

Michigan Cyber Summit 10-7-2011

Track #4 - Law Enforcement

Stopping Cybercriminals and Cyberterrorists in Their Tracks

Moderator:

Dr. Faith Heikkila, Ph.D, CIPP, CISM

CISO – Greenleaf Companies and

InfraGard Michigan Members Alliance, Inc. President

Panelists:

Gary Miliefsky, CISSP, Contributor to *Hacking Magazine* & Founder /CTO, NetClarity, Inc.

Jon Oberheide, Co-Founder & CTO Duo Security

Agenda

Moderator and Panelist Introductions

- Dr. Faith Heikkila
- Gary Miliefsky
- Jon Oberheide

Presentations by the Panelists

- **“Cybercrime and Cyberwar”**
- **“5 LEO-Relevant Cyber Security Myths”**

Questions to Panelists

- Moderator Questions
- Audience Questions - Please use microphone



Cybercrime and Cyberwar

**Stopping Cybercriminals and
Cyberterrorists in their tracks**

by Gary S. Miliefsky, FMDHS, CISSP®

Fact: Nothing with an IP Address Is Secure

- No device is safe – all IP-based devices are exposed to exploitation:

It is a target

It can be spoofed

It can be infected

It can be remotely controlled

It is probably already infected



Fact: Wireless Will Never Be Secure!

- **WEP was easy to crack; now WPA is also...**

Recently deployed tools such as Back Track v4.0 allow you to break wireless encryption by attacking the smaller 24-bit session initiation key and then gaining full "trusted" access to a wireless router.

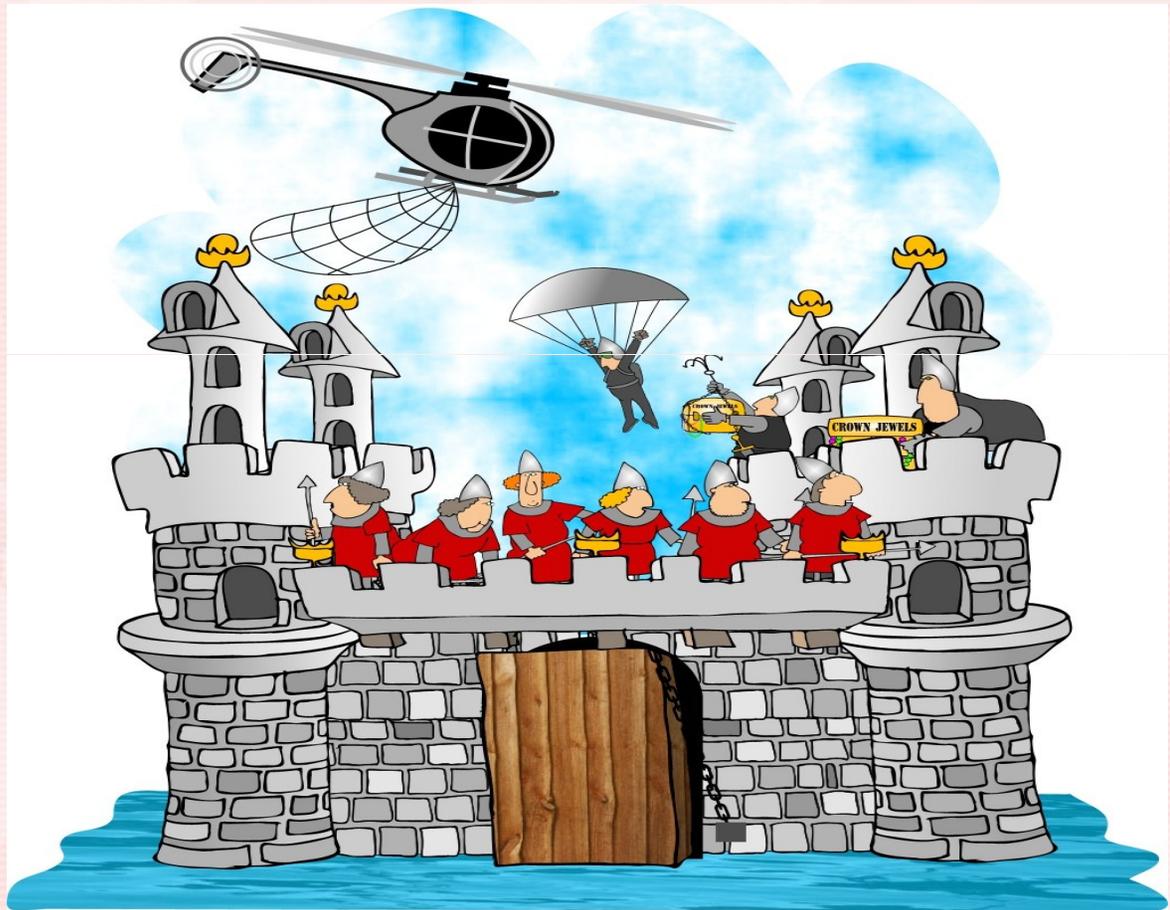
- **Wireless Routers have Critical Flaws (CVEs)**

Now you can break into the admin interface of a wireless router by sending malformed packets from your laptop and pringles can...not worrying about the encryption, see NVD.NIST.GOV and type in "wireless"

IPS GRADE IS A “D-”

NSS Labs Inc. tested 13 of the world’s most powerful IPS products in December 2010. They caught 62% of the attacks, missing 38%.

While the NSS Labs test is revealing, most of the attacks don’t come through the front door (the firewall or IPS) anyway, they come through the back door.



Fact: Anti-virus is dead!

No One Can Keep Up With New Malware

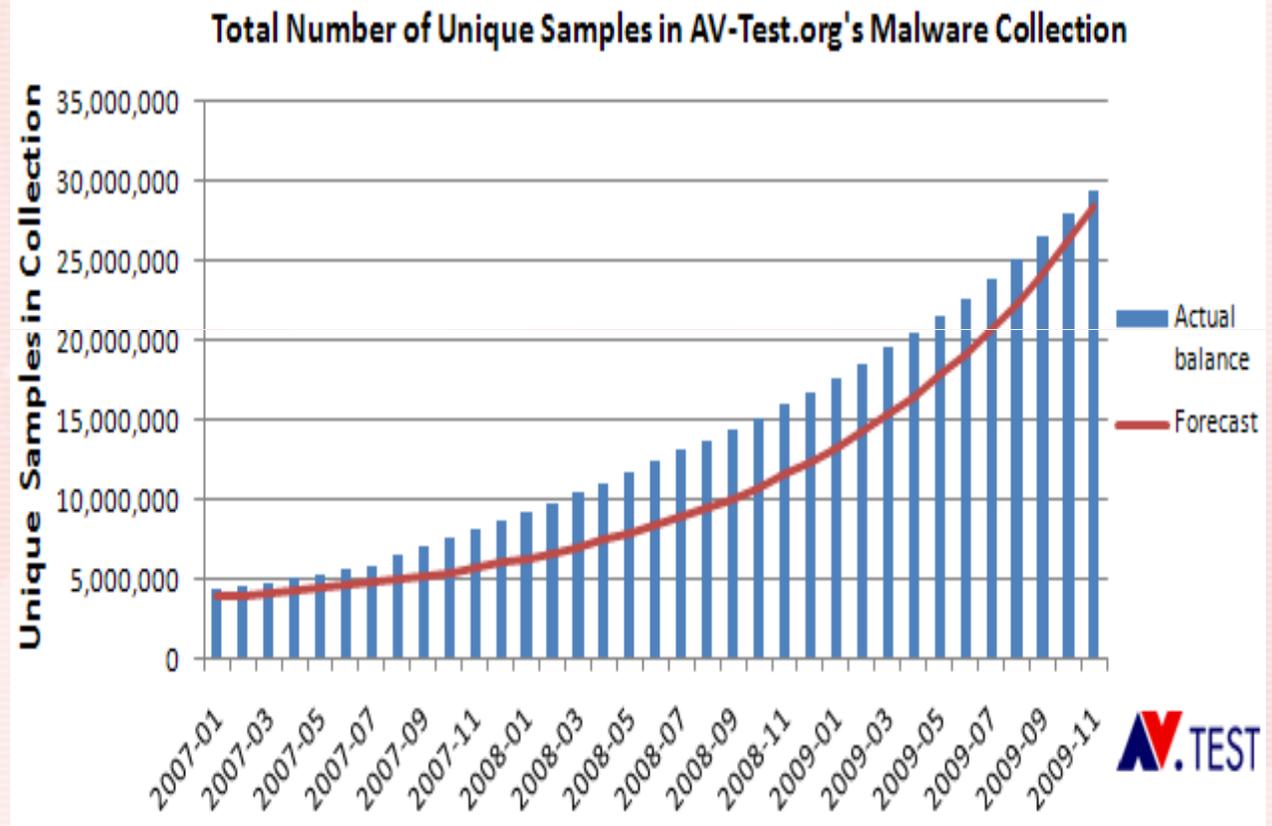
According to independent malware test labs, ALL ANTI-VIRUS software agents FAILED to stop ALL new threats, known as zero-day malware.

See:

<http://www.anti-malware-test.com>

<http://blogs.zdnet.com/security/?p=5365>

<http://av-test.org>



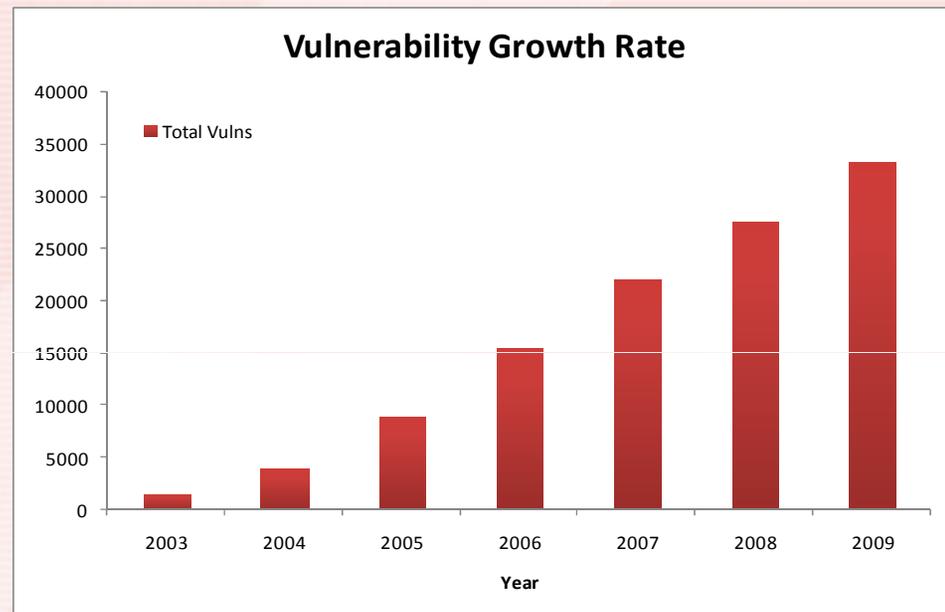
Report: 48% of 22 million scanned computers infected with malware

Fact: Everyone can be exploited!

All of our Systems have Holes! (CVEs)

According to the USCERT, SANS, FBI and MITRE, over 95% of security breaches are a direct result of exploiting a Common Vulnerability and Exposure (CVE®).

See: <http://nvd.nist.gov>



In addition, 80% of all successful attacks occur from the inside (malicious insider, rogue wireless, the 'cleaning company' tapping of your network with an unknown and untrusted laptop)

Fact: Your Identity Was Stolen!

~350M Americans & 516M records stolen

PrivacyRights.org



- More than 516M Personally Identifiable Information (PII) records for more than 350M citizens in America. How many have been lost, hacked and stolen?

According to PrivacyRights.org, the total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005:

**516,942,944 RECORDS BREACHED
from 2,392 DATA BREACHES made public since 2005**

- Still think you are secure?
- Still believe your anti-virus and firewall can truly secure your network or your personal computer?

What is Cybercrime?

Traditional criminal techniques

Burglary: Breaking into a building with the intent to steal.



Deceptive callers: Criminals who telephone their victims and ask for their financial and/or personal identity information.



Extortion: Illegal use of force or one's official position or powers to obtain property, funds, or patronage.



Fraud: Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.



Identity theft: Impersonating or presenting oneself as another in order to gain access, information, or reward.



Child exploitation: Criminal victimization of minors for indecent purposes such as pornography and sexual abuse.



Cybercrime

Hacking: Computer or network intrusion providing unauthorized access.



Phishing: A high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.



Internet extortion: Hacking into and controlling various industry databases (or the threat of), promising to release control back to the company if funds are received or some other demand satisfied.



Internet fraud: A broad category of fraud schemes that use one or more components of the Internet to defraud prospective victims, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.



Identity theft: The wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception, typically for economic gain.



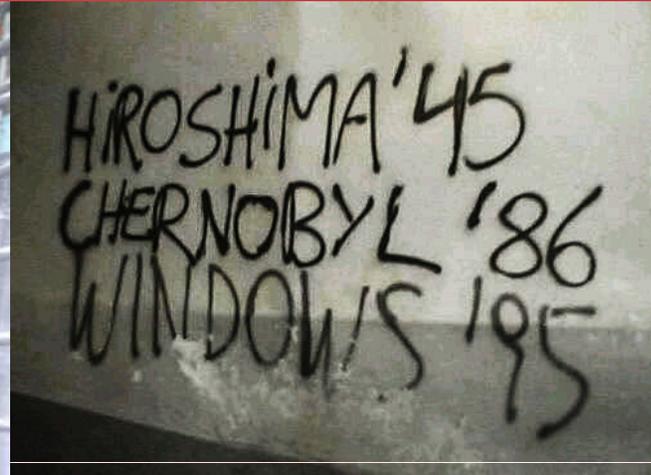
Child exploitation: Using computers and networks to facilitate the criminal victimization of minors.



Cybercrime – Purely “Digital” Paradigm



What is Cyberwar?



Cyberwar – Nations Attacking Nations, Digitally, Daily

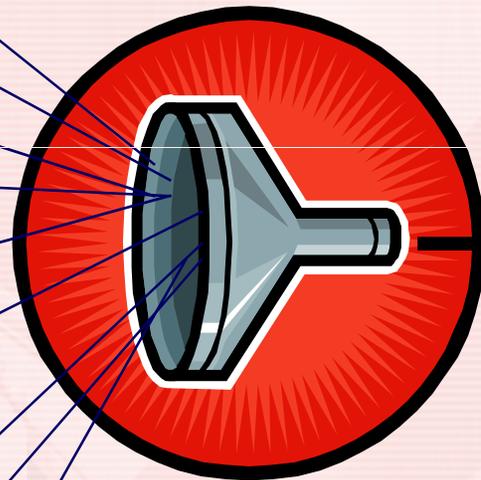
- Distributed Denial of Service (DDoS)
- Espionage (Spyware, Backdoors, Data theft)
- Critical Infrastructure (Stuxnet, etc.)
- Propaganda (Facebook, Twitter, etc.)
- Covert Channels (MUDS, Avatars, Virtual Worlds, Proprietary Encryption)

Here's What We've Faced this Year...

1. Retail and E-tail Outlet Attacks will Outpace Attacks Targeting Banks
2. Hospitals will become the Most Exploitable of All Vertical Markets
3. Cloud Computing and Virtual Machines (VM) will be specifically targeted
4. New and innovative attacks will be launched by rogue and competing Nations
5. Early stages of Growing Cellphone and PDA attacks
6. New and Sophisticated VoIP Attacks are coming
7. Exponential Growth of More Intelligent Zero-day Malware
8. New Sophisticated UTM firewall and IPS exploits are coming
9. More Creative Social Engineering for Cyber Crime Profits
10. Increases in Microsoft® Windows™ Application Layer Vulnerabilities leading to Rapid Exploitation
11. Growing Privacy Rights Violations by Governments and their Contractors in the name of Cyber Defense.

With Sophisticated New Malware

- Virus
- Trojan
- Worm
- Rootkit
- Botnet
- Zombie
- Keylogger
- Adware
- Spyware



BLENDED THREATS

*...designed mostly for Cybercrime
and Cyberterrorism....*



Malware Root Cause - CVEs

- **Common Vulnerabilities and Exposures (CVEs)**
 1. Although there might be 9,000,000 signatures in your McAfee or Symantec anti-virus scanner database (and growing exponentially), there are only 47,000 CVEs. If you close just one CVE, for example, you can block more than 110,000 variants of the W32 malware.
 2. If you aren't visiting <http://nvd.nist.gov> to see what kind of exploitable holes you have in your network, cyber criminals CERTAINLY are...
 3. Everything with an IP address has a CVE, you need to figure out which ones are critical holes and how to patch, reconfigure and remove them—i.e. system hardening.

...and MALWARE LOVES TO EXPLOIT THESE HOLES...

WHAT CAN YOU DO ABOUT IT?

- **Get More Proactive**
 - Learn and use the FOUR D's
 - Manage the RISK FORMULA
 - Document Policies
 - Educate Employees
 - Harden systems regularly
 - Review logs regularly
 - Review and Enforce Policies regularly
 - Encrypt Everything You Can
 - Deploy PAC, NAC, UBAP and HIPS (huh?)

In appreciation of your time today...

- ✓ ***Please feel free to download:***
 - ✓ ***“Extended Edition” of this PowerPoint, 50 Slides with links to free tools and much more information***
 - ✓ ***Full year of Hakin9 Magazine for educational purposes all zipped up in PDF format***

Grab these online at:

<http://www.netclarity.com/michigan2011.zip>

(The url goes straight to the file for an anonymous download...)

QUESTIONS?

garym@netclarity.net



Thank you.

Gary S. Miliefsky, FMDHS, CISSP®
NetClarity, Inc. <http://www.netclarity.net>

Introduction



- My background
 - Academic
 - BS, MS, PhD from University of Michigan
 - Defensive
 - Duo Security, no vendor pitches allowed!
 - Offensive
 - I write kernel exploits when I'm bored
- My goal
 - Confuse, offend, or provoke you into asking a question to the panel afterwards! :-)

Myth #1: You have a chance



**Myth #1: You have a chance
against motivated adversaries.**

Only takes one



- What does it take to compromise your network?
 - One exploit?
- How large is your client-side attack surface?
 - IE, Firefox, Flash, Adobe Reader, Office, etc



Users are the weakest link



- Employees names and email addresses are enumerable on social networking sites?
- Employees answer external email and access web sites on the same machine that they handle sensitive data?
- Are their e-mail addresses `firstname.lastname@company.com`?



Exploit markets



- Well-developed markets to buy and sell 0day vulns/exploits
 - Underground, corps, defense contractors, governments
- How much does an average client-side 0day cost?
 - Estimated ~\$50k-100k USD
 - Adobe JBIG2 exploit sold for \$75k on underground market
 - If $\text{cost}(\text{exploit}) < \text{value}(\text{your network})$, you're already owned
- Does your adversary have that kind of funding available?
 - Most definitely, yes.

Myth #2: Trust your tools



Myth #2: You can trust your tools.

Anti-Forensics



“Attempts to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct.”

- Anti-forensics (AF) is not new
 - Passive countermeasures are well known
 - Munging timestamps, identifiers, etc

```
Phrack magazine extraction utility Phrack Staff
Title : Defeating Forensic Analysis on Unix Comments +
Author : the grugq Text mode
=====
==Phrack Inc.==
Volume 0x0b, Issue 0x3b, Phile #0x06 of 0x12
|-----[ Defeating Forensic Analysis on Unix ]-----|
|-----[ the grugq <grugq@anti-forensics.com> ]-----|
|-----[ www.anti-forensics.com ]-----|
```

Targeting the investigator/examiner



Attacking the Investigator:
AF techniques that exploit CFT bugs.

Craft packets to exploit buffer-overflow bugs in network monitoring programs like **tcpdump**, **snort** and **ethereal**.

Create files that cause EnCase to crash.

Successful attacks provide:

- ➔ Ability to run code on the forensic appliance
- ➔ Erase collected evidence
- ➔ Break the investigative software
- ➔ Leak information about the analyst or the investigation
- ➔ Implicate the investigator

- Parsing is *hard*

- Exploits targeting EnCase, FTK, etc

MALWARE **FORENSIC TOOLS**

SO WHAT DOES THIS MEAN?

- Once we control the forensic tool, we control the examiner's experience arbitrarily
- We can implement a rootkit that targets the specific tool used
 - File hiding
 - Incorrect search results
 - Planted evidence
- We don't even have to worry about payload size or delivery as we have unlimited storage in the drive image
- Typically, forensic examiners' systems should not have network connectivity so our payload should be a self contained package



Recognize this? Michigan LEO should. ;-)



Do you know when Cellebrite last patched their jpeg/png parsing libraries?

Myth #3: Training scales



Myth #3: You can train your way to success.

Training at a local level



- Training is expensive!

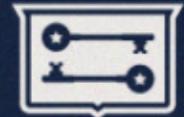
Immunity Master Class

Contact admin@immunityinc.com to reserve a slot for the next class!

Pricing: **\$6,000**

- Specialization vs. generalization
 - Specialization and deep expertise needed
 - But infeasible at small scale
- And in the end...
 - Attackers don't care how many acronyms you have after your name

Training at a federal level



- USCYBERCOM
- Recruit, train, retain?
 - Easy, medium, hard!
- Traditional military training
 - Recruit → Boot camp → Soldier
- “Cyber” military training
 - Recruit → ??? → l33t h4x0r?
- Organizational, culture incompatibilities



How to build a cyber army



Kim Jong-il and me:

How to build a cyber army to attack the U.S.

Charlie Miller

Independent Security Evaluators

cmiller@securityevaluators.com



Myth #4: Supply chain and vendors



Myth #4: Your supply chain is secure.

Built on sand



- How do you build a secure infrastructure, when the underlying components are untrusted?

Operation Cisco Raider

Sam King @ UIUC

PCWorld » Networking & Wireless

Recommend: Like 0 +1 0 Email 1 Comment Print

Counterfeit Cisco Gear Seized

By Grant Gross, IDG News Feb 29, 2008 11:10 am

U.S. and Canadian law enforcement authorities have seized more than US\$78 million worth of counterfeit Cisco Systems networking equipment in an ongoing investigation into imports from the U.S. Department of Justice and other agencies announced Friday.

HOME TECHNOLOGY SCIENCE ENTERTAINMENT BUSINESS GREEN

Scientists create malicious hardware

Posted on April 30, 2008 - 17:27 by Wolfgang Gruener

Urbana-Champaign (IL) – You are concerned about spam and viruses? You ain't seen nothing yet, believe researchers from the University of Illinois at Urbana-Champaign (UIUC): A next phase of more sophisticated viruses may not only exist in software, but may be deeply embedded in hardware, or what the scientists describe as “malicious circuits”.

RSA breach



- RSA, defense contractor breach
- If you're a hard target
 - Go after your vendors instead!
- To butcher a Fight Club quote:
 - *“On a long enough timeline, everyone gets owned.”*



Myth #5: Cyber war and terrorism



Myth #5: You should be frightened by cyber warfare and cyber terrorism.

What is cyber warfare?



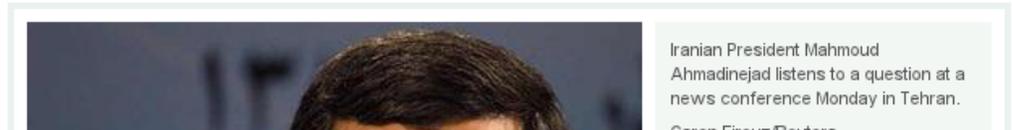
- Hacktivism?
 - NO.
- Comodo hacker?
 - NO.
- Stuxnet?
 - Maybe.
- Titan Rain?
 - I suppose...
- Attribution is hard.



Stuxnet: Ahmadinejad admits cyberweapon hit Iran nuclear program

President Mahmoud Ahmadinejad says that a computer worm incapacitated some centrifuges of the Iran nuclear program. The worm was surely Stuxnet, experts say.

By [Mark Clayton](#), Staff writer / November 30, 2010



Cyber terrorism



- What is “cyber terrorism”?

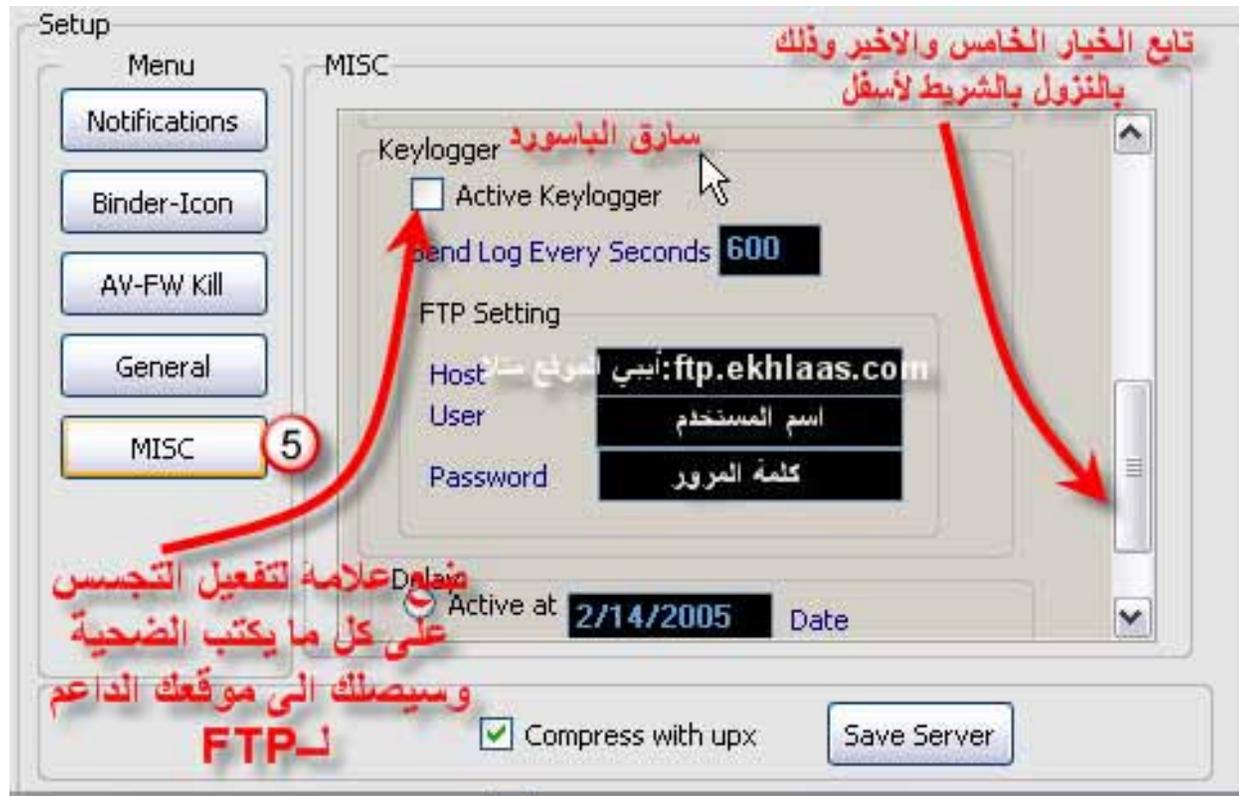
“If you ask 10 people what 'cyberterrorism' is, you will get at least nine different answers!”

When those 10 people are computer security experts, whose task it is to create various forms of protection against 'cyberterrorism', this discrepancy moves from comedic to rather worrisome.

When these 10 people represent varied factions of the governmental agencies tasked with protecting our national infrastructure and assets, it becomes a “critical issue.”

<http://www.symantec.com/avcenter/reference/cyberterrorism.pdf>

Not even close...



“Keylogger jihad”??? NO!

SCADA attacks



- SCADA attacks?
 - Yes, but extortion is more lucrative than terrorism...

www.ioactive.com **IOActive**
COMPREHENSIVE COMPUTER SECURITY SERVICES

Myth vs. Legend

- Lots of myths in SCADA
 - “Digital Pearl Harbor”
 - “Terrorist can take down the nation”
 - “I now have to fear my toaster”
- First let’s have a reality check

www.ioactive.com **IOActive**
COMPREHENSIVE COMPUTER SECURITY SERVICES

Incidents

- JavaScript scans
- Extortion
- CIA statement



- LEO faces the same problems as the private sector
 - Your adversaries are more skilled
 - Your tools are broken
 - Your analysts are undertrained
 - Your vendors are owned
 - Your terminology is misunderstood
- Sufficiently provoked yet? ;-)
 - Ask a question!

Questions from the Audience



Questions to Panelists:

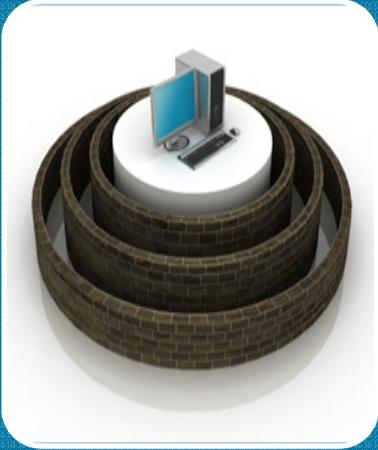


1. Who is the biggest target from a) cybercrime standpoint, b) cyber-terror and why?

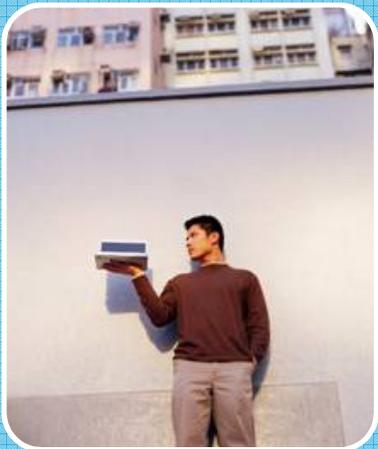


2. Do you have any suggestions as to how law enforcement can more effectively combat BitCoin (digital anonymous currency often double spent) and Zeus/SpyEye (a banking Trojan middleman) attacks?

Questions to Panelists:



3. As companies place their confidential data in the cloud, what are the cybercrime threats that should be considered and mitigated?



4. If you are so sure Anti-virus is dead, then what's the alternative?

Questions to Panelists:

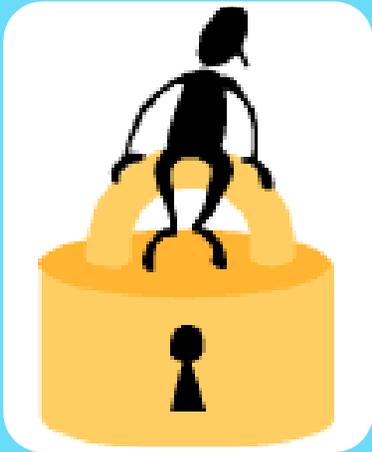


5. What tool would you recommend be in law enforcement investigator's cyber toolbox?



6. With regard to the rise in data security breach incidents and the exposure of so many people's personally identifiable information (PII), how can law enforcement assist companies with preventing these types of cyberattacks?

Questions to Panelists:



7. Why are you so certain that CVEs are the biggest holes we need to plug?



8. How has encryption use by cybercriminals changed the landscape for cybercrime law enforcement investigations? Any recommendations for combatting encryption usage?

Questions to Panelists:



9. Do you think that hackivists (unidentified political hackers) are working under foreign government support/direction or are truly merely committing acts of civil disobedience?

CONTACT INFORMATION

- **Faith M. Heikkila, Ph.D., CIPP, CISM**
• E: MI-InfraGard-President@charter.net

- **Gary Miliefsky, FMDHS, CISSP®**
E: garym@netclarity.net

- **Jon Oberheide**
E: jon@oberheide.org