New Opportunities for Criminal Growth

Forecasting Cyber-Crime during the IPv6 Transition

Barry Raveendran Greene
bgreene@isc.org
Version 1.0
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.
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.

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

- BIND
- AFTR
- RPKI
- DHCP
- PCP
- (TBA)

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.
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
Stage Domain Name

- SPAM BOTNET
- Drive-By
- Secondary Malware
- Controller
- Proxy
- BOT Herder
- Get Domain
- Malware
- Packer
- TLD Domain
- Victim of Crime
- Stage on NS or FF NS
- IPv6
Prepare Drive-By

SPAM BOTNET

Name Servers

Drive-By

Secondary Malware

Controller

Proxy

Send Malware

Hacker

Load Malware

Malware

Packer

Victim of Crime

TLD Domain

IPv6

IPv6
Social Engineered SPAM to Get People to Click (Spear Phishing)

- SPAM BOTNET
- Name Servers
- Victim of Crime
- Send SPAM
- TLD Domain
- Click on me now
- IPv6
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

Victim of Crime

Anti-Virus Vendor

Name Servers

SPAM BOTNET

Drive-By

Secondary Malware

Controller

Proxy

Hacker

Malware

Packer

TLD Domain

Anti-Virus Vendor

Name Servers

SPAM BOTNET

Drive-By

Secondary Malware

Controller

Proxy

Hacker

Malware

Packer

TLD Domain
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
- Go get New Module
- IPv6
- IPv6
- Hacker
- Malware
- TLD Domain
- Victim of Crime
- Packer
Start Worming, Scanning, & Spreading

- Drive-By
- Secondary Malware
- Controller
- Proxy

- SPAM BOTNET
- Name Servers
- Victims of Crime
- IPv6

- BOTNET Herder
- Malware
- Packer
- TLD Domain
Load a Proxy with Trigger

Corporate Network

Drive-By

Secondary Malware

Controller

Proxy

IPv6

Go get my proxy

Victim of Crime

Hacker

Malware

Packer

TLD Domain

Name Servers
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

Corporate Network

Drive-By
Secondary Malware
Controller
Proxy

IPv6

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

Hacker

TLD Domain

Name Servers

Victim of Crime

SSL VPN

IPv6

Malware
Packer
Proxy Behind the Bank Login

Cool! Let's see what I can find to steal.
We do not know how to lock this guy in jail!

OPSEC Community’s Action

- Make SPAM Harder
- We do not know how to lock this guy in jail!
- Disrupt Drive-By Phishing
- Disrupt Controllers
- Clean Violated Data Centers
- Filter Based on TLD
- Help your victimized customers
- Victim of Crime
- Disrupt the NS Infrastructure
- SPAM BOTNET
- Drive-By
- Secondary Malware
- Controller
- Proxy
- Name Servers
- Malware
- Packer
- TLD Domain
- Bot Herder

Make SPAM Harder
Disrupt Drive-By Phishing
Help your victimized customers
Disrupt Controllers
Clean Violated Data Centers
Filter Based on TLD

We do not know how to lock this guy in jail!
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.
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?
Three Major Threat Vectors

- Critical Infrastructure has three major threat drivers:
  - Community #1 Criminal Threat
    - Criminal who use critical infrastructure as a tool 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
    - Large 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 bottled.
  – Someone addicted to chat is targeted to get bottled.
  – 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
- 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
- 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

- Expansion
- Recession
- Expansion

Total Incidents

- Jan.-Mar
- Apr.-June
- July-Sept
- Oct.-Dec
- Jan.-Mar
- Apr.-June
- July-Sept
- Oct.-Dec
- Jan.-Mar
- Apr.-June

Incident Growth Trend

- Boom
- Peak
- Downturn
- Trough
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 for how long .....

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
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).

   - 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.
Summary and Questions
Internet Systems Consortium (ISC)

How we can help your IPv6 Journey
ISC’s Beginnings

ISCs Original Goal:
Develop and Support BIND – Berkley Internet Name Domain as managed open source for the best interest of the Internet’s growth

Founded in 1994 by Internet pioneers
Rick Adams, Paul Vixie, Carl Malamud

Added: In 1994, IANA (Internet Pioneer Jon Postel) designated ISC as a F-root name server operator
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.

"we can't be bought, but we can't remain strong without your support"

“We’re the operational experts around names and numbers infrastructure. ”

Working together for a Robust and Open Internet
Our Activity in the Industry

DNS Everywhere
IPv6
DNSSEC
OPS-SEC

Secondary DNS Services

DNS F-Root

Security Data Peering

Hosted @ w/ Open Source Community and Others
ISC’s Core Public Benefit Capabilities & Capacities

**Services**
- DNS “F-ROOT”
- Managed Open Source Support
- DNS Secondary Server Resiliency (SNS)
- Global Network for the Public Benefit (hosting a range of open source code)

**Professional Open Source Development**
- DNS Servers – BIND
- DHCP
- AFTR (IPv4 to IPv6 & Overlay Serveris)
- PCP
- RPKI (Securing BGP)
- More to come … first reference, standards based code.

**Empowering New Generations**
- Operations Meeting Empowerment (APRICOT, AFNOG, NANOG, etc)
- Training based on Operational Deployment
- Empowering Decision & Policy Realms.

**Maintaining the Spirit of the Internet through Global Convergence**
- 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.
How can ISC Help?  
(Keeping it Simple)

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

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.