

---

# The Bad Guys Are Winning: Now What?

---

By Ed Skoudis

Copyright 2009, All Rights Reserved  
Version 1Q09

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

1

---

## Outline

---

- ➡ State of the Hack
  - Some of the Implications...
    - For Pen Testers
    - For Enterprise Security Professionals
    - For the Military
  - Q&A

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

2

# This Presentation

- Based on discussions and brainstorming with some of the best penetration testers, computer attackers, and defenders I know
- I've been working in computer security for 14 years...
  - Pen tests, incident response, digital forensics, security architecture
- ...Trying to get a feel for evolutionary trends in that time
- This is a talk I could not have given two years ago
- It's a relatively recent mindset for me based on trends in the past 12 months
- It may be controversial
- I'm not expecting you to agree with me
- I'm not sure I even agree with myself on all of this... but it's got me thinking, and I hope you find these concepts worth at least considering

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

3

# State of the Hack

- Thesis:
  - A sufficiently determined, but not necessarily well-funded attacker can break into almost any modern organization
  - Gaining control of critical systems within the organization
  - Exfiltrating sensitive information
  - Acting unnoticed for sufficient periods of time to damage that organization

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

4

## Why Is This So? Vulnerabilities

- Increased attack surface
  - Client-side exploitation
    - Browsers (IE and Firefox), document rendering programs (Adobe, Word, Excel), media players (Real Player, Windows Media Player), program execution environments (Java Runtime Environment), etc.
  - Wireless (almost) everywhere
    - Wifi and Bluetooth
  - Webification of most applications
    - Web 2.0
    - SQL Injection still rampant (sad, sad, sad)
    - Cross-Site Scripting and Cross-Site Request Forgery
  - Such attacks can be combined together
    - See the *Pen Test Perfect Storm Trilogy* of webcasts by Josh Wright, Kevin Johnson, and Ed Skoudis

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

5

## More Why Is This So? Repeated Mistakes

- We're not learning from the mistakes of the past
  - Buffer overflow vulns still prevalent
  - Misconfigurations abound
  - Comprehensive patching processes remain elusive
  - New languages and environments to run them are embedded in nearly everything
  - General-purpose computer systems are hungry to run code...
  - ...and attackers are happy to provide it

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

6

## Why Is This So? Asymmetry and Botnets

- Computer attackers have always benefited from the fact that they only need to find one way in, while the “good guys” need to block almost every avenue in...
- ...or at least police every entry point
- A crucial asymmetry in offense vs. defense...
  - Making attackers’ jobs easier than defenders’
- Plus, with the rise of the botnet, the attackers increasingly have computer firepower that matches or even exceeds the target organization

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

7

## Outline

- State of the Hack
- Some of the Implications...
  - ➡ For Pen Testers
    - For Enterprise Security Professionals
    - For the Military
- Q&A

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

8

## Implications for Penetration Testers

- If a test scope is defined broadly enough, we almost always get in
  - Sure, if you take all of the interesting attack vectors off the table, you may thwart us... but not the real bad guys
  - “Just look at these four servers... see what you can do...”
    - The real attackers aren’t limited that way
- So what? If pen testers can’t help target organizations actually improve their security, they’re just showing off
  - Thus, it is more important than ever to express findings in business terms... and to emphasize the appropriate defenses

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

9

## Further Implications for Penetration Testers

- Actual bad guys can spend their time focusing exclusively on offense... considering defense only to thwart it
- Most pro pen testers spend time learning both offense *and* defense... trying to strike a balance
- What if... it might be ok to be unbalanced here?
- Spend more time and effort becoming *really* good at attacks, less time on defenses
- That way, a pen tester can better model actual attackers
- Unless you are a genius, of course... then work on both
- Also, I’m not advocating abandoning defensive knowledge altogether
- You need some knowledge of defenses to thwart them!
  - Note the change in emphasis... I said to thwart them, not to improve them


Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

10

## An Analogy

- The best defenders don't have to be good at offense
  - They need to anticipate what bad guys will do... but they don't need to be able to actually perform the attack
  - Defense should be informed by offense, but it doesn't require offensive capabilities
  - Observation: You can flip offense and defense and the argument is still reasonable
- The best gun manufacturers in the world likely cannot design Kevlar vests
  - But, if they make armor-piercing weaponry, they know a lot about those vests... but not how to manufacture them

## Outline

- State of the Hack
- Some of the Implications...
  - For Pen Testers
  -  – For Enterprise Security Professionals
  - For the Military
- Q&A

## Implications for Enterprise Security Personnel

- Most enterprises spend the vast majority of their infosec resources on prevention
  - Firewalls, anti-virus, system hardening, patching, etc.
  - Even audit and vuln assessment are a form of prevention – proactively finding flaws and fixing them before exploitation
- But, if exploitation has already occurred, your preventative measures have already failed... that gets back to the main thesis

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

13

## Implications for Enterprises... So What?

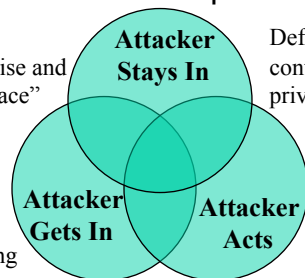
- We should divert some enterprise security resources from prevention to...
- ...detection and eradication
- Where has the bad guy already compromised me?
- How can I get rid of or disrupt attackers in our midst?

Defenses focus on detecting compromise and reducing "living space"

Defenses focus on controlling superuser privileges (admin and root)

Defenses focus on decreasing attack surface and hardening

Defenses focus on disrupting attacker command and control of implanted malware



\* Hat tip for diagram idea to NIAEC, Wende.Peters@jhuapl.edu


Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

14

## Implications for Enterprises... How?

- Intrusion Detection Systems
  - Not just Intrusion Prevention Systems... they often are tuned to a point where they can be dodged
- Log Analysis
  - Sounds painful, but a lot can be gained from it
- Looking for anomalous traffic
- Honeypots (honeyd, thp) and tarpits (Labrea)
- Then, clean up – re-imaging has good benefits
- Also, such detection and eradication efforts can provide insight in how to better position preventative measures (i.e., iterate to improve)

## Outline

- State of the Hack
- Some of the Implications...
  - For Pen Testers
  - For Enterprise Security Professionals
  -  – For the Military
- Q&A



## Implications for the Military

- This is where things get ugly and scary
- It is widely rumored and in some cases actually reported that major government, military, and civilian infrastructure systems have been compromised
- So what?
  - Direct denial of service
  - Planting of “kill switches”
  - Or, more insidiously... information theft
  - Attacks against the integrity of important data

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

17

## Estonia 2007, Georgia 2008, and Kyrgyzstan 2009

- Massive flood each year:
  - 2007, Estonia in aftermath of demonstrations over moving a Soviet-era statue
  - 2008, Georgia, just before and during Russian invasion
  - 2009, Kyrgyzstan, possibly tied to Russian requests to prohibit establishment of US airbase there
- The attacks evolved through various distinct phases
- Was it merely Russian nationalists and organized crime, or was the Russian government involved?
- The government denies involvement, but the New York Times reports that someone paid for a rented bot-net for some of these attacks

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

18

## Blockade, Anyone?

- A blockade (barring entry to a port of trade) is an act of war
- If someone brings down the Internet so that e-commerce is halted... is that an act of war?
- If someone brings down Amazon.com or Google, is that?
- What are their motivations? Who is funding them?

## Cyber Attacks As a Precursor to Kinetic Attacks

- Before kinetic attacks occur, an actor could prepare the battlefield with cyber attack
  - Disable critical infrastructure
  - Alter it so that it doesn't function properly
- Could incite the following kinetic warfare...
- Or inhibit it

## Difficulty of Attribution

- Direct attribution in the cyber world is very difficult if the attacker is a) clever and b) desires anonymity
- A large nation could attack another one and deny action
- A small actor could incite two larger players into a conflict
- Some countries have stated that they consider a cyber attack on their territory to be the equivalent of the use of WMD against them... and they will respond *in kind*
- Would the US be willing to engage militarily without knowing *for sure* who triggered a cyber attack?

Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

21

## Conclusions

- The world is changing...
- More reliance on IT... more reliance on information security professionals
- But, infosec itself is rapidly evolving, possibly in ways that aren't all rainbows and unicorns
- But, the militarization of cyber space was likely inevitable
- We could try to resist it... or embrace it



Bad Guys Are Winning... Now What? - ©2009, Ed Skoudis

22