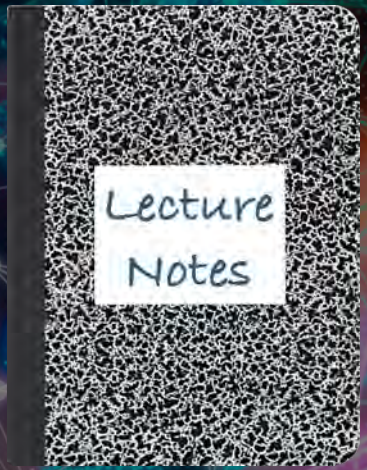
CS 419: Computer Security

Week 10: Malware – Part 2

Social Engineering & Specialized Components



Paul Krzyzanowski

Social Engineering Attacks

The Human Vulnerability

Why attack technology when you can attack people?

- **Social engineering: manipulate people into doing something that is against their best interest (e.g., breaking security procedures)**
- **Why it's effective**
  - Humans are trusting by nature; we want to be helpful
  - We're busy and make quick decisions
  - We're scared, rushed, or excited

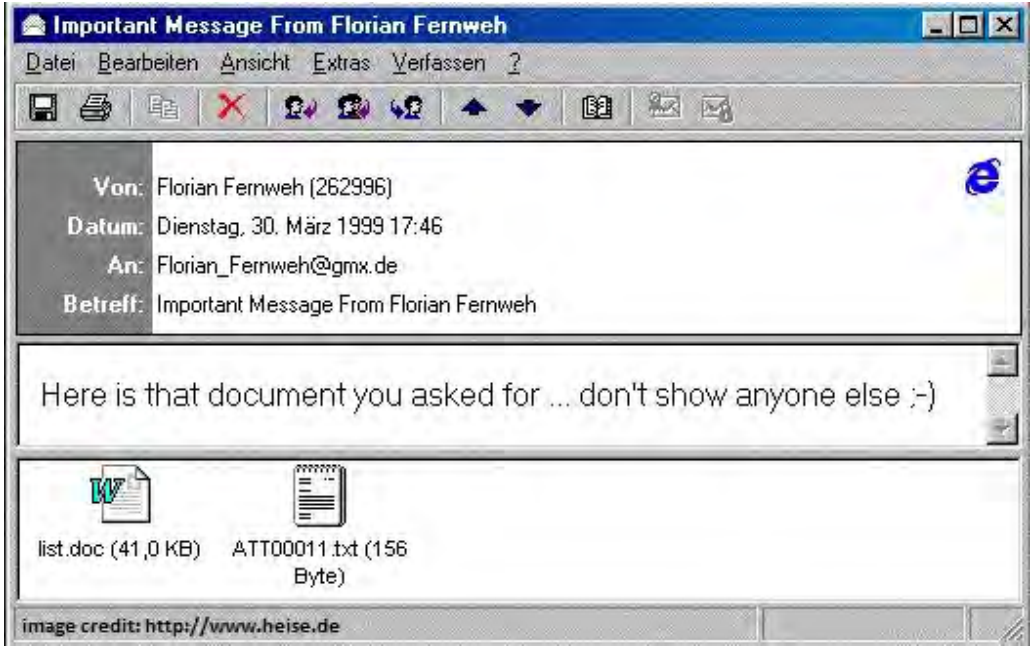
> *"It's easier to trick someone into giving you their password than to hack the system"*
>
> – Kevin Mitnick (approximate quote)

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



Psychological Principles Attackers Exploit

Authority
- "This is IT support..."
- "The CEO needs this wire transfer now"

Urgency
- "Your account will be closed in 24 hours"
- "Limited time offer"

Trust
- "Your colleague sent you this document"
- Impersonating trusted brands

Fear
- "Your computer is infected"
- "Legal action will be taken..."

Curiosity
- "Photo from last night"
- "Your package delivery..."

Greed
- "You've won a prize"
- "Free gift card"

Phishing Attacks

Phishing: fraudulent messages attempting to trick recipients

- **Typical attack**
  - Mass email sent to thousands/millions
  - Appears to be from a legitimate source (bank, tech company, government)
  - Contains an urgent message
  - Includes a malicious link or attachment
  - Small % of recipients fall for it, but the attacker wins with volume (0.1% ⇒ thousands of victims)
- **What happens when you click**
  - Fake login page (credential harvesting)
  - Malware download
  - Exploit kit on malicious website
  - Ransomware infection

Common lures:

- "Verify your account"
- "Your password will expire"
- "Suspicious login detected"
- "Package delivery failed"
- "You've received a secure document"
- "IRS tax refund pending"

Phishing Techniques

- **Email spoofing**
  - Forging sender address: email protocols don't verify sender by default
- **Domain lookalikes**
  - `paypa1.com` (number 1 instead of letter L)
  - `paypal-security.com` (adding words)
  - `paypal.com` (Unicode tricks: Cyrillic 'p' looks like 'p')
- **Visual deception**
  - Copying legitimate email templates, logos, and branding
- **Link obfuscation**
  - Different link than displayed; shortened URLs
  - `storage.googleapis.com` is a common domain – since many legitimate services use it

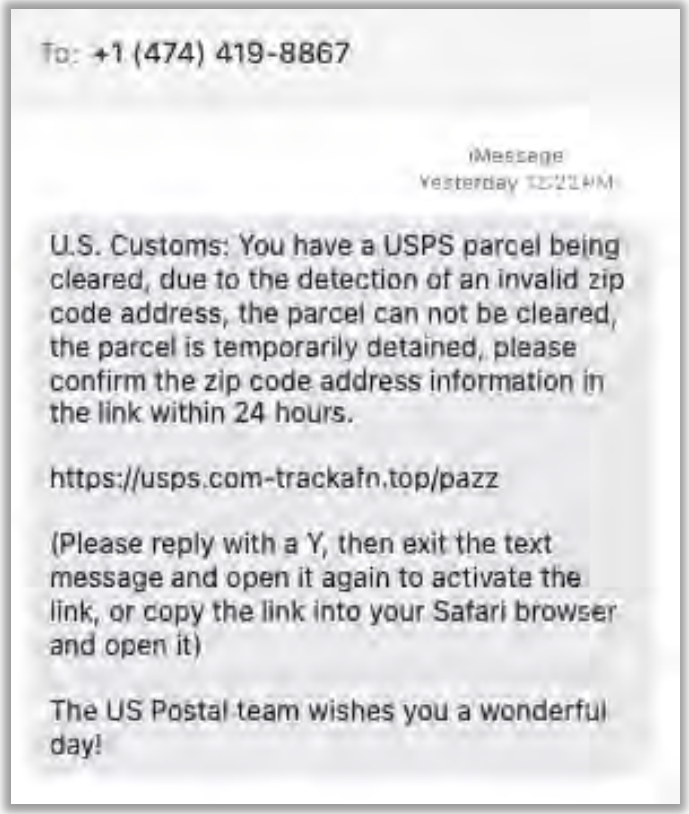
Spear Phishing: Targeted Attacks

Spear Phishing: customized phishing for specific individual or org

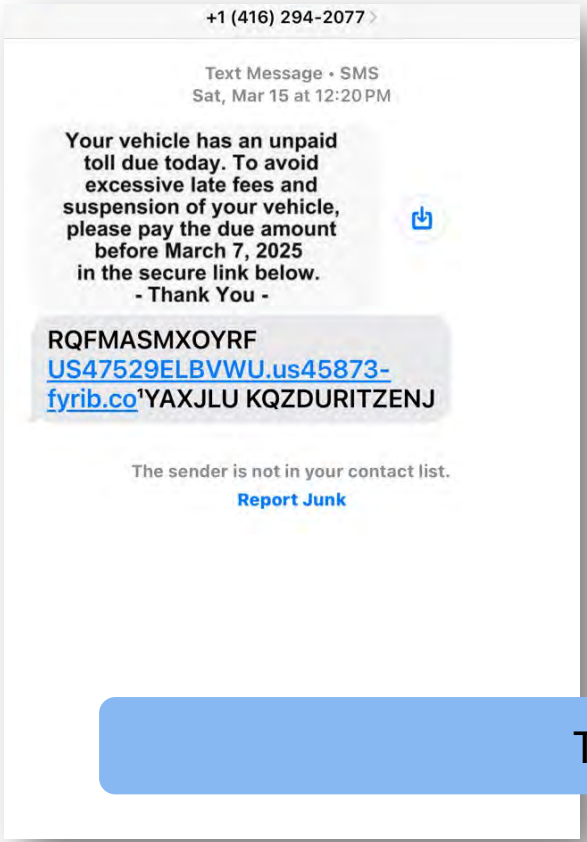
- **Key differences from phishing**
  - Research target beforehand
  - Personalized message
  - More convincing lure
  - Higher success rate
- **Research sources**
  - LinkedIn (job titles, connections, projects)
  - Facebook, X, Instagram (interests, travel, family)
  - Company website (press releases, products)
  - Public records (property, vehicles)
  - Data breaches (previous passwords, logins)

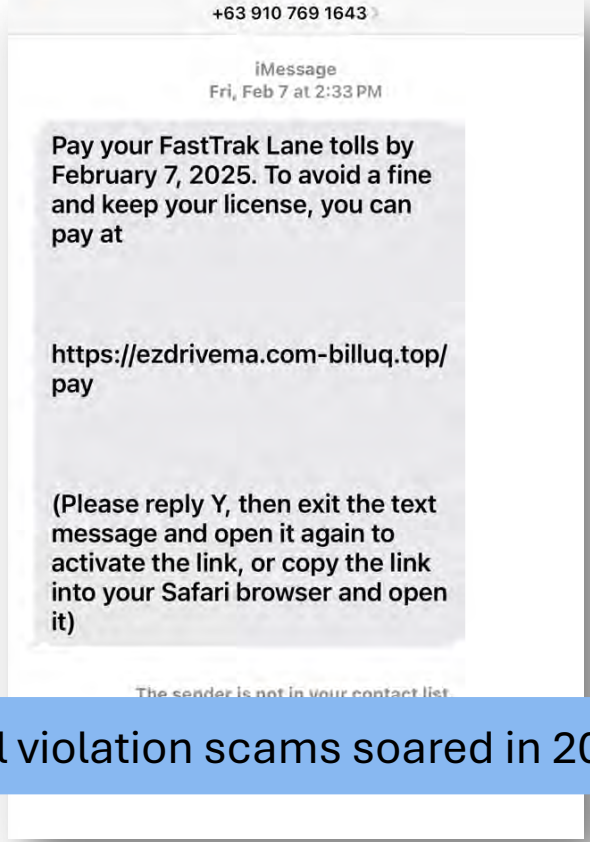
Phishing: Voice & SMS too

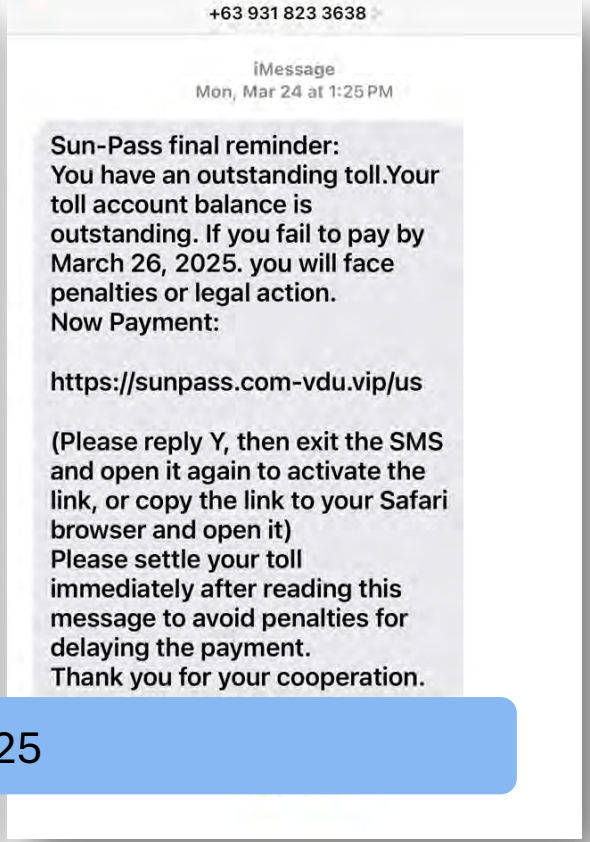
- **Vishing (voice phishing)**
  - Microsoft tech support
  - IRS refund
  - Bank withdrawal confirmation
- **Smishing (SMS phishing)**
  - People trust text more than email
  - Mobile devices have smaller screens – harder to verify the sender
  - Sense of urgency



Smishing Example: Toll Payment Phishing Attacks







Toll violation scams soared in 2025

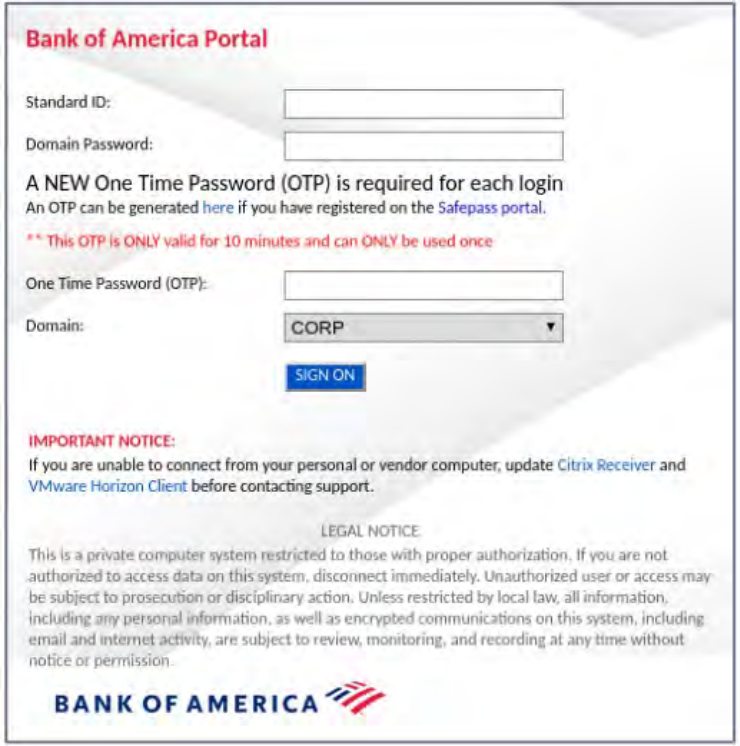
Voice Phishing (vishing) Example: IT Support

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

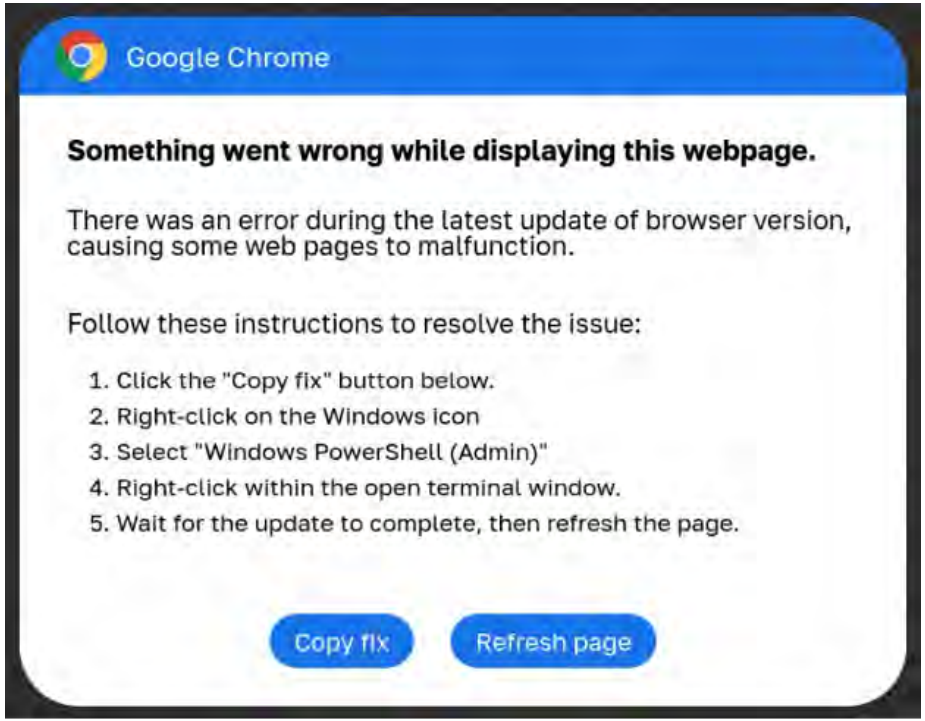
- Created lots of company-branded phishing pages targeting some of the world's biggest companies
- Place calls to employees working at home
- Explain that they are calling from the IT department to troubleshoot VPN issues
- Goal: convince employee to divulge credentials
- Hackers may create corporate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

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



ClickFix Attacks: 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**
- **The instructions to copy, paste, & run a command may be disguised as a fake reCAPTCHA: press these keys to prove you're a human**



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

https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape

Similar Domains: Typosquatting & Combosquatting

- **Exploit mistakes users might make: *recognition* or *typing***
- **Typosquatting: Registering domains similar to legitimate sites**

Typosquatting
- gooogle.com (extra 'o')
- amazom.com (n→m)

Character substitution
- g00gle.com (o→0)
- paypa1.com (L→1)

Omitted characters
- gogle.com (missing 'o')
- amazn.com (missing 'o')

Wrong domain
- google.net (.com→.net)
- microsoft.org

Combosquatting
- microsoft-support.com
- amazon-security.com

Typosquatting Examples

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”

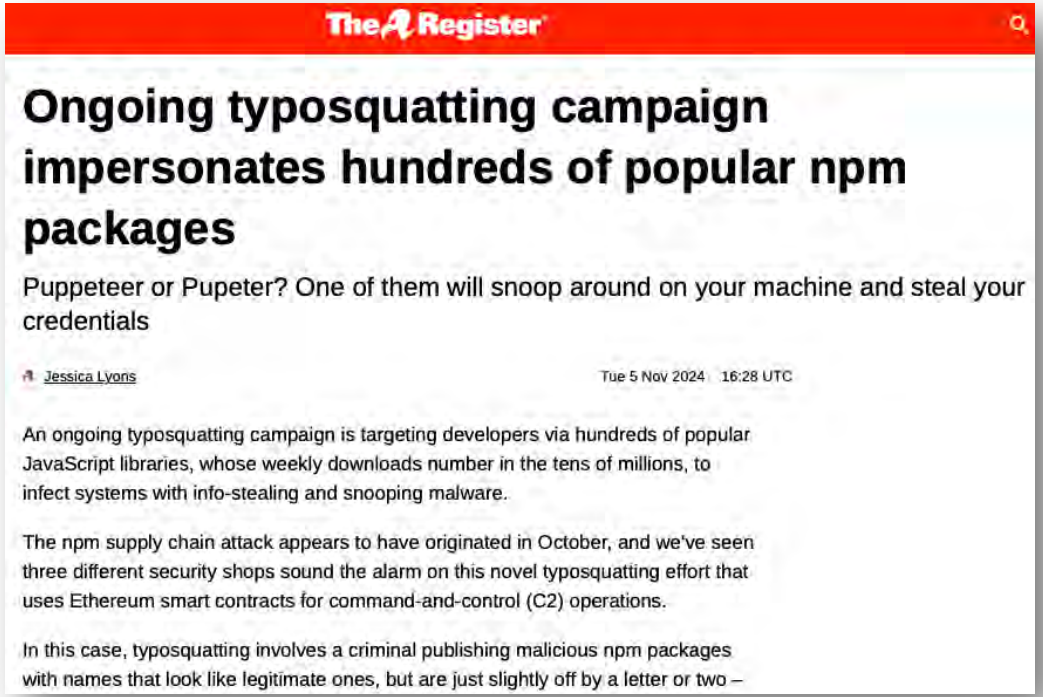
cointelegraph.com

Typosquatting Example

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 Example



The Register

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/

PyPI Halts Sign-Ups Amid Surge of Malicious Package Uploads Targeting Developers

The Hacker News

March 29, 2024

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

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

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

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

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

More Fake QR Codes

Fake QR Codes reported in NYC in June 2025

And other places

- Birmingham, & Mobile, Alabama
- Orlando, Florida
- 1,386 reports of QR parking scams in the UK in 2024

https://www.reddit.com/r/nyc/comments/1l3i7lo/parking_meter_qr_code_scam/

Specialized Components

Specialized Malware Components

- **Let's look at**
  - Data collection tools (**keyloggers**)
  - Remote control infrastructure (**bots & botnets**)
  - Stealth mechanisms (**rootkits, bootloaders**)
- **What makes these specialized?**
  - Often modular
  - Often combined with other malware types
  - Each solves a specific problem for attackers

Keyloggers: Record keystrokes

- **Capture anything typed**
  - Passwords, PINs, credit card numbers, messages & emails, documents
- **Software keyloggers**
  - User-mode: run as regular applications – Windows API hooks (SetWindowsHookEx)
  - Kernel-mode: run in kernel space, intercepting keyboard driver
  - Form grabbers: specifically designed to capture web form data before submission
- **Hardware keyloggers**
  - Inline keyboard devices
  - Modified keyboards
  - Keyboard overlays (e.g., ATM skimming)

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.

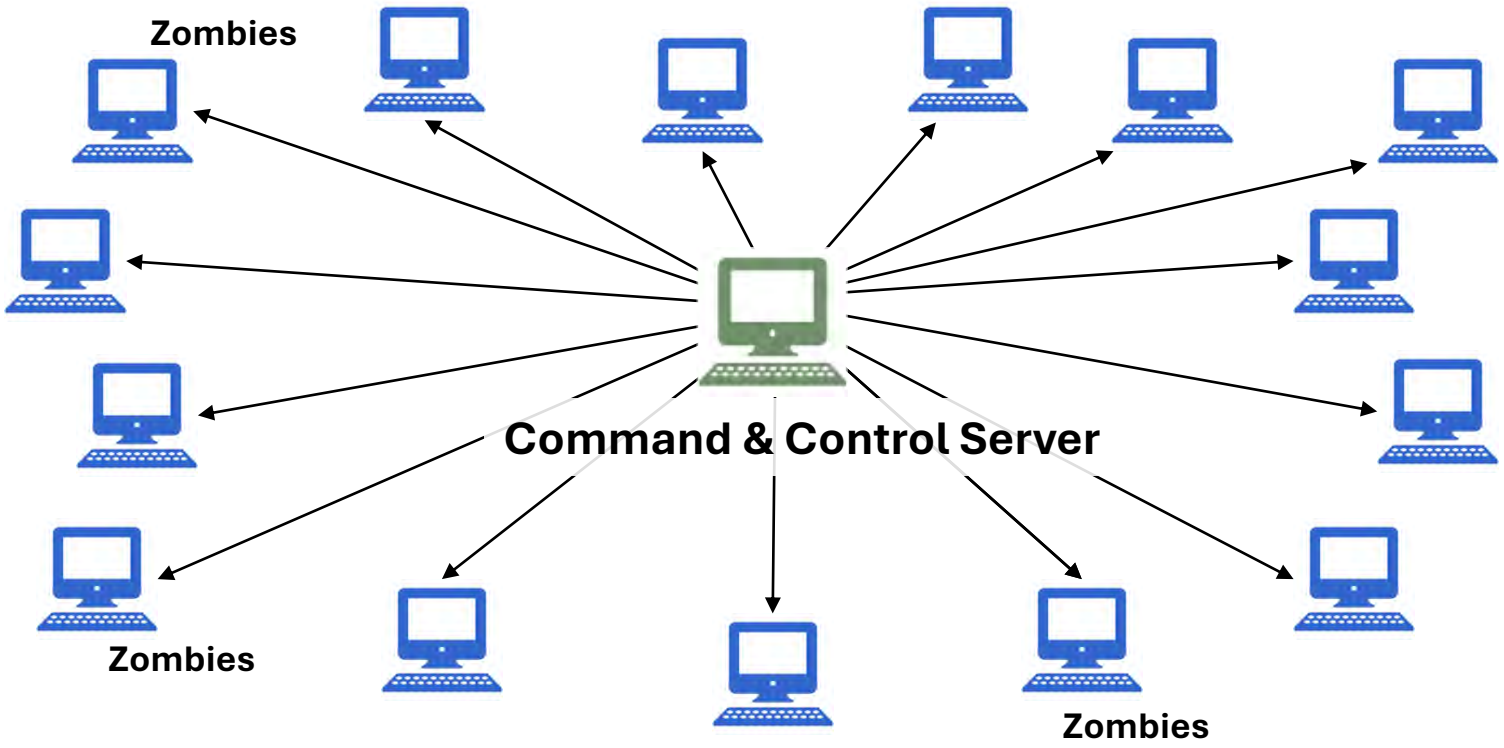
https://www.vice.com/en/article/k789me/omg-cables-keylogger-usbc-lightning

Bots and Botnets

- **Bot = zombie: compromised computer under attacker control**
  - Infected with malware that connects to C2 (command-and-control server)
  - Waits for commands from operator
  - Can be controlled individually or as a group
  - Owner usually unaware
- **Uses**
  - Send spam email
  - Host phishing sites
  - Launch DDoS attacks
  - Mine cryptocurrency
  - Proxy traffic (hide attacker location)
  - Store illegal content
  - Participate in click fraud
  - Scan for other vulnerable systems

An individual bot has limited value – the power is in numbers

Bots & Botnets



Stealth access

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 into the software 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.

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/

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

Rootkits: Stealth

Rootkit: software that hides malware from detection

- **Primary goal: concealment**
  - Hide files, processes, network connections, registry entries, other malware
  - A user or administrator can look around the system and not see anything abnormal
- **Secondary goals**
  - Backdoor access, persistence, disable security software, escalate privileges
- **Started on Unix Systems in 1990**
  - NTRootkit in 1999
  - HackerDefender for Windows NT/2000/95 in 2003
  - Mac OS X rootkit in 2009

Rootkits are not standalone malware – they hide other malware

Types of Rootkits

- **User-mode rootkits**
  - Replace commands
  - Hook Windows API calls
  - Patch commonly-used APIs
    - Use LD_PRELOAD to hook & intercept system calls & common library functions

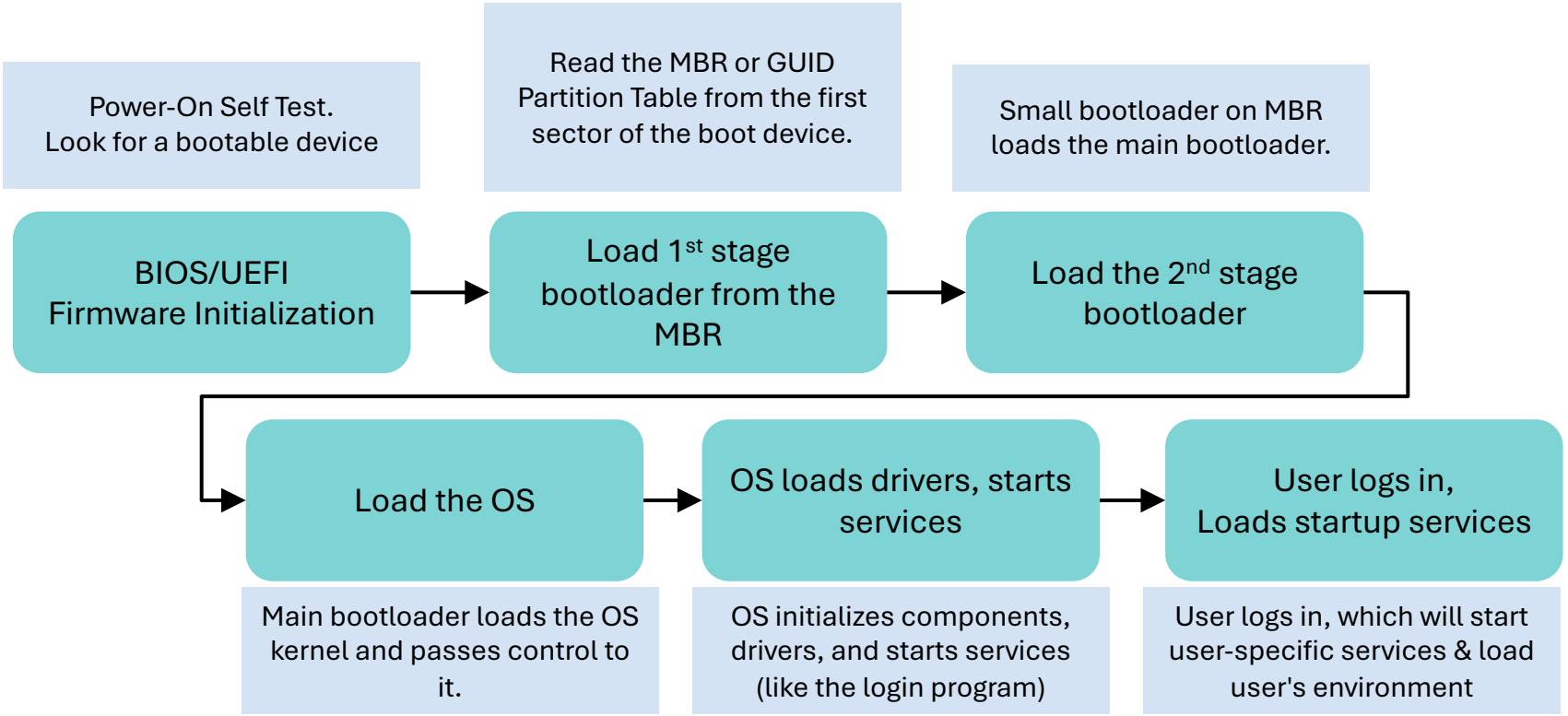
- **Kernel-mode rootkits**
  - Installed as kernel modules: highest privilege level
  - Gives the rootkit unrestricted access
    - Can modify the system call table and any kernel structures
  - Difficult to detect: all commands and libraries look normal

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**

Other types of rootkits

416 Review: How a System Boots



Other Types of Rootkits – Overview

- **Bootkit: infects bootloader or boot sector**
  - Loads before operating system
  - Can compromise the OS from the start
  - Survives OS reinstalls
  - **Firmware rootkits** - infect BIOS/UEFI firmware
    - Persists even after hard drive replacement
    - These are rare
- **Microcode hacking (theoretical)**
  - Reprogram the behavior of instructions in the CPU
- **Hypervisor rootkit (mostly theoretical)**
  - Runs below OS as a hypervisor – nothing in the OS is modified
  - All access to devices goes through the hypervisor

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.

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

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/

CPU-Level Attacks: Microcode Hacking

- **Change the microcode in a CPU**
  - AMD & Intel CPUs support a mechanism to download microcode patches to fix bugs in the hardcoded silicon
  - Changes the behavior of a processor & its instructions
  - Patches can be loaded during system boot and are encrypted and cryptographically signed with RSA keys
  - To save space, a hash of the public key is stored on the chip to validate the public key in the microcode update
- **The attack**
  - AMD Zen CPUs use a weak hash function
  - A Google team was able to create a new key pair where the public key hashed to the same value as AMD's public key (see the article for info on additional work that had to be done)

Microcode toolchain with source code & tutorials released in 2025

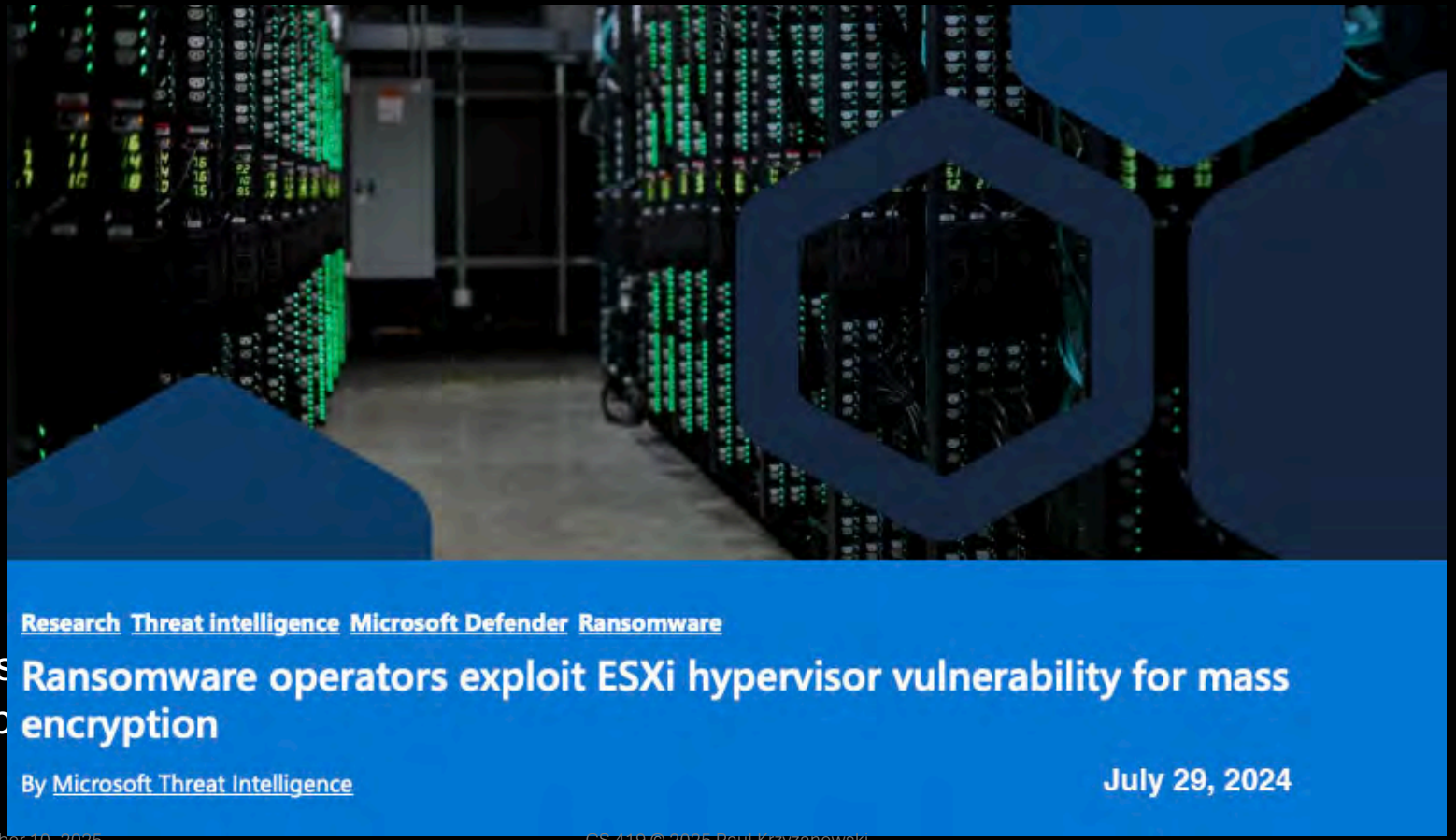
https://bughunters.google.com/blog/5424842357473280/zen-and-the-art-of-microcode-hacking

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.

Hyperjacking: hypervisor attacks

This
Rep



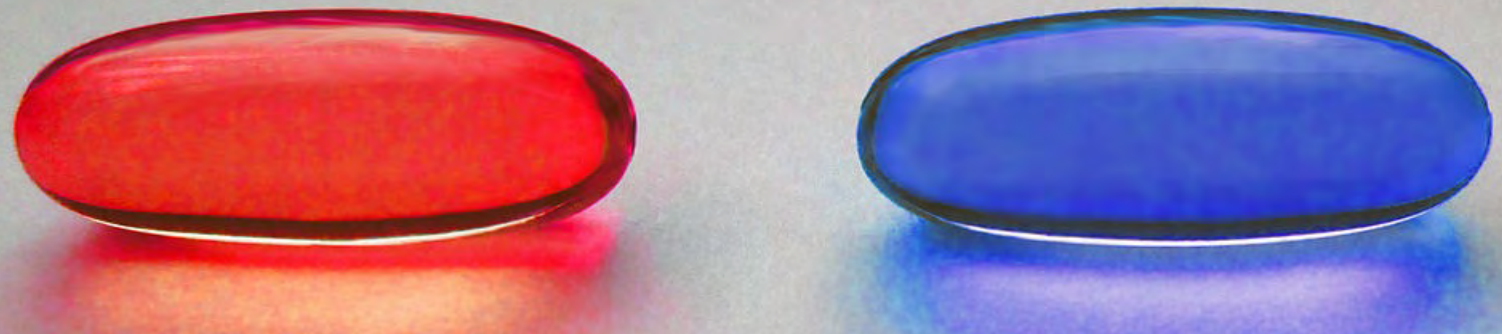
Research Threat intelligence Microsoft Defender Ransomware

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 in a VM

- **Attackers can deploy a virtual machine containing malware**
  - It won't run security software & won't be detected by other systems
- **Example: Maze ransomware – 2020**
  - Demands $100,000+ for decryption key
  - Delivered inside of a Windows .msi installer file
  - Copy of VirtualBox is also inside the installer
- **Example: Curly COMrades – 2025**
  - Spyware/credential harvesting
  - Attackers enabled Microsoft Hyper-V virtualization
  - Deployed a small Linux-based VM
  - Contained reverse shell and tools for bidirectional data transfer & credential harvesting

The Hacker News

Hackers Weaponize Windows Hyper-V to Hide Linux VM and Evade EDR Detection

Nov 06, 2025 Ravie Lakshmanan

The threat actor known as **Curly COMrades** has been observed exploiting virtualization technologies as a way to bypass security solutions and execute custom malware.

According to a new report from Bitdefender, the adversary is said to have enabled the Hyper-V role on selected victim systems to deploy a minimalistic, Alpine Linux-based virtual machine.

"This hidden environment, with its lightweight footprint (only 120MB disk space and 256MB memory), hosted their custom reverse shell, CurlyShell, and a reverse proxy, CurlCat," security researcher Victor Vrabie, along with Adrian Schipor and Martin Zugec, said in a technical report.

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

https://businessinsights.bitdefender.com/curly-comrades-evasion-persistence-hidden-hyper-v-virtual-machines

The End