



- 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`?





- 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.



“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 [icon]

==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

- Exploits targeting EnCase, FTK, etc

- Parsing is *hard*

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.



- 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 0 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.

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!



communications

- 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



Iranian President Mahmoud Ahmadinejad listens to a question at a news conference Monday in Tehran.
Caran Firuz/Reuters



- What is “cyber terrorism”?

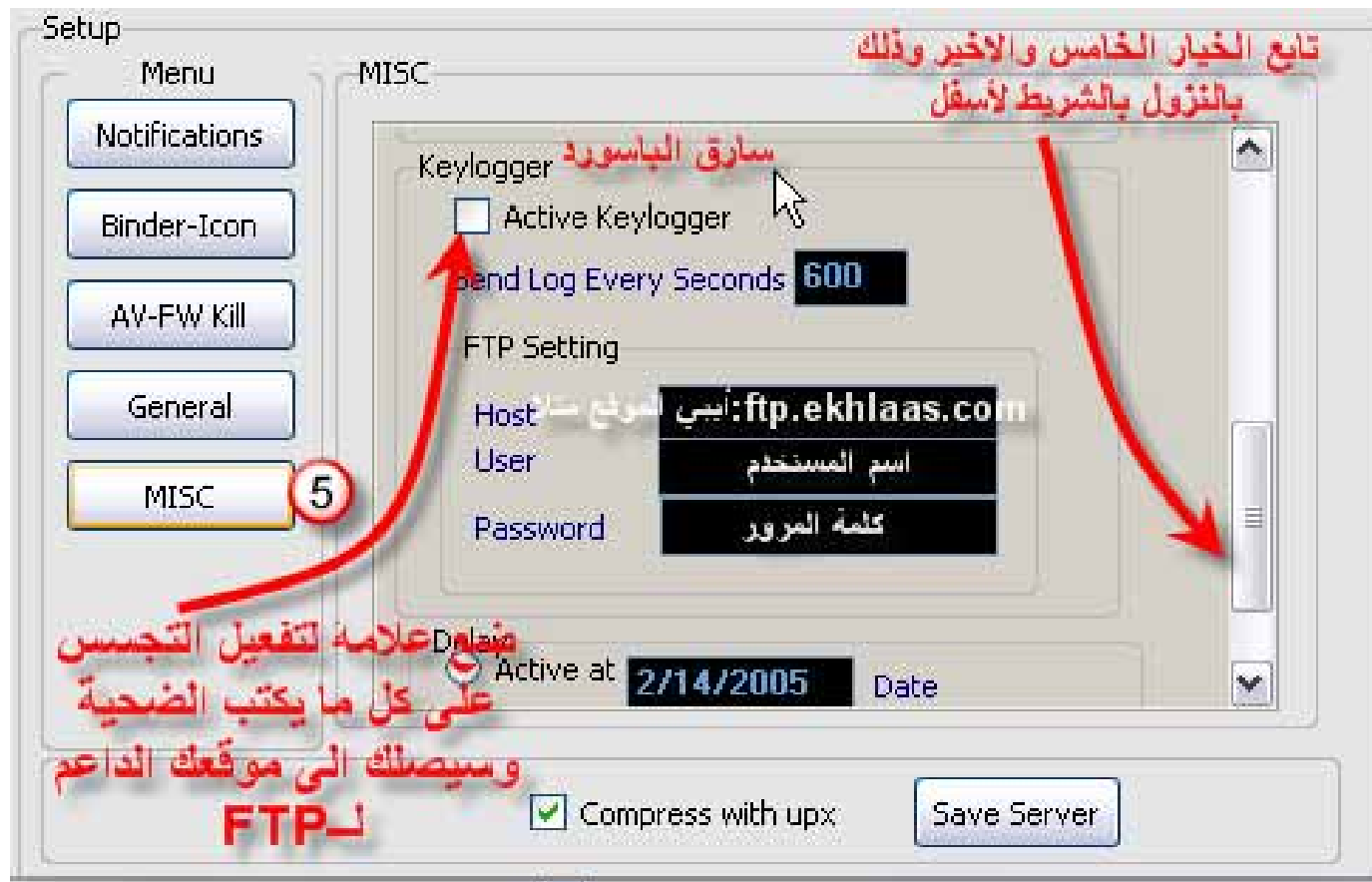
“If you ask 10 people what 'cyberterrorism' is, you will get at least nine different answers!

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?
 - 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!