Practical Malware Analysis

Ch 1: Malware Analysis Primer

Updated 1-15-16

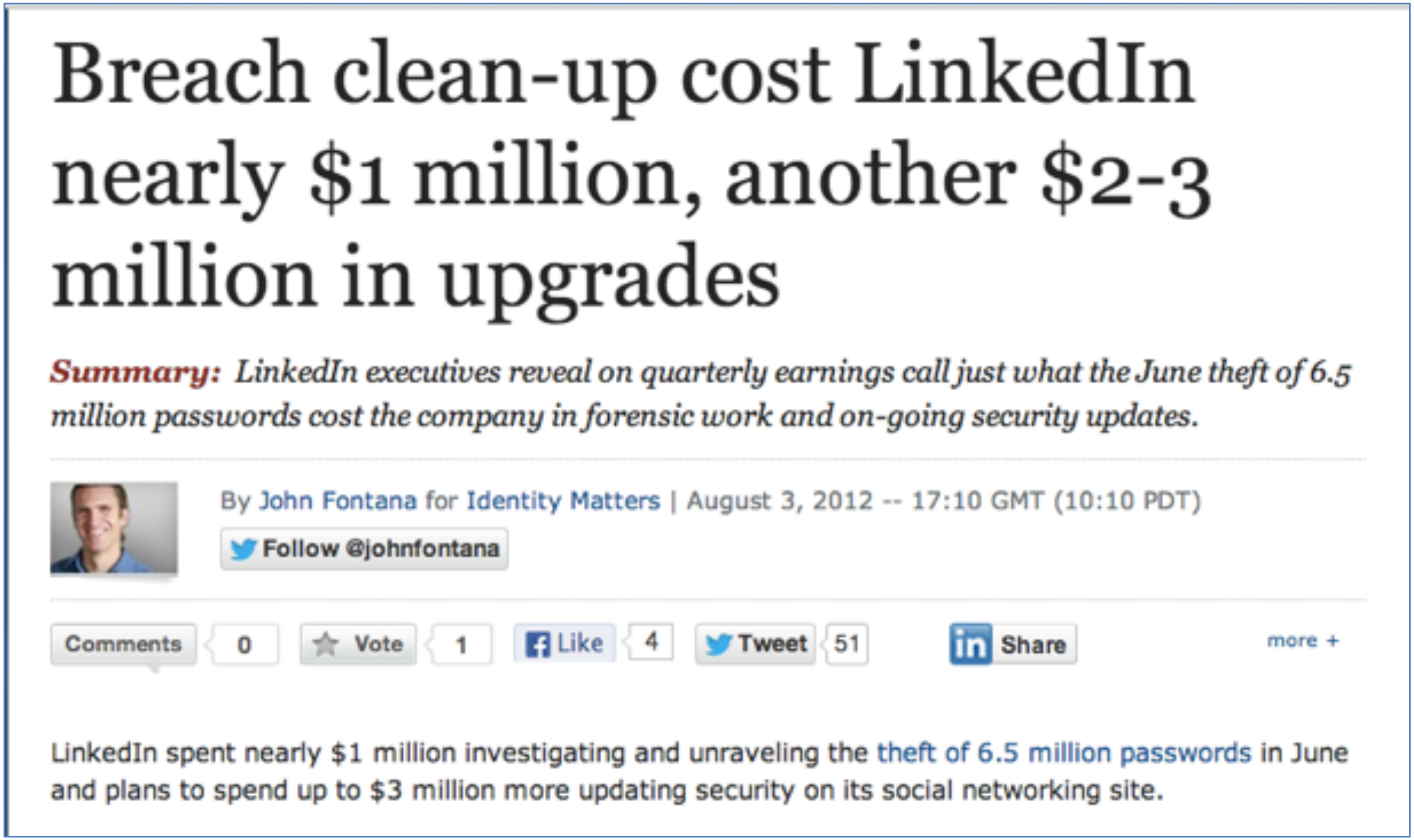
The Goals of Malware Analysis

Incident Response

- Case history
  - A medical clinic with 10 offices found malware on one of their workstations
  - Hired a consultant to clean & re-image that machine
- All done—case closed?

Incident Response

- After malware is found, you need to know
  - Did an attacker implant a rootkit or trojan on your systems?
  - Is the attacker really gone?
  - What did the attacker steal or add?
  - How did the attack get in
    - Root-cause analysis



Breach clean-up cost LinkedIn nearly $1 million, another $2-3 million in upgrades

***Summary:** LinkedIn executives reveal on quarterly earnings call just what the June theft of 6.5 million passwords cost the company in forensic work and on-going security updates.*

By John Fontana for Identity Matters | August 3, 2012 -- 17:10 GMT (10:10 PDT)

LinkedIn spent nearly $1 million investigating and unraveling the theft of 6.5 million passwords in June and plans to spend up to $3 million more updating security on its social networking site.

- Link Ch 1a

Malware Analysis

- Dissecting malware to understand
  - How it works
  - How to identify it
  - How to defeat or eliminate it
- A critical part of incident response

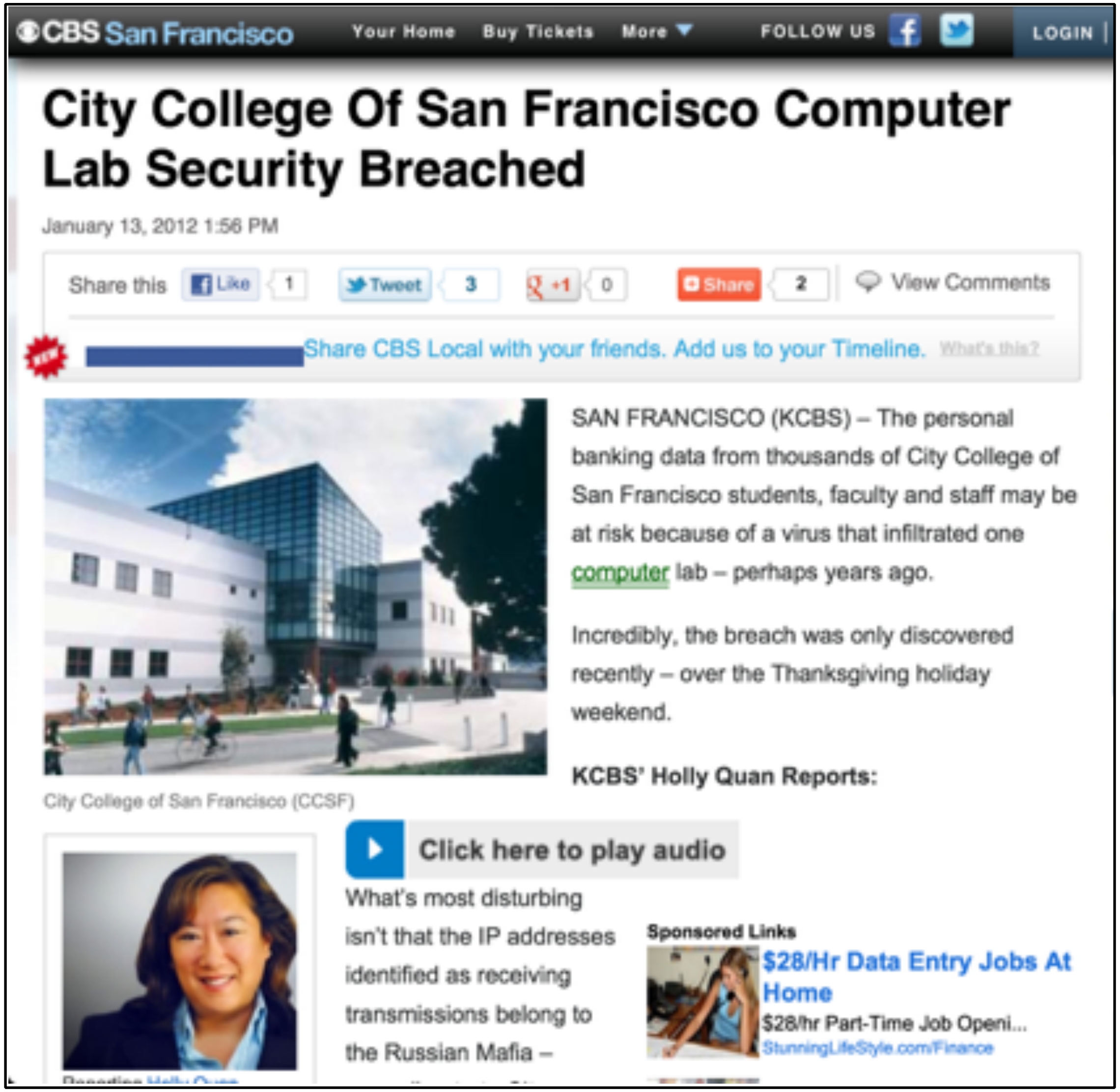
The Goals of Malware Analysis

- Information required to respond to a network intrusion
  - Exactly what happened
  - Ensure you’ve located all infected machines and files
  - How to measure and contain the damage
  - Find signatures for intrusion detection systems

Signatures

- Host-based signatures
  - Identify files or registry keys on a victim computer that indicate an infection
  - Focus on what the malware did to the system, not the malware itself
    - Different from antivirus signature
- Network signatures
  - Detect malware by analyzing network traffic
  - More effective when made using malware analysis

False Positives



City College Of San Francisco Computer Lab Security Breached

January 13, 2012 1:56 PM

City College of San Francisco (CCSF)

SAN FRANCISCO (KCBS) – The personal banking data from thousands of City College of San Francisco students, faculty and staff may be at risk because of a virus that infiltrated one computer lab – perhaps years ago.

Incredibly, the breach was only discovered recently – over the Thanksgiving holiday weekend.

KCBS' Holly Quan Reports:

What's most disturbing isn't that the IP addresses identified as receiving transmissions belong to the Russian Mafia –

Reporting Holly Quan

Malware Analysis Techniques

Static v. Dynamic Analysis

- Static Analysis
  - Examines malware without running it
  - Tools: VirusTotal, strings, a disassembler like IDA Pro
- Dynamic Analysis
  - Run the malware and monitor its effect
  - Use a virtual machine and take snapshots
  - Tools: RegShot, Process Monitor, Process Hacker, CaptureBAT
  - RAM Analysis: Mandant Redline and Volatility

Basic Analysis

- Basic static analysis
  - View malware without looking at instructions
  - Tools: VirusTotal, strings
  - Quick and easy but fails for advanced malware and can miss important behavior
- Basic dynamic analysis
  - Easy but requires a safe test environment
  - Not effective on all malware

Advanced Analysis

- Advanced static analysis
  - Reverse-engineering with a disassembler
  - Complex, requires understanding of assembly code
- Advanced Dynamic Analysis
  - Run code in a debugger
  - Examines internal state of a running malicious executable

Types of Malware

Types of Malware

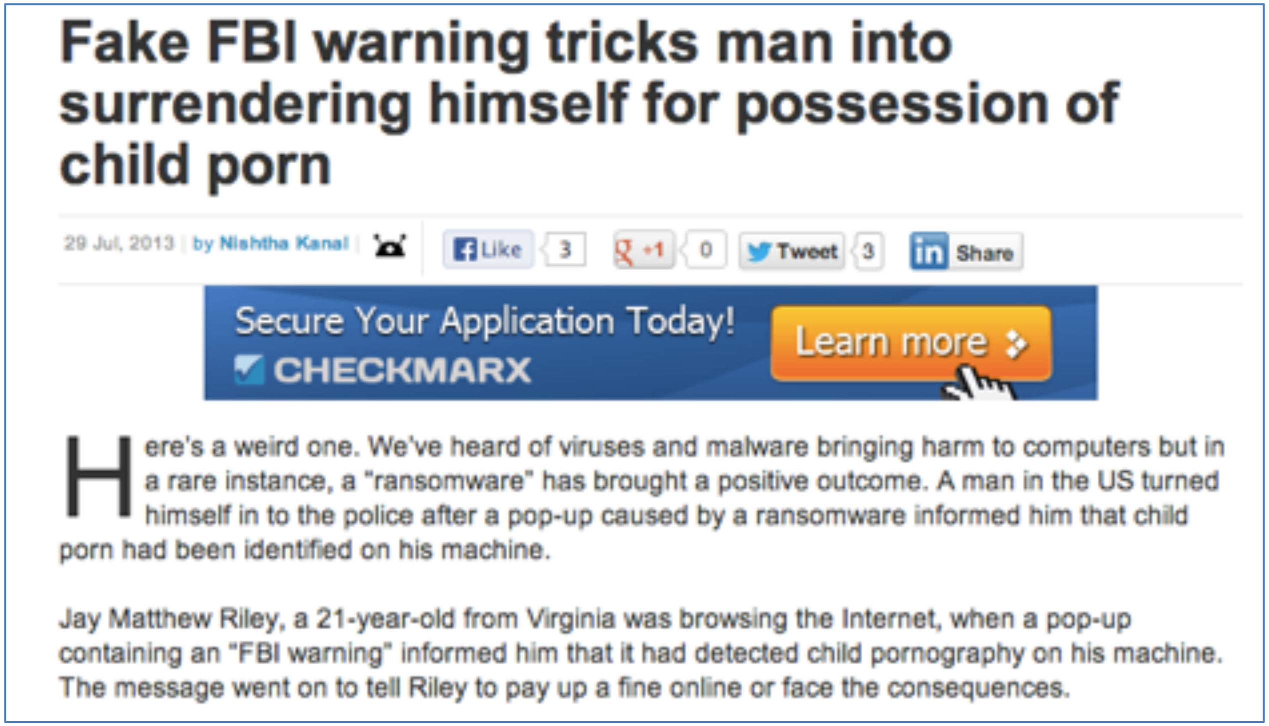
- Backdoor
  - Allows attacker to control the system
- Botnet
  - All infected computers receive instructions from the same Command-and-Control (C&C) server
- Downloader
  - Malicious code that exists only to download other malicious code
  - Used when attacker first gains access

Types of Malware

- Information-stealing malware
  - Sniffers, keyloggers, password hash grabbers
- Launcher
  - Malicious program used to launch other malicious programs
  - Often uses nontraditional techniques to ensure stealth or greater access to a system
- Rootkit
  - Malware that conceals the existence of other code
  - Usually paired with a backdoor

Types of Malware

- Scareware
  - Frightens user into buying something
  - Link Ch 1b



Fake FBI warning tricks man into surrendering himself for possession of child porn

29 Jul, 2013 | by Nishtha Kanal |

Here's a weird one. We've heard of viruses and malware bringing harm to computers but in a rare instance, a "ransomware" has brought a positive outcome. A man in the US turned himself in to the police after a pop-up caused by a ransomware informed him that child porn had been identified on his machine.

Jay Matthew Riley, a 21-year-old from Virginia was browsing the Internet, when a pop-up containing an "FBI warning" informed him that it had detected child pornography on his machine. The message went on to tell Riley to pay up a fine online or face the consequences.

Types of Malware

- Spam-sending malware
  - Attacker rents machine to spammers
- Worms or viruses
  - Malicious code that can copy itself and infect additional computers

Mass v. Targeted Malware

- Mass malware
  - Intended to infect as many machines as possible
  - Most common type
- Targeted malware
  - Tailored to a specific target
  - Very difficult to detect, prevent, and remove
  - Requires advanced analysis
  - Ex: Stuxnet

General Rules for Malware Analysis

General Rules for Malware Analysis

- Don’t Get Caught in Details
  - You don’t need to understand 100% of the code
  - Focus on key features
- Try Several Tools
  - If one tool fails, try another
  - Don’t get stuck on a hard issue, move along
- Malware authors are constantly raising the bar