Understanding the Real Cyber Security Threat
& what you can do to protect yourself

Barry Greene
bgreene@senki.org

www.senki.org (location of the slides)
"[T]he malware that was used would have gotten past 90 percent of the Net defenses that are out there today in private industry and [would have been] likely to challenge even state government," said Joe Demarest, assistant director of the Federal Bureau of Investigation’s cyberdivision."
Your are an key executive of the company. You hear from you colleagues, read in the press, and get private briefings on the cyber-security damage happening to businesses throughout the world.

You see the increase of nation-state security penetrations into business with countries like China, North Korea, Israel, Iran, United Kingdom, and the United States all using global corporate assets as their new “cyber cold war” battleground.

Is the accountable executive, you ask you team “what do are we doing” and “what do we need to do?” Their response is to start talking to vendors.

These “security” vendors happily present the materials that illustrate threats and how their products are the only solutions to your problems.

At the end of these vendor conversations, the teams have a long list of potential “solutions,” but no real answers.

The organization is back at the beginning, asking the same questions - “what are we doing” and “what needs to be done?”

Frustration increases. You are looking for answers, but get no answers. In the mean time, the security risk continues to increase.

DOES THIS SOUND FAMILIAR?
SECURITY? WHAT DO YOU DO?

✔ Ask a vendor for help ask for “vendor bias” to into the door. The vendor’s #1 job is to sell their product, not do what is in the best interest of your organization.

✔ Asking for the Boston Consulting, Deloitte, and other “big consulting” organizations do not help. These organizations consult. They have “experts” with the academic insight of security, but not the field or operational experience to take that theory and apply it to your organization’s best interest.

✔ Asking security gurus to come in, look at your organization, perform audits, and deliver recommendations is a traditional option. But, what normally happens is that the “recommendations” don’t align with the organizational culture or are counter to the business interest of the organization. It is extremely difficult for an outside expert to make recommendations that are effectively tuned to the organization’s business interest.

✔ You could send several people to lots of security training. Security training is important, but it does not result in the core answers you are looking for ….“what are we doing now” and “what do we need to do to safe guard our business interest?”
To gain a understanding of how we’ve been battling cyber-crime, we must understand the fundamentals of the threat vector:

1. Context: What is really happening?

2. Today’s Cybercriminal Toolkit – The Criminal Cloud ...

3. Understanding Today’s Cyber-Criminal Behavior Drivers

4. Now What? What you do?
Context: What is really happening ....
What Do You Tell the Boss?
'Immense' network assault takes down Yahoo

Cyber-attacks batter Web heavyweights

Strikes on eBay, Amazon, CNN.com follow Monday Yahoo! attack

February 9, 2000
Web posted at 6:59 a.m. EST (1459 GMT)
Hackers Take Down the Most Wired Country in Europe

By Joshua Davis  
08.21.07  |  2:00 AM

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 own protected border — the Internet.
Who really stopped the Estonian DDOS?

• The Community of Trusted and Vetted network operators all around the world ... 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 – which was “US government coordination”

When BOTs Attack – Inter AS

• No Operators (ASN) can protect themselves in isolation.
• The Internet is a Community of ASNs.
• It takes a Community to Defend and Respond to any security attack.

http://www.wired.com/politics/security/magazine/15-09/ff_estonia_bots
Private-to-Private Collaboration with Public Participation

✔ Our industry effectiveness is based on private industry’s ability to collaborate with their peers (i.e. many time competitors).

✔ We share information, exchange data, do join investigative work.

✔ Once there is enough understanding of the threat actors, private industry reached out to public (law enforcement) to move to next stage of the investigation.
Miscreant - Incident Economic Cycles

These Cycles Repeat
Where is these insights coming from?

What we’re doing today.

- Empowerment
- Hardware
- Software
- BCPs

Work the Problem
- Tactical Mitigation
- Post Mortem

Mitigation & Operations Communities
- Ops Meetings One-on-One Beer Meetings

Craft Strategic Response
The Original Top 10

- **Prepare your NOC** - Ensure everyone in the NOC/SOC knows how to use the entire toolkit.

- **Mitigation Communities** - Invest in Communities of peer who you work with to investigate and resolve the security issues facing your customers.

- **iNOC-DBA Hotline (Inter ASN Communication)** - have clear inter-ASN communications that allows NOCs to talk to NOC. This enables the direct communications required to investigate, mitigate, and remediation security incidents.

- **Point Protection on Every Device** - Assume the whole network is a potential threat vector. Each element on the network requires point protection to minimize the threat.

- **Edge Protection** - Protection tools on the edge of the ASN
Remote Triggered Black Hole Filtering - Set up BGP & MPLS to use the full strength of “moving/removing” traffic flows updated at routing protocol speeds.

Sink Holes - Set up sections of the network to move bad traffic to sections that allow for detailed forensics.

Source Address Validation on all customer traffic. All device traffic should be checked to ensure the source address and DSCP and other spoofable fields are validated.

Control Plane Protection - Today’s Control Plan protection expands beyond routing protocols. “Controllers,” cloud systems, and configurations systems all expand the surface area of attack.

Total Visibility (Data Harvesting – Data Mining). Traceback, backtrace, PCAPs, and extensive visibility logs are essential.
The World has Changed
It is time for a Refresh

✓ We will build a new set of “Operator’s Security Toolkit.”
✓ The materials will be used @ tutorials in the Internet Operations Meeting (see http://www.senki.org/sp-security/network-operations-groups-meeting/) with “passionate presenters.”
✓ We will learn from the past, this time having White Paper/Guides, Presentation Materials, and Labs.
✓ “Customer RFP Checklist,” Targeted Interaction @ NOGs, and Smoke Jumping
What is Smoke Jumping?

Smoke Jumping is a “security intervention” technique where we have a team of “volunteers” or “vendors” target an Operator (ASN) who has known “Hot Spots” of nefarious activities.

The Team works with the Operator to deploy the “Security Toolkit” to mitigate the risk AND to set up telemetry to “clear the path” for investigation/operation actions.
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.
The “Toolkit” Approach
“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
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**
Results – DNS Changer Take Down

• The "DNS Changer" (aka ‘Ghost Click’) crew that has been hijacking your constituent's DNS configs were arrested, infrastructure seized, and a major data center shutdown.

• www.dcwg.org
Top List of Operator Security Fundamentals

1. Prepare your NOC
2. Mitigation Communities
3. iNOC-DBA Hotline (build communications channels)
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
12. DNS Resolver as a Security Tool

This list applies to Enterprises, Banks, Governments, On-line providers, Cloud deployments, etc ...
But first, you need to understand the threat!

“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
Pause for Questions
Example – SP Security
SP Security in the NOC - Prepare

**PREPARATION**
- Prep the network
- Create tools
- Test tools
- Prep procedures
- Train team
- Practice

**IDENTIFICATION**
- How do you know about the attack?
- What tools can you use?
- What’s your process for communication?

**CLASSIFICATION**
- What kind of attack is it?

**TRACEBACK**
- Where is the attack coming from?
- Where and how is it affecting the network?

**REACTION**
- What options do you have to remedy?
- Which option is the best under the circumstances?

**POST MORTEM**
- What was done?
- Can anything be done to prevent it?
- How can it be less painful in the future?
Aggressive Collaboration is the Key

Note: We are not trying to illustrate actual inter-relational or interactive connections between the different communities.
Build the Direct and Out of Band Channels

• Build the direct peer to peer communications channels and out of band access before there is a security crisis.

• Example:
  • 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
Edge Protection

• Core routers individually secured PLUS
• Infrastructure protection
• Routers generally NOT accessible from outside
Destination Based RTBH

NOC

IBGP Advertises List of Black Holed Prefixes
Sink Holes

- Remote Triggered Sink Hole
- Garbage packets flow to the closest Sink Hole
- 171.68.19.0/24
- 171.68.19.1
- Primary DNS Servers
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

- Static access list on the edge of the network
- Dynamic access list with AAA profiles
- Unicast RPF
- Cable Source Verify (MAC & IP)
- Packet Cable Multimedia (PCMM)
- IP Source Verify (MAC & IP)
- Carrier Grade NAT (CGN)

96.0.20.0/24
96.0.21.0/24
96.0.19.0/24
96.0.18.0/24
BGP Prefix Filtering

AS 500

AS 400

AS 300

AS 100

AS 200

Customer

Egress Filter Prefixes to Internet; Ingress Filters Coming from Internet

Ingress Filter Customer’s Prefixes

Customer Filters In and Out
Total Visibility

Anomaly for DNS Queries

Investigate the spike

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.
Pause for Questions
Cyber Criminal Toolkit that is the foundation for the *Criminal Cloud*
Cyber Criminal’s Goal

• Build a BOTNET that can be used for:

- Extortion
- Theft
- Hijacking
- Vandalism
- Racketeering
- Terrorism
- Political Intimidation
- Bullying
- Fraud
- Theft
- 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

<table>
<thead>
<tr>
<th>AV Engine</th>
<th>Country</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ahnlab</td>
<td>KR</td>
<td>no_virus</td>
</tr>
<tr>
<td>Aladdin (esafe)</td>
<td>IL</td>
<td>no_virus</td>
</tr>
<tr>
<td>Alwil (avast)</td>
<td>CZ</td>
<td>no_virus</td>
</tr>
<tr>
<td>Authentium</td>
<td>US</td>
<td>no_virus</td>
</tr>
<tr>
<td>Avira (antivir)</td>
<td>DE</td>
<td>HEUR/Crypted</td>
</tr>
<tr>
<td>BitDefender</td>
<td>RO</td>
<td>no_virus</td>
</tr>
<tr>
<td>CA (E-Trust Ino)</td>
<td>US</td>
<td>no_virus</td>
</tr>
<tr>
<td>CA (E-Trust Vet)</td>
<td>US</td>
<td>no_virus</td>
</tr>
<tr>
<td>CAT (quickheal)</td>
<td>IN</td>
<td>no_virus</td>
</tr>
<tr>
<td>ClamAV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dr. Web</td>
<td>RU</td>
<td>no_virus</td>
</tr>
<tr>
<td>Eset (nod32)</td>
<td>US</td>
<td>no_virus</td>
</tr>
<tr>
<td>Ewido</td>
<td>DE</td>
<td>no_virus</td>
</tr>
<tr>
<td>Fortinet</td>
<td>US</td>
<td>no_virus</td>
</tr>
<tr>
<td>Frik (f-prot)</td>
<td>IS</td>
<td>no_virus</td>
</tr>
<tr>
<td>Frik (f-prot4)</td>
<td>IS</td>
<td>no_virus</td>
</tr>
<tr>
<td>F-Secure</td>
<td>FI</td>
<td>Trojan.Crypted-4</td>
</tr>
<tr>
<td>Grisoft (avg)</td>
<td>CZ</td>
<td>no_virus</td>
</tr>
<tr>
<td>Ikarus</td>
<td>AT</td>
<td>Backdoor.VB.EV</td>
</tr>
<tr>
<td>Kaspersky</td>
<td>RU</td>
<td>no_virus</td>
</tr>
<tr>
<td>McAfee</td>
<td>US</td>
<td>no_virus</td>
</tr>
<tr>
<td>Microsoft</td>
<td>US</td>
<td>no_virus</td>
</tr>
<tr>
<td>Norman</td>
<td>NO</td>
<td>Hupigon.gen130</td>
</tr>
<tr>
<td>Panda</td>
<td>ES</td>
<td>no_virus</td>
</tr>
<tr>
<td>Prevx</td>
<td>GB</td>
<td>no_virus</td>
</tr>
<tr>
<td>Securecomputing</td>
<td>US</td>
<td>Heuristic.Crypted</td>
</tr>
<tr>
<td>Sophos</td>
<td>GB</td>
<td>no_virus</td>
</tr>
<tr>
<td>Sunbelt</td>
<td>US</td>
<td>VIPRE.Suspicious</td>
</tr>
<tr>
<td>Symantec</td>
<td>US</td>
<td>no_virus</td>
</tr>
<tr>
<td>TheHacker</td>
<td>PE</td>
<td>no_virus</td>
</tr>
<tr>
<td>UNA</td>
<td>UA</td>
<td>no_virus</td>
</tr>
<tr>
<td>VirusBlokAda (vba32)</td>
<td>BY</td>
<td>no_virus</td>
</tr>
</tbody>
</table>
We do not know how to lock this guy in jail!

OPSEC Community’s Action

Make SPAM Harder

SPAM BOTNET

Drive-By

Secondary Malware

Controller

Proxy

Disrupt Drive-By Phishing

Disrupt Controllers

Clean Violated Data Centers

Malware

Packer

Help your victimized customers

Name Servers

Disrupt the NS Infrastructure

Victim of Crime

Disrupt the NS Infrastructure

Filter Based on TLD

Malware

Domain

BOT Herder
Example of a Threat Actor’s Work Day

✓ Cyber-Criminal Specialist
✓ Job is to use Malware to get into Organizations
✓ $$$ is made through selling BOTNETs & Infected Sites
Step 1: Stage New Domain Name

- SPAM BOTNET
  - Drive-By
  - Secondary Malware
  - Controller

- Fast Flux DNS
  - Stage on NS or FF NS

- Anonymous Proxy
  - Get Domain
  - Malware
  - Packer
  - TLD Domain

- Victim of Crime

- Stage Domain
Step 2: Prepare Drive-By

- SPAM
- BOTNET
- Fast Flux DNS
- Drive-By
- Secondary Malware
- Controller
- Anonymous Proxy
- Load Malware
- Hacker
- TLD Domain
- Send Malware
- Victim of Crime
- Packer
- Malware
Step 3: SPAM to Get People to Click (Spear Phishing)

- SPAM BOTNET
- Fast Flux DNS
- Drive-By
- Secondary Malware
- Controller
- Anonymous Proxy
- Hacker
- TLD Domain
- Malware
- Packer
- Victim of Crime
- US Fantasy Football

Click on me now
Step 4: Drive-By Malware Inserted into the Victim

- SPAM BOTNET
- Fast Flux DNS
- Drive-By
- Secondary Malware
- Controller
- Anonymous Proxy
- Hacker
- Malware
- Packer
- TLD Domain
- Victim of Crime

Click on me now
Malware Success!

- SPAM BOTNET
- Fast Flux DNS
- Drive-By
- Secondary Malware
- Controller
- Anonymous Proxy
- Victim of Crime
- Owned!
- Hacker
- Malware
- TLD Domain
- Packer
Poison Anti-Virus Updates

Poison the anti-virus updates
All updates to 127.0.0.1
Prepare Violated Computer

SPAM BOTNET

Fast Flux DNS

Spam Botnet

Drive-By

Secondary Malware

Controller

Anonymous Proxy

Anonymous Proxy

Anti-Virus Vendor

Victim of Crime

Fast Flux DNS

Malware

Packer

Hacker

TLD Domain

Call to secondary Malware site
Load secondary package

Prepare Violated Computer
Call Home

SPAM BOTNET

Fast Flux DNS

Drive-By
Secondary Malware
Controller
Anonymous Proxy

Hacker

Malware
Packer
TLD Domain

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
- Fast Flux DNS
- Drive-By
- Secondary Malware
- Controller
- Anonymous Proxy
- Go get New Module
- Victim of Crime
- Hacker
- Malware
- Packer
- TLD Domain
Start Worming, Scanning, & Spreading

SPAM BOTNET

Fast Flux DNS

Drive-By  Secondary Malware  Controller

Anonymous Proxy

BOTNET Herder

Malware  Packer  TLD Domain

Victims of Crime

IPv6  IPv6
Load a Proxy with Trigger

Corporate Network

Name Servers

Drive-By
Secondary Malware
Controller

Anonymous Proxy

Go get my proxy

Victim of Crime

Anonymous Proxy

Hacker

Malware
TLD Domain

Packer

Load a Proxy with Trigger

Anonymous Proxy

Go get my proxy

Victim of Crime

Anonymous Proxy

Hacker

Malware
TLD Domain

Packer
Watch for the SSL VPN Connection

Tell me when the SSL VPN Connection is Established

Cool! Let's see what I can find to steal.
Set up the Proxy Tunnel

Cool! Let's see what I can find to steal.

Anonymous Proxy

SSL VPN

Corporate Network

Victim of Crime

Drive-By
Secondary Malware
Controller

IPV6

Hacker

Malware
Packer

TLD Domain

Name Servers

Set up the Proxy Tunnel

SSL VPN

Corporate Network

Victim of Crime

Drive-By
Secondary Malware
Controller

IPV6

Hacker

Malware
Packer

TLD Domain

Name Servers
Proxy Behind the Bank Login

Victim of Crime

Anonymous Proxy

Cool! Let's see what I can find to steal.

Drive-By
Secondary Malware
Controller

Name Servers

BANKS

IPv6

Hacker

Malware
Packer

TLD Domain

IPv6

HTTPS
DNS WAS PART OF EVERY STEP THE MALWARE INFECTION!

We know the SPAM addresses

SPAM BOTNET

We knew the infrastructure addresses!

Name Server

Drive-By

Secondary Malware

Controller

Anonymous Proxy

We can see this guy’s DNS Activity!

BOT Herder

We knew the controller addresses!

Malware

Anonymous Proxy

We knew the back end systems!

Packer

TLD Domain

We needed to stop this computer from doing all the DNS lookups to bad domains!

Victim of Crime

We knew the NS used for the criminal activity!
rDNS Blacklist would have stopped the Phishing

- SPAM BOTNET
- Fast Flux DNS
- Drive-By
- Secondary Malware
- Controller
- Hacker
- Packer
- Malware
- TLD Domain
- Victim of Crime
- Anonymous Proxy
- DNS
- RESOLVER
- Blacklisted with a rDNS with a “DNS Firewall”
- SOC Alert!
rDNS with Blacklist would have disrupted the Malware
Pause for Questions
Scary Consequences

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*. 
Scary Consequences

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.
Pause for Questions
Understanding Today’s Cyber-Criminal Behavior Drivers
The Good Guys are a 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 do you project civic society and the rule of law where there is no way to enforce the law?
Four Major Threat Vectors

- Critical Infrastructure has four 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, , Nation State, 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

  - **Community #4 – Corporate**
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*

* The cyber-criminal “economic cycles” were first observed in 2001 by Rob Thomas (Team CYMRU) and Barry Greene during a postmortem investigation. This “Miscreant Economy” has been growing exponentially since that time.
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 untraceability 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

2007 Prediction: 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
- 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

Peak
- Lots of Problems & Attacks
- Community Mitigation
- Survive the Next Attack
- New Criminal Revenue Opportunities
- Miscreant & Criminal R&D
- Drive the Post Mortem
- Drive the Preparation
- These Cycles Repeat

Recession

Trough

Incidents

Expansion

time
Miscreant Economic Cycles

Expansion
Recession

Incident Growth Trend

Total Incidents

0

The dire trap – the *Chasm* of No Action

No Pain
No Business Justification for Action
Cyber Crime Cost are Huge!

- 2012 Data!
- Bigger than the illegal drug trade!
- Bigger than human trafficking trade!
Pause for Questions
Community Action Can Have an Impact

Source: http://voices.washingtonpost.com/securityfix/2008/11/64_69_65_73_70_61_6d_64_69_65.html
But you cannot stop preparing …..

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 Lanza, 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
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.

• The 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.
Cyber Warfare’s Consequences …

Target is taken out
… Extend beyond the perceived “Battle Space.”
Nation State Attacks – Reality Check

• In the past, we trusted the “Generals” to maintain control over the troops. Post Snowden, we now know that the troops cannot be trusted.

• Nation State Attacks are 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.
Pause for Questions

• Q1 – Has anyone planned for the "nation state battle" that will happen on your network?

• Q2 – We’ve all seen Snowden’s Data. What does that mean to your network?
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.""

Pause for Questions
Taking Action
If we know the problem, can we coordinate action?

• If we have enough people within the “Community” who know the tools, know the threat, and know that means to remediate/mitigate … can we plan on coordinated action?

YES
Example Industry Strategy from 2012

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

- Situational Consultation (Map the Crime Vector): **OPSEC Trust’s Main Team**
- Situational Awareness: BTFC, Anti-S, SCADASEC (and others)
- Dissecting Malware: **YASMIL, II** (perhaps MWP)
- Big Back Bone Security and IP Based Remediation: **NSP-SEC**
- Domain Name Takedown: **NX-Domain**
- DNS System Security: **DNS-OARC**
- Anti SPAM, Phishing, and Crime: **MAAWG & APWG**
- Vulnerability Management: **FIRST**
- Many other Confidential Groups specializing into specific areas, issues, incidents, and vulnerabilities.
- Investigative Portals providing focused, confidential investigation: **OPSEC Trust Investigative Teams**
2012 - Optimistically

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

- **Private-to-Private Collaboration with Public participation.** Public policy around the world needs to facilitate the flexibility of private industry to collaboration with each other and with global public partners – moving beyond National constraints.

- **Public – Private Partnership activities need to optimize around private industry flexibility, clarity, and action.** Models like NCFTA are successful because of the interface with aggressive Private-to-Private Collaboration Communities. **We know this works through our results.**
Cyber Strategy of Action

• **Existing Technology for Detecting, Tracking, and Identifying malicious activity is at a level to allow for broad adoption – resulting in new levels of cyber-criminal visibility.** This technology has been validated in enough small and large commercial networks to have a good grape on the operational cost and impact.

• **Existing Technologies for Remediation have proven to work.** Industry who have deployed remediation are prepared to share the business model impact to foster a sustainable and persistent remediation effort.
• Action Now is the key to preparing for Cyber-Security Defense. It is imperative for industry to prepare for critical cyber security incidents. Action now is the best way to prepare and build new security capability/capacity. DCWG, Conficker, and other malware take downs are golden opportunities to build the remediation tools that might save the business in the future.
Effective Collaboration

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

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

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

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

Take Back the DNS!

Passive DNS – Tool to Find the Badness behind the DNS

E-mail dnsdb@isc.org for an account.
Summary = Action

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

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 TDL4, Alureon, Tidser 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.
Pause for Questions
What’s Next?

• Download White Papers, Blogs, Workshop Materials from www.senki.org

• Connect! Barry connects to peers, colleagues and aspiring talent via Linkedin (www.linkedin.com/in/barryrgreene/). You can also follow on Barry on Twitter (@BarryRGreene) or his blogs on Senki (www.senki.org).