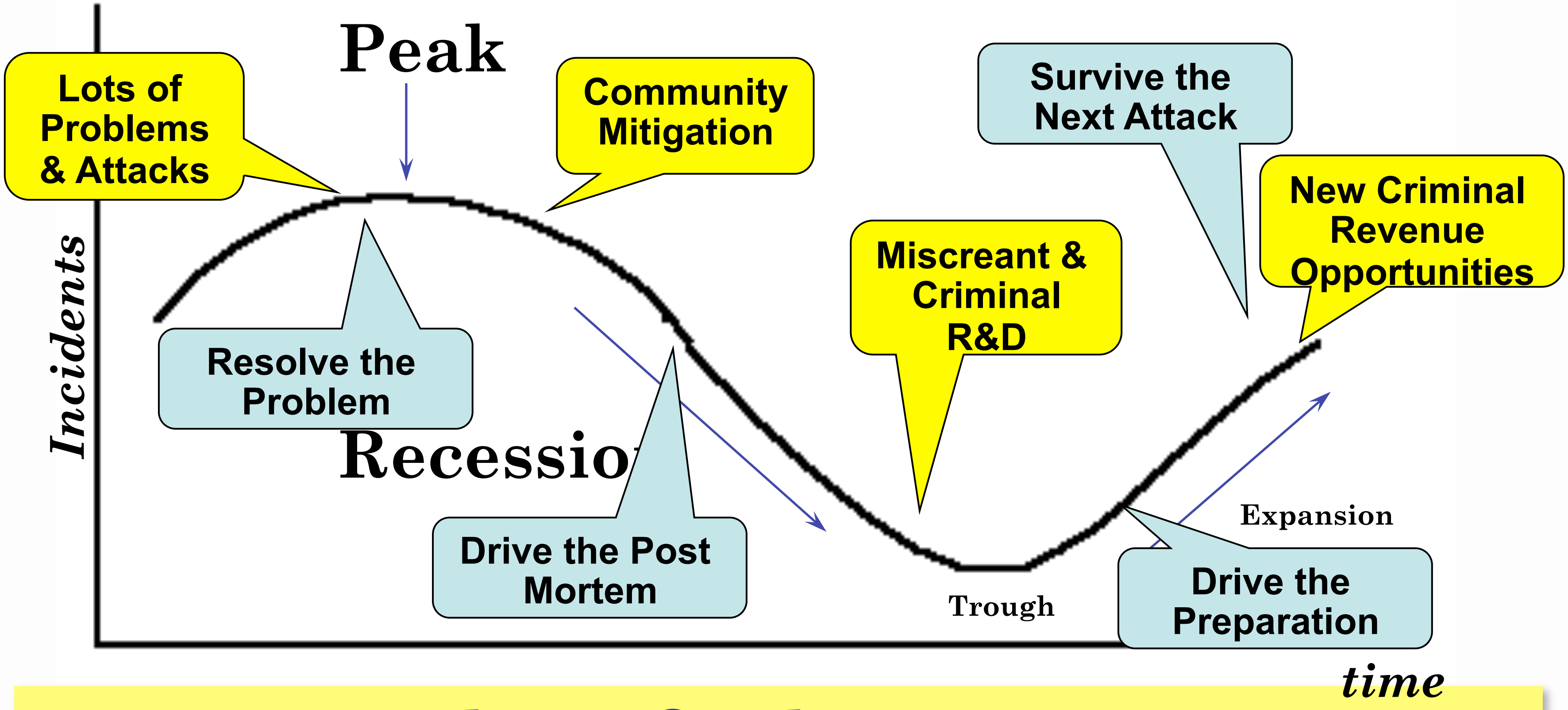
Fraudulent Sales

Click-Through Revenue

Financial Fraud

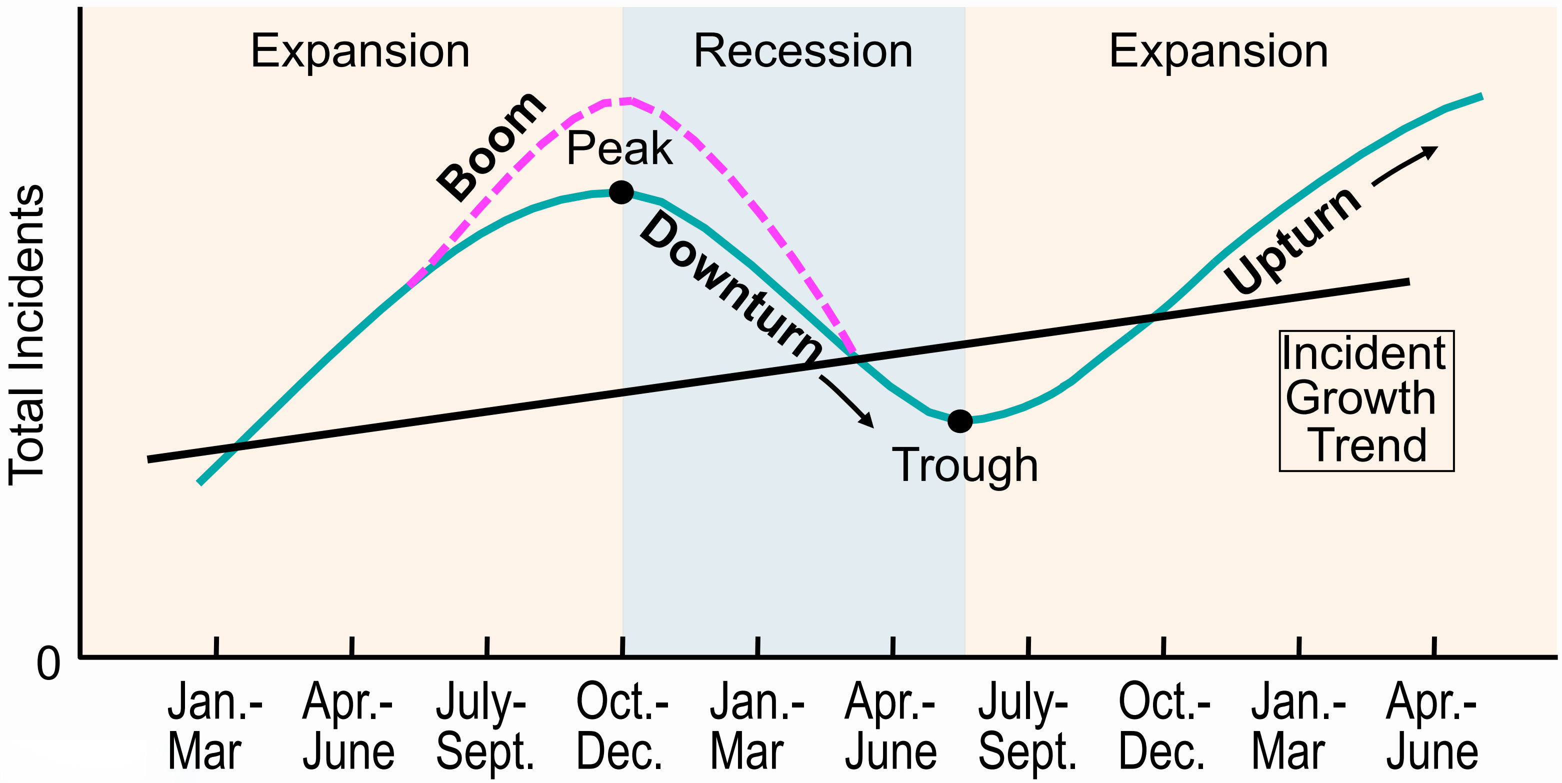
$$$ Flow of Money $$$

Miscreant - Incident Economic Cycles



These Cycles Repeat

Miscreant Economic Cycles



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.

Criminal Complicity, Internet Embargo, Chain of Consequence

“Brand” Jeopardy

“Once a ccTLD, ASN, IP, Hosting company is assumed to be bad it has a detrimental effect on both its industry standing as well as its brand (and ultimately bottom line). So if a ccTLD or hosting provider becomes known as "the bad guy (s)" and it becomes acceptable from an end user organizations perspective to filter/block that portion of infrastructure it will have very real effects on any legitimate commerce that crosses into/over the that infrastructure. Real examples of this can be found in various IDS, IP Block lists, reputation engines, and spam scoring engines (spam assassin comes to mind) and the responses of the organizations who were effected by them.”

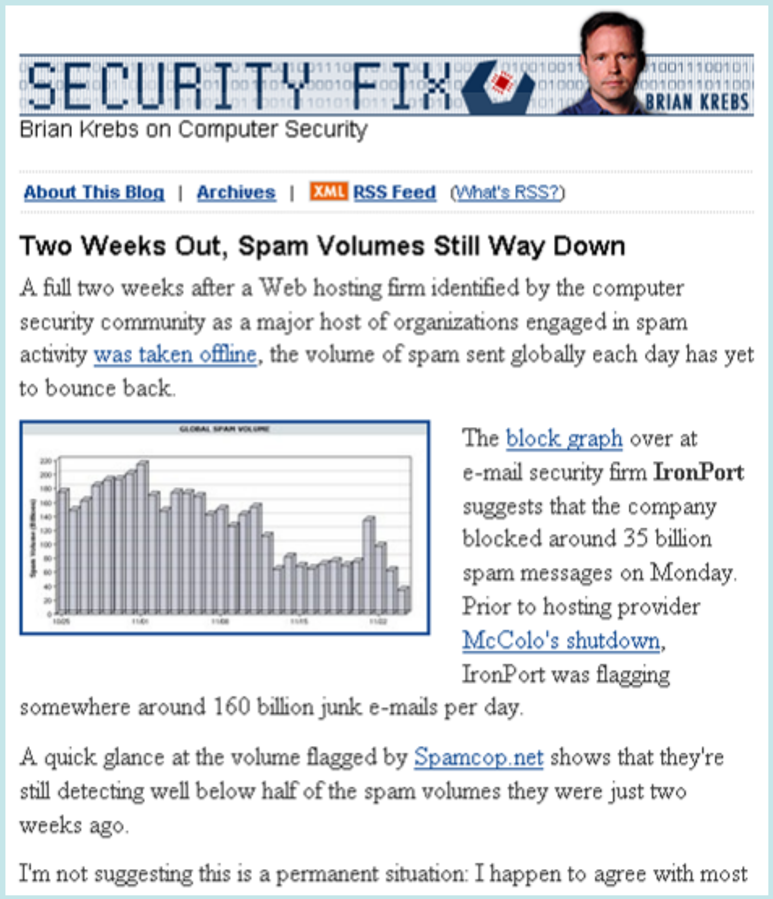
- Andre Ludwig aludwig@packetspy.com

In other words, perception is reality. The ccTLD’s problem is that the Paul Bauran – End-to-End model puts the power of action in the hands of the many.

Autonomous Systems

- Within the Internet, an **Autonomous System** (**AS**) is a collection of connected Internet Protocol (IP) routing prefixes under the **control** of one or more **network operators** that presents a **common, clearly defined routing policy** to the Internet.
- In this system, "control" is defined by the "operator" based on the contractual needs of their "constituents."
- "Clearly Defined Routing Policy" can be BGP, Packet Filtering, Services, and DNS
- ***In other words, the power of who connects to whom is in the hands of the ASN.***

Community Action Can Have an Impact



Brian Krebs on Computer Security

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

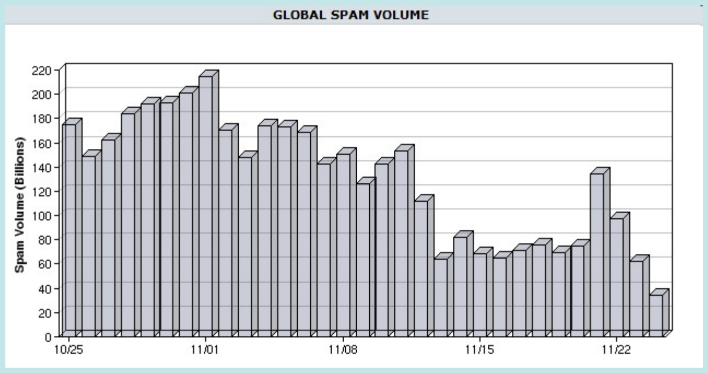
Two Weeks Out, Spam Volumes Still Way Down

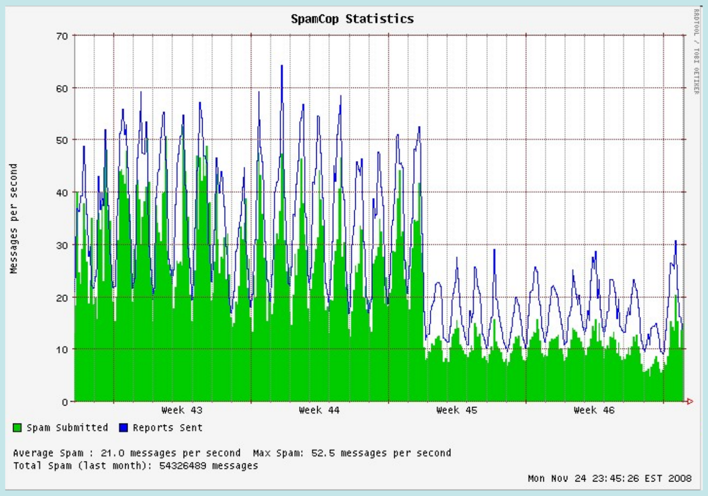
A full two weeks after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline, the volume of spam sent globally each day has yet to bounce back.

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





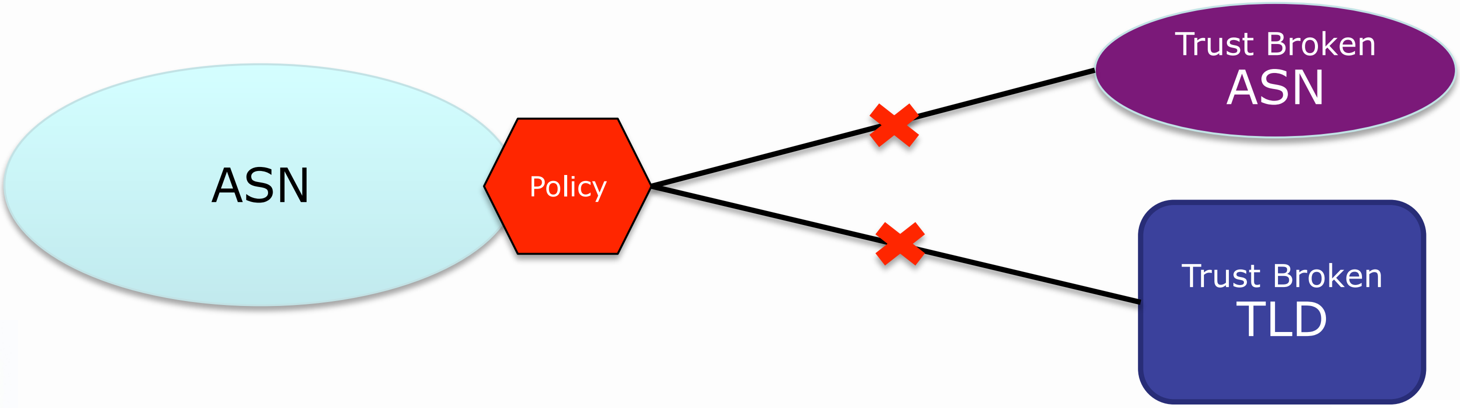
Average Spam : 21.0 messages per second Max Spam: 52.5 messages per second
Total Spam (last month): 54326489 messages

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

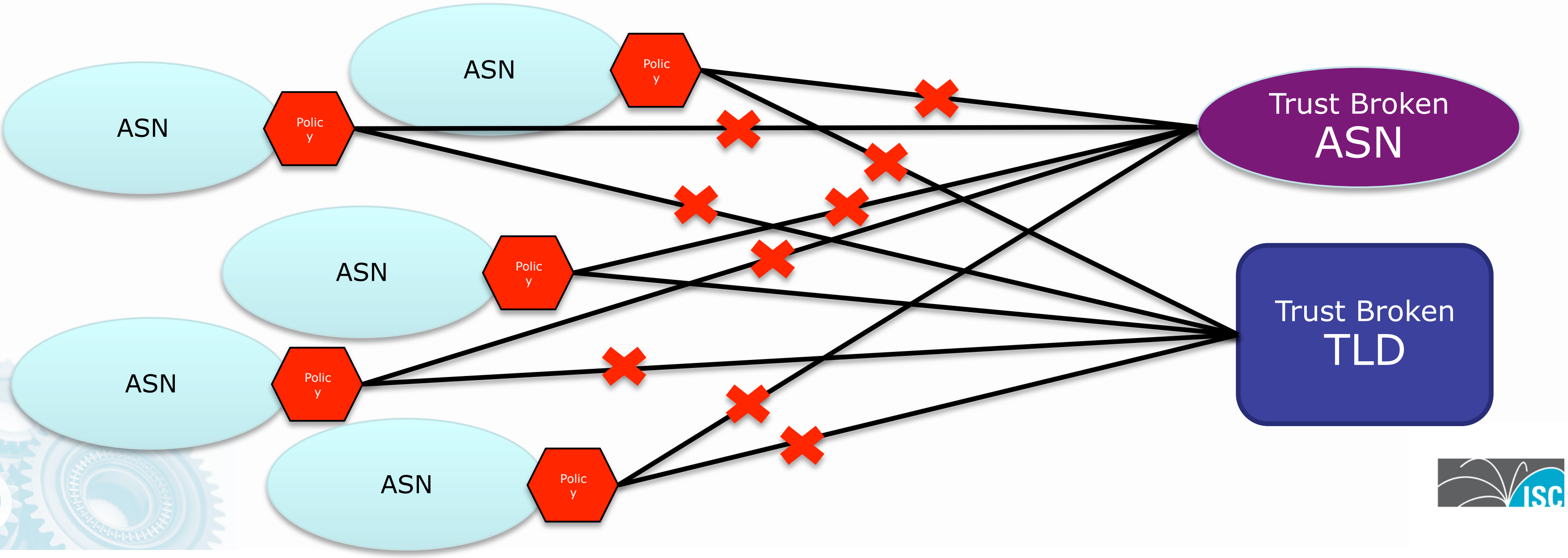
ASN and TLD Filtering

- Any organization – be it a ASN or a end point – has control over who the communicate.
- It is not a technology limitation anymore. The tools are available via vendors and open source to block access to locations on the Net which are the empirical source of risk.



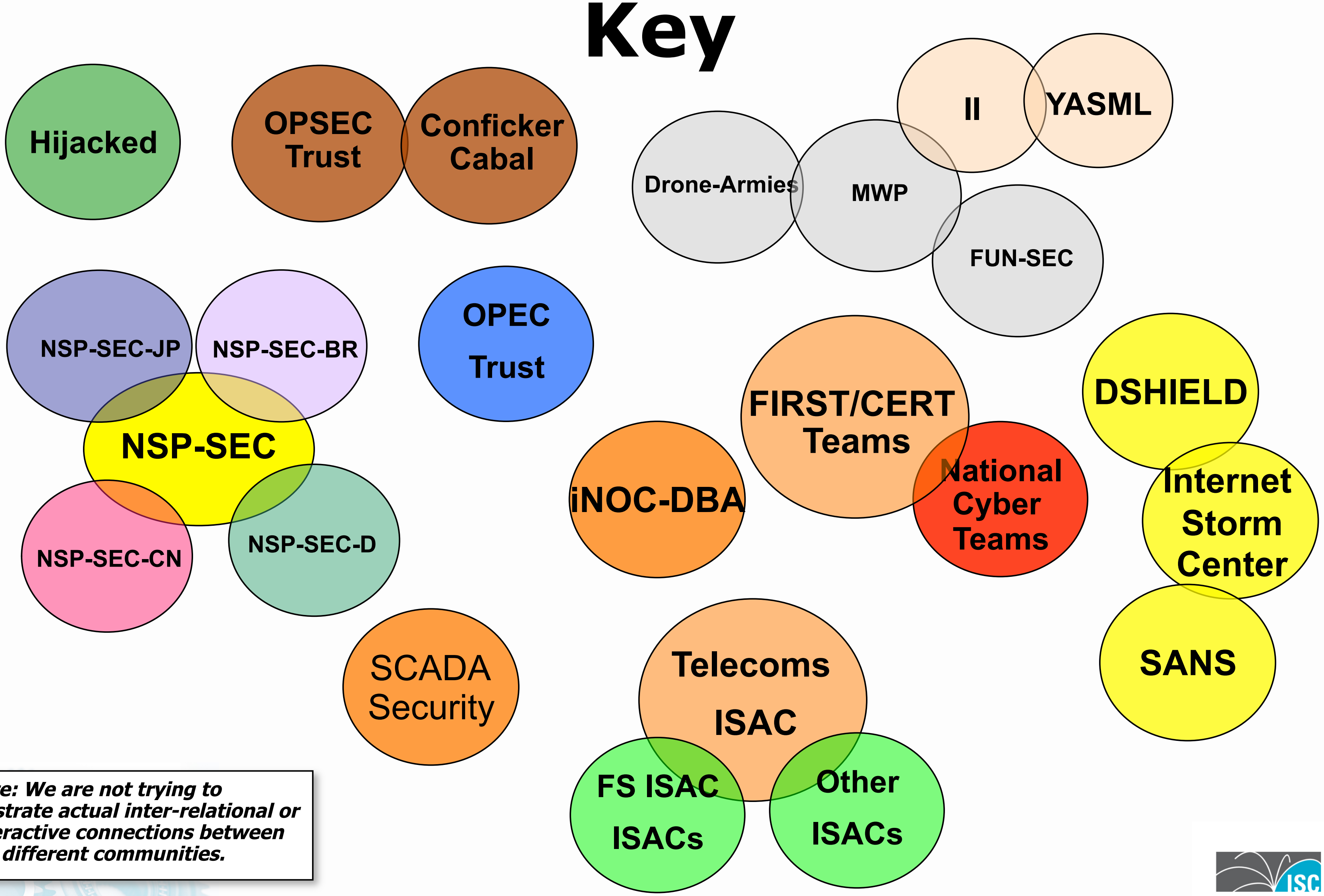
Internet Embargo

- When a group of organizations all collectively band together to protect themselves from imposed business risk, you move from simple filtering to a “Internet Embargo.”
- Internet Embargo has co-lateral impact. Think Hospitals, Business, E-Gov, & other critical institutional organizations who depend on the TLD.



What can a ccTLD do now?

Aggressive Collaboration is the Key



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

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?
- Four Recommendations for TLDs Organizations to get started:
  - NXDomains
  - ICANN Training and Guidelines (Engagement with SSAC).
  - Alliance with your Upstream Transit Providers
  - DNS OARC

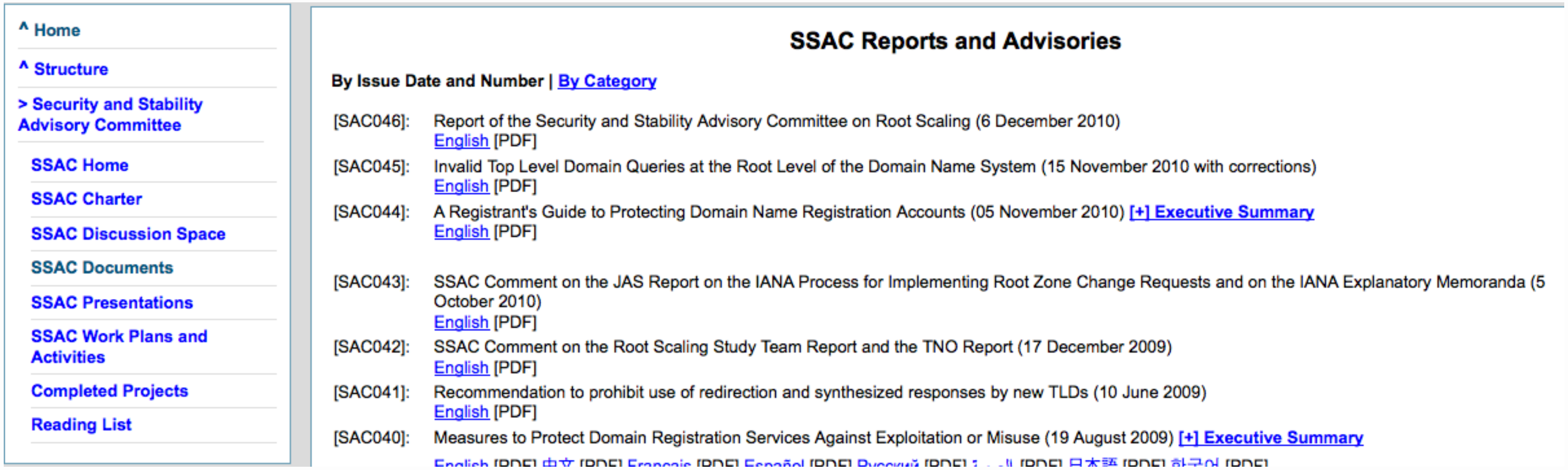
NXDomains

- This list is dedicated to the notification, investigation, and takedown of malicious domains.
  - This is the community who works within the DNS Registry/ Registrar system to remove validated malicious domains.
  - Interface between the Operational Security Community and the DNS Registry/Registrar system
  - "best effort" community, that operates based on all parties expending their best level of effort to tackle an issue.
- Members range from registries, registrars, law enforcement, to vetted security professionals.
- E-mail to nxadmins@opensecnet.com to apply for membership.

NxDomains results is a way to demonstrate a desire to act through best effort action.

ICANN SSAC

- Take advantage of the focused effort to build security and resiliency in the TLD community.
  - http://www.icann.org/en/committees/security/



^ Home
^ Structure
> Security and Stability Advisory Committee
SSAC Home
SSAC Charter
SSAC Discussion Space
SSAC Documents
SSAC Presentations
SSAC Work Plans and Activities
Completed Projects
Reading List

SSAC Reports and Advisories

By Issue Date and Number | By Category

[SAC046]: Report of the Security and Stability Advisory Committee on Root Scaling (6 December 2010)
English [PDF]

[SAC045]: Invalid Top Level Domain Queries at the Root Level of the Domain Name System (15 November 2010 with corrections)
English [PDF]

[SAC044]: A Registrant's Guide to Protecting Domain Name Registration Accounts (05 November 2010) **[+] Executive Summary**
English [PDF]

[SAC043]: SSAC Comment on the JAS Report on the IANA Process for Implementing Root Zone Change Requests and on the IANA Explanatory Memoranda (5 October 2010)
English [PDF]

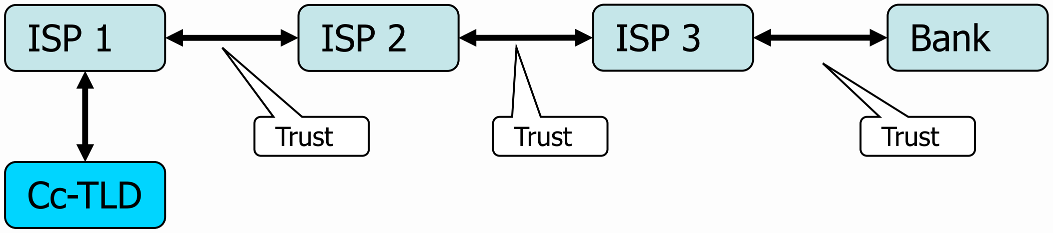
[SAC042]: SSAC Comment on the Root Scaling Study Team Report and the TNO Report (17 December 2009)
English [PDF]

[SAC041]: Recommendation to prohibit use of redirection and synthesized responses by new TLDs (10 June 2009)
English [PDF]

[SAC040]: Measures to Protect Domain Registration Services Against Exploitation or Misuse (19 August 2009) **[+] Executive Summary**
English [PDF] 中文 [PDF] Français [PDF] Español [PDF] Русский [PDF] العربية [PDF] 日本語 [PDF] 한국어 [PDF]

Build a “Upstream” Relationship

- How will the world know to trust your ccTLD as one who has the collective best interest as an important value?
- Working with your upstream ISP’s security and operations teams is a first step. It builds a working **relationship of action and trust** that can be used as a reference to others.



Because ISP 1 trust cc-TLD, ISP 2 , ISP 3, and the “Bank” can also trust the cc-TLD.

DNS Operations

DNS-OARC

- An open public forum for informal reporting, tracking, resolving, and discussing DNS operational issues including outages, attacks, errors, failures, and features. Note that discussion of non-ICANN root systems is explicitly off-topic.
- https://lists.dns-oarc.net/mailman/listinfo/dns-operations
- Sponsored by DNS-OARC
  - www.dns-orac.net
  - The operational equivalent of “DNS-CERT”

Summary and Quetions