

Computer Security
06. Malware

Paul Krzyzanowski
Rutgers University
Spring 2019

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 1

The New York Times
November 5, 1988

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 2

Author of Computer 'Virus' Is Son Of N.S.A. Expert on Data Security
Cornell Graduate Student Described as 'Brilliant'

By JOHN MARKOFF

The "virus" program that has introduced, and secretly and slowly made copies that would move from computer to computer. But a design error caused it instead to replicate madly out of control, ultimately jamming more than 6,000 computers nationwide in this country's most serious computer "virus" attack.

The dem's program jammed the computers of corporate research centers including the Rand Corporation and SRI International universities like the University of California at Berkeley and the Massachusetts Institute of Technology as well as military research centers and bases all over the United States.

The virus's creator could not be reached for comment yesterday. The source said the student flew to Washington yesterday and is planning to hire a lawyer and meet with officials of the Defense Communications Agency, in charge of the Arpanet network.

Friends of the student said he did not intend to cause damage. They said he created the virus as an intellectual challenge to explore the security of computer systems.

His father, Robert T. Morris Sr., has written widely on the security of the Unix operating system, the computer master program that was the target of the son's virus program. He is now chief scientist at the National Computer Security Center in Bethesda, Md., the arm of the National Security Agency devoted to protecting computers.

Poland is buying 3 Boeing airliners for \$220 million. U.S. East Coast airlines order a first sale to be financed through a lease-purchase accord with Western banks.

MOSCOW SUSPENDS PULL-OUT OF ITS AFGHANISTAN FORCES. CHARGES VIOLATIONS OF PACT.

BETTER JUNE SOFT. Stocks set at a high. Pacific is leading in performance.

WHY ELIMINATED. Defense aides say.

Unemployment declines to 6.2%. Marking lowest rate since '74.

Study Says Immigration Law Is Leading to Discrimination.

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 3

Robert Tappan Morris Jr.'s Internet Worm

Attacked VAX systems running BSD

1. Attempt to crack local passwords
 - Guess passwords via dictionary attack
 - 432 common passwords and combinations of account name and user name
2. Look for readable .rhost files — that may give you free rsh access to another system
3. Do a buffer overflow exploit on fingerd via gets to load a small program
 - 99 lines of C
 - Program connects to sender and downloads the full worm
4. Use the DEBUG command of sendmail
 - Allowed remote command execution on a remote system

Then propagate the program onto any system you can log into

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 4

Buffer Overflows

Some high-profile buffer overflow attacks

- 2001: Code Red worm
 - Buffer overflow attack on Microsoft's IIS
- 2003: SQL Slammer
 - Buffer overflow attack on Microsoft's SQL Server
- 2003: X-Box attack
 - Buffer overflow attack bypasses license checking
- 2010: PS2 Independence exploit
 - Buffer overflow attack bypasses license checking

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 5

Malware

Etymology

Mal = prefix: bad, wrong
French *mal*; Old French *mal*; Latin *male/malus/mala*

Ware = suffix: software
Proto-Germanic *warzja* ("dwellers of")

Any malicious software

- Viruses
- Worms
- Trojan horses
- Spyware
- Adware
- Backdoors
- Ransomware

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 6

Motivation

- Steal account credentials
 - Get credentials for other systems
- Espionage
 - Steal content
 - Spyware: monitor user activity
- Sabotage: destroy content or connected devices
- Host services
 - Host contraband data
 - Send spam
 - Mine cryptocurrency
 - Botnet for DDoS attacks
- Ransomware

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

7

Infiltration

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

8

How does malware get onto a computer?

- You installed it
 - Social engineering (convincing you to install it)
 - E.g., security software, "cleaner" software, software "updates"
 - Clicking on an attachment or a URL
 - File sharing downloads (e.g., pirated software from peer-to-peer services like BitTorrent)
- Infected removable media
 - Initially floppies & CDs, then USB media
- Direct attack to system services

Zero-day exploits

Take advantage of **zero-day vulnerabilities** to break into a system or elevate privileges.
Bugs that have been discovered but not reported & not patched.

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

9

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

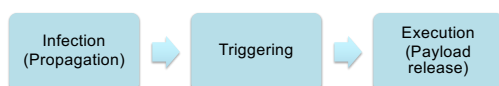
March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

10

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



March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

11

Worms vs. Viruses

- Conceptually similar
 - Software that replicates itself onto other systems
 - May be spread automatically (via network access) or manually (e.g., email attachments, flash drives)
 - Key distinction is whether they are standalone
- **Worm**
 - Standalone software
- **Virus**
 - Requires a host program: a virus attaches itself to another piece of software

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

12

Infected flash drives

- People share flash drives the way they used to share floppies
- Old Windows systems (there are still lots of them deployed)
 - Exploit AutoRun feature of Microsoft Windows
 - **autorun.inf**, originally created for CD-ROM drives
 - Automatically runs a program on the drive when the drive is detected
- **The 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

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 13

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 of sharing documents

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 14

Social engineering helps a lot

Dominant form of transporting malware


- Early examples
 - 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

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 15

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



March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 16


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

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 17

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)

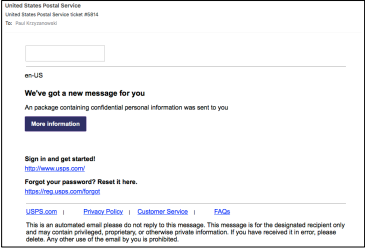


http://bgr.com/2017/01/17/gmail-phishing-attack-attachment-address-bar/

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 18

Deception

A package from the postal service ...
"containing confidential personal information"



United States Postal Service
United States Postal Service Issue #0414
To: Paul Krzyzanowski

en-US

We've got a new message for you
An package containing confidential personal information was sent to you

[More information](#)

Sign in and get started!
<http://www.usps.com>

Forgot your password? Reset it here.
<https://req.usps.com/forgot>


[USPS.com](#) | [Privacy Policy](#) | [Customer Service](#) | [FAQs](#)

This is an automated email please do not reply to this message. This message is for the designated recipient only and may contain privileged, proprietary, or otherwise private information. If you have received it in error, please delete. Any other use of the email by you is prohibited.

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 19

Deception

Weird URLs – I'd expect usps.com



United States Postal Service
United States Postal Service Issue #0414
To: Paul Krzyzanowski

en-US

We've got a new message for you
An package containing confidential personal information was sent to you

[More information](#)

Sign in and get started!
<http://www.usps.com>

Forgot your password? Reset it here.
<https://req.usps.com/forgot>

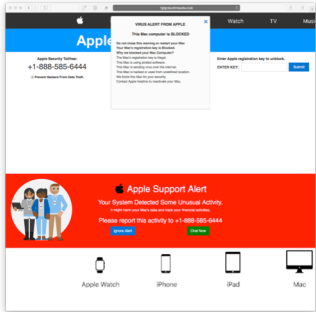
[USPS.com](#) | [Privacy Policy](#) | [Customer Service](#) | [FAQs](#)

This is an automated email please do not reply to this message. This message is for the designated recipient only and may contain privileged, proprietary, or otherwise private information. If you have received it in error, please delete. Any other use of the email by you is prohibited.

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 20

Deception

When I click on the link, I get



Apple Security System
+1-888-585-6444
Apple Security System

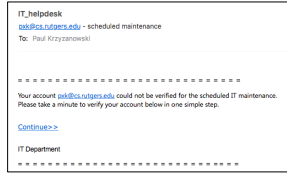
Apple Support Alert
Your System Detected Some Unusual Activity.
Right now you may not even be using your system.
Please report this activity to us at 1-888-585-6444

Apple Watch iPhone iPad Mac

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 21

Deception

Uh oh! Something's wrong with my Rutgers account??



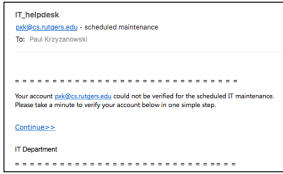
IT_helpdesk
it_helpdesk@cs.rutgers.edu - scheduled maintenance
To: Paul Krzyzanowski

Your account it_helpdesk@cs.rutgers.edu could not be verified for the scheduled IT maintenance. Please take a minute to verify your account below in one simple step.
[Continue >>](#)
IT Department

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 22

Deception

Uh oh! Something's wrong with my Rutgers account??



IT_helpdesk
it_helpdesk@cs.rutgers.edu - scheduled maintenance
To: Paul Krzyzanowski

Your account it_helpdesk@cs.rutgers.edu could not be verified for the scheduled IT maintenance. Please take a minute to verify your account below in one simple step.
[Continue >>](#)
IT Department

But why is this link taking me to <https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.iglemdv.com%2F031MWCS3D%2Findex&data=...>

protection.outlook.com is a URL rewrite by Microsoft Office 365 and takes you to Microsoft's Threat Protection service, which checks the requested URL

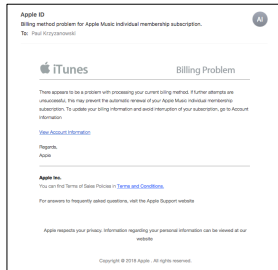
But why is Rutgers trying to send me to iglemdv.com, which is registered in Argentina?

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 23

Deception

Uh oh! A billing problem with my iTunes account

But I don't even subscribe to Apple Music!



Apple ID
Billing method problem for Apple Music individual membership subscription.
To: Paul Krzyzanowski

iTunes Billing Problem

There appears to be a problem with processing your current billing method. Further details are unavailable. We may prevent the automatic renewal of your Apple Music individual membership subscription. To update your billing information and avoid suspension of your subscription, go to Account Information.

[View Account Information](#)

Reports:
Apple

Apple Inc.
This is in the Terms of Sale Privacy & Terms and Conditions.
For answers to frequently asked questions, visit the Apple Support website.

Apple respects your privacy. Information regarding your personal information can be viewed at our website.

Copyright © 2018 Apple. All rights reserved.

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 24

Deception

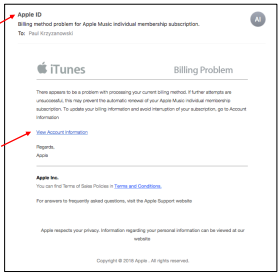
Uh oh! A billing problem with my iTunes account

But the return address is vormweg@t-online.de

vormweg@t-online.de sounds German
T-online is Deutsche Telekom

But "View Account Information" is a link to https://novoleather.com.tr/libraries/joomla/...

Huh?



March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 25

Deception

Mail clients try show a clean interface so they hide most mail headers

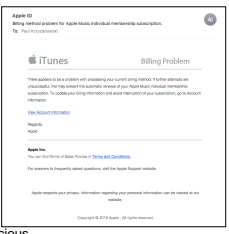
Fair enough: there are 71 lines of headers

If we look through them we see:

```
Return-path: <vormweg@t-online.de>
Received: from mailout07.t-online.de [mailout07.t-online.de [194.25.134.83]]
by st11p00m-smtpin012.me.com ...
Received: from fwd12.aui.t-online.de [fwd12.aui.t-online.de [172.20.26.241]]
by mailout07.t-online.de (Postfix) with SMTP id A510442D0CE3...
Received: from WIN-HDR00258J4
[EXJhzz2eg ... 399RFV6EzntTEwa+J5gJtA@89.43.30.27]]
by fwd12.t-online.de with (TLSV1,DES-CBC3-SHA encrypted)
esmtp id 1efGxq0LcoT0; Sat, 27 Jan 2018 04:15:34 +0100
From: Apple ID <vormweg@t-online.de>
```

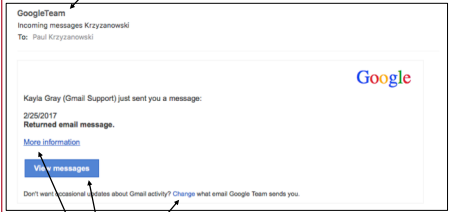
Mail headers can be forged but they give us some opportunities to do basic forensics ... or at least set off alarms that there's something suspicious.

The first IP address we see is 89.43.30.27.
That's provided by the ISP Netinternet Bilisim Teknolojileri AS in Turkey
Why is Apple sending me a message from Turkey, relaying it through Deutsche Telekom mail relays, and sending it back to Apple?



March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 26

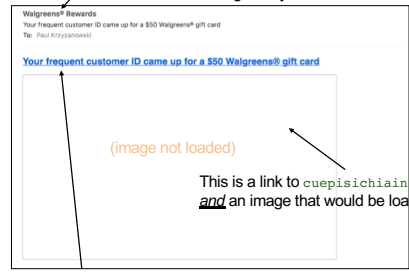
From: GoogleTeam <csalans@salans.com>
But it came from 107.170.47.71, which is lemp.frosticsatellite.com.



These are links to playground.omg-bg.com/. . . , not Google!

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 27

From: Removal.walglmco27890@cuepisichaiin.w220.luamev.top
But came from 46.3.221.220,
which belongs to Vyacheslav S. Bashin of Moscow

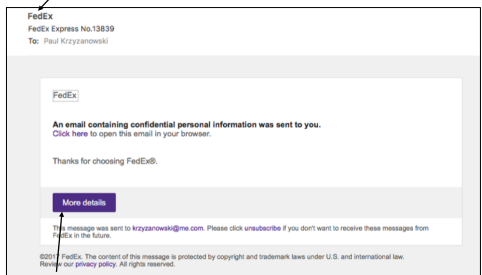


This is a link to cuepisichaiin.w220.luamev.top/... and an image that would be loaded from the site

This is a link to cuepisichaiin.w220.luamev.top/...

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 28

From: FedEx <detacher@net4webmail.com>
But came from detacher@net4webmail.com



This is a link to www.ethoscontabilidad.net.br/...

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 29

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
 - Repopulated 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

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 30

Residence

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

31

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
- Difficult with systems where users have restricted permissions or where the OS validates the digital signature of software and system files

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

32

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!

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

33



March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

34

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 $*
```

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

35

Trojan Horses

- What they might do
 - Add backdoors
 - Enable remote camera access
 - Run key loggers
 - Run web clickers
 - Enable proxy services (allow your machine to help anonymize connections)
 - Run spam engines – enable the sending of spam
 - Run DDoS engines – be part of a botnet running a DDoS attack
- How do you get people to install them?
 - Lure the user to think it's useful software – *hacker tools, anti-virus tools*

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

36

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

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

37

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 28, 2019

CS 419 © 2019 Paul Krzyzanowski

38

Source repositories

- 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>

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

39

Source repositories

- June 28, 2018

Gentoo repository at GitHub hacked

Hackers gained access to the GitHub repositories and tampered the source code of Gentoo by introducing a malicious script to delete all of your files.

- July 31, 2018

Homebrew's GitHub repository hacked

Eric Holmes, a security researcher gained access to Homebrew's GitHub repo easily. Homebrew is a free and open-source software package management system with well-known packages like node, git, and many more. It simplifies the installation of software on macOS.

- Sept 4, 2018

Almost 400k websites risk hacking, data theft via open .git repos

Smitka recently scanned 230 million "interesting" sites across the globe over one month and found 390,000 web pages with an open .git directory.

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

40

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
 - Perform kernel-level modifications to hide the presence of files or processes
- 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

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

41

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

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

42

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

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

43

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.

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

44

"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**.

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

45

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

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

46

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

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

47

File-less malware

- People are wary of unexpected email with attachments
- Anti-malware software catches a lot of malware via file scanning
- Fileless malware
 - Goal: escape detection by anti-virus software
 - Often leverage zero-day exploits for privilege escalation
 - Malware code resides in RAM or Windows registry
 - Registry entries can help restart scripts after a system has been restarted
 - Propagates through scripts (e.g., Windows PowerShell)
- Still not common ... but its use is increasing

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

48

Function

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 49

Spyware

- Type of malware that monitors some activity
 - Browsing history
 - Messages sent/received
 - Files accessed
 - Keyboard activity
 - Camera/microphone access

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 50

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?

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 51


Ransomware

- Denial-of-service malware that
 - Encrypts victim's data
 - Or even encrypts 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
- McAfee 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

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 52

Ransomware

- Ransomware is directly lucrative
 - Cryptocurrency made it hugely popular
 - Anonymous payments

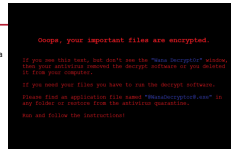


<https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/>

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 53

WannaCry ransomware

- Spread rapidly through Windows computers in May 2017
 - Spread to 74 countries within days – initial target may have been Russia
 - Estimated to have infected 200,000 computers across 150 countries
 - Hit some high-profile systems, such as Britain's National Health Service
- What does it do?
 - Encrypts files
 - Demands ransom payment in bitcoin
 - \$300 in bitcoin to unlock files
 - Price doubles after three days
 - Permanently deleted if ransom not paid in one week
- How did it propagate?
 - Exploited Windows vulnerability in the SMB (Server Message Block) protocol
 - Vulnerability allows use of specially-crafted messages to do remote code execution
 - Vulnerability discovered by the NSA, but not reported – kept as part of a cyber arsenal
 - Exploit was stolen by hackers called the Shadow Brokers
 - Shadow Brokers released it in a Medium.com post on April 8 2017
 - Microsoft issued a patch two months before the attacks but
- What's in it?
 - Comes as a "dropper" – self-contained program that extracts other components within it:
 - Encryption/decryption app
 - Files with encryption keys
 - Copy of Tor (anonymous web access)
 - Configuration files
- Speculated that it may have originated in North Korea ... but we don't really know



March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 54


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*
- Sendmail
 - 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*

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 55

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**



March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 56

Military malware

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

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 57

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

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 58

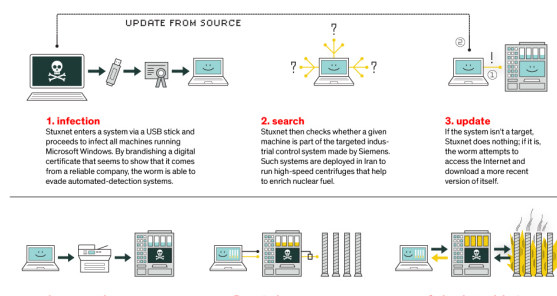
Ramifications

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

March 28, 2019 CS 419 © 2019 Paul Krzyzanowski 59

<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 transcribing 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.

Stuxnet: Zero-day exploit

- Stuxnet also took advantage of a zero-day vulnerability
 - The rendering of shortcut icons by viewing them in Windows Explorer allowed attackers to run arbitrary code
 - Payload was launched when the target simply viewed the files

See <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568>

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

61

Defenses

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

62

File Protection

- Embedded devices & older Microsoft Windows systems
 - User processes ran with full admin powers
 - This made it incredibly easy to install malware – even kernel drivers
 - Still a problem with most embedded devices (routers, printers, ...)
- Lack of file protection makes it easier to spread viruses
 - But it can be a pain even if only your files are affected
 - Viruses can override DAC permissions
- Warning users
 - Today's systems warn users about requests for installation or elevated privileges
 - For Trojans, many users will enter their password and say "yes" – they think they want the software
- MAC permissions
 - Can stop some viruses if users cannot install or override executable files
 - But macro viruses can still be a problem

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

63

Anti-virus software

No way to recognize all possible viruses

Two main approaches

1. Signature-based
2. Behavior-based

- Signature-based systems
 - Anti-malware companies collect malware
 - Often study software in sandboxed environments to see what it tries to do
 - **Signature** = set of bytes that are considered to be unique to the malware
 - Signature scanning:
 - Presence of those bytes in a file tells us the code as malicious

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

64

Anti-virus software: Behavior-based

- Monitor process activity and stop the process if it is deemed malicious
- Sandboxing
 - Anti-virus software can run suspected code in a sandbox – or interpreted environment – and see what it tries to do
- Anomaly detection
 - Look for abnormal-looking behavior patterns

Behavior-based detection tends to have much higher false positive rates

Most AV products use signature-based detection

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

65

Defeating signatures

Viruses can defend themselves

- Encryption: encrypt most of the virus – decrypt on execution
 - Only pattern we can detect is the decryption code
- Pack the code – unpatch during execution
 - Need run-time detection or else use a signature of the packer
 - Packers compress, encrypt, or simply xor the payload with a pattern.
- Polymorphic viruses:
 - Modify the code but keep it functionally equivalent
 - Add NOPs, use equivalent instruction sequences
 - This changes the signature
 - Do this each time the code propagates

Better yet...

- Write your own malware.
- Maybe you can get away with just writing a packer.

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

66

Defeating signatures

- Detection requires scanning incoming data streams
 - But they can be encrypted
- Malware via HTTP/SMTP content
 - Admins often set up black lists for SMTP attachments and HTTP content
 - **Blacklisting** = list of disallowed content
 - E.g., people might disallow windows EXE files.
 - **Whitelisting** = list of allowed content
 - White lists are preferable it harder to manage
 - There could be a huge number of acceptable file types.
 - Similarly, black lists are dangerous since there are many formats that could transport executable files.
 - Microsoft lists 25 file formats that can be directly executable by double clicking
 - Attackers can exploit bugs in allowable content, such as PDF or Excel files

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

67

Defeating signatures

- Social engineering-based defeats
 - The attacker can pick an arbitrary format and use social engineering to ask a user to rename it.
 - Executable malware can also be embedded directly into Microsoft Office documents as an object. You then have to get users to click on it.

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

68

Removing admin rights helps a lot

Feb 25, 2017 Avecto Microsoft Vulnerabilities Report

- 530 Microsoft vulnerabilities reported in 2016
 - 94% of them could be mitigated by removing admin rights
 - 100% of vulnerabilities impacting IE and Edge could be mitigated by removing admin rights
- Breakdown
 - Windows 10 had 395 vulnerabilities
 - Window 8 & 8.1 had 265 each
 - Office was hit with 79 vulnerabilities
 - Removing admin rights would mitigate 99% of vulnerabilities in older versions
 - would remove 100% of vulnerabilities in Office 2016

Note: the analysis only covers known vulnerabilities

<http://www.computerworld.com/article/3173246/security/94-of-microsoft-vulnerabilities-can-be-easily-mitigated.html>

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

69

Solving the problem

- Access controls don't stop the problem
- Privilege escalation limiting mechanisms work better
 - Removing admin rights is great ... but user files remain at risk
 - Containment mechanisms (like containers) work well for servers
 - But not for end-user software
- Running software in a sandbox is great
 - Mobile phones rely on this
 - Often too restrictive for computers
 - You have to trust that users won't be convinced to grant the wrong access rights
- Trojans/worms that exploit human behavior are hard to prevent
 - We're dealing with human nature
 - We're used to accepting a pop-up message and entering a password
 - Better detection in browsers & mail clients helps ... but risks junking legitimate content
- Simple software – without automatically-run macros is also good
 - *vi* vs. *MS-Word* ... but isn't acceptable to a lot of users

It's still a big problem

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

70

The end

March 28, 2019

CS 419 © 2019 Paul Krzyzanowski

71