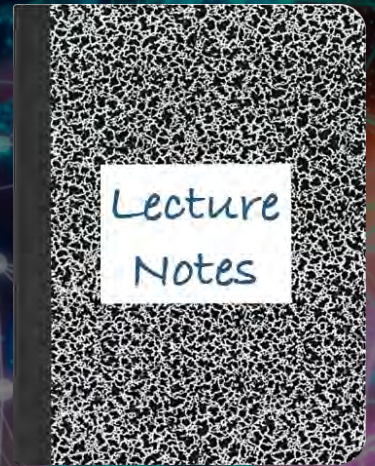


CS 419: Computer Security

# Week 9: Malware

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

56 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 unclassified network.

## 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

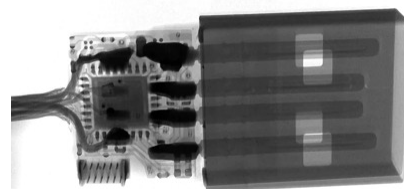


# Exfiltration, Spyware

- **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**)



**O.M.G cable x-ray**  
<https://hak5.org/omg>

## • **Hardware loggers**

# 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.

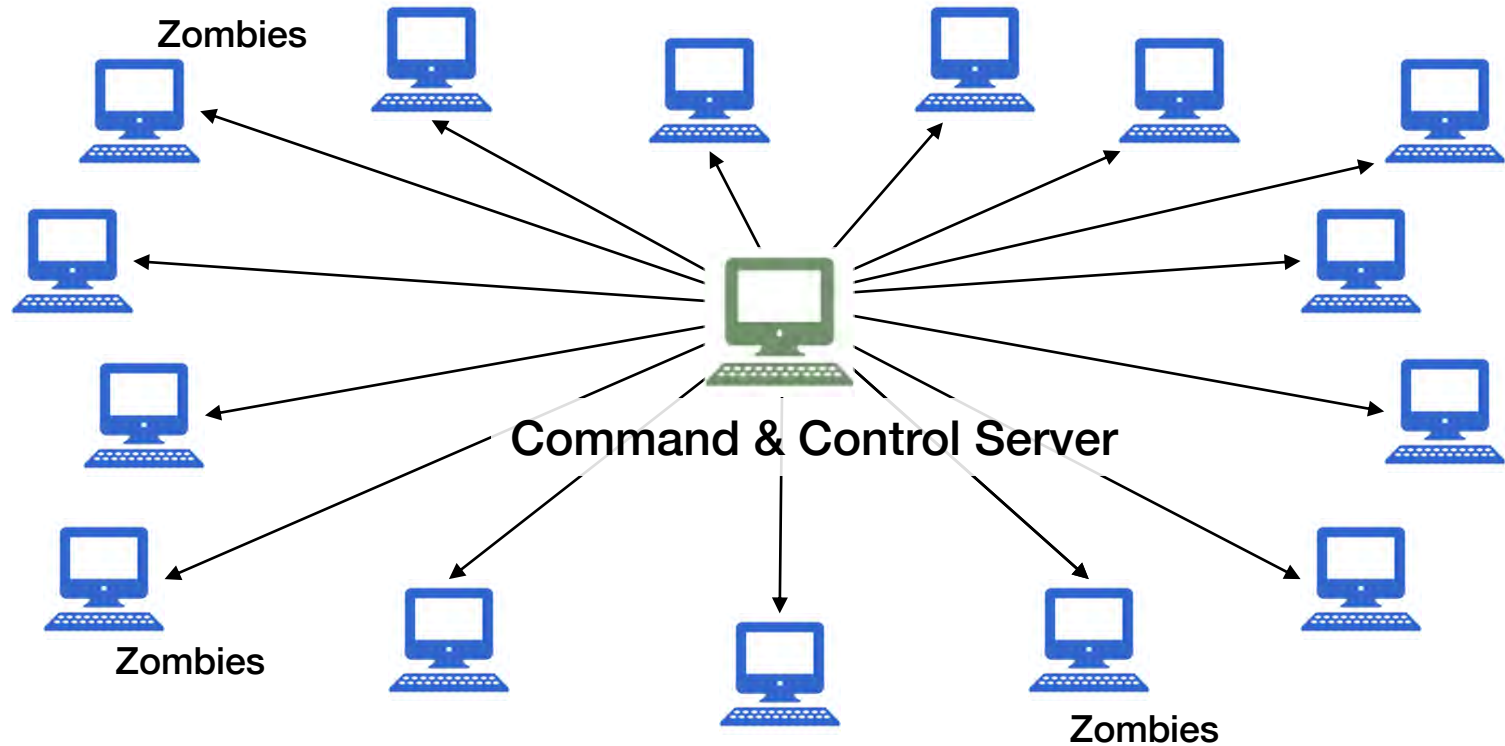
MG said that the new cables now have geofencing features, where a user can trigger or block the device's payloads based on the physical location of the cable.

<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**
  - These systems are called **zombies**
- **Zombies 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

# Bots & Botnets



# Backdoors

- **Remember Robert Morris' Internet worm?**
  - Exploited *gets* buffer overflow
  - Tried to crack passwords
  - Connect to remote hosts
  - Also used a backdoor in *sendmail*
- **Sendmail's backdoor**
  - Eric Allman, author of *sendmail*, wanted development access on a production system
  - The sys admin said, “no”
  - So he installed a password-protected backdoor in the next release
    - The backdoor was generally unprotected

# Backdoors

## Backdoor:

- Hidden mechanism to bypass normal authentication or access controls
- Backdoors in malware can provide future access to the attacked system
- Ken Thompson's modified C compiler installed a back door to *login*
- A modification to the XZ Utils compression library discovered in 2024 enabled remote command execution
- Backdoors may be built in or added later via an exploit

# Legitimate Backdoors

- **Backdoors may be installed for legitimate purposes, such as maintenance**
  - This is why the author of *sendmail* installed a backdoor
- **But attackers can discover and exploit these backdoors**
  - The Morris attack checked for the *sendmail* backdoor
  - A 2024 cyberattack on broadband providers (AT&T, Verizon, ...) provided access to information from systems the federal government uses for court-authorized network wiretapping requests





# Millions of PC Motherboards Were Sold With a Firmware Backdoor

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 Eclipsium 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, Eclipsium 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 Eclipsium.

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

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

"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 **DARK**READING Chinese Websites

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 ".fsevents" 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

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 can pay well

## Ransomware is lucrative

Cryptocurrency enabled it by making it easy to use anonymous payments

## 2024 Crypto Crime Mid-year Update Part 1: Cybercrime Climbs as Exchange Thieves and Ransomware Attackers Grow Bolder



August 15, 2024

2024 has seen the largest ransomware payment ever recorded at approximately \$75 million to the Dark Angels ransomware group.

...

The median ransom payment to the most severe ransomware strains has spiked from just under \$200,000 in early 2023 to \$1.5 million in mid-June 2024, suggesting that these strains are prioritizing targeting larger businesses and critical infrastructure providers that may be more likely to pay high ransoms due to their deep pockets and systemic importance.



# One of the classics: WannaCry ransomware

## Spread rapidly through Windows computers in May 2017

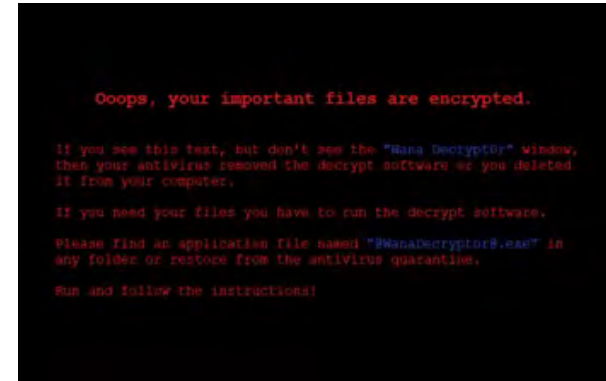
- Estimated to have infected >230,000 computers across 150 countries
- Hit some high-profile systems, such as Britain's National Health Service

## 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

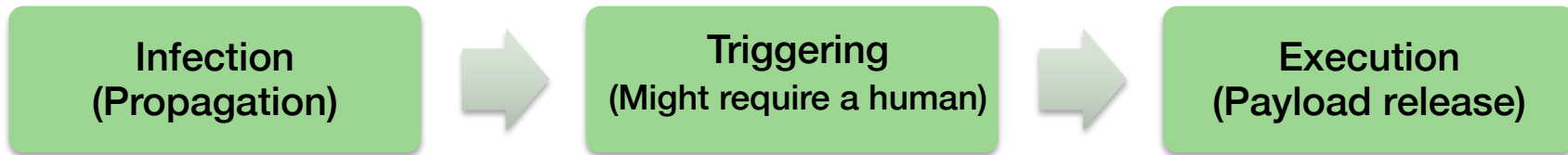
## **Dropper:**

Software that installs malware onto a system

**1-stage:** malware is in the dropper

**2-stage:** dropper downloads the malware

## Sequence of operations



## 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



## Zero-click exploits

Attack where the victim does not need to take any action, like clicking a link or opening a malicious file, for the attack to be successful.

# Chinese Spies Exploited VMware vCenter Server Vulnerability Since 2021



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

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

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](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



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

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

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 point 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



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](https://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>

# Bash Bunny: \$119.99

**Simultaneously mimic multiple trusted devices to trick targets into divulging sensitive information without triggering defenses. The Bash Bunny is truly the world's most advanced USB attack platform.**

**Compromise a locked machine, capture credentials, exfiltrate loot, plant backdoors...**



<https://shop.hak5.org/products/bash-bunny>

# USB Rubber Ducky for Exfiltration

- **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=thetack.technology>



# BadUSB explained: How rogue USBs threaten your organization

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



**SECURITY RISK** Microsoft has blocked macros from running because the source of this file is untrusted.

[Learn More](#)



# Social Engineering

# Social Engineering Attacks

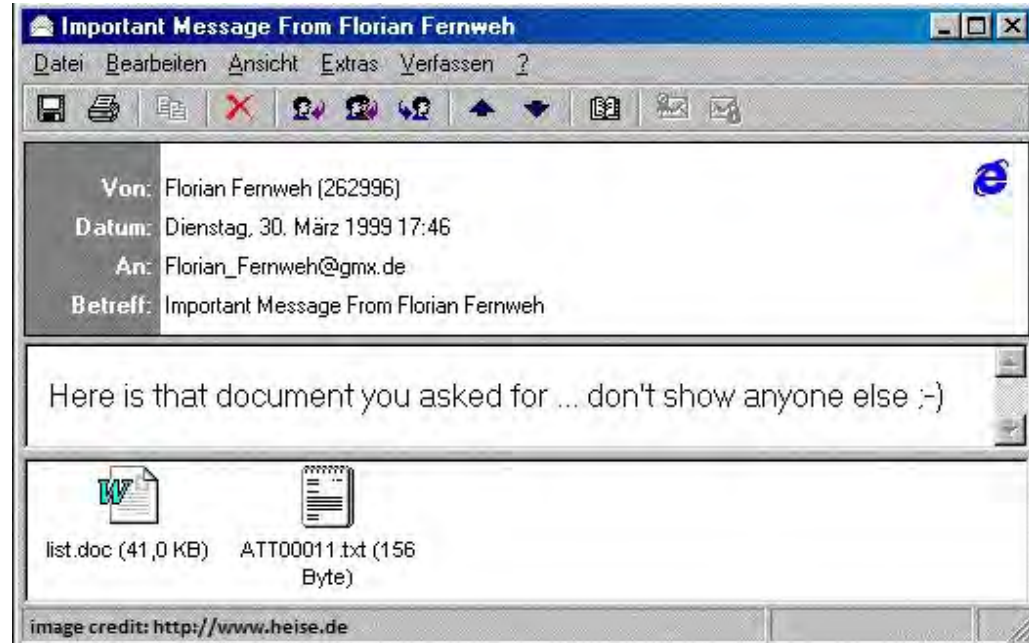
- **Social engineering:**  
*Attackers try to trick you into taking action that is against your interest*
- **It's a deception attack that may take advantage of:**
  - **Impersonation**
  - **Fear:** your account has been hacked
  - **Greed:** you have a chance to make \$, get free software (or license key generators)
  - **Confusion:** instructions to guide you to do the wrong thing, typographic errors
  - **Helpfulness/friendship/lust:** offers of friendship, helping someone with a problem
- **Creating a sense of urgency helps**
  - Your account will be suspended if you don't act now by clicking this
  - A package couldn't be delivered; it will be returned if you don't act now

# Social engineering: dominant malware delivery strategy

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
- Used IE 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 a sense of urgency 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

## Phishing is currently the main form of cyber attacks

- Accounts for 90% of data breaches

### Smishing:

Phishing attacks from text messages rather than email

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



# A note from U.S. Customs?

- Asking me to go to `usps.com-trackafn.top` ???
- With instructions on how to activate the link or copy & paste it

**Urgency**

To: +1 (474) 419-8867

iMessage  
Yesterday 12:21PM

U.S. Customs: You have a USPS parcel being cleared, due to the detection of an invalid zip code address, the parcel can not be cleared, the parcel is temporarily detained, please confirm the zip code address information in the link within 24 hours.

<https://usps.com-trackafn.top/pazz>

(Please reply with a Y, then exit the text message and open it again to activate the link, or copy the link into your Safari browser and open it)

The US Postal team wishes you a wonderful day!

# Deception via phishing

My “Prime Account Will be Removed Today”

But the link takes me to:

<https://storage.googleapis.com/loblaman996655/lobla.html#GhLNafq...>

**Urgency**

Prime®

Paulkrzyzanowski! Your Prime Account Will be Removed Today - 10/19/2024 \_\_\_\_take action! \_\_\_\_ 65240

To: Paul Krzyzanowski,

Your PRIME Membership has expired!



**Your membership has expired!**

Your Subscription for Prime  
expired **on 10/19/2024**

Dear customer, We tried to renew your subscription at the end of each billing cycle, but your monthly payment has failed. We therefore had to cancel your subscription. Obviously, we would love to see you again. If you wish to renew your subscription click on the link below

[UPDATE MY PAYMENT DETAILS](#)

Subscription ID : 44759193008243603103

Product : Prime 90 days

Expiration Date : 10/19/2024

**Confirm**

\*Available ONLY TODAY

\* After signing up, you have to insert your credit card details for validation of your account.

We will not withdraw any amount.

# Deception via phishing

I've been charged \$420.77 for a MacAfee Anti-Virus subscription???

And I have to call if I didn't authorize this payment.

**Panic**



Naeem Ali

Thanks For Your Purchase [54589748]

To: paypal408axe@mail.com



McAfee



BILL NO: 2090

Invoice No. 49745683479639

**Invoice**

**Contact US: +1(859) 809-9212**

Dear User,

We are grateful for your great assistance. This is a reminder that your "McAfee" subscription for 2 years, automatic upgrade of antivirus protection renewed on **Wed Oct 16, 2024**. Your account linked to our system will show a charge of **\$420.77** within the next 24 hours.

DESCRIPTION	QUANTITY	UNIT PRICE (\$)	AMOUNT (\$)
McAfee Anti-Virus	1	320.77	320.77
McAfee 360 Deluxe	1	100.00	100.00
Gift Items McAfee Security Lock	1	Free	Free
			<b>TOTAL (\$): 420.77</b>

Auto Renewal

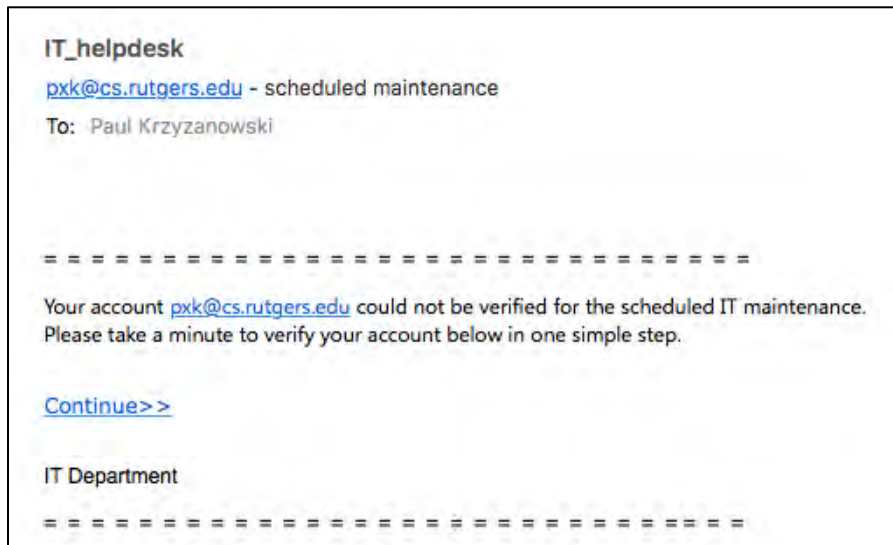
**CALL US: +1(859)809-9212**

Note: If you did not authorize this payment reach our Help Line immediately and raise a refund, you have 24 hours from the date of the transaction to open a dispute in the Resolution Centre.

# 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=...>



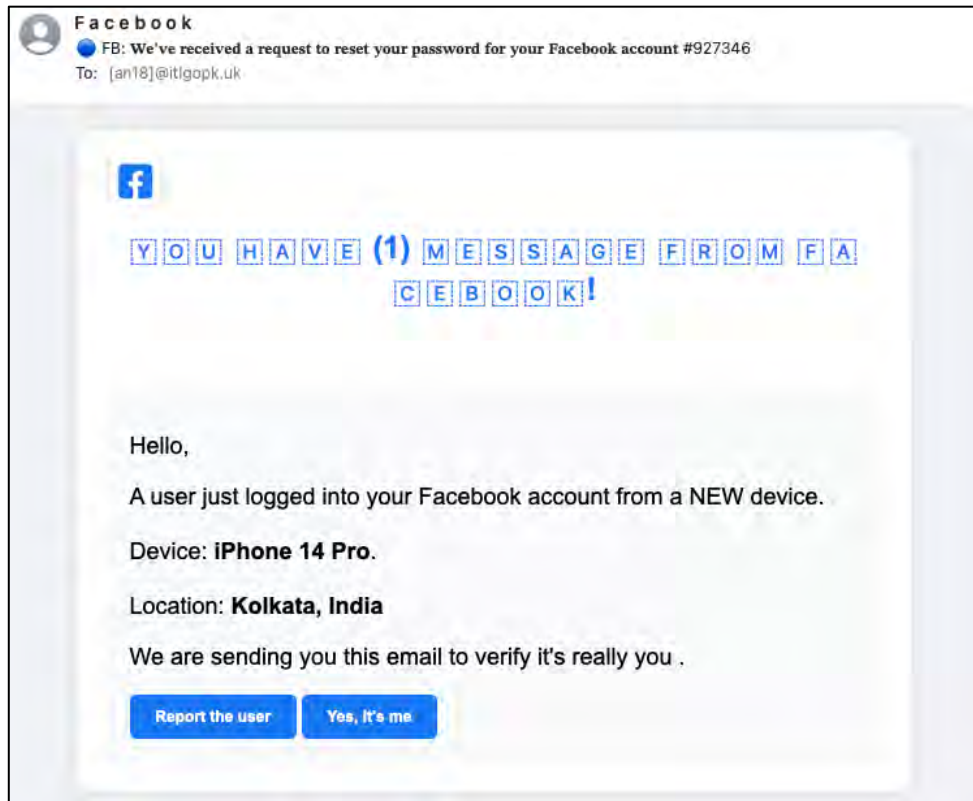
**protection.outlook.com** is a URL rewrite by Microsoft Office 365 and takes you to Microsoft's Threat Protection service, which checks the requested URL

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

# Deception via phishing

## Strange:

- The buttons are a `mailto:` link to compose a message to 219 users with a subject of *Report this user*
- No idea what they're trying to accomplish!



# Email → QR Code

The QR code is a link to

<https://www.primecargoship.com/>

- Disguised to look like a DHL shipping page asking for payment of “2.99\$”

**DHL** Payment is required

**NOW ON WHATSAPP!**  
Get your notifications via WhatsApp

From **LIGHT IN THE BOX CO.LTD**  
9555648992661

Shipment closed  
**November 10, 2024**  
20:46

Picked up In transit **Payment required**

**IMPORT DUTY/TAX PAYMENT IS REQUIRED**

Your DHL shipment with had arrived in the country and cleared customs. There is import duty/tax and an advance payment fee due on your shipment.  
The amount is: **2.99\$**

Shipment will be moved or delivered once the issue is resolved. Please continue to monitor the progress online.

Note: As of March 1, 2019, DHL no longer accepts cash or checks and all shipping payments must be made online.

**PAY NOW**



DHL Service Alert Noreply  
Shipping Confirmation: Your Package  
To: Paul Krzyzanowski

**DHL** ON DEMAND DELIVERY

**YOUR PACKAGE IS READY FOR SHIPPING FEE PAYMENT**

Dear Customer

Your package has arrived and is ready for the shipping fee payment. We prioritize security and reliable delivery service, and we are happy to assist you throughout this process. Please confirm your payment of \$2.99 by scanning the QR code below.

Note: Online payment must be completed within 24 hours to ensure prompt delivery of your shipment.

**YOUR SHIPPING INFORMATION:**

**Date:** 2024-11-04

**Waybill Number:** 9555648992661

Thank you for using On-Demand Delivery

**Express - Excellence. Simply delivered.**

2024 © JL International GmbH. All rights reserved.

# Deception via phishing

A message from UPS with a delivery error

Strange that UPS uses a Liechtenstein domain

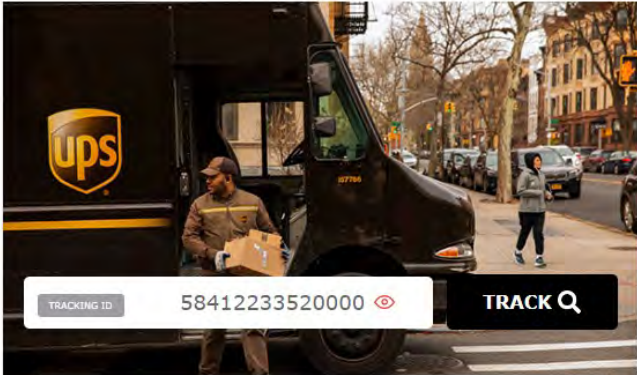
[https://did.li/EUfgT#cl/653820\\_md/72/709148/6817/62560/1352830](https://did.li/EUfgT#cl/653820_md/72/709148/6817/62560/1352830)

UPS  
768391387988892  
To: Paul Krzyzanowski,  
Reply-To: abuse@vipkjmngavf.su


Inbox - Gmail March 22, 2024, 11:59 AM


**EXPRESS** Your package delivery Notification  
ID# 34632900-371?

Track Packages Anytime, Anywhere | Register / Sign In | Register / Sign In



TRACKING ID 58412233520000 TRACK Q

 We were unable to deliver your parcel as there was no one present to sign for the delivery.

 We are here to inform you that we need an address confirmation to reconfirm the parcel shipping.

**CHECK HERE**

# 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-ECDHE-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

UPS

768391387988892

To: Paul Krzyzanowski,

Reply-To: abuse@vipkjmngavf.su

Inbox - Gmail March 22, 2024, 11:59 AM

**EXPRESS** Your package delivery Notification  
ID# 34632900-371?

Track Packages Anytime, Anywhere | Register / Sign In | Register / Sign In

ups

TRACKING ID 58412233520000 TRACK Q

We were unable to deliver your parcel as there was no one present to sign for the delivery.

We are here to inform you that we need an address confirmation to reconfirm the parcel shipping.

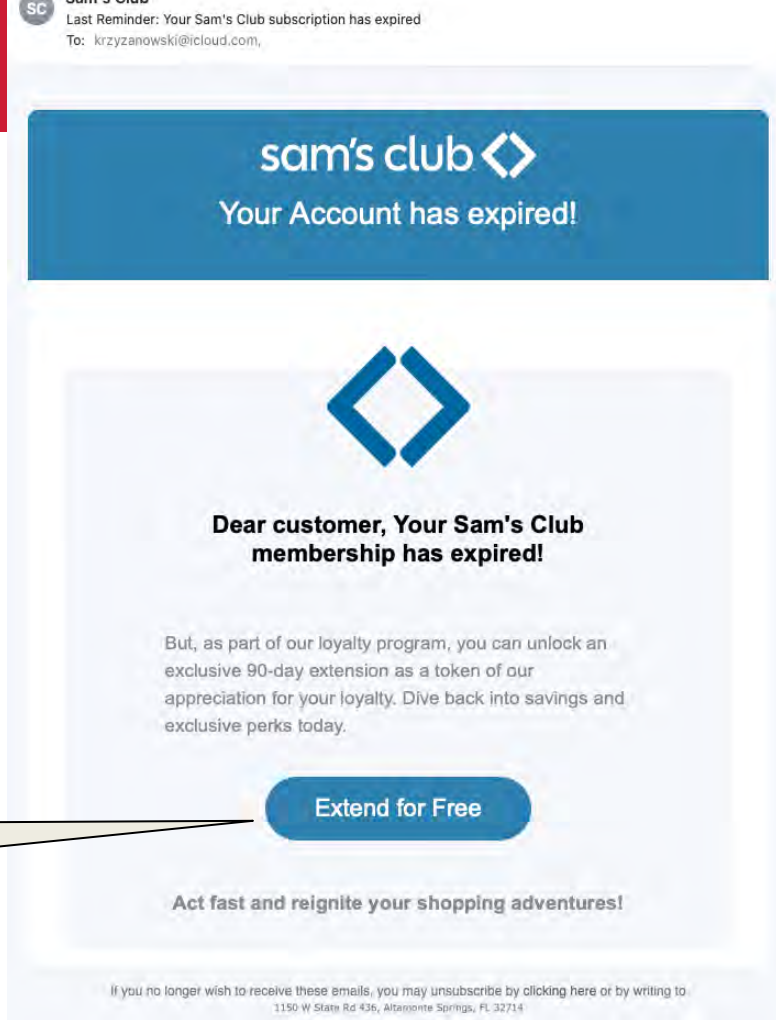
CHECK HERE



# 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](https://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

Greed

## [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 1984  
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](mailto: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`

?

Greed

## 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 1984  
1502677097 4589 87391512  
528528732197






 Issued to:  
 Paulkrzyzanowski  
 Member ID # 84840

Δ Funds Available Δ

**\$\$\$\*\*\*\*25,000.00**

 **ACCEPT SETTLEMENT PAYMENT** 

## YOUR ACCOUNT INFORMATION

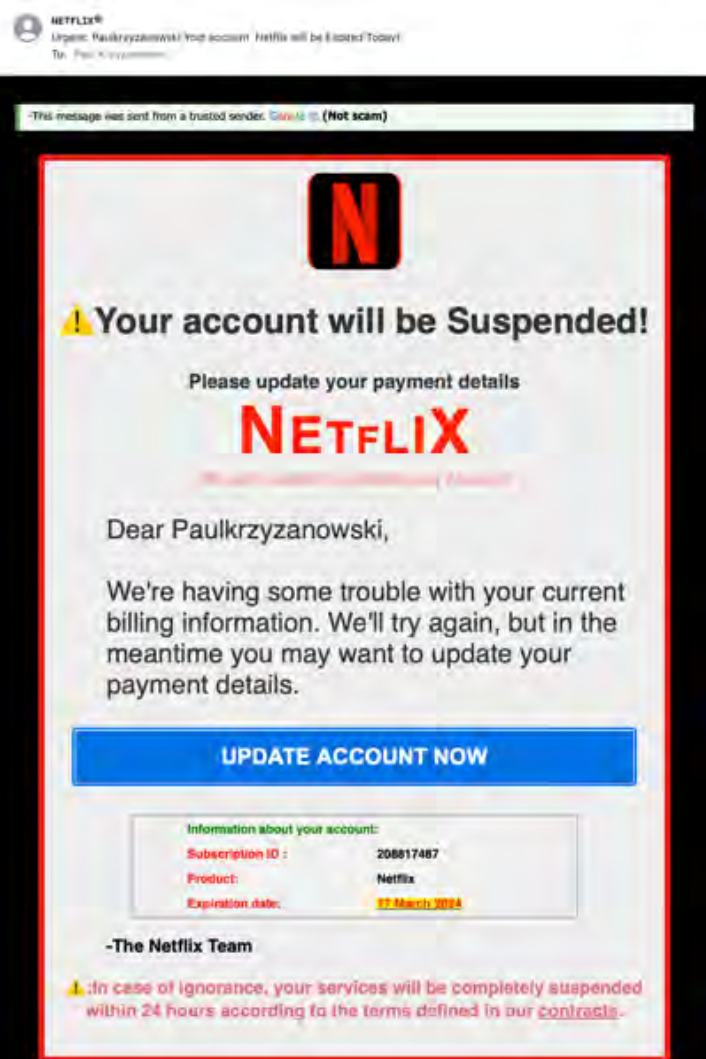
-  Name: ✓ Paulkrzyzanowski Verify\*
-  EMAIL: ✓ pxk@cs.rutgers.edu Verify\*
-  Date: ✓  Thu, 17 Feb 2022 17:15:00 -0500 (EST) Verify\*
-  Code vérification : 79336958 Verify\*

# 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
  - Unicode lookalike “Netflix” text avoids correlation
- 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](mailto: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](mailto: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



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

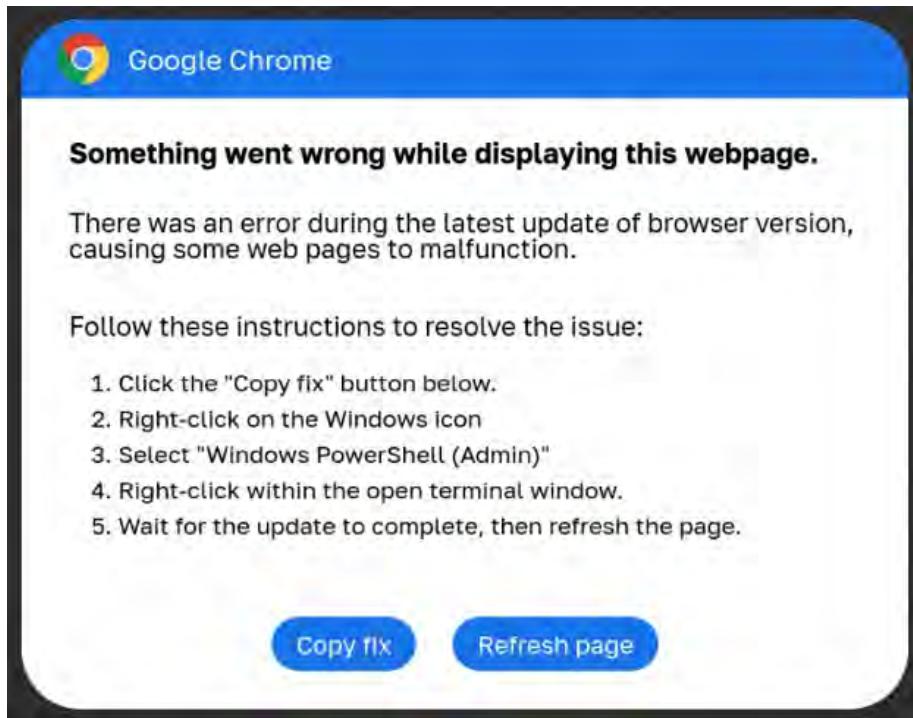
We understand that saving money is important and we appreciate the time we spend in keeping your PayPal account secure and safe for both sides .

Thank you for allowing us to serve you

Team PayPal

# Deceptive pop-ups

- Pop-up windows that look like legitimate error or update messages
- In this case, the attacker gives step by step instructions to the victim to run a PowerShell script



See <https://www.bleepingcomputer.com/news/security/fake-google-chrome-errors-trick-you-into-running-malicious-powershell-scripts/>

# Advance Fee Scheme (Nigerian Letter, 419 Fraud)

From: MA <borders@carissahillsinternationalschools.sch.ng>  
To: pxk@cs.rutgers.edu  
Subject: 6mJ / Investment Opportunity for: pxk@cs.rutgers.edu  
Date: 7 Nov 2024 06:04:10 +0100

**Greed**

Greetings.

I am looking to engage you in profit oriented ventures, I have the directive of SHK Mubarak from Qatar to look for a foreigner that is capable of managing 200,000,000 U.S.D held abroad.

If you are interested, kindly get back to me for further discussion.

Best regards,  
MA.

# Advance Fee Scheme (Nigerian Letter, 419 Fraud)

From: Sarafine Douglas <sarafinedouglas@gmail.com>

Date: Sun, 10 Nov 2024 10:05:03 +0100

Subject: Read From Sarafine Douglas.

Kindly permit me to inform you of my desire to go into a business partnership/relationship with you. I have a business proposal for you and I believe you are a reputable and trustworthy person to handle my project with your knowledge and experience.

I am Ms. Sarafine Douglas the only daughter to my late parents Late Mr. and Mrs. Donald Douglas. My father was a well-known former Oil and Gas entrepreneur before he was murdered before my presence in our home. My father told me that he had a total sum of (US\$4,500,000.00) deposited in a fixed deposit account, and my name stands as the next of Kin in deposit.

However, I have constantly received a life threat from my wicked uncle who conspired to murder my father; I have left my father's house for the security of my life. I have now decided to come over to your country in order to continue my living and to continue my study and also invest the fund in a profitable investment, Such as real estate management, hotel management, transport company or hospital equipment.

I seek your help in the following ways:

- 1) To provide a bank account which this money will be transferred to.
- 2) To serve as the custodian of this fund and investment as I continue my study.
- 3) To make arrangements for me to come to your country to continue my study.
- 4) And also help me to secure a residence permit in your country.

In addition, I am ready to reward you with 30% of the total sum once this fund has been moved into your bank account. Please also let me know your options to support me, as I believe that this transaction will be completed within a few banking days. I have already discussed my intention with the manager of the bank. I will forward you every detail once I receive your quick response.

I expect to hear from you as soon as possible.

Thanks for your humble attention and understanding towards my request.

Greetings  
Sarafine



# Email Ransom Scams

**From:** trill@preprsmadef.sbs  
**Date:** Fri, 1 Nov 2024 04:08:58 +0100  
**Subject:** You have been accepted!

**Fear**

Time is running out for you.

Good Day. This is the final warning. I hacked your computer thru the router you were connected to. A couple of months prior, I accessed the devices that you previously used to get on-line. All the info from the gadgets and devices was immediately replicated to my hosting space. I can take advantage of all your mobile device messengers, social networks, emails, chats, and contact information.

My virus constantly changes its signatures (driver type), therefore it remains not visible to antivirus applications. I reckon that at this point you fully grasp, the reason why I remained unseen until today. While getting together info with regards to you, I discovered that you're a huge fan of adult web pages & more. You really prefer to stop by porno web sites & look at kinky clips while having an orgasmic pleasure. I have already created a web cam shooting videos of you wanking off. Your face is clearly seeable.



# Email Ransom Scams



I do not believe this particular information would-be really good for your status. I can easily send this footage out to everyone who realize who you are. I additionally have no issue with rendering all your confidential information public in cyberspace. I'm sure you understand what i am talking about. It would be a true failure for you. I can mess up your way of life for a long time. I think that you seriously don't need that to take place.

Let's fix it in this way: you transfer me 1495\$ using btc equivalent at the moment of exchange) & i'll asap get rid of all your information from my machines. Afterward, we'll disregard each other. My btc transaction address for transfer:  
1E C7Kp AFfCA9w bhq6M rp vHy557Yvcz3zqH (del whitespaces if any)

In case you don't realize how to transmit money & exactly what Bitcoin is. Simply just type in the Google "purchase Bitcoin". I present you with only two days to transfer the funds. The time launched monitoring instantly once you opened this email I will see a notice when this email is open. Do not try to look for aid, as the payment address can't be traced, email the note is coming from and can not be tracked also and created automatically, therefore there isn't any reason for writing to me. Don't try to get hold of the law enforcement & some other protection solutions, if you do, your personal data will undoubtedly be revealed.

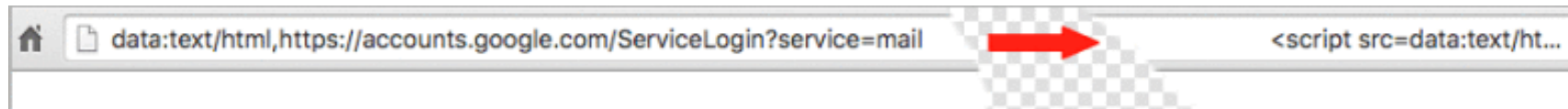
# Spear Phishing

- **Phishing:** email disguised to look like it's from a trusted sender
  - 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 legi



# 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/>

# Typosquatting

- **Use names that could be confused with legitimate names**
  - tensorflow: temsorrow, tensoflow, tencourflow, tensoflaw, tensoflw, tensoflpw, ...
- **March 28, 2024:**
  - Maintainers of the Python Package Index (PyPI) briefly suspended new user signups after an influx of malicious projects were uploaded in a typosquatting campaign
  - 566 malicious packages, including 100 packages targeting ML libraries
  - Malware steals files, discord tokens, and data from web browsers and crypto wallets
    - Attempts to download a Python script (hvnc.py) to the Windows Startup folder

**This also happened in May 2023, November 2024, December 2023**

<https://thehackernews.com/2024/03/pypi-halts-sign-ups-amid-surge-of.html>

# PyPI Halts Sign-Ups Amid Surge of Malicious Package Uploads Targeting Developers The Hacker News

March 29, 2024

The maintainers of the Python Package Index (PyPI) repository briefly suspended new user sign-ups following an influx of malicious projects uploaded as part of a typosquatting campaign.

PyPI said "new project creation and new user registration" was temporarily halted to mitigate what it said was a "malware upload campaign." The incident was resolved 10 hours later, on March 28, 2024, at 12:56 p.m. UTC.

Software supply chain security firm Checkmarx said the unidentified threat actors behind flooding the repository targeted developers with typosquatted versions of popular packages.

"This is a multi-stage attack and the malicious payload aimed to steal crypto wallets, sensitive data from browsers (cookies, extensions data, etc.), and various credentials," researchers Yehuda Gelb, Jossef Harush Kadouri, and Tzachi Zornstain said. "In addition, the malicious payload employed a persistence mechanism to survive reboots."

<https://thehackernews.com/2024/03/pypi-halts-sign-ups-amid-surge-of.html>

# 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`  $\Rightarrow$  `128.6.48.158`  $\Rightarrow$  `0x8006309e`  $\Rightarrow$  `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`

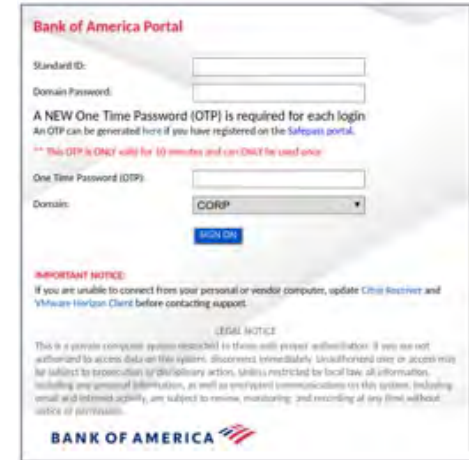


# Calendar Injection

- **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 a 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/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>

# Example: North Korean Hidden Risk Campaign

## Nov 7, 2024: North Korean hackers use new macOS malware against crypto firms

- **Lures victims with email containing fake news about cryptocurrency**
  - Disguised to look like it's forwarded by a cryptocurrency influencer
  - Link to read a PDF file with info but points to a domain controlled by the attackers
- **1<sup>st</sup> stage: dropper app – signed with a valid Apple Developer ID (now revoked)**
  - When run, downloads a decoy PDF from Google Drive
  - Opens it in the default PDF viewer to distract the victim
  - Downloads the next stage payload in the background
- **2<sup>nd</sup> stage: binary – contains backdoor**
  - Modifies `.zshenv` (zsh env file) to run the payload in each user session
  - This avoids any detection of changes to LaunchAgents
  - Connects to command-and-control server, checking for new commands every 60 seconds

<https://www.bleepingcomputer.com/news/security/north-korean-hackers-use-new-macos-malware-against-crypto-firms/>



# 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 "coronavirus 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.



# Glupteba Botnet Adds UEFI Bootkit to Cyberattack Toolbox

A malware with every malicious feature in the book is adding new pages, with a fresh ability to invade the lowest levels of a Windows machine.

Nate Nelson • February 13, 2024

The widespread, multitooled Glupteba malware has adopted a Unified Extensible Firmware Interface (UEFI) bootkit, allowing it to stealthily persist inside of Windows systems despite reboots, by manipulating the process by which the operating system is loaded.

...

Now the botnet has incorporated a new open source tool called EfiGuard, which achieves even more sophisticated, lower-level access by taking advantage of UEFI, a specification which replaced the basic input/output system (BIOS), used to connect a machine's firmware to its operating system.

In short, the bootkit contains an implant for the EFI system partition (ESP) — located in a machine's boot device and containing the Windows Boot Manager — which disables driver signature enforcement as well as PatchGuard, the Windows function that prevents changes to the kernel. It allows Glupteba to operate in this privileged space, executing its code before Windows is able to start up in the first place, making the job of detecting and removing it far more difficult for affected organizations.

<https://www.darkreading.com/threat-intelligence/glupteba-botnet-burrows-windows-systems-new-uefi-bootkit>

# 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

1. **Overt purpose:** known to a user
2. **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

It creates a setuid shell that will run their ID

They think they just ran the real **ls** command. The fake **ls** command deletes itself.

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
    - This is called a **Remote Access Trojan (RAT)**
  - 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 malicious and be embedded in web pages & PDF files**
  - Most browser security holes involve JavaScript
  - Deception via overlaying images, controlling clicks, form entry, etc.
  - **JavaScript can connect to other sites**
    - It can do things like port scans, connect to servers, download content
    - Any website you connect to can leverage your machine
- **PDF files have become the dominant file format for malware distribution**
  - Microsoft did a good job blocking macros  
(attackers usually have to rely on social engineering to ask users to disable them)
  - **PDF files can contain JavaScript**
    - Most PDF attacks use JavaScript: e.g., steal credentials, establish a connection to a remote server
    - PDF files can also contain malicious links, embedded malicious media
      - Download & run a Windows PowerShell script



# PDF remote code execution bug

## 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 place malicious code (often back doors) in popular repositories

December 2021

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

March 2021

**Backdoor added to PHP source code in Git server breach**

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

January 2022

**Hackers Planted Secret Backdoor in Dozens of WordPress Plugins and Themes**

February 2024

**Over 100,000 Infected Repos Found on GitHub**

# GitHub besieged by millions of malicious repositories in ongoing attack



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/>

# Hundreds of code libraries posted to NPM try to install malware on dev machines



These are not the the developer tools you think they are.

Dan Goodin • Nov 4, 2024

An ongoing attack is uploading hundreds of malicious packages to the open source node package manager (NPM) repository in an attempt to **infect the devices of developers who rely on code libraries there**, researchers said.

The **malicious packages have names that are similar to legitimate ones for the Puppeteer and Bignum.js code libraries and for various libraries for working with cryptocurrency**. The campaign, which was active at the time this post was going live on Ars, was reported by researchers from the security firm Phylum. The discovery comes on the heels of a similar campaign a few weeks ago targeting developers using forks of the Ethers.js library.

## Beware of the supply chain attack

“Out of necessity, malware authors have had to endeavor to find more novel ways to hide intent and to obfuscate remote servers under their control,” Phylum researchers wrote. “This is, once again, a persistent reminder that supply chain attacks are alive and well.”

<https://arstechnica.com/security/2024/11/javascript-developers-targeted-by-hundreds-of-malicious-code-libraries/>

# 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
  - Many, many more...

## The Hacker News

North Korean Hackers Deploy FudModule Rootkit via Chrome Zero-Day Exploit

Aug 31, 2024 Ravie Lakshmanan



A recently patched security flaw in Google Chrome and other Chromium web browsers was exploited as a zero-day by North Korean actors in a campaign designed to deliver the FudModule rootkit.

The development is indicative of the persistent efforts made by the nation-state adversary, which has made a habit of incorporating rafts of Windows zero-day exploits into its arsenal in recent months.

# Types of Rootkits

- **User mode**

- Replace commands
  - Replace common admin commands with ones that conceal the existence of the intruder (*ps, ls, find, top, netstat*)
- 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**

# Hyperjacking: 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

- **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

# Email Authentication: DMARC, DKIM, SPF

- **SPF (Sender Policy Framework)**
  - Allows a recipient to detect if someone is spoofing a mail host
- **DKIM (DomainKeys Identified Mail)**
  - Allows a recipient to detect if mail is from the domain & hasn't been tampered
- **DMARC**  
**(Domain-based Message Authentication, Reporting, and Conformance)**
  - Allows domain owners to specify how to handle emails that fail SPF or DKIM checks and enables receiving feedback



# SPF (Sender Policy Framework)

- Allows a recipient to detect if someone is spoofing a mail host
- Domain owners specify which IP addresses are authorized to send email on behalf of their domain
- Receiving mail servers check the SPF record in DNS to verify if the incoming email matches an authorized address

```
$ dig txt +short irs.gov|grep spf  
"v=spf1 ip4:152.216.0.0/20 ip6:2610:30::/32 -all"
```

```
$ dig txt +short usps.com|grep spf  
"v=spf1 ip4:56.0.0.0/16 -all"
```

# DKIM (DomainKeys Identified Mail)

- **Allows a recipient to detect if mail is from the domain & hasn't been tampered**
- **Sender adds a digital signature in the email headers**
  - Sender identifies which elements of the message (e.g., which headers) to include
- **Recipient's mail server can verify using a public key published in the sender's DNS**
  - The DNS field is identified in the mail header

# DKIM (DomainKeys Identified Mail)

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=nyu.edu;  
h=content-type:from:mime-version:subject:to:cc:content-type:from:  
subject:to;  
s=s1; bh=KI3sb+L2lmYRgCGwEOPJW7kyZaRA7a7DSZpeWx7csWE=;  
b=B8qurn4z9KvdkemigGbx2YmZMga404OuFWAdNr1NvC2Bqlkov47cCpH9FpWpnKKGoge  
ti1J2ND1afBox19EN9X9vqbsg2Dpo294DhSPb/KsWyV+dXTdlE9emQfcGSYPDBsJ2ZZ1Xo  
2RslZA/dvBjAMu1fURXNTnlgaQM5q+OjDuyZywI3i58kZiJVzsEJD3+4+4YOpLor+zU1i1  
ORP7wkWbc6FJqDlk54J6J6TnNQBnRvNiVi15rpL50vhnJLbIn/aWtoic2jl+z4HyRK49RG  
1pNiPnfN1zXEh5IizvGRO2RYyOJc11LJaZT0YzZSslgUT3TRPp+rooJKqMujTk1A==
```

*The s1 in the header is the selector – identifies which public key to access.*

```
$ dig txt +short s1._domainkey.nyu.edu
```

```
s1._domainkey.technolutions.net.
```

```
s1.domainkey.u511372.wl.sendgrid.net.
```

```
"k=rsa; t=s; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1CJ6+q+N264DhEGxi9 ..."
```

# DMARC (Domain-based Message Authentication, Reporting, and Conformance)

- **Allows domain owners to specify how to handle emails that fail SPF or DKIM checks and enables receiving feedback**
- **E.g., mark as spam, deliver, or drop.**

```
$ dig txt +short _dmarc.irs.gov  
"v=DMARC1; p=reject; rua=mailto:dmarc-agg-feed@ofdp.irs.gov,  
mailto:reports@dmarc.cyber.dhs.gov; ruf=mailto:dmarc-for-feed@ofdp.irs.gov; fo=1"
```

# 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 runs suspected code in a sandbox – or interpreted environment –and sees 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 but harder to manage – a form of *principle of least privilege*
    - There could be a huge number of acceptable file types.
    - Similarly, blacklists are dangerous since many formats 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: enforce the principle of least privilege**

The End