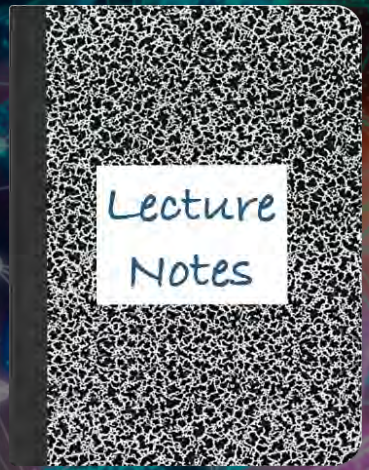
CS 419: Computer Security

Week 10: Malware & Sandboxing



Paul Krzyzanowski

© 2024 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 50 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 introduced, 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 to

'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 unclassified military computer network

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 transacton 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.

Associated Press

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

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

By ROBERT D. HERSHEY Jr.

Robert Tappan Morris Jr.'s Internet Worm

Attacked VAX computer 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	-	Ransomware	-	Adware
Rootkits	-	Backdoors	-	Wipers
Bots	-	Cryptojacking		

Motivation: Why deploy it?

For the same reasons 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**
- **Extortion - ransomware**
- **Hijacking resources – host services**
  - Botnets, cryptomining, hosting contraband services, sending spam
- **Masquerading (impersonate users/systems) – launch other attacks**

Functions

Some things malware does

Wipers & Destruction

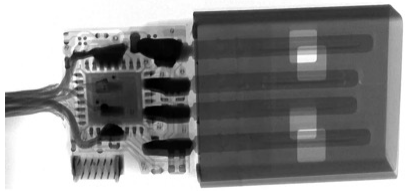
- **Destruction & denial of service**
  - Wipe data on the targeted system
  - Wipe an entire operating system
  - Flood the the network with requests to make services inoperative
  - Lock user access
  - Destroy connected devices

Exfiltration, Spyware

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

Spyware: Keyloggers

- **Record everything you type (sometimes mouse movements too)**
  - Allows attackers to get login names, passwords, messages
- **Various 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**



O.MG cable x-ray
https://hak5.org/omg

This Seemingly Normal Lightning Cable Will Leak Everything You Type

A new version of the OMG Cable is a USB-C to Lightning Cable that hackers can use to steal your passwords or other data.

Joseph Cox • September 2, 2021

It looks like a Lightning cable, it works like a Lightning cable, and I can use it to connect my keyboard to my Mac. But it is actually a malicious cable that can record everything I type, including passwords, and wirelessly send that data to a hacker who could be more than a mile away.

This is the new version of a series of penetration testing tools made by the security researcher known as MG. MG previously demoed an earlier version of the cables for Motherboard at the DEF CON hacking conference in 2019. Shortly after that, MG said he had successfully moved the cables into mass production, and cybersecurity vendor Hak5 started selling the cables.

…

The OMG Cables, as they're called, work by creating a Wi-Fi hotspot itself that a hacker can connect to from their own device. From here, an interface in an ordinary web browser lets the hacker start recording keystrokes. The malicious implant itself takes up around half the length of the plastic shell, MG said.

MG said that the new cables now have geofencing features, where a user can trigger or block the device's payloads based on the physical location of the cable.

https://www.vice.com/en/article/k789me/omg-cables-keylogger-usbc-lightning

Bots & Botnets

- **Attackers install malware in thousands of computers**
- **Software usually sits dormant**
- **Periodically contacts a Command & Control (C&C) server**
  - Gets directions for attack
  - Often downloads additional software as needed for the attack
- **Common for Distributed Denial of Service (DDoS) attacks**
  - Also useful for cryptomining, where you want the processing power of a large # of computers

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**

Millions of PC Motherboards Were Sold With a Firmware Backdoor

WIRED

Hidden code in hundreds of models of Gigabyte motherboards invisibly and insecurely downloads programs—a feature ripe for abuse, researchers say.

Andy Greenberg • May 31, 2023

Hiding malicious programs in a computer's UEFI firmware, the deep-seated code that tells a PC how to load its operating system, has become an insidious trick in the toolkit of stealthy hackers. But when a motherboard manufacturer installs its own hidden backdoor in the firmware of millions of computers—and doesn't even put a proper lock on that hidden back entrance—they're practically doing hackers' work for them.

Researchers at firmware-focused cybersecurity company Eclypsium revealed today that they've discovered a hidden mechanism in the firmware of motherboards sold by the Taiwanese manufacturer Gigabyte, whose components are commonly used in gaming PCs and other high-performance computers. Whenever a computer with the affected Gigabyte motherboard restarts, Eclypsium found, code within the motherboard's firmware invisibly initiates an updater program that runs on the computer and in turn downloads and executes another piece of software.

…

"If you have one of these machines, you have to worry about the fact that it's basically grabbing something from the internet and running it without you being involved, and hasn't done any of this securely," says John Loucaides, who leads strategy and research at Eclypsium.

https://www.wired.com/story/gigabyte-motherboard-firmware-backdoor/

4-year campaign backdoored iPhones using possibly the most advanced exploit ever

WIRED

"Triangulation" infected dozens of iPhones belonging to employees of Moscow-based Kaspersky.

Dan Goodin • December 27, 2023

Researchers on Wednesday presented intriguing new findings surrounding an attack that over four years backdoored dozens if not thousands of iPhones, many of which belonged to employees of Moscow-based security firm Kaspersky. Chief among the discoveries: the unknown attackers were able to achieve an unprecedented level of access by exploiting a vulnerability in an undocumented hardware feature that few if anyone outside of Apple and chip suppliers such as ARM Holdings knew of.

“The exploit's sophistication and the feature's obscurity suggest the attackers had advanced technical capabilities,” Kaspersky researcher Boris Larin wrote in an email. “Our analysis hasn't revealed how they became aware of this feature, but we're exploring all possibilities, including accidental disclosure in past firmware or source code releases. They may also have stumbled upon it through hardware reverse engineering.”

…

Over a span of at least four years, Kaspersky said, the infections were delivered in iMessage texts that installed malware through a complex exploit chain without requiring the receiver to take any action.

With that, the devices were infected with full-featured spyware that, among other things, transmitted microphone recordings, photos, geolocation, and other sensitive data to attacker-controlled servers. Although infections didn’t survive a reboot, the unknown attackers kept their campaign alive simply by sending devices a new malicious iMessage text shortly after devices were restarted.

https://arstechnica.com/security/2023/12/exploit-used-in-mass-iphone-infection-campaign-targeted-secret-hardware-feature/

Stealthy New macOS Backdoor Hides on Chinese Websites

DARKREADING

Modified malware from the Khepri open source project that shares similarities with the ZuRu data stealer harvests data and drops additional payloads.

Elizabeth Montalbano • January 18, 2024

A sneaky macOS backdoor that allows attackers to remotely control infected machines has been hiding in trojanized applications for the platform that are hosted on Chinese websites. The ".fseventsd" binary bears some resemblance to known malware baddies, but adds a new layer of stealth that sets it apart.

Researchers from Jamf Threat Labs discovered the series of poisoned apps being hosted on the Chinese site macyy[.]cn; they have been modified to communicate to attacker infrastructure, though "it's highly likely they're being hosted on other application-pirating websites as well," Jaron Bradley, director at Jamf Threat, tells Dark Reading.

"These applications are being hosted on Chinese pirating websites in order to gain victims," he wrote in a blog post about the research published Jan. 18. "Once detonated, the malware will download and execute multiple payloads in the background in order to secretly compromise the victim's machine."

https://www.darkreading.com/vulnerabilities-threats/stealthy-backdoor-found-hiding-in-pirated-macos-apps

Windows 10 Security Alert: Hidden Backdoor Found By Kaspersky Researchers

Forbes

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

threat post

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

Tara Seals • September 9, 2019

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

WIRED

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/

Ransomware

- **Demands payment to re-enable access or avoid disclosure**
  - May include wipers if the ransom isn't paid
- **Variations**
  - **Crypto ransomware**
    - Denial of service malware that encrypts files or storage devices
    - Or even encrypts the Master File Table (NTFS version of inode table)
  - **Locker ransomware**
    - Denial of service malware that locks users out of their devices
  - **Extortion ransomware**
    - Exfiltrates data to a remote site and threatens to expose it
  - **Double extortion**
    - Exfiltrate data to a remote site before encrypting it
    - Threaten to disclose it if ransom isn't paid

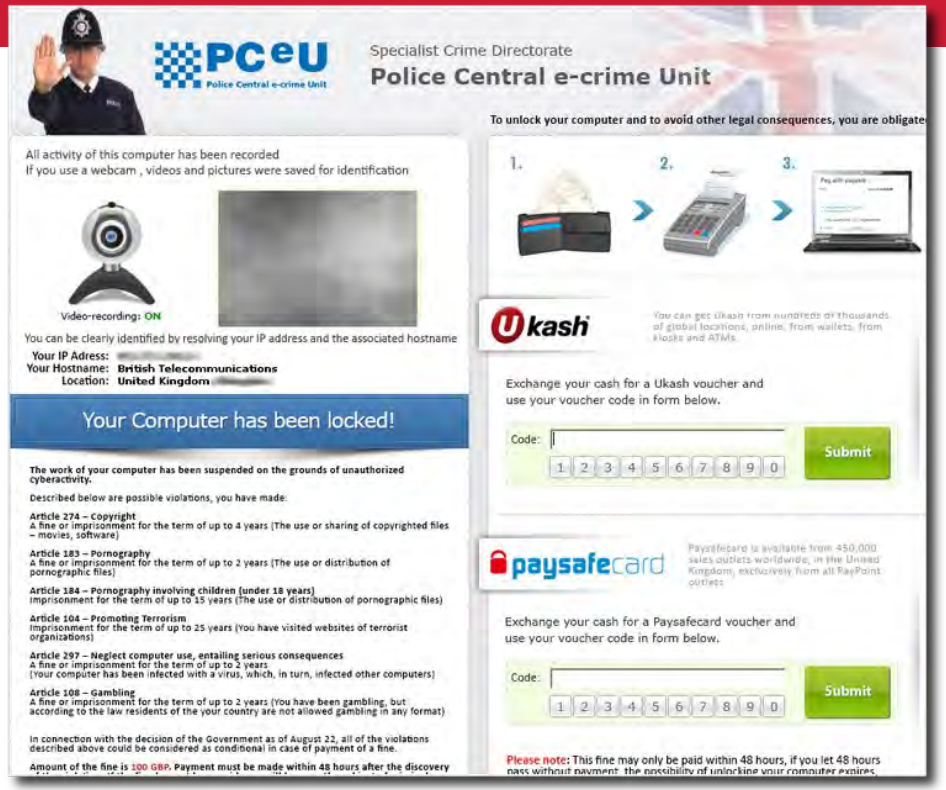
https://dataprot.net/statistics/malware-statistics/

Ransomware

Ransomware is lucrative

- Cryptocurrency made it hugely popular
- Anonymous payments

According to new data from crypto forensics startup Chainalysis, known ransomware payments almost doubled in 2023 to surpass the $1 billion mark, calling the year a “major comeback for ransomware.” That's the highest figure ever observed, and almost double the amount of known ransom payments tracked in 2022



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

https://techcrunch.com/2024/02/17/why-ransomware-makes-so-much-money/

One of the classics: WannaCry ransomware

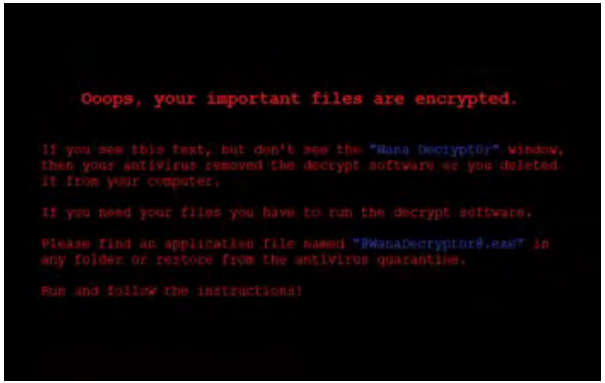
Spread rapidly through Windows computers in May 2017

- Estimated to have infected >230,000 computers across 150 countries
- Hit some high-profile systems, such as Britain's National Health Service

What did it do?

- Encrypted 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**" – a 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 know

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

Infiltration mechanisms: overview

Some ways in which malware enters a system

How does malware get onto a computer?

- **You installed it**
  - Supply chain attacks
    - You installed software from a legitimate vendor who used compromised libraries or installers
  - 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 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
  - Business processes: You were given a document or spreadsheet with malicious macros or
- **Infected removable media**
  - USB drives with malicious firmware, installers, malicious software
- **Stolen credentials**
- **Attackers exploiting vulnerabilities in software running on the computer**
  - Command injection, backdoors, Code injection, SQL injection, remote execution, or login vulnerabilities

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
- **Or launches email with malicious content**
- **Usually spread by sharing files or software or via unintentional downloads**

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

Infection (Propagation) → **Triggering (Might require a human)** → **Execution (Payload release)**

Zero-Day Vulnerabilities & Exploits

Zero-day exploits

Take advantage of **zero-day vulnerabilities** to break into a system or elevate privileges

Zero-day vulnerabilities: 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 developed patches.

Zero day = once the vulnerability is made known, developers and system administrators have zero days to produce a fix

Chinese Spies Exploited Vmware vCenter Server Vulnerability Since 2021

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

CVE-2023-34048, a vCenter Server vulnerability patched in October 2023, had been exploited as zero-day for a year and a half.

Ionut Arghire • January 22, 2024

The flaw, tracked as CVE-2023-34048 (CVSS score of 9.8), is an out-of-bounds write bug in VMware's implementation of the DCERPC protocol that could allow an attacker with network access to execute arbitrary code remotely.

VMware released patches for the vulnerability in October, noting that, due to the severity of the bug and the lack of workarounds, it had decided to make the fix available for product versions that reached end-of-life (EoL) status as well.

Last week, the virtualization technology company updated its advisory to warn that it was aware of in-the-wild exploitation of CVE-2023-34048, without providing specific information on the observed attacks.

On Friday, cybersecurity firm Mandiant, which is part of Google Cloud, revealed that the exploitation of CVE-2023-34048 likely started a year and a half ago, and that a sophisticated China-linked espionage group tracked as UNC3886 is responsible for it.

https://www.securityweek.com/chinese-spies-exploited-vmware-vcenter-server-vulnerability-since-2021/

Hackers exploited Windows 0-day for 6 months after Microsoft knew of it

ars technica

Technically, Microsoft doesn't consider such bugs vulnerabilities. It patched it anyway.

Dan Goodin • March 4, 2024

Hackers backed by the North Korean government gained a major win when Microsoft left a Windows zero-day unpatched for six months after learning it was under active exploitation.

Even after Microsoft patched the vulnerability last month, the company made no mention that the North Korean threat group Lazarus had been using the vulnerability since at least August to install a stealthy rootkit on vulnerable computers. The vulnerability provided an easy and stealthy means for malware that had already gained administrative system rights to interact with the Windows kernel. Lazarus used the vulnerability for just that. Even so, Microsoft has long said that such admin-to-kernel elevations don't represent the crossing of a security boundary, a possible explanation for the time Microsoft took to fix the vulnerability.

"When it comes to Windows security, there is a thin line between admin and kernel," Jan Vojtěšek, a researcher with security firm Avast, explained last week. "Microsoft's security servicing criteria have long asserted that '[a]dministrator-to-kernel is not a security boundary,' meaning that Microsoft reserves the right to patch admin-to-kernel vulnerabilities at its own discretion. As a result, the Windows security model does not guarantee that it will prevent an admin-level attacker from directly accessing the kernel."

https://arstechnica.com/security/2024/03/hackers-exploited-windows-0-day-for-6-months-after-microsoft-knew-of-it/

Urgent: Apple Issues Critical Updates for Actively Exploited Zero-Day Flaws

The Hacker News

March 6, 2024

Apple has released security updates to address several security flaws, including two vulnerabilities that it said have been actively exploited in the wild.

The shortcomings are listed below -

- CVE-2024-23225 - A memory corruption issue in Kernel that an attacker with arbitrary kernel read and write capability can exploit to bypass kernel memory protections.

- CVE-2024-23296 - A memory corruption issue in the RTKit real-time operating system (RTOS) that an attacker with arbitrary kernel read and write capability can exploit to bypass kernel memory protections.

…

With the latest development, Apple has addressed a total of three actively exploited zero-days in its software since the start of the year. In late January 2024, it plugged a type confusion flaw in WebKit (CVE-2024-23222) impacting iOS, iPadOS, macOS, tvOS, and Safari web browser that could result in arbitrary code execution.

https://thehackernews.com/2024/03/urgent-apple-issues-critical-updates.html

CVE-2024-21412: Water Hydra Targets Traders With Microsoft Defender SmartScreen Zero-Day

The APT group Water Hydra has been exploiting the Microsoft Defender SmartScreen vulnerability (CVE-2024-21412) in its campaigns targeting financial market traders. This vulnerability, which has now been patched by Microsoft, was discovered and disclosed by the Trend Micro Zero Day Initiative.

Peter Girnus, Aliakbar Zahravi, Simon Zuckerbraun • February 13, 2024

The Trend Micro Zero Day Initiative discovered the vulnerability CVE-2024-21412 which we track as ZDI-CAN-23100, and alerted Microsoft of a Microsoft Defender SmartScreen bypass used as part of a sophisticated zero-day attack chain by the advanced persistent threat (APT) group we track as Water Hydra (aka DarkCasino) that targeted financial market traders.

https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html

Recent Zero-Day Could Impact Up to 97,000 Microsoft Exchange Servers

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Shadowserver Foundation has identified roughly 28,000 Microsoft Exchange servers impacted by a recent zero-day.

Ionut Arghire • February 20, 2024

There are more than 28,000 internet-accessible Microsoft Exchange servers affected by a recently disclosed zero-day vulnerability, non-profit cybersecurity organization The Shadowserver Foundation warned on Monday.

Approximately 68,000 other Exchange instances are considered ‘possibly’ vulnerable, meaning that they have mitigations installed, which brings the total of potentially exploitable servers to roughly 97,000, Shadowserver says.

The vulnerability, tracked as CVE-2024-21410 (CVSS score of 9.8), is a privilege escalation flaw leading to pass-the-hash attacks, allowing an attacker to relay a user’s Net-NTLMv2 hash against a vulnerable server and authenticate as that user.

https://www.securityweek.com/recent-zero-day-could-impact-up-to-97000-microsoft-exchange-servers/

Failed Microsoft Patch Leaves All Windows Versions Open To Zero-Day Hack

Forbes

Gordon Kelly • November 29, 2021

Early this month a botched security patch left every version of Windows exposed to a zero-day hack. Now millions of Windows users need to be on high alert once more, because it has happened again.

The new vulnerability, which is already being exploited by hackers, was publicly disclosed by security researcher Abdelhamid Naceri. The vulnerability bypasses a previous flaw (CVE-2021-41379), which Microsoft believed it had successfully patched in November, and enables a hacker to elevate privileges allowing them to take over a computer and spread their attacks across the victim's network. Moreover, the new hack applies to all the latest versions of Windows, including Windows 11, Windows 10 and Windows Server 2022.

11/29 Update: in a remarkable turn of events, Naceri has now uncovered a further Windows zero-day vulnerability (CVE-2021-24084) which is also being actively exploited by hackers and it is also a result of Microsoft unsuccessfully attempting to fix the flaw in a previous patch. The vulnerability has the same outcome as well: enabling hackers to elevate privileges so they can take over a computer and spread their attacks.

https://www.forbes.com/sites/gordonkelly/2021/11/29/microsoft-windows-10-windows-11-warning-zero-day-hack-new-attack-update-windows/

Thousands of routers and cameras vulnerable to new 0-day attacks by hostile botnet

Internet scans show 7,000 devices may be vulnerable. The true number could be higher.

Dan Goodin • November 22, 2023

Miscreants are actively exploiting two new zero-day vulnerabilities to wrangle routers and video recorders into a hostile botnet used in distributed denial-of-service attacks, researchers from networking firm Akamai said Thursday.

Both of the vulnerabilities, which were previously unknown to their manufacturers and to the security research community at large, allow for the remote execution of malicious code when the affected devices use default administrative credentials, according to an Akamai post. Unknown attackers have been exploiting the zero-days to compromise the devices so they can be infected with Mirai, a potent piece of open source software that makes routers, cameras, and other types of Internet of Things devices part of a botnet that's capable of waging DDoSes of previously unimaginable sizes.

https://arstechnica.com/security/2023/11/thousands-of-routers-and-cameras-vulnerable-to-new-0-day-attacks-by-hostile-botnet/

100 million IoT devices affected by zero-day flaw

ITPro™

Vulnerability could affect car, fire detection, and patient data sensors

Rene Millman • September 24, 2021

Security researchers have uncovered a zero-day vulnerability in open source software from EMQ that could cause systems to crash and affect medical equipment.

Researchers found the flaw in NanoMQ, an MQ Telemetry Transport (MQTT) messaging engine and multi-protocol message bus for edge computing that is used for collecting real-time data from smartwatches, car sensors, fire detection sensors, and more, according to researchers at cyber security firm Guardara.

The same technology is used to monitor health parameters via sensors for patients leaving the hospital and motion detection sensors to prevent theft.

Zsolt Imre, founder and CTO of Guardana, said on GitHub the problem lies in the MQTT packet length. This messaging protocol for IoT devices is designed to be an extremely lightweight publish/subscribe messaging transport for connecting remote devices with a small code footprint and minimal network bandwidth. Imre said when the MQTT packet length is tampered with and is lower than expected, a memcpy operation receives a size value that makes the source buffer location points to or into an unallocated memory area. "As a result, nanomq crashes," he said.

https://www.itpro.com/network-internet/internet-of-things-iot/361010/100-million-iot-devices-affected-by-zero-day-flaw

Researchers wait 12 months to report vulnerability with 9.8 out of 10 severity rating

ars technica

Palo Alto Networks patches critical buffer overflow bug in its GlobalProtect VPN.

Dan Goodin • November 11, 2021

About 10,000 enterprise servers running Palo Alto Networks' GlobalProtect VPN are vulnerable to a just-patched buffer overflow bug with a severity rating of 9.8 out of a possible 10.

Security firm Randori said on Wednesday that it discovered the vulnerability 12 months ago and for most of the time since has been privately using it in its red team products, which help customers test their network defenses against real-world threats. The norm among security professionals is for researchers to privately report high-severity vulnerabilities to vendors as soon as possible rather than hoarding them in secret.

Moving laterally

CVE-2021-3064, as the vulnerability is tracked, is a buffer overflow flaw that occurs when parsing user-supplied input in a fixed-length location on the stack. A proof-of-concept exploit Randori researchers developed demonstrates the considerable damage that can result.

"Our team was able to gain a shell on the affected target, access sensitive configuration data, extract credentials, and more," researchers from Randori wrote on Wednesday. "Once an attacker has control over the firewall, they will have visibility into the internal network and can proceed to move laterally."

https://arstechnica.com/gadgets/2021/11/vpn-vulnerability-on-10k-servers-has-severity-rating-of-9-8-out-of-10/

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 removable media

- **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

- **Unprotected firmware**
  - BadUSB – available on GitHub
  - 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
- **USB Drop Attack**
  - Attackers leave malicious USB devices for people to find and plug into their computers
- **Malicious software & links**
  - Curious users may click on installers, documents, photos
- **Data leakage**
  - They're easy to lose

USB Rubber Ducky

- **USB keystroke injection device: $79.99 at shop.hak5.org**
- **DuckyScript**
  - Create commands that Rubber Ducky will enter into a target
  - Script has functions, variables, conditionals
  - Can test for machine type and execute code appropriate for that machine
- **Pseudorandom delays between keystrokes to simulate humans**

https://www.theverge.com/23308394/usb-rubber-ducky-review-hack5-defcon-duckyscript

https://shop.hak5.org/collections/best-selling/products/usb-rubber-ducky

USB Rubber Ducky for Exflitration

- **Side-channel attack**
- **Steal data from a target by transmitting it through signals that tell a keyboard when to light up CapsLock or NumLock LEDs**
- **When a CapsLock, NumLock, or ScrollLock key is pressed on one keyboard, the LED is illuminated on all attached keyboards**
  - This can be used to encode data
  - Data is gathered from a target and encoded as "lock keystrokes"
  - The USB Rubber Ducky listens for these keystrokes and records the data stream
  - At no time does the computer detect that it has a mass storage flash drive connected

See *Keystroke Reflection*: https://shop.hak5.org/pages/keystroke-reflection?ref=thestack.technology

BadUSB explained: How rogue USBs threaten your organization

CSO FROM IDG

The FBI has warned of an attack campaign that sends USB drives containing malicious software to employees. Here is what you need to know about BadUSB and mitigating its risks.

Michael Hill • January 20, 2022

In January 2022, the FBI issued a public warning over a USB attack campaign in which numerous USB drives, laced with malicious software, were sent to employees at organizations in the transportation, defense, and insurance sectors between August and November 2021. The USBs came with fake letters impersonating the Department of Health and Human Services and Amazon, sent via the U.S. Postal Service and UPS. The campaign has been dubbed "BadUSB," and the FIN7 hacker organization has been named as the culprit. Here is what you need to know about BadUSB and mitigating the risks of this USB attack.

BadUSB definition

"The BadUSB attack provides the victim with what looks like a physical USB stick and a lure to plug it into the victim's system, such as promising a gift card as a thank you or invoices that need to be processed," explains Karl Sigler, senior security research manager at Trustwave SpiderLabs. His malware research team initially discovered the campaign in 2020 while examining a malicious thumb drive as part of a forensic investigation for a U.S. hospitality provider.

"The USB drive is actually configured as a USB keyboard, and the computer will identify it and configure it as such," he tells CSO. "Once inserted, the USB keyboard will automatically start typing and will typically invoke a command shell and inject commands to download malware."

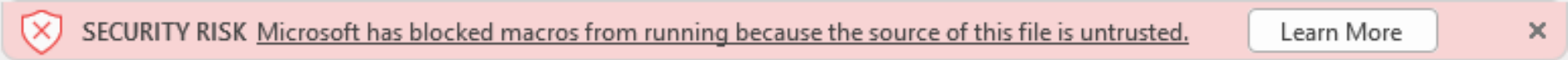
https://www.csoonline.com/article/3647173/badusb-explained-how-rogue-usbs-threaten-your-organization.html

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 protection 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
- **2022**
  - Microsoft announced that they will block macros from content downloaded from the Internet
  - CVE-2022-30190: attackers exploited MSDT, a Microsoft support tool used to allow code to run, even if macros were disabled or when the user simply opened a preview of the file



Social Engineering

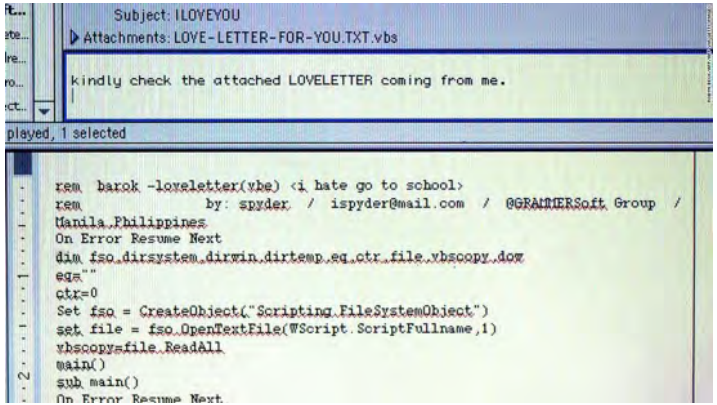
Social engineering helps a lot

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: people are driven by greed and fear**
  - 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

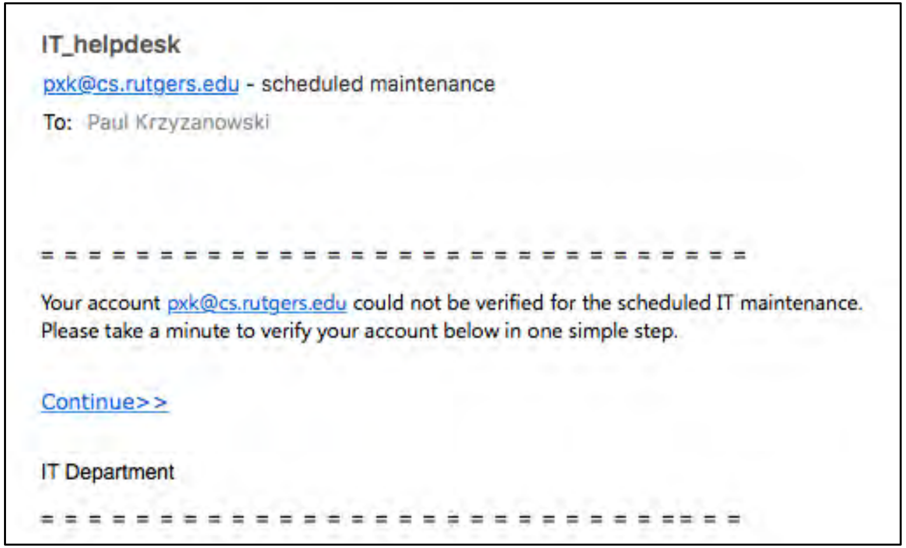
Phishing is currently the main form of cyber attacks
  - Accounts for 90% of data breaches

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=....



IT_helpdesk

pxk@cs.rutgers.edu - scheduled maintenance

To: Paul Krzyzanowski

= =

Your account pxk@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

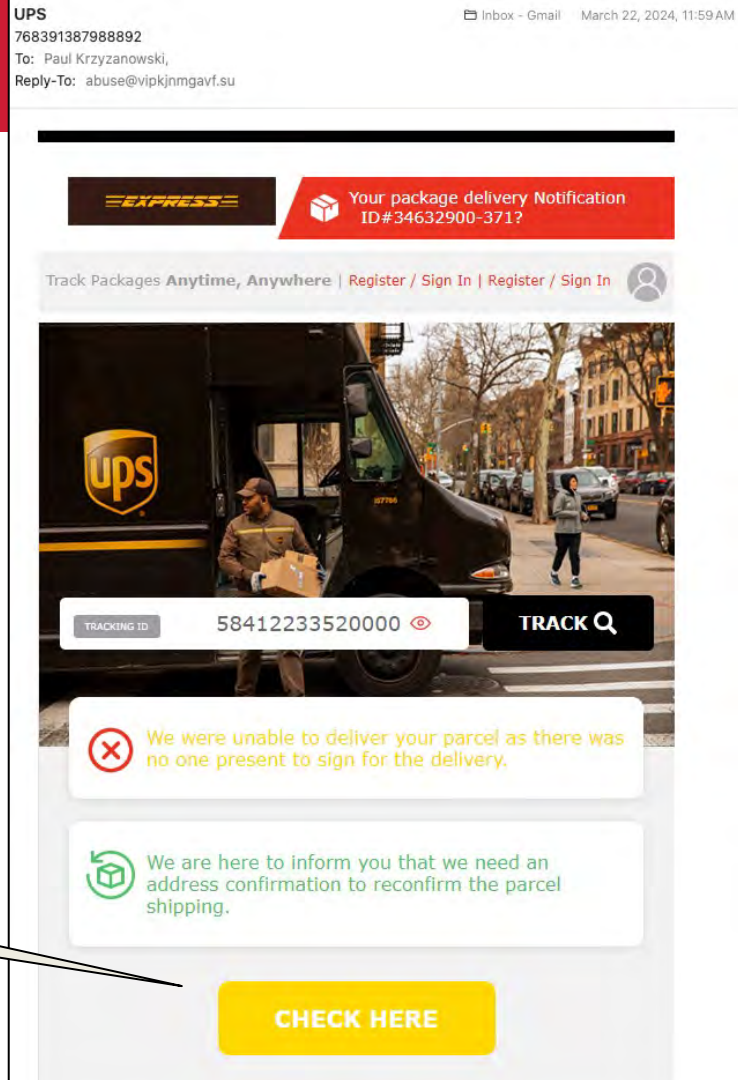
= =

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 message from UPS with a delivery error



Strange that UPS uses a Liechtenstein domain

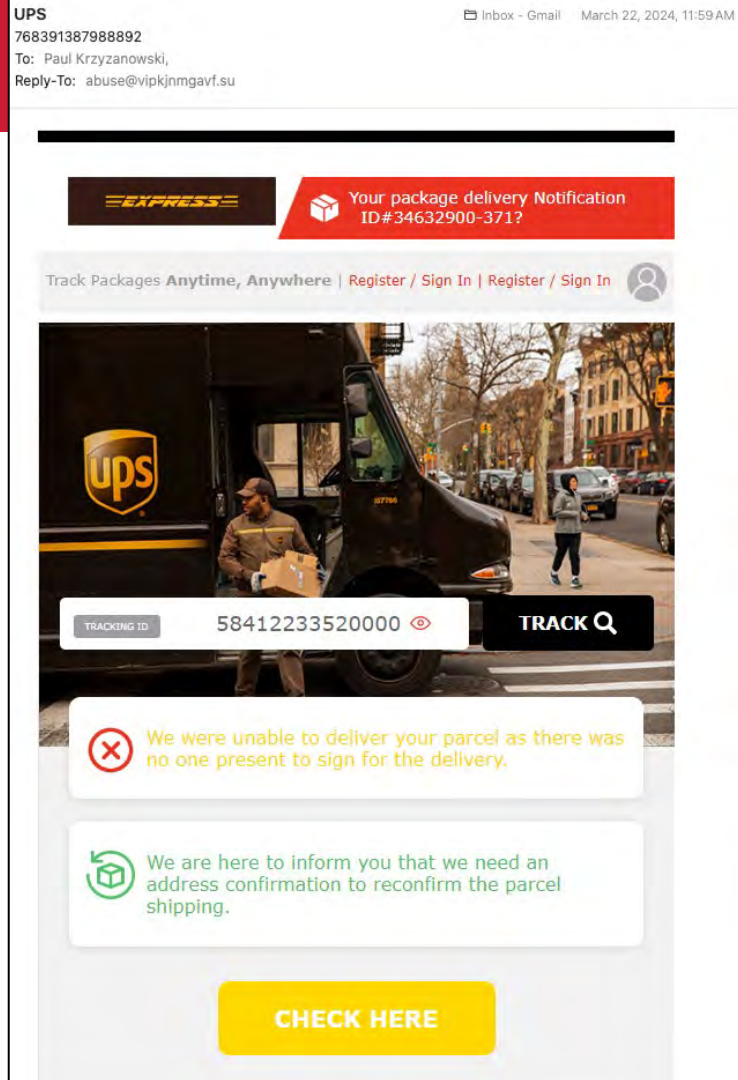
https://did.li/EUfgT#cl/653820_md/72/709148/6817/62560/1352830

CS 419 © 2024 Paul Krzyzanowski

Deception via phishing

```
Return-Path: <postmaster@rpsb.us>
Received: from armbrustusa.com (ec2-3-79-34-17.eu-central-
1.compute.amazonaws.com. [3.79.34.17])
        by smtp-relay.gmail.com with ESMTPS id js15-
20020a17090797cf00b00a4732cc6234sm30294ejc.165.2024.03.22.
08.59.00
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-
SHA256 bits=128/128);
        Fri, 22 Mar 2024 08:59:00 -0700 (PDT)
X-Relaying-Domain: rpsb.us
```

The raw headers show the message relayed through `rpsb.us`, which is the Rapides Parish School Board in Louisiana and supposedly comes from `armbrustusa.com`, which is a company that sells N95 masks



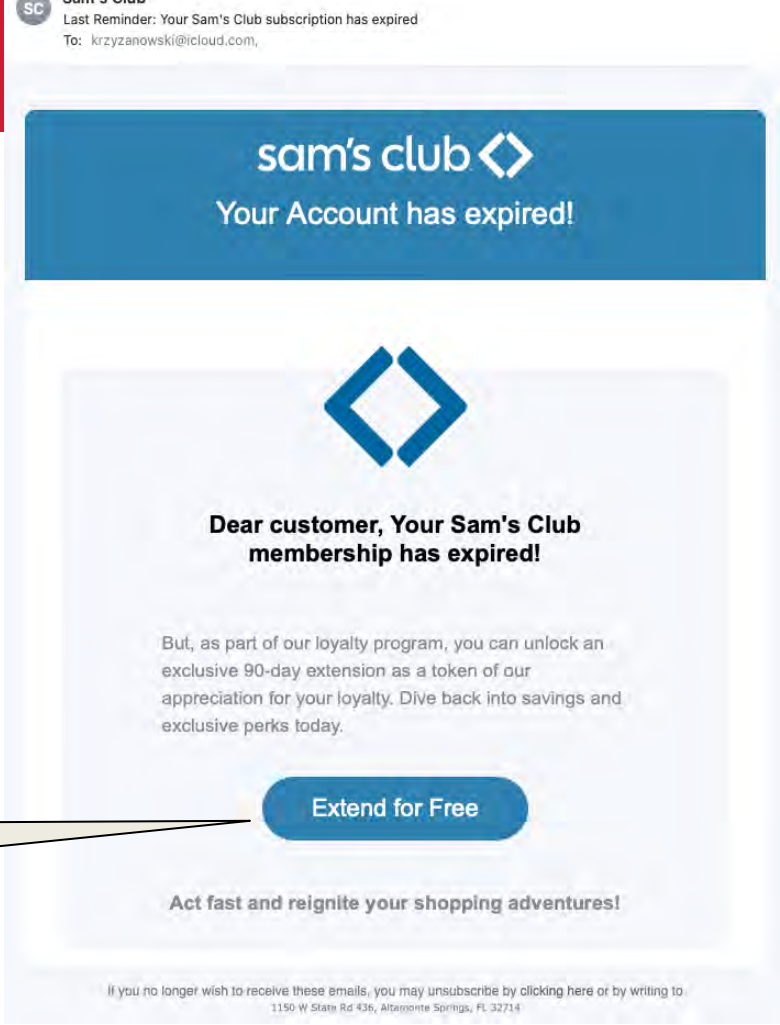
CS 419 © 2024 Paul Krzyzanowski

Deception via phishing

- **Uh oh. My Sam's Club membership expired!**
  - Let's ignore the fact that I've never had one and have never been in a Sam's Club
- **The "Extend for Free" link uses an X URL shortener, so it's not clear where it goes**
  - The site `unshorten.it` can expose it:

    `https://yonicspatula.com/0/0/0/4a...`
  - Not the `samsclub.com` I expected!

https://t.co/89YKideH...



Deception via phishing

⚠ Payout Verification ⚠

Paulkrzyzanowski

We need to confirm your info... Don't wait Claim the money You deserve! Go there now to accept what's reserved in your name.

SETTLEMENT CHECK

Pay **TWENTY-FIVE THOUZSAND AND 00 CENTS**

Check no 1944
1502677097 4589 87391512
528528732197

Issued to:
Paulkrzyzanowski
Member ID # 84840

⚠ Funds Available ⚠

$$$****25,000.00

✅ ACCEPT SETTLEMENT PAYMENT ✅

⛔ YOUR ACCOUNT INFORMATION ⛔:

Name: ✔ Paulkrzyzanowski Verify*
EMAIL: ✔ pxk@cs.rutgers.edu Verify*
Date: ✔ ⌛ Thu, 17 Feb 2022 17:15:00 -0500 (EST) Verify*
Code vérification : 79336958 Verify*

Deception via phishing

Do I trust
`https://storage.googleapis.com/barssaloon68976/html%20new.html#dVEZ.F5DHDh?f1V8xVcc2lT3cx546cdcLzcScyBy5dlB0cbb`
?

⚠ Payout Verification ⚠

Paulkrzyzanowski
We need to confirm your info... Don't wait Claim the money You deserve! Go there now to accept what's reserved in your name.

SETTLEMENT CHECK

Pay **TWENTY-FIVE THOUZSAND AND 00 CENTS**

Check no 1944
1502677097 4589 87391512
528528732197

Issued to:
Paulkrzyzanowski
Member ID # 84840

⚠ Funds Available ⚠

$$$****25,000.00

✅ ACCEPT SETTLEMENT PAYMENT ✅

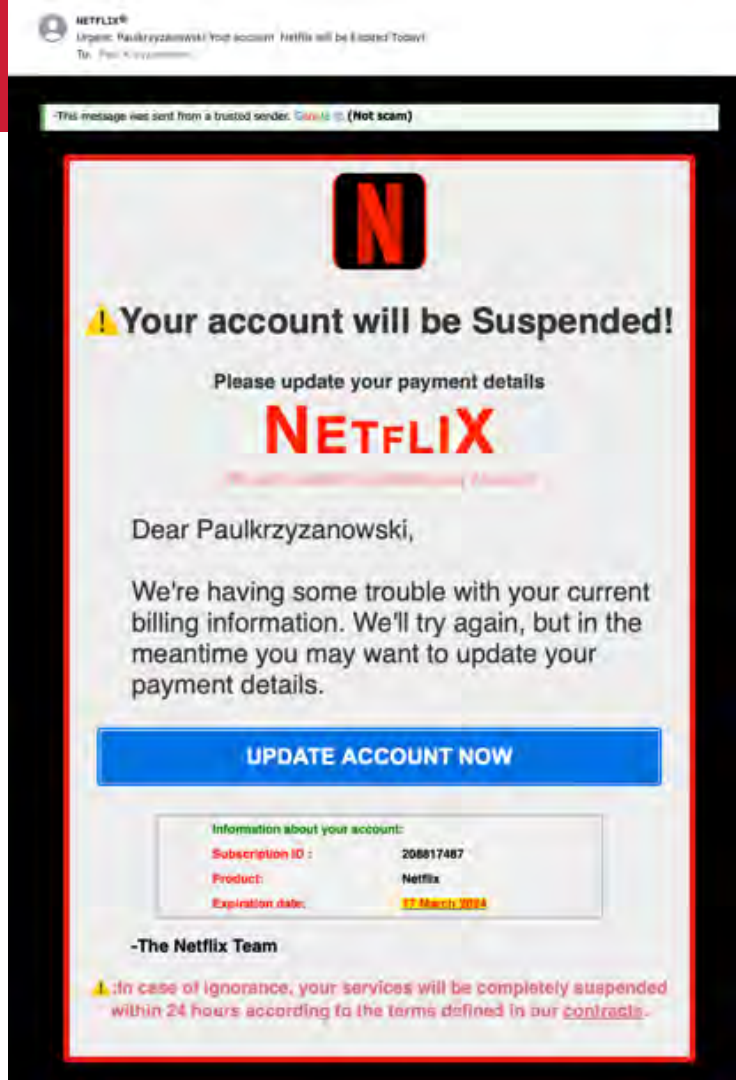
⛔ YOUR ACCOUNT INFORMATION ⛔:
Name: ✓ Paulkrzyzanowski Verify*
EMAIL: ✓ pxk@cs.rutgers.edu Verify*
Date: ✓ ⌛ Thu, 17 Feb 2022 17:15:00 -0500 (EST) Verify*
Code vérification : 79336958 Verify*

My Netflix account!

Looks legitimate – the message states:

-This message was sent from a trusted sender. Google © **(Not scam)**

- **The message comes from**
  - `NETFLIX® <nooreply@703.sqwfsjtdhob.us>`
  - Most mail readers hide the address
- **The "Update Account Now" link goes to**
  - https://storage.googleapis.com/7r664cf....
  - Malicious sites can be served from Google- or Amazon-hosted services, making them appear legitimate
- **The raw headers show:**
  - Received: from pdr8-services-05v.prod.PYY28AGM.org …



Better look into this!

My "order for Penting has been confirmed"

- I don't remember buying $599.99 of Bitcoin
- Odd that Team PayPal has a return address of
  - dawsonbarr978@gmail.com
- And the message was relayed through google APIs:

```
Received: from 407851765985 named unknown
by gmailapi.google.com with
HTTPREST; Mon, 26 Feb 2024 17:49:29 +0000
```

service@paypal.com <dawsonbarr978@gmail.com>
Invoice From Paypal 764LXX-QB-PO
To: Paul Krzyzanowski

Your order for Penting has been confirmed. We can't wait for you to receive it

PayPal

Dear paul.krzyzanowski

We have noticed an unauthorized transaction on your PayPal account with reference to an amount of **$599.99** USD, which was charged today February 26, 2024.

If you are uncertain, about this transaction then kindly get in touch with us within the next 12 hours by calling on our Helpline Number : +1(801) 853-8467 and inform us of about the transaction using the Trade-ID given below.

Upon verification , we will be able to refund the amount into your account within 6 hours from the time of reporting .

Transaction Details

Product name	Amount	Quantity	Trade ID
Bitcoin (Crypto- currency)	$599.99	0.020	764LXX-QB-PO

However ,if no response is received within this time-frame , then we shall release this transaction and it will ne reflected on your account statement soon .

If you didn't make this transaction the kindly contact our support team to cancel it or to claim your refund +1 (801) 853-8467

We understand that saving money is important and we appreciate the time we spend in keeping your PayPal account secure and safe for both sides .

Thank you for allowing us to serve you

Team PayPal

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

Masquerading links

Goal: bypass email filters

- **Use URL shorteners**
  - bit.ly, tinyurl.com, etc.
  - `bit.ly/3MxB2FR` instead of `https://www.cs.rutgers.edu/`
- **Use a different format**
  - `https://128.6.48.178` instead of `https://www.cs.rutgers.edu/`
  - Hexadecimal, octal, and decimal #s for IP addresses work too!

These are all equivalent!

```
https://www.cs.rutgers.edu
https://128.6.48.178
https://0200.06.60.0262
https://0x80.0x06.0x30.0xb2
https://0x800630b2
https://020001430262
https://2147889330
```

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

More on masquerading links

- **URL hostnames support delegating the namespace to a naming authority**
  `userinfo@hostname:port`
  - See RFC 3986 section 3.2.1.

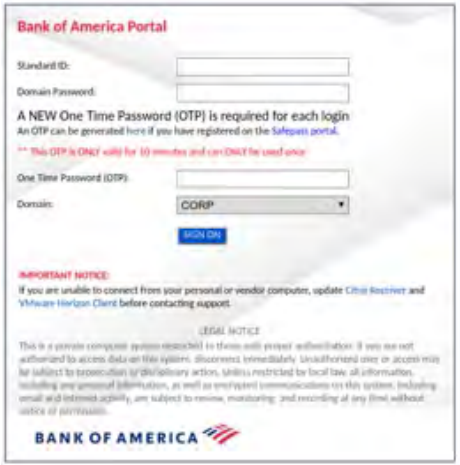
- **But the `userinfo` is almost never processed by web servers**
  - It can contain deceptive info, such as an innocent-looking domain:
    `https://microsoft.com@people.cs.rutgers.edu/~pxk/`
  - Now we can masquerade the `people.cs.rutgers.edu` part by using its IP address:
    `people.cs.rutgers.edu` ⇒ 128.6.48.158 ⇒ 0x8006309e ⇒ 2147889310
- **So instead of `https://people.cs.rutgers.edu/~pxk`, we can show**
  - https://microsoft.com@2147889310/~pxk
  - Or encode the ~pxk part too: https://microsoft.com@2147889310/%7e%70%78%6b

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 company-branded 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



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

Fake QR Codes

Deploy malicious QR codes to deceive users

- Direct them to fraudulent websites to download malware perform phishing attacks

Example:
In August 2024, fake QR codes were discovered on 150 parking meters in Redondo Beach, CA that directed users to a fraudulent PayByPhone website: `poybyphone.online`

Scam Warning: Fake QR Codes Found On Parking Meters In SoCal

Police discovered fake QR codes on about 150 parking meters that redirected people to a fraudulent website to collect payment.

Rachel Barnes, Patch Staff

Posted Mon, Aug 26, 2024 at 11:19 am PT

The Redondo Beach Police Department said the codes lead to a website called "poybyphone" that mimics the two companies officially contracted by the city — ParkMobile and PayByPhone. (Courtesy of Tim Lee)

PACIFIC PALISADES, CA — Police in Southern California warned of a new type of scam after scam QR codes were found on parking meters in a popular beach community aimed at tricking residents and visitors into submitting their payment information to scam websites for parking.

The fraudulent QR codes were found on approximately 150 meters along the Esplanade and in the Riviera Village area of Redondo Beach. Fake QR code stickers were placed adjacent to the official labels on parking meters.

https://patch.com/california/pacificpalisades/scam-warning-fake-qr-codes-found-parking-meters-socal

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 as system service**
  - Ideally, disguise the name as a legitimate service
  - Or installed because the user thought it was a legitimate program
- **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/LauchAgents
  /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!

CORONAVIRUS TROJAN OVERWRITING THE MBR

March 31, 2020

SonicWall Capture Labs Threat Research team recently found a new malware taking advantage of the CoViD19 pandemic which makes disks unusable by overwriting the MBR.

INFECTION CYCLE

Upon execution, a number of helper files are dropped inside a temporary folder:

FileName	Size	MD5
Update.vbs	156 bytes	BFBAFDF20DADF4E83476228F2F86E80C
Wallpaper.jpg	1.72 KB	087F4545E13BD7B8E1F36C941A62F8A4
Cursor.cur	13.70 KB	21F48A9E113317B8E2B3CE5366621AA1
End.exe	47.50 KB	7DEF1C942EEA4C2024164CD5B7970EC8
MainWindow.exe	148.00 KB	E6CCC960AE38768664E8CF40C74A9902
Run.exe	21.50 KB	B1349CA048B6B09F2B8224367FDA4950
Coronavirus.bat	1.63 KB	E9B2F5E9305DC2A39258D69264647C53

One of the helper files named "coronavirus.bat", which identifies itself as "coronovirus Installer" performs most of the setup work. It creates a folder named "COVID-19" where all the previously dropped helper files are moved. In order to go unnoticed, "COVID-19" folder is hidden. It further goes on to disable Windows Task Manager, User Access Control (UAC), disables options to add/modify wallpaper after changing the user's current wallpaper. It also adds entries in registry for persistence.

ars technica

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

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*

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 can contain JavaScript**
  - Most PDF attacks use JavaScript
    - E.g., establish connection to a remote server
  - PDF files can also contain malicious links, embedded malicious media
- **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

PDF remote code execution

CVE-2023-26369: Adobe Acrobat PDF Reader RCE when processing TTF fonts

- **Discovered by the Google Threat Analysis Group**
- **Bug**
  - Heap buffer out-of-bounds write when parsing a malformed TrueType font in Adobe libCoolType.
- **Exploit**
  - Use the out-of-bounds write to corrupt adjacent EScript objects previously allocated from the PDF.

https://googleprojectzero.github.io/0days-in-the-wild//0day-RCAs/2023/CVE-2023-26369.html

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

March 2021

Backdoor added to PHP source code in Git server breach

January 2022

Hackers Planted Secret Backdoor in Dozens of WordPress Plugins and Themes

March 2021

Gaming mods, cheat engines are spreading Trojan malware and planting backdoors

Malicious NPM packages are part of a malware “barrage” hitting repositories

ars technica

People trust repositories, which makes them the perfect vectors for malware.

Dan Goodin • December 8, 2021

Researchers have found another 17 malicious packages in an open source repository, as the use of such repositories to spread malware continues to flourish.

This time, the malicious code was found in NPM, where 11 million developers trade more than 1 million packages among each other. Many of the 17 malicious packages appear to have been spread by different threat actors who used varying techniques and amounts of effort to trick developers into downloading malicious wares instead of the benign ones intended.

This latest discovery continues a trend first spotted a few years ago, in which miscreants sneak information stealers, keyloggers, or other types of malware into packages available in NPM, RubyGems, PyPi, or another repository. In many cases, the malicious package has a name that’s a single letter different than a legitimate package. Often, the malicious package includes the same code and functionality as the package being impersonated and adds concealed code that carries out additional nefarious actions.

https://arstechnica.com/information-technology/2021/12/malicious-packages-sneaked-into-npm-repository-stole-discord-tokens/

GitHub besieged by millions of malicious repositories in ongoing attack

ars technica

GitHub keeps removing malware-laced repositories, but thousands remain.

Dan Goodin • February 28, 2024

GitHub is struggling to contain an ongoing attack that's flooding the site with millions of code repositories. These repositories contain obfuscated malware that steals passwords and cryptocurrency from developer devices, researchers said.

The malicious repositories are clones of legitimate ones, making them hard to distinguish to the casual eye. An unknown party has automated a process that forks legitimate repositories, meaning the source code is copied so developers can use it in an independent project that builds on the original one. The result is millions of forks with names identical to the original one that add a payload that's wrapped under seven layers of obfuscation. To make matters worse, some people, unaware of the malice of these imitators, are forking the forks, which adds to the flood.

"Most of the forked repos are quickly removed by GitHub, which identifies the automation," Matan Giladi and Gil David, researchers at security firm Apiiro, wrote Wednesday. "However, the automation detection seems to miss many repos, and the ones that were uploaded manually survive. Because the whole attack chain seems to be mostly automated on a large scale, the 1% that survive still amount to thousands of malicious repos."

https://arstechnica.com/security/2024/02/github-besieged-by-millions-of-malicious-repositories-in-ongoing-attack/

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**

Blue Pill

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

- **Attackers can deploy malware in a virtual machine**
  - It won't run security software & won't be detected by other systems
- **Example: 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 (anti-malware) 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:
  - The 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 ⇒ 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
  - Machine learning often used, trained on anomalous behavior

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

  - Whitelists 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://assets.beyondtrust.com/assets/documents/BeyondTrust-Microsoft-Vulnerabilities-Report-2021.pdf
https://assets.beyondtrust.com/assets/documents/2023-Microsoft-Vulnerability-Report_BeyondTrust.pdf

Sandboxes

Restricting what applications can do

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, ʼsan(d)-ˈbäks, *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

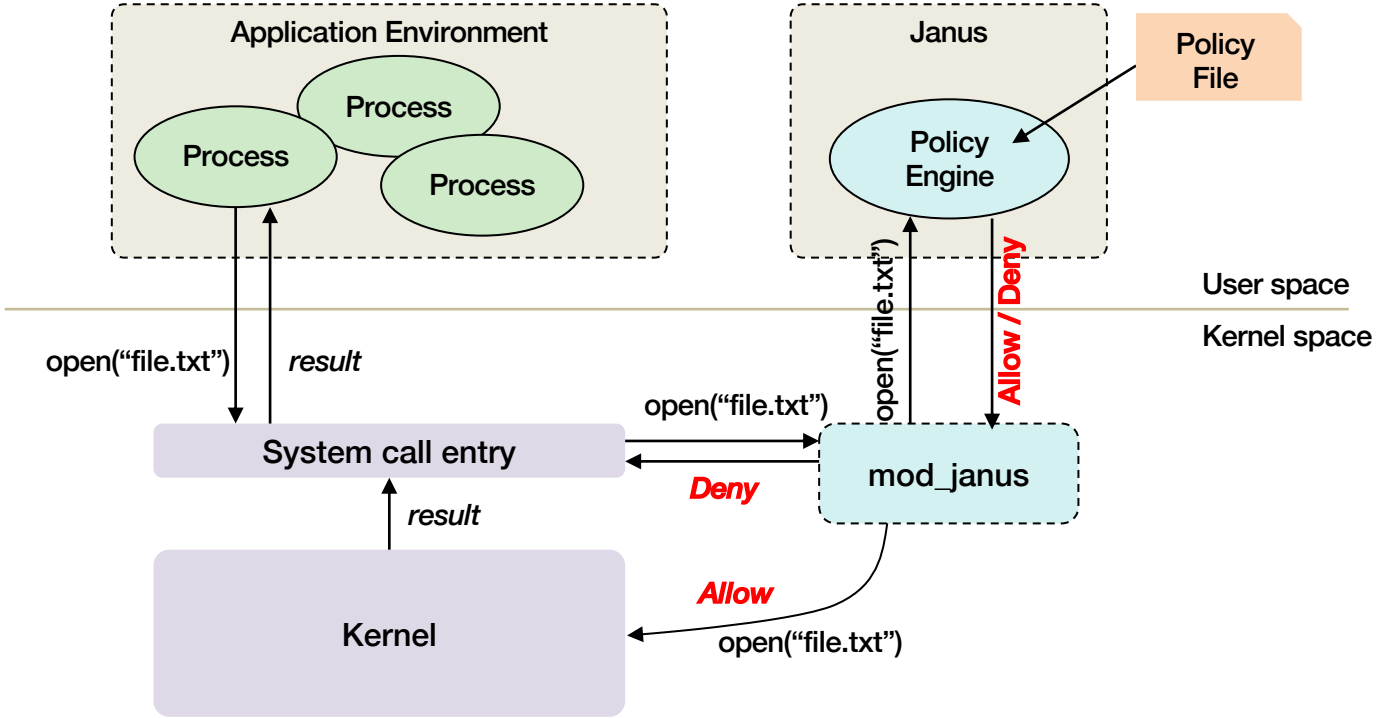
- **Sandboxing via system call interposition**
  - Intercept, inspect, and approve an app's system calls

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 must 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 and Firefox**

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

Docker containers use 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 elevated 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

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

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?

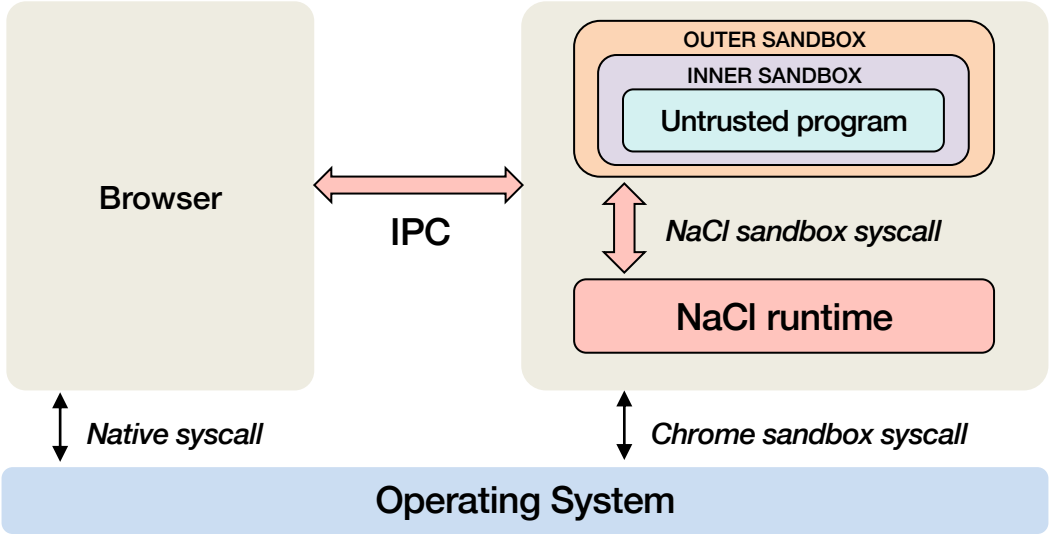
Chromium Native Client (NaCl)

- **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 exectution

The End