Computer Security

06. Malware

Paul Krzyzanowski

Rutgers University

Spring 2017

Malware

- Etymology
  - **Mal** = prefix: bad, wrong
    - French *mal*; Old French *mal;* Latin *male/malus/mala*
  - **Ware** = suffix: software
    - Proto-Germanic *warjaz* (“dwellers of”)
- Any malicious software
  - Viruses
  - Worms
  - Trojan horses
  - Spyware
  - Adware
  - Backdoors
  - Ransomware

Virus

- Software that attaches itself to another piece of software or content that will be accessed by specific software
- Replicates by copying itself or modifying:
  - Other programs
  - Files read by other programs
  - Boot sector
- Usually spread by sharing files or software

Worms vs. Viruses

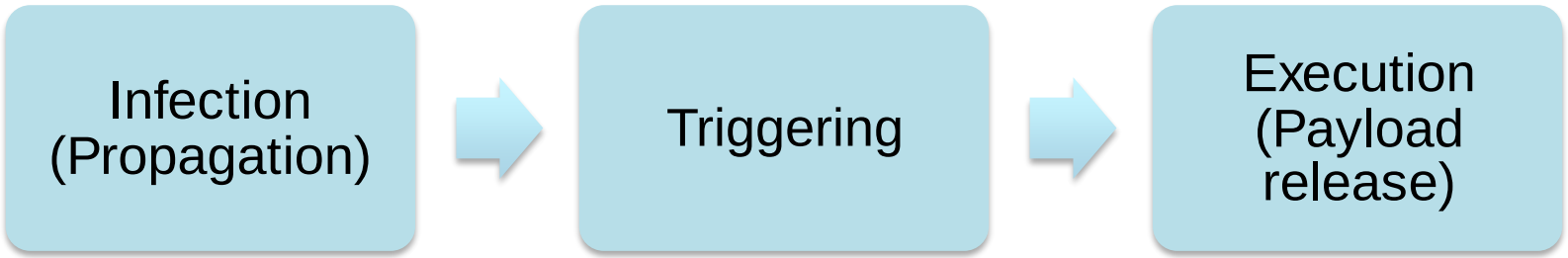
- Conceptually similar
  - Key distinction is whether they are standalone

- Worm
  - Standalone software that replicates itself to spread to other computers
  - Some spread automatically; others require human intervention

- Virus
  - Requires a host program

Virus components

- Infection mechanism
  - Search for infection targets: other programs, specific files, disk areas
- Payload
  - The malicious part of the virus
- Trigger (logic bomb)
  - Executed whenever a file containing the virus is run
  - Determines whether the *payload* should be delivered
    - Virus may stay dormant for some time



File infector viruses

- Virus adds itself to the end of an executable program file
- Patches a branch to that code at the start of the program
- Ideally
  - Hidden in some unused part of the file so file length remains unchanged

Boot sector viruses

- Infect the Master Boot Record (MBR) of a drive
  - Originally – infect boot sector of floppy drives
- Infected code runs when the system is booted
  - Will try to infect other disks
- Largely extinct
  - We don't use floppy disks
  - Used DOS commands to spread to floppy disks
- Bootkits: malware to place code in the MBR
  - Runs before the operating system starts!

Infected flash drives

- People share flash drives the way they used to share floppies
- Older systems (there are still lots of them)
  - Exploit AutoRun feature of Microsoft Windows
    - **autorun.inf**, orginally created for CD-ROM drives
  - Automatically runs a program on the drive when the drive is detected
- Main problem now
  - Unprotected firmware
  - Malware can replace firmware on a USB device to make it act like another device: e.g., make a flash drive behave like a keyboard
  - Can act like a regular storage device until the system is rebooted and the firmware detects it is talking to the BIOS
- The other problem with flash drives: data leakage
  - They're easy to lose

Macro viruses

- Microsoft Office apps have a powerful macro language
  - VBScript – based on Visual Basic
  - Extra features make it easy to get to
    - Network printers
    - Network shares
    - Special folders
    - User information
    - Script execution on remote systems
    - Etc.

- Microsoft Office documents can be used to spread viruses
  - Usually infect `normal.dot` – default template file
  - This will cause new Word documents to get infected

- Spread by ordinary business behavior

Macro viruses

- **ILOVEYOU** virus: 2000
  - Propagated via email
  - Subject of the message stated it's a love letter from a secret admirer
  - **`LOVE-LETTER-FOR-YOU.TXT.vbs`**
- .vbs suffix = Visual Basic Scripting
- What it did:
  - Copied itself several times into various folders
  - Added new files to the victim's registry keys
  - Replaced several different kinds of files (music, multimedia) with copies of itself
  - Sent itself through Internet Relay Chat clients and email
  - Download a file called `WIN-BUGSFIX.EXE` & executed it
    - Instead of fixing bugs, this stole passwords and emailed them to the hacker

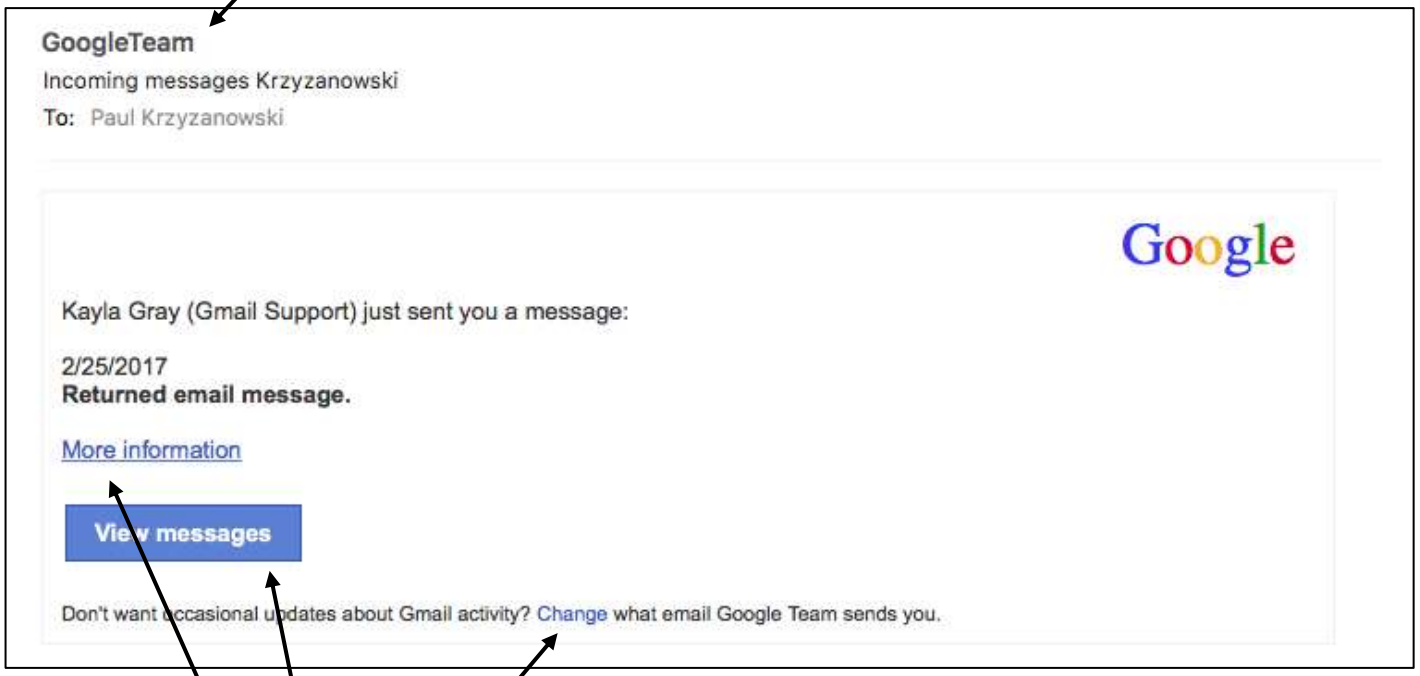
Social engineering helps

- ILOVEYOU
  - Mail often came from a sender you knew
- Melissa (earlier virus)
  - Promised a list of passwords for X-rated web sites

Email-based transmission dramatically increased the spread of malware

From: GoogleTeam <csalans@salans.com>

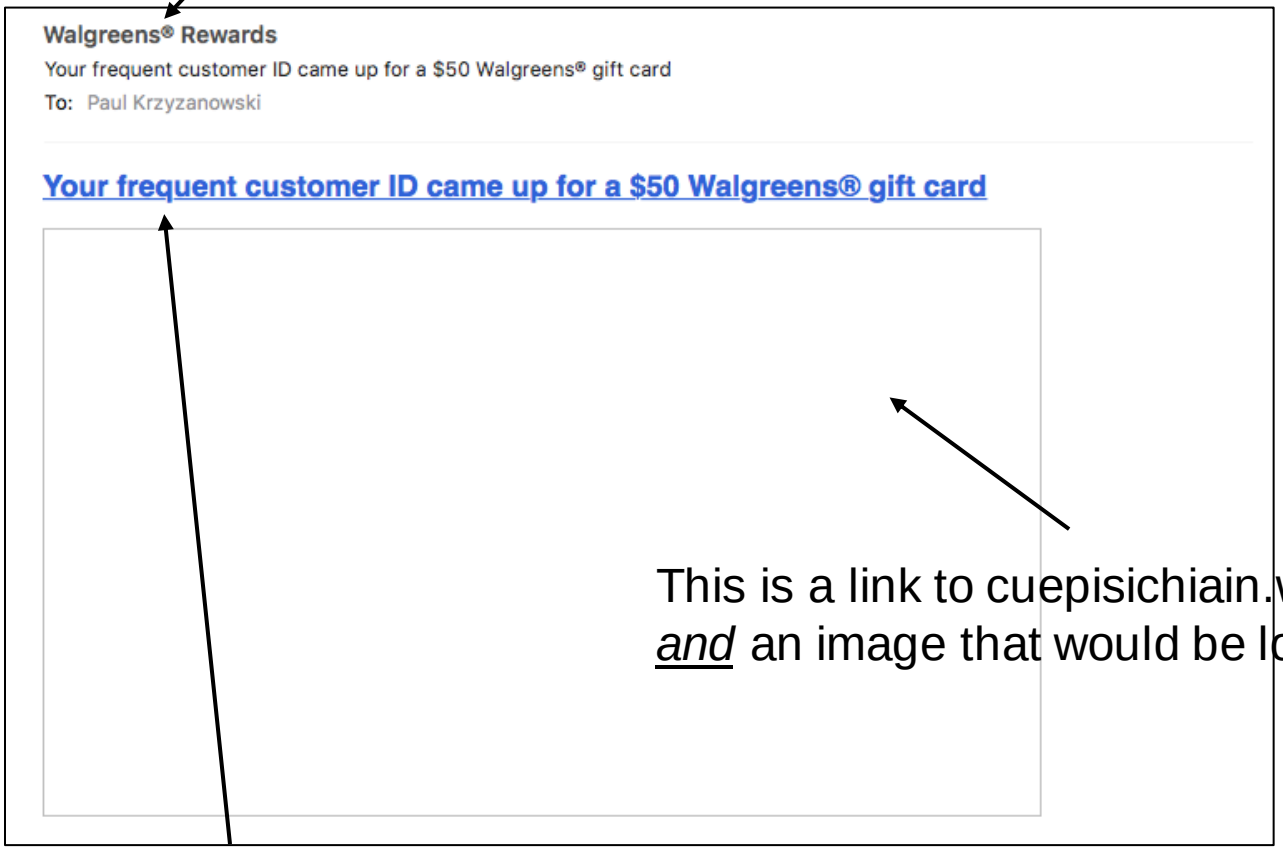
But it came from 107.170.47.71, which is lemp.frosticsatellite.com.



These are links to `playground.omg-bg.com/...`

From: Removal.walg1gmco27890@cuepisichiain.w220.luamev.top

But came from 46.3.221.220,
which belongs to Vyacheslav S. Bashin of Moscow

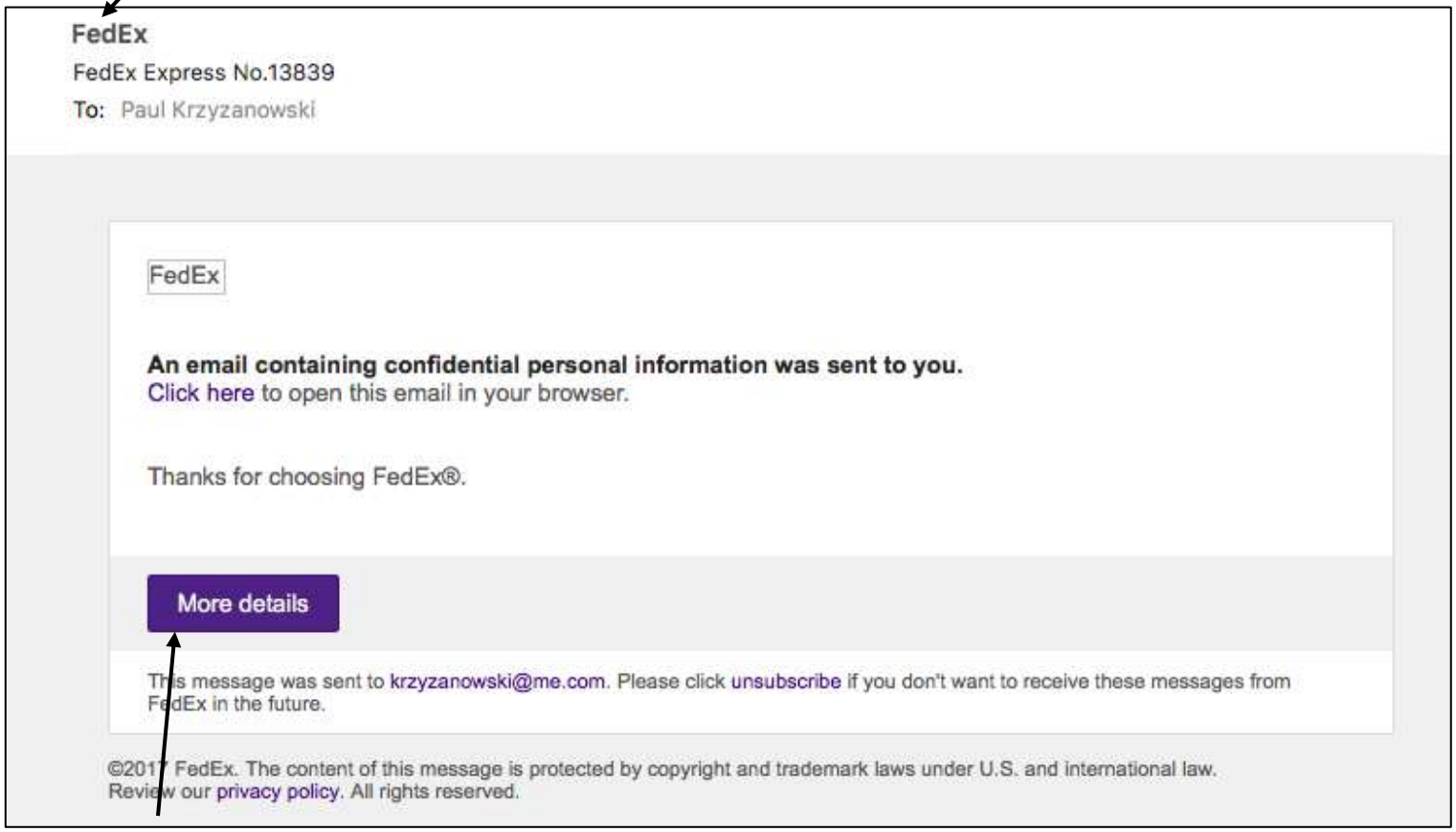


This is a link to cuepisichiain.w220.luamev.top/…
and an image that would be loaded from the site

This is a link to cuepisichiain.w220.luamev.top/…

From: FedEx <detacher@net4webmail.com>

But came from detacher@net4webmail.com



This is a link to `www.ethoscontabilidade.net.br/…`

Trojan Horses

Trojan Horses

Program with two purposes

- Overt purpose: known to a user
- Covert purpose: unknown to a user

Name the script *ls*

Place it in someone's shell PATH to get them to execute it

You get a setuid shell to their ID

They think they ran the real *ls* command

```
cp /bin/sh /tmp/.xyz
chmod u+s,o+x /tmp/.xyz
rm ./ls
ls $*
```

Trojan Horses

- What they might do
  - Back doors
  - Remote camera access
  - Key loggers
  - Web clickers
  - Proxies (allow your machine to help anonymize connections)
  - Spam engines
  - DDoS engines
- How do you get people to install them?
  - Lure the user to think it's useful software – *hacker tools, anti-virus tools*

Backdoors

- Remember Robert Morris' Internet worm?
  - Exploited *gets* buffer overflow
  - Tried to crack passwords
  - Connect to remote hosts
  - Also used a back door in `sendmail`
- Sedmail
  - Eric Allman, author of *sendmail*, wanted development access on a production system
  - The sys admin said, "no"
  - He installed a password-protected back door in the next release
    - Back door was generally unprotected
- Ken Thompson's modified C compiler installed a back door to `login`

Phishing

- Social engineering attack
- Try to get personal information or login data
- Instilling panic helps
  - Your eBay or PayPal accounts may be canceled
  - We noticed a fraudulent transaction in your account
  - We couldn't deliver your package and it will be sent back

Spear phishing

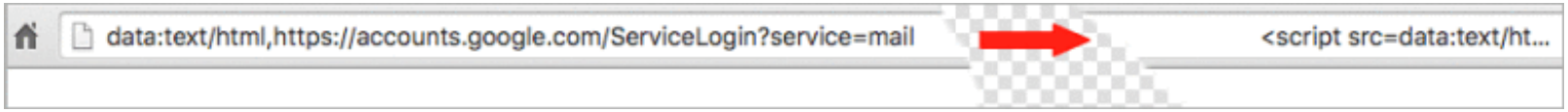
- Phishing attacks are impersonal
- Spear phishing
  - Attacks are customized with information about the target
  - More likely to trick a target into thinking the content is legitimate

The 2016 Democratic National Committee (DNC) was facilitated by spear phishing

- Russian hacking group Fancy Bear used bit.ly links
  - Short URLs help mask malicious URLs
- Redirect victims to a URL: looks like a legitimate Google accounts login page
  - Prepopulated with the victim's Gmail address
- From October 2015 – May 2016, 8,909 bit.ly links targeted 3,907 accounts
  - 20 clicks on malicious links were recorded on hillaryclinton.com
  - 4 clicks were recorded on dnc.org

Recent: Gmail spear phishing

- Hackers send email to contacts of compromised accounts
  - Email contains an innocent-looking attachment
- When the user clicks the attachment
  - A new tab opens that looks like the Google sign-in page
  - Login information goes to the attacker
- Attackers log in to your account immediately
  - Use one of your actual attachments & one of your actual subject lines
  - Send mail to people in your contact list
  - Mail contains a thumbnail image of the attachment
    - But the link is a script (but pre-padded with spaces)



http://bgr.com/2017/01/17/gmail-phishing-attack-attachment-address-bar/

Keyloggers

- Record everything you type (sometimes mouse movements too)
  - Allows attackers to get login names, passwords, messages
- Several ways to do this
  - A malicious hypervisor can intercept & log all keyboard & mouse operations
  - Kernel-based rootkit
  - Windows hook mechanism
    - Procedure to intercept message traffic before it reaches a target windows procedure
    - Can be chained
    - Installed via SetWindowsHookEx WH_KEYBOARD and WH_MOUSE
      - Capture key *up*, *down* events and *mouse* events
  - Browser-based
    - JavaScript onKeyUp()
    - Intercept form submission (form grabbing)
- Hardware loggers

PDF, JavaScript

- JavaScript can be dangerous (powerful scripting)
  - Most browser security holes involve JavaScript
  - PDF files now can contain JavaScript
- JavaScript can connect to other sites
  - It can do things like port scans
  - Any web site you connect to can leverage your machine

Source repositories

Do you just download and compile code from github?

- Or do you inspect it? … or assume someone else has?

Hackers often plant Trojan horses (often back doors) in popular software

- October 13, 2013

  PHP source code compromised?

  It was announced that the PHP website was hacked and serving malware. If the attackers had access to their internal servers, can we trust the PHP sourcecode anymore?

- September 1, 2011

  Linux source code repository compromised

  The Kernel.org website – home to the Linux project and the primary repository for the Linux kernel source code – sports a warning notifying its users of a security breach that resulted in the compromise of several servers in its infrastructure.

https://barracudalabs.com/2013/10/php-net-compromise/

https://www.helpnetsecurity.com/2011/09/01/linux-source-code-repository-compromised/

– March 5, 2012

GitHub hacked, millions of projects at risk of being modified or deleted

GitHub, one of the largest repositories of commercial and open source software on the web, has been hacked. Over the weekend, developer Egor Homakov exploited a gaping vulnerability in GitHub that allowed him (or anyone else with basic hacker know-how) to gain administrator access to projects such as Ruby on Rails, Linux, and millions of others. Homakov could've deleted the entire history of projects such as jQuery, Node.js, Reddit, and Redis.

– October 4, 2013

Adobe Source Code and Customer Data Hacked

Adobe has confirmed the company was the victim of a long term network breach which exposed consumer data including passwords and credit card data, as well as exposing the source code for some of their leading products.

https://www.extremetech.com/computing/120981-github-hacked-millions-of-projects-at-risk-of-being-modified-or-deleted

Rootkits

- Mechanisms to
  - Install software (usually malware)
  - Hide its existence
- How
  - Replace common admin commands (*ps, ls, find, top, netstat*) with ones that conceal the existence of the intruder
- Started on Unix Systems in 1990
  - NTRootkit in 1999
  - HackerDefender for Windows NT/2000/95 in 2003
  - Mac OS X rootkit in 2009
  - Stuxnet worm

Rootkits

- User mode
  - Replace commands
  - Intercept messages
  - Exploit vulnerabilities
  - Patch commonly-used APIs
- Kernel mode
  - Installed as kernel modules
  - Gives the rootkit unrestricted access
    - Can modify the system call table and any kernel structures
  - Difficult to detect
    - All commands and libraries look normal

Sony BMG DRM (2005)

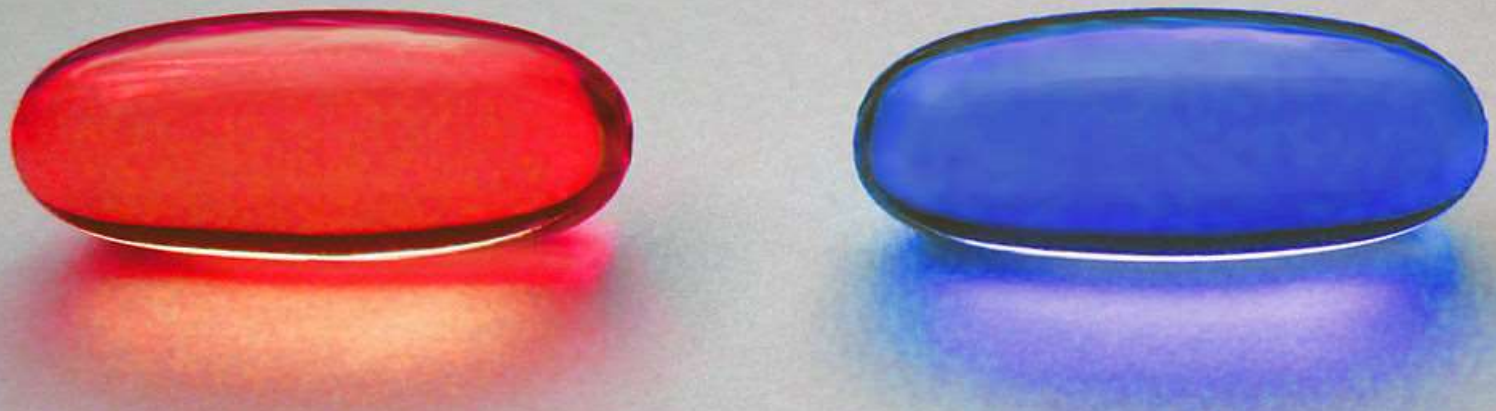
- Sony didn't want you making copies of their music
  - .. So they added digital rights management (DRM) software
- When you played certain Sony music CDs on your computer, Sony installed a DRM package
  - It modified the operating system to prevent copying the CD
- Sony also installed a rootkit to "protect" the DRM software
  - The software could not be installed
- The software also phoned home every time you played the CD

Hypervisor rootkits

- A system with no virtualization software installed but with hardware support for virtualization can have a hypervisor-based rootkit installed

- Rootkit runs at a higher privilege level than the OS.
  - It's possible to write it in a way that the kernel will have a limited ability to detect it.

"You take the blue pill, the story ends. You wake up in your bed and believe whatever you want to believe. You take the red pill, you stay in Wonderland, and I show you how deep the rabbit hole goes."



The term *red pill* refers to a human that is aware of the true nature of the **Matrix**.

Hypervisor attacks

- A hypervisor sits below the operating system
- All device access goes through the VM
  - Memory page tables, interrupts, clock, display, disk I/O, network I/O, etc.

Blue Pill – rootkit based on x86 virtualization (AMD & Intel)

- The hypervisor *is* the rootkit
- Essentially undetectable
  - OS, all system programs, all libraries, all applications, and all files look clean
  - Hypervisors are designed to be seamless – an OS cannot query to see if it's running on a hypervisor
- Detection may be possible via a *timing attack*
  - Analyze time it takes for privileged operations to take place
  - An OS running on a hypervisor will take longer
  - You don't know if it's malicious but you can suspect that you're running over a hypervisor
  - A really good blue pill will adjust the time – you'll need to check via the network

Hypervisor attacks

Red Pill – detect the presence of a hypervisor (AMD & Intel)

- Intel/AMD SIDT instruction
  - Stores contents of interrupt descriptor table register (IDTR) into a memory location
  - The Interrupt Descriptor Table Register contains a memory location
- Does not require privileged mode
  - Returns contents of the IDTR, which *is* sensitive
- The CPU has only one IDTR, so the VMM needs to juggle copies
- The magic:
  - Running SIDT does *not* cause an interrupt
  - Process gets the *relocated* address of the SIDT

Goals

- Corrupt files
- Encrypt files
- Encrypt files and hold for ransom
- Change BIOS settings
- Erase flash BIOS
- Steal information
- Hide

Adware

- Ads show up when a user is online
- Collects marketing data & other information without the user's knowledge
- A lot of peer-to-peer software includes third-party adware
  - What does it really monitor?

Ransomware

- Denial-of-service malware that
  - Encrypts victim's data
    - Or even encrypt the Master File Table (NTFS version of inode table)
  - Threatens to publish victim's data
  - Or locks the system
- Demands payment to decrypt
- Usually distributed via a Trojan whose payload looks like a legitimate file
- MacAfee collected >250,000 unique samples of ransomware in 2013
  - CryptoLocker spread via infected email attachments
    - Got $3 million before it was shut down by the FBI and Interpol
  - Cryptowall
    - Spread via spam emails, exploit kits hosted through malicious ads or compromised sites
    - Got $18 million before it was shut down in 2015

Military malware

- Viruses are a key part of most military cyberarsenals
- Espionage & attack
- They get to the target when you cannot reach it directly

Stuxnet

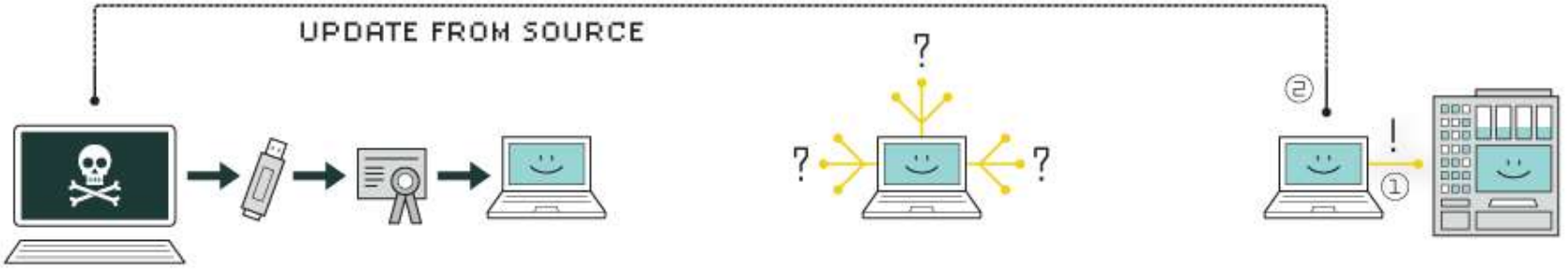
- Most sophisticated known cyberattack
  - 500 KB worm
  - Infected software of at least 14 industrial sites in Iran, including a uranium enrichment plant
  - Used four different 0-day attacks
- What it did
  - Targeted Microsoft Windows systems, replicating itself & propagating
    - Via USB thumb drives and LAN attacks
  - Searched for Siemens Step7 software
    - Windows-based software used to program industrial control equipment such as centrifuges
  - Compromised the programmable logic controllers
- Allowed authors to spy on the industrial systems and cause centrifuges to over-spin while the control panel showed everything was OK

Ramifications

- Not much is safe
- Similar attacks can affect
  - Banks
  - Water supplies
  - Power plants
  - Airlines
  - Soon … cars, trucks, buses

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Security Threats

- Hypervisor-based rootkits
- A system with no virtualization software installed but with hardware-assisted virtualization can have a hypervisor-based rootkit installed.
- Rootkit runs at a higher privilege level than the OS.
  - It's possible to write it in a way that the kernel will have a limited ability to detect it.

The end