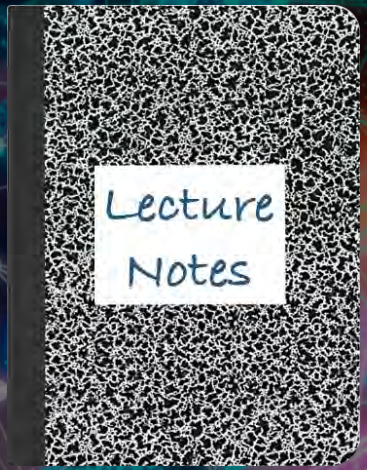
CS 419: Computer Security

Week 1: Part 1

Foundations



Paul Krzyzanowski

September 6, 2025

Columbia University data breach hits 870,000 people

Unauthorized party accessed university systems and stole 460 GB of admissions and financial aid records

June 30, 2025

US government warns of new Iran-linked cyber threats on critical infrastructure.

Companies should disconnect operational technology from the internet and enforce strong protections for user accounts, a joint alert from CISA, the FBI, NSA and DoD said.

September 8, 2025

NETSCOUT research confirms DDoS threats surge worldwide

The company has articulated that DDoS attacks have evolved into precision-guided weapons of geopolitical influence capable of destabilising critical infrastructure.

August 19, 2025

Russian Hacktivists Take Aim at Polish Power Plant, Again

This attack was seemingly more successful than the first iteration, causing disruptions at the plant.

September 5, 2025

Jaguar Land Rover production stopped for four days and counting due to ransomware attack, company has now officially shut down — teenaged hackers from Scattered Lapsus$ Hunters take responsibility.

No cars are being produced in multiple countries.

September 5, 2025

TransUnion breach exposes personal data of 4.4M Americans

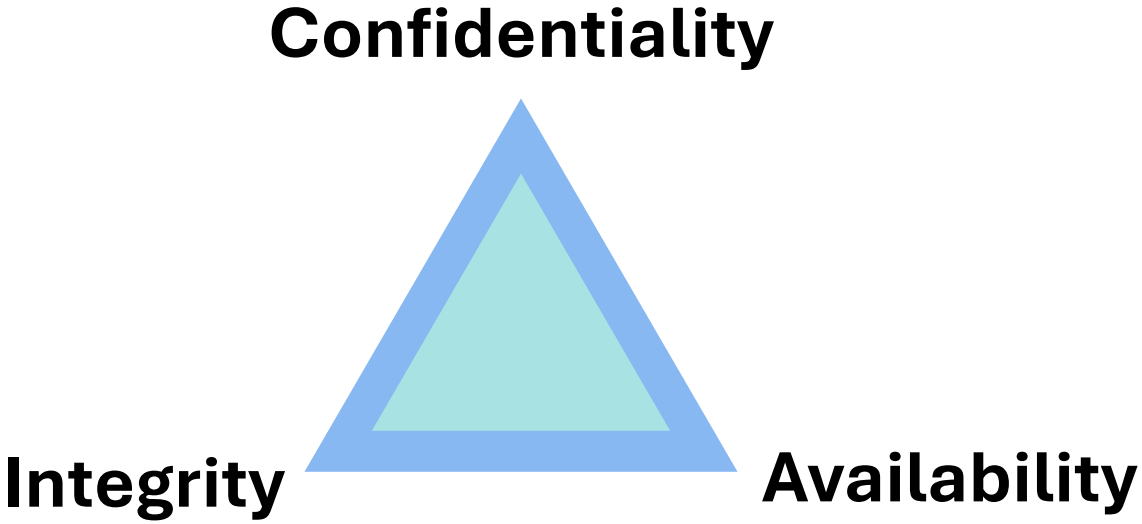
Unauthorized party accessed university systems and stole 460 gigabytes of admissions and financial aid records

Security as a Problem of Trust

Computers do not enforce security on their own

The goal of computer security is to keep systems, programs, and data “safe”

The CIA Triad*



**No relationship to the Central Intelligence Agency*

Confidentiality

- **Keep data & resources hidden**
  - Data will only be shared with authorized individuals
  - Sometimes – conceal the existence of data or communication
- **Traditional focus of computer security**
  - Usually accomplished with access control and encryption

Data confidentiality:

"The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]."

– *RFC 4949, Internet Security Glossary*

Confidentiality – Privacy – Secrecy – Anonymity

Privacy

- Limit what information can be shared with others
- Control others' use of information about you
- Freedom from intrusion

The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others.

See: HIPAA, personal information, Privacy Act of 1974
RFC 4949, Internet Security Glossary

Privacy is a reason for confidentiality

Anonymity: conceal the individual's identity – e.g., anonymous surveys
Secrecy: hide the existence of information – e.g., classified projects

Privacy is increasingly harder to attain

- **"Free" services**
  - Facebook, Google, X, LinkedIn, Instagram, TikTok, …
  - Information collection, tracking web sessions
- **More data is online and widely accessible**
  - No need to go to town halls to get real estate transactions
- **Phone companies know every place you go**
- **Big data analytics**
  - It's increasingly easy to correlate data:
    Credit card spending, travel, jobs, marriages/divorces, kids, cars, …

"If you are not paying for it, you're not the customer; you're the product being sold"

– blue_beetle (Andrew Lewis), 2010

Privacy & data mining … on a national level

- **U.S. credit scores**
  - Credit reporting companies track employment, spending, home ownership, loan repayment, …
  - Credit scores affect the ability to borrow money, buy a home
- **China's Social Credit System**
  - Track the trustworthiness of everyday citizens, corporations, and government officials
  - Track behavior: frivolous spending, major & minor infractions
  - Boost public confidence and fight problems like corruption and business fraud
  - Has not yet become a single score but a collection of data
- **AI simplifies data analysis but…**
  - UNESCO adopted a Recommendation on the Ethics of AI in 2021

    "AI systems should not be used for social scoring or mass surveillance purposes"

Attacks on privacy: data breaches

Exfiltration

Exfiltration – getting data

Why steal data?

- **Corporate/national espionage:**
  - Strategy, schedules, employees, and intellectual property
- **Obtaining credentials:**
  - Your login/password for your AT&T account might be the same as your Chase bank account
- **Extortion (ransomware):**
  - Threaten disclosure or destruction of data if not paid
- **Impersonation:**
  - Masquerade as that user for social engineering

Recent Major Data Breaches

National Public Data (NPD)	Apr 2024	2.9 billion user records One of the largest breaches in history affecting people in US, UK, and Canada
Ticketmaster	May 2024	~ 560M customer records
Change Healthcare/UnitedHealth	Feb 2024	190M+ customer records largest breach of medical data in U.S. history – months of outages
AT&T	May 2024	Personal data on 73M+ current and former customers
McDonald's (AI hiring bot)		64 million job applications
PowerSchool	Dec 2024	62.4 million students worldwide and 9.5 million educators
FBCS (Financial Business and Consumer Solutions)	Feb 2024	4.25 million individuals – debt collection

Some earlier big data breaches

- **National Public Data – April 2024**
  - Personal data of over 2.9 billion people: SSNs, current & past addresses, family info, …
  - Full names, email, chat transcripts, payment logs, IP addresses
- **Microsoft – January 2021**
  - Attack on Exchange servers, affecting 60,000 companies worldwide
- **India Govt – Aadhaar database – March 2018**
  - Personal information of more than 1.6 billion Indian citizens stored in the world's largest biometric database leaked via website
  - Names, unique identity numbers, bank details, photos, thumbprints, retina scans
  - *Attacked again in July 2023 – 810+ million user accounts*
- **Verifications.io – February 2019**
  - Email validation service exposed 763 million unique addresses
  - Public MongoDB instance with no password
  - Names, phone numbers, dates of birth, genders
- **Yahoo – October 2017**
  - Three billion user accounts compromised
  - Names, security questions & answers

Some earlier big data breaches

- **Alibaba – July 2022**
  - 1.1 billion customer records from its cloud hosting servers
  - Names, phone numbers, physical addresses, criminal records
- **First American Financial – 2019**
  - 885 million customer records from its Title Insurance unit
  - *Attacked again in* December 2023
- **Facebook – April 2019**
  - Two 3rd-party app datasets exposed to the public Internet
  - Contains comments, likes, reactions, account names
  - 540 million users affected
- **Marriott – November 2018**
  - Data from about 500 million Starwood hotel customers from 2014-2016
  - Names, contact info, passport numbers, Preferred Guest numbers, etc.
  - Credit & debit card numbers and expiration dates from 100 million customers
- **CAM4 – March 2020 (data leak – exposed data due to misconfiguration)**
  - Adult video site – 10.88 billion records
  - Full names, email, chat transcripts, payment logs, IP addresses

cybernews

The Mother of All Breaches (MOAB)

January 2024:
12 TB, 26 billion records

An indexed compilation of records from breaches and privately-sold databases

https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/

Integrity

- **The trustworthiness of the data or resources**
- **Preventing unauthorized changes to the data or resources**

Data integrity

Property that data has not been modified or destroyed in an unauthorized or accidental manner

Origin integrity & Recipient integrity

Identification & authentication

System integrity (Functional integrity)

The ability of a system to perform its intended function, free from deliberate or inadvertent manipulation

Integrity is often more important than confidentiality!

Attacks on Integrity

Data modifications usually don't make the news

Companies usually are not required to disclose them
(GDPR requires only the disclosure of breaches containing personal information)

- **Email spoofing, caller ID spoofing**
- **Redirect network traffic**
  - Route table poisoning, DNS poisoning, BGP hijacking
- **Poisoning AI models**
  - 2020 – University of Maryland experiment on the Google Auto ML image recognition platform
    - 0.1% of poisoned (modified) data caused the algorithm to identify a frog as an airplane in 80% of cases

https://www.tributech.io/blog/cybersecurity-threat-data-tampering

Availability

- **Being able to use the data or resources**
- **Property of a system being accessible and capable of working to required performance specifications**

Turning off a computer provides confidentiality & integrity but hurts availability

Denial of Service (DoS) attacks target availability

Amazon Outage Took Citi Bike Offline At Height Of Rush Hour

gothamist

Security isn't always about adversaries attacking … sometimes it's services failing

Jake Offenhartz • December 22, 2021

Citi Bike riders were left stranded on Wednesday after an outage at an Amazon data center knocked out service to the bike-share system during the height of the morning rush hour.

The disruption began shortly after 7:00 a.m., sparking complaints and confusion from monthly subscribers unable to unlock a bike. A spokesperson for Lyft, the Citi Bike parent company, said stations were beginning to come back online as of 9:20 a.m., though some riders continued to report issues.

Outside Bellevue Hospital in Manhattan on Wednesday morning, would-be commuters stood in front of a docking station fruitlessly trying to connect to the bikes with their phones.

https://gothamist.com/news/amazon-outage-took-citi-bike-offline-height-rush-hour

University loses 77TB of research data due to backup error

BLEEPINGCOMPUTER

Bill Toulas • December 30, 2021

Sometimes it's human error

The Kyoto University in Japan has lost about 77TB of research data due to an error in the backup system of its Hewlett-Packard supercomputer.

The incident occurred between December 14 and 16, 2021 and resulted in 34 million files from 14 research groups being wiped from the system and the backup file.

After investigating to determine the impact of the loss, the university concluded that the work of four of the affected groups could no longer be restored. All affected users have been individually notified of the incident via email, but no details were published on the type of work that was lost.

At the moment, the backup process has been stopped. To prevent data loss from happening again, the university has scrapped the backup system and plans to apply improvements and re-introduce it in January 2022.

https://www.bleepingcomputer.com/news/security/university-loses-77tb-of-research-data-due-to-backup-error/

Terabytes of Deleted Case Data Forces Dallas PD to Revise Policy

A Dallas Police employee accidentally deleted 22 TBs of case files when trying to migrate data between servers. Officials say they're now working to recover what they can and prevent future issues.

Jule Pattison-Gordon • August 17, 2021

In Dallas, at least one murder trial has been delayed after a police employee accidentally destroyed 8 terabytes of digital case files and materials during a routine data migration process gone wrong.

A Dallas Police Department (DPD) employee attempting to move older case files out of a cloud-based archive and onto an on-premise server housed in the city's data center accidentally deleted 22 terabytes worth of files, the DPD told media in an emailed statement.

Police recovered 14 terabytes, but DPD believes the remaining 8 terabytes are "permanently deleted and unrecoverable from the archive location," per its statement.

The impacted files include audio recordings, case notes, images, videos and other materials, the DPD said. According to an Aug. 11 memo released by the Dallas County Criminal District Attorney's Office, the data loss affects prosecution of cases for which the offending event occurred before July 28, 2020.

https://www.govtech.com/public-safety/terabytes-of-deleted-case-data-forces-dallas-pd-to-revise-policy

OpenAI accidentally deleted potential evidence in NY Times copyright lawsuit

TechCrunch

Kyle Wiggers • November 22, 2024

Lawyers for The New York Times and Daily News, which are suing OpenAI for allegedly scraping their works to train its AI models without permission, say OpenAI engineers accidentally deleted data potentially relevant to the case.

Earlier this fall, OpenAI agreed to provide two virtual machines so that counsel for The Times and Daily News could perform searches for their copyrighted content in its AI training sets.
...
But on November 14, OpenAI engineers erased all the publishers' search data stored on one of the virtual machines, according to the aforementioned letter, which was filed in the U.S. District Court for the Southern District of New York late Wednesday.

OpenAI tried to recover the data — and was mostly successful. However, because the folder structure and file names were "irretrievably" lost, the recovered data "cannot be used to determine where the news plaintiffs' copied articles were used to build [OpenAI's] models," per the letter.

https://techcrunch.com/2024/11/22/openai-accidentally-deleted-potential-evidence-in-ny-times-copyright-lawsuit/

Oslo warns of escalating Russian cyber threat after dam breach, citing Moscow as biggest risk to national security

Sometimes it's sabotage via software

August 15, 2025

The Norwegian Police Security Service (PST) confirmed this week that pro-Russian hackers took control of a dam in Bremanger, western Norway, in April, opening a floodgate and allowing water to flow unnoticed for four hours. PST said the incident was a deliberate demonstration of Moscow's ability to remotely compromise the country's critical infrastructure. The attribution marks the first time Oslo has formally linked the attack to Russia, describing it as part of a broader hybrid warfare strategy aimed at causing harm and showcasing capability.

Speaking at the Arendalsuka annual national forum in the city of Arendal, Beate Gangås, head of PST, said, "Over the past year, we have seen a change in activity from pro-Russian cyber actors." The Bremanger incident was an example of such an attack, she added. "The aim of this type of operation is to influence and to cause fear and chaos among the general population. Our Russian neighbour has become more dangerous."

https://industrialcyber.co/industrial-cyber-attacks/oslo-warns-of-escalating-russian-cyber-threat-after-dam-breach-citing-moscow-as-biggest-risk-to-national-security/

Thinking about security

Thinking about security

Security is <u>not</u>

- adding encryption
- … or using a 512-bit key instead of a 64-bit key
- … or changing passwords
- … or setting up a firewall

It is a systems issue

= Hardware + firmware + OS + app software + networking + people

= Processes & procedures, policies, detection, forensics

"Security is a chain: it's only as secure as the weakest link"

– Bruce Schneier

Security is hard

Software is complex

- Windows 11: 60-100 million lines of code
- Google services comprise ~2 billion lines of code
- Linux distribution: over 200 million lines of code
  - Linux kernel: ~40M lines of code across over 65,000 files
  - Linux kernel at the end of 2024: 75,314 commits from 4,807 authors
  - 3,694,098 new lines of code and 1,490,601 lines of code removed
  - Linux Git source tree: 1,324,647 commits in 2024 from 29,380 different authors

Try to find the bugs … or keep up with the changes!

Systems are complex

- Lots of layers: microcode + firmware + OS + libraries + apps + devices
- Interaction with cloud services
- Third-party components
- Complex interaction models, concurrency
- All parts are not always under the control of one administrator

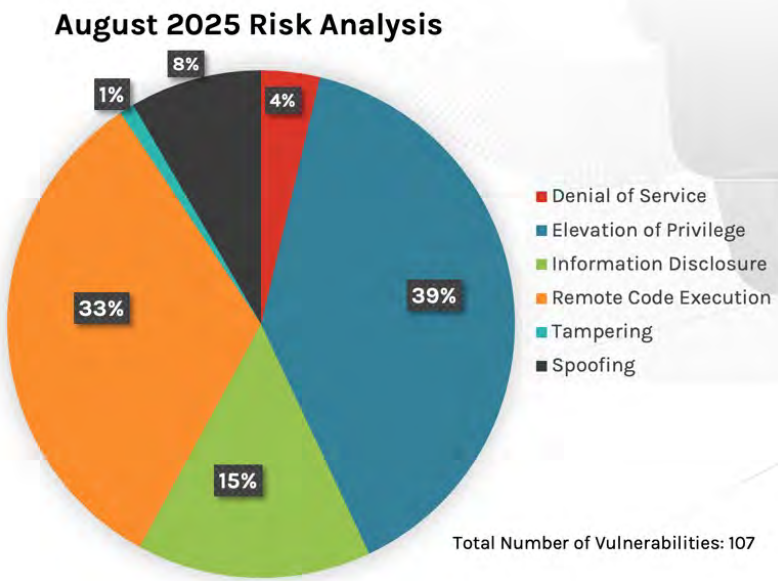
The human factor

- People make mistakes: coding, configuration, usage

Microsoft's August 2025 Patch Tuesday:
One Zero-Day and 13 Critical Vulnerabilities Among 107 CVEs

August 12, 2025

- 67 patches to Windows
- 19 patches to Office



What's a CVE?

Common Vulnerabilities & Exposures

Standard reference for publicly known vulnerabilities.

Maintained by the MITRE Corporation with funding from the U.S. government.

Security Goals

Prevention: prevent attackers from violating the security policy

- Implement mechanisms that users cannot override
- *Example: ask for a password*

Detection: detect & report attacks

- Important when prevention fails
- Indicates & identifies weaknesses in prevention
- Also: detect attacks even if prevention is successful

Recovery: stop the attack, repair the damage

- … Or continue to function correctly even if an attack succeeds
- **Forensics**: identify what happened so you can fix it
- *Example: restoration from backups*

Policies & Mechanisms

Policy: what is or is not allowed

- Can be expressed in natural language ("this is our security policy")
- … or formally via mathematics
- **Policy language** – goal is to provide precision together with ease of understanding

Mechanisms: implement and enforce policies

- E.g., password entry & authentication
- **Technical mechanisms**: access controls, cryptography, locked doors, …
- **Procedural mechanisms**: ID checks, audits, separation of duties, …

- ***What mechanisms do we need to secure a system?***
- ***What level of assurance is associated with them?***

Principals vs. Subjects

Principal: any entity that can be uniquely identified & authenticated

Describes *who*

Subject: any entity that actually performs operations o behalf of a principal

Your web browser, your shell, the app you're running

Security Engineering

Security Architecture ⇒ Design

- How do we put a secure system together?
- How do we identify potential weaknesses?

Security Engineering ⇒ Implementation

- Implement mechanisms & policy into a system

Engineering = making compromises

- Understand tradeoffs
- Security vs. cost, performance, acceptability, usability
- Cost-benefit analysis
  - Is it cheaper to prevent an attack or recover?
  - Who pays & who gets punished?

> Microsoft and the device manufacturer and installer exclude all implied warranties and conditions, including those of merchantability, fitness for a particular purpose, and non-infringement. …. you may not under this limited warranty, under any other part of this agreement, or under any theory, recover any damages or other remedy, including lost profits or direct, consequential, special, indirect, or incidental damages.
>
> Microsoft Windows 10 End-User License Agreement

Risk analysis

Should we protect something?

- If so, how carefully?
- And how much should we spend?

Laws & customs

- **Are any security measures illegal?**
  - Example: types of encryption
- **Are any measures unlikely to be used?**
  - Examples: retina scans, urine tests
  - Conformance: balance security vs. effort

Trust in the system & software

Security Assumptions

The heart of all security rests on assumptions about:

- Type of security needed
- The environment where the system is deployed
- **Trusted** components & principals (users, other systems)

Example: *You need a key to open a locked door*

- You assume that the lock is a trusted component and is secure against lock-picking
- BUT … a skilled lock picker can open the lock

Your assumptions are wrong *IF*

- The key is available to unauthorized people (bad policy)
- The environment has a skilled, untrustworthy lock picker
  (bad mechanism – wrong assumption about the environment)
- The lock is trivial to pick (bad mechanism)

Trust: Trustworthy components

Trustworthy components may have the capabilities to break security policies … but will not do so: they will follow the policy

Examples

- A *trustworthy* lock picker will not bypass security unless properly authorized
- A *trustworthy* CPU will correctly enforce memory protections and not allow a user to read regions of memory disallowed by the operating system
- A trustworthy operating system will not allow you to read or modify files to which you do not have access permissions

- **If a core component turns out to be *not trustworthy* then the security of the *entire system* may be at risk**
- **Example: a malicious boot loader can patch the code of the operating system, which can then run a malicious program or change the behavior of programs**

Assurance = our faith in the system

Assurance = how much we can trust a system

This includes

Specifications	Statement (formal or informal) of the desired functioning of the system
Design	The components that will implement the specification
Implementation	• The creation of a system that satisfies the design • Difficult (impossible) to prove the correctness of the implementation of a complex system
Testing & auditing	• **Auditing** = inspecting the code for security-critical bugs • Because we usually cannot prove the correctness of a system, we rely on extensive testing to get that lucky feeling that it works – **Functional testing** to assess that the system works as desired – Also **penetration testing** to assess that the system follows policy and is resilient to bad inputs, missing components, unexpected events, etc.

Trusted Computing Base (TCB)

TCB = All hardware & software of a computing system critical to its security

> "The totality of protection mechanisms within it, including hardware, firmware, and software, the combination of which is responsible for enforcing a computer security policy."
>
> – *Orange* Book
> *U.S. Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)*

If the TCB is compromised, we can no longer guarantee the security of a system

Software that is part of the TCB must protect itself against tampering

- Operating system memory protection is an example of this: an application may be compromised but the operating system is still intact and unaffected

Jan 2018 – Meltdown & Spectre

Intel chips do not have full memory protection when doing speculative execution

Vulnerability existed for 20 years!

- **Meltdown**
  - Allows processes to access kernel memory
- **Spectre**
  - Allows processes to steal data from the memory of other processes
- **Also affects ARM & AMD CPUs**

Critical "Meltdown" and "Spectre" Flaws Break Basic Security for Intel, AMD, ARM Computers | WIRED

One of the most basic premises of computer security is isolation: If you run somebody else's sketchy code as an untrusted process on your machine, you should restrict it to its own tightly sealed playpen. Otherwise, it might peer into other processes, or snoop around the computer as a whole. So when a security flaw in computers' most deep-seated hardware puts a crack in those walls, as one newly discovered vulnerability in millions of processors has done, it breaks some of the most fundamental protections computers promise—and sends practically the entire industry scrambling.

Earlier this week, security researchers took note of a series of changes Linux and Windows developers began rolling out in beta updates to address a critical security flaw: A bug in Intel chips allows low-privilege processes to access memory in the computer's kernel, the machine's most privileged inner sanctum. Theoretical attacks that exploit that bug, based on quirks in features Intel has implemented for faster processing, could allow malicious software to spy deeply into other processes and data on the target computer or smartphone. And on multi-user machines, like the servers run by Google Cloud Services or Amazon Web Services, they could even allow hackers to break out of one user's process, and instead snoop on other processes running on the same shared server.

On Wednesday evening, a large team of researchers at Google's Project Zero, universities including the Graz University of Technology, the University of Pennsylvania, the University of Adelaide in Australia, and security companies including Cyberus and Rambus together released the full details of two attacks based on that flaw, which they call Meltdown and Spectre.

"These hardware bugs allow programs to steal data which [is] currently processed on the computer," reads a description of the attacks on a website the researchers created. "While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs."

Rowhammer

- **Hardware-based attack discovered by Google Project Zero in 2014**
  - Exploits a weakness in modern DRAM chips.
- **Vulnerability**
  - Repeatedly accessing (or "hammering") a row of memory cells at high speeds can cause electrical interference that flips the bits in adjacent rows of memory cells
- **Attackers were able to**
  - **Corrupt sensitive data**, potentially crashing applications or the OS
  - **Gain escalated privileges** by modifying data such as page tables in the OS
  - **Bypass security mechanisms** to execute malicious code
- **Affects multiple operating systems and platforms**

Rowhammer attack can backdoor AI models with one devastating bit flip

CSO

Security researchers have devised a technique to alter deep neural network outputs at the inference stage by changing model weights via row hammering in an attack dubbed ‘OneFlip.’

Lucian Constantin • August 25, 2025

team of researchers from George Mason University has developed a new method of using the well-known Rowhammer attack against physical computer memory to insert backdoors into full-precision AI models. Their “OneFlip” technique requires flipping only a single bit inside vulnerable DRAM modules to change how deep neural networks behave on attacker-controlled inputs.

“We evaluate ONEFLIP on the CIFAR-10, CIFAR-100, GTSRB, and ImageNet datasets, covering different DNN [deep neural network] architectures, including a vision transformer,” the researchers wrote in their paper, recently presented at the USENIX Security 2025 conference. “The results demonstrate that ONEFLIP achieves high attack success rates (up to 99.9%, with an average of 99.6%) while causing minimal degradation to benign accuracy (as low as 0.005%, averaging 0.06%). Moreover, ONEFLIP is resilient to backdoor defenses.”

https://www.csoonline.com/article/4044876/rowhammer-attack-can-backdoor-ai-models-with-one-devastating-bit-flip.html

The Supply Chain

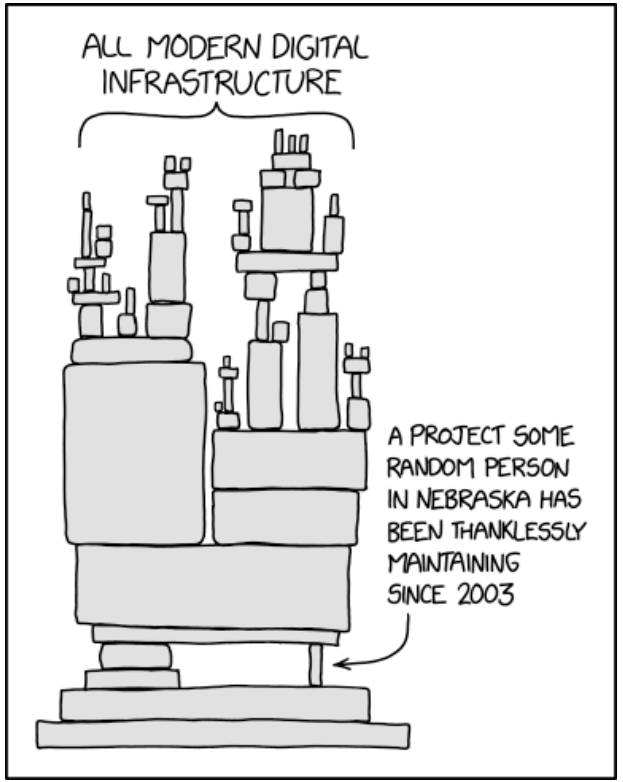
The Trusted Computing Base includes all the hardware and software you depend on:

CPUs, bootloaders, operating systems, compilers, utilities, libraries

They're part of the ***supply chain*** that makes software and devices that run the software

Supply chain problems

- **Do you trust the hardware?**
- **Do you trust every piece of code that is required to run your infrastructure?**
- **Do you know where it comes from?**
- **How actively it's maintained?**
- **Whether it's been audited for vulnerabilities?**



https://xkcd.com/2347/

4.5% of breaches now extend to fourth parties

Help Net Security • May 27, 2025

Security teams can no longer afford to treat third-party security as a compliance checkbox, according to SecurityScorecard. Traditional vendor risk assessments, conducted annually or quarterly, are too slow to detect active threats.

35.5% of all breaches in 2024 were third-party related, a 6.5% increase from 2023. This figure is likely conservative due to underreporting and misclassification. So while you're updating your firewall rules, somewhere in your supply chain a vendor might be inadvertently letting in the very attackers you've been working to keep out.

46.75% of third-party breaches involved technology products and services, a drop from last year's 75%, signaling a diversification of attack surfaces. File transfer software remained the top third-party breach enabler, with Cl0p exploiting vulnerabilities in Cleo software (CVE-2024-50623 and CVE-2024-55956) to launch large-scale attacks.

4.5% of breaches now extend to fourth parties, one breach triggers multiple organizational failures.

https://www.helpnetsecurity.com/2025/05/27/third-party-breaches-increase/

Hackers hijack npm packages with 2 billion weekly downloads in supply chain attack

BLEEPINGCOMPUTER

Sergiu Gatlan • September 8, 2025

In a supply chain attack, attackers injected malware into NPM packages with over 2.6 billion weekly downloads after compromising a maintainer's account in a phishing attack.

Josh Junon (qix), the package maintainer whose accounts were hijacked in this supply-chain attack, confirmed the incident earlier today, stating that he was aware of the compromise and adding that the phishing email came from support [at] npmjs [dot] help, a domain that hosts a website impersonating the legitimate npmjs.com domain.

In the emails, the attackers threatened that the targeted maintainers' accounts would be locked on September 10th, 2025, as a scare tactic to get them to click on the link redirecting them to the phishing sites.

"As part of our ongoing commitment to account security, we are requesting that all users update their Two-Factor Authentication (2FA) credentials. Our records indicate that it has been over 12 months since your last 2FA update," the phishing email reads.

https://www.bleepingcomputer.com/news/security/hackers-hijack-npm-packages-with-2-billion-weekly-downloads-in-supply-chain-attack/

Supply chain attack hits Chrome extensions, could expose millions

The Register

Threat actor exploited phishing and OAuth abuse to inject malicious code

Connor Jones • Jan 22, 2025

Cybersecurity outfit Sekoia is warning Chrome users of a supply chain attack targeting browser extension developers that has potentially impacted hundreds of thousands of individuals already.

Dozens of Chrome extension developers have fallen victim to the attacks thus far, which aimed to lift API keys, session cookies, and other authentication tokens from websites such as ChatGPT and Facebook for Business.

Chrome support impersonation

The attacker targeted dev teams with phishing emails seemingly from Chrome Web Store Developer Support, mimicking official communication, according to Yusoff and Sekoia.

The sample email, which appears in the report, shows the warnings that extensions may be pulled from Chrome over fake rule violations, such as unnecessary details in the extension's description.

Victims were lured into clicking a link disguised as an explanation of Chrome Web Store policies. The link led to a legitimate Google Accounts page, where they were prompted to approve access for a malicious OAuth app. Once developers granted the app permission, the attacker gained everything needed to upload compromised versions of their extensions to the Chrome Web Store.

https://www.theregister.com/2025/01/22/supply_chain_attack_chrome_extension/

Popular NPM library hijacked to install password-stealers, miners

BLEEPINGCOMPUTER

Lawrence Abrams • October 23, 2021

Hackers hijacked the popular **`UA-Parser-JS`** NPM library, with millions of downloads a week, to infect Linux and Windows devices with cryptominers and password-stealing trojans in a supply-chain attack.

The UA-Parser-JS library is used to parse a browser's user agent to identify a visitor's browser, engine, OS, CPU, and Device type/model.

The library is immensely popular, with millions of downloads a week and over 24 million downloads this month so far. In addition, the library is used in over a thousand other projects, including those by Facebook, Microsoft, Amazon, Instagram, Google, Slack, Mozilla, Discord, Elastic, Intuit, Reddit, and many more well-known companies.

…

On October 22nd, a threat actor published malicious versions of the UA-Parser-JS NPM library to install cryptominers and password-stealing trojans on Linux and Windows devices.

According to the developer, his NPM account was hijacked and used to deploy the three malicious versions of the library.

https://www.bleepingcomputer.com/news/security/popular-npm-library-hijacked-to-install-password-stealers-miners/

Log4J: severe vulnerability in a common 3rd party Java library

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE | I WOULD LIKE TO...

Home » News & Events » Blogs » Tech@FTC » FTC warns companies to remediate Log4j security vulnerability

FTC warns companies to remediate Log4j security vulnerability

By: This blog is a collaboration between CTO and DPIP staff and the AI Strategy team | Jan 4, 2022 9:19AM

SHARE THIS PAGE

TAGS: Accountability | Data security | Patches

Log4j is a ubiquitous piece of software used to record activities in a wide range of systems found in consumer-facing products and services. Recently, a serious vulnerability in the popular Java logging package, Log4j (CVE-2021-44228) was disclosed, posing a severe risk to millions of consumer products to enterprise software and web applications. This vulnerability is being widely exploited by a growing set of attackers.

When vulnerabilities are discovered and exploited, it risks a loss or breach of personal information, financial loss, and other irreversible harms. The duty to take reasonable steps to mitigate known software vulnerabilities

Subscribe

Subscribe to Tech@FTC Blog updates

Upcoming FTC Tech Events

Currently we have no upcoming Tech events. Please check back soon.

Additional Information

Office of Technology Research & Investigation

https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability

XZ Utils – the almost disaster

XZ Utils: an attempt to add a backdoor to a common Linux library

- **XZ Utils: set of open-source software for compression and decompression**
- **Included with many Linux distributions & widely used**
- **Around 2021:**
  - A developer with the name Jia Tan started to make requests for bug fixes and improvements
  - Jia built trust and eventually got permission to commit and then be a release manager
  - Social engineering: Fake accounts created for sending lots of bug & feature requests pressured the original maintainer into adding Jia Tan as another maintainer
- **In 2023:**
  - After two years of fixing bugs, Jia Tan introduced a few changes to XZ. Among these changes was a sophisticated backdoor.
  - This would enable an attacker to run arbitrary commands on software that used XZ Utils, like ssh, the secure shell
  - It almost made it to every major Linus distribution
- **But in March 2024:**
  - A Microsoft employee, Andres Freund, discovered an unexpected 500 ms latency after doing an update
  - He traced it to this unexpected code in XZ Utils.

New UEFI vulnerabilities send firmware devs industry wide scrambling

The ability to attack the boot process

PixieFail is a huge deal for cloud and data centers. For the rest, less so.

Dan Goodin • January 17, 2024

UEFI firmware from five of the leading suppliers contains vulnerabilities that allow attackers with a toehold in a user's network to infect connected devices with malware that runs at the firmware level.

The vulnerabilities, which collectively have been dubbed PixieFail by the researchers who discovered them, pose a threat mostly to public and private data centers and possibly other enterprise settings. People with even minimal access to such a network—say a paying customer, a low-level employee, or an attacker who has already gained limited entry—can exploit the vulnerabilities to infect connected devices with a malicious UEFI.

Short for Unified Extensible Firmware Interface, UEFI is the low-level and complex chain of firmware responsible for booting up virtually every modern computer. By installing malicious firmware that runs prior to the loading of a main OS, UEFI infections can't be detected or removed using standard endpoint protections. They also give unusually broad control of the infected device.

…

The implementation is incorporated into offerings from Arm Ltd., Insyde, AMI, Phoenix Technologies, and Microsoft.

https://arstechnica.com/security/2024/01/new-uefi-vulnerabilities-send-firmware-devs-across-an-entire-ecosystem-scrambling/

Malicious Chinese SDK In 1,200 iOS Apps With Billions Of Installs Causing ‘Major Privacy Concerns To Hundreds Of Millions Of Consumers’

Unknowingly bundling spyware into an app

John Koetsier • August 24, 2020

Forbes

A Chinese ad network named Mintegral is accused of spying on user activity and committing ad fraud in more than 1,200 apps with 300 million installs per month since July 2019. Mintegral is headquartered in Beijing, China, and is owned by another Chinese ad network, Mobvista, which has a head office in Guangzhou, China.

One of the apps, Helix Jump, has over 500 million total installs. Other popular apps that are impacted include Talking Tom, PicsArt, Subway Surfers and Gardenscapes.

All together, this likely impacts billions of total app installs on iPhone and iPad.

There’s no exact number on how many devices or iPhone users are impacted, but Snyk says this is a “major privacy concern to hundreds of millions of consumers.”

https://johnkoetsier.com/malicious-chinese-sdk-in-1200-ios-apps-with-billions-of-installs-causing-major-privacy-concerns-to-hundreds-of-millions-of-consumers/

Cisco's warning: Critical flaw in IOS routers allows 'complete system compromise'

Cisco has delivered updates to address four critical flaws affecting its industrial routers.

Liam Tung • June 4 2020

Cisco has disclosed four critical security flaws affecting router equipment that uses its IOS XE and IOS software.

The four critical flaws are part of Cisco's June 3 semi-annual advisory bundle for IOS XE and IOS networking software, which includes 23 advisories describing 25 vulnerabilities.

The 9.8 out of 10 severity bug, CVE-2020-3227, concerns the authorization controls for the Cisco IOx application hosting infrastructure in Cisco IOS XE Software, which allows a remote attacker without credentials to execute Cisco IOx API commands without proper authorization.

IOx mishandles requests for authorization tokens, allowing an attacker to exploit the flaw with a specially crafted API call to request the token and then execute Cisco IOx API commands on the device, according Cisco.

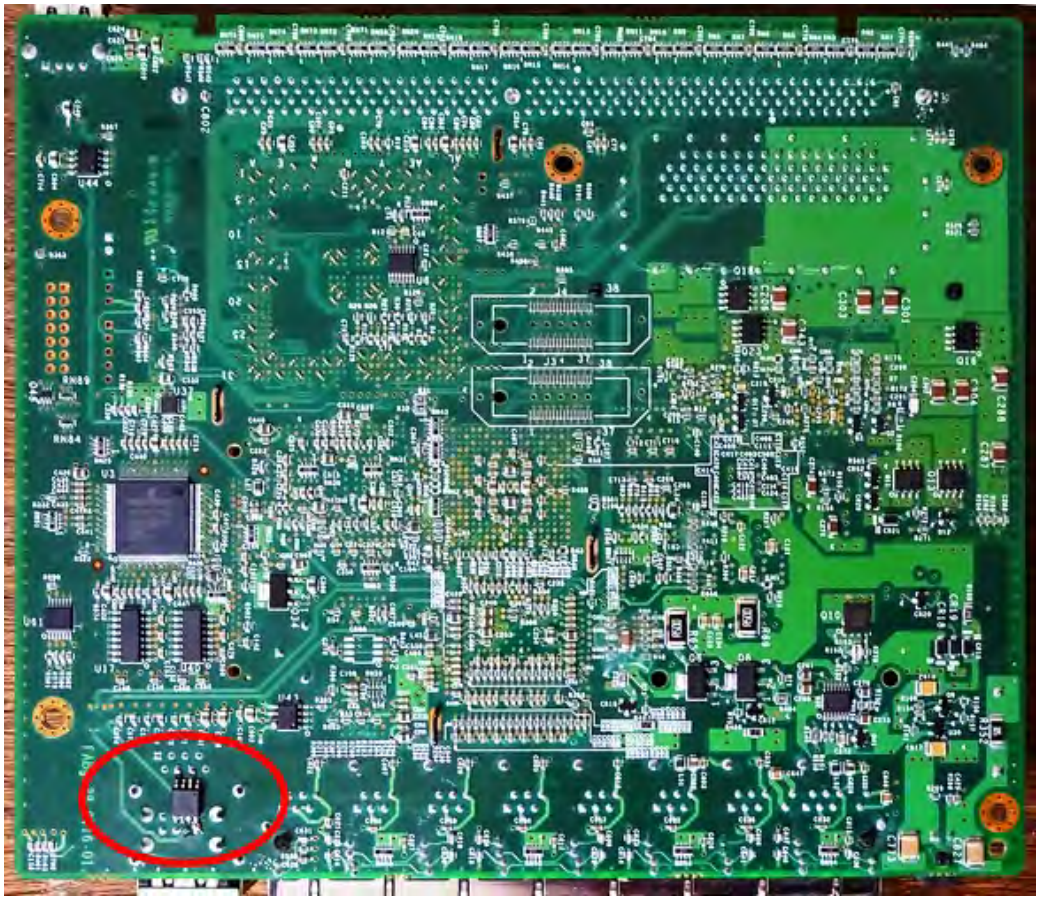
https://www.zdnet.com/article/ciscos-warning-critical-flaw-in-ios-routers-allows-complete-system-compromise/

Attacks on 3rd party software, services, hosting sites

- **June 2024: CDK Global ransomware attack – 15,000 auto dealerships**
  - Backend system used by car dealers
  - Crippled operations of 15,000 auto dealerships across the U.S. & Canada
- **July 2024: Snowflake data breach – 100s of millions of AT&T records (and many others)**
  - Attackers downloaded hundreds of millions of phone call and text message records of AT&T customers
  - AT&T uses Snowflake for data warehousing & analytics
  - Attackers used stolen credentials to log in
- **July 2024: CrowdStrike bug – 8.5 million Windows servers worldwide**
  - CrowdStrike provides endpoint protection software
  - Not an attack! A buggy update (NULL pointer dereference) caused the program to crash
  - Largest IT outage in history: 8.5 millions servers affected (auto, healthcare, aviation, broadcasting, banking)
  - More than 6,700 flights were canceled as a result

Do you trust the entire supply chain?

- **Alter the circuit design**
- **Add components after the fact**
- **Modify the CPU**
- **Modify the bootloader, firmware, or pre-installed software**
- **Add malware to the compiler used to build the software**
- **Add malware to libraries used by the apps**

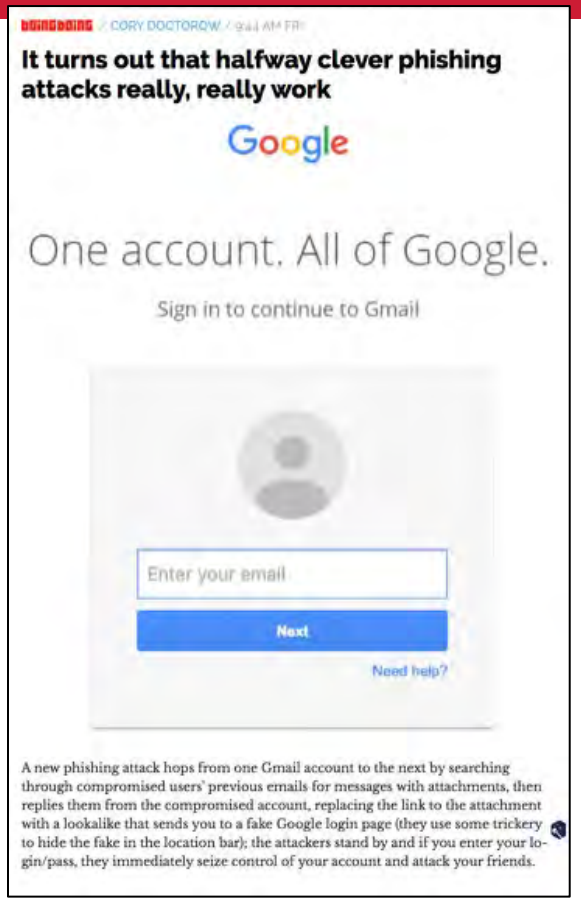


Don’t underestimate the human element

Humans are

- Bad at storing keys
- Poor at estimating risk
- Not accurate
- Careless
- Gullible

https://xkcd.com/1777/



Social engineering is the top threat

But don’t blame the user

It’s not the user’s fault if they click on a link and it infects their system. It’s not their fault if they plug in a strange USB drive or ignore a warning message that they can’t understand.

It’s not even their fault if they get fooled by a look-alike bank website and lose their money.

The problem is that we’ve designed these systems to be so insecure that regular, nontechnical people can’t use them with confidence.

We’re using security awareness campaigns to cover up bad system design.

— Bruce Schneier, May 28, 2025

https://www.darkreading.com/cybersecurity-operations/why-take9-will-not-improve-cybersecurity

Examples:
A few recent security attacks

British Museum forced to partly close following cyberattack by ex-worker

techradar

A disgruntled employee cyberattack meant some exhibits had to close

Benedict Collins • January 27, 2025

A former employee of the British Museum has been arrested on suspicion of burglary and criminal damage after allegedly performing an on-site cyberattack which shut down exhibits for several days.

“An IT contractor who was dismissed last week trespassed into the museum and shut down several of our systems. Police attended and he was arrested at the scene,” a spokesperson for the British Museum said.

The former contractor’s actions caused the ticketing system for the museum to cease functioning, leading to exhibits only being open to pre-booked bookings and members.

Insider threat + bad policies when insiders become outsiders

https://www.techradar.com/pro/security/british-museum-forced-to-partly-close-following-cyberattack-by-ex-worker

Cyberattack on American Water: A warning to critical infrastructure

Security Intelligence

Jonathan Reed • November 4, 2024

American Water, the largest publicly traded United States water and wastewater utility, recently experienced a cybersecurity incident that forced the company to disconnect key systems, including its customer billing platform. As the company's investigation continues, there are growing concerns about the vulnerabilities that persist in the water sector, which has increasingly become a target for cyberattacks.

The breach is a stark reminder of the critical infrastructure risks that have long plagued the industry. While the water utility has confirmed that its operations and water quality were not affected, American Water's shutdown of its billing system and customer portal highlights the critical intersection between operational technology (OT) and information technology (IT) vulnerabilities in essential services.

Real-world infrastructure

https://securityintelligence.com/news/cyberattack-on-american-water-warning-critical-infrastructure/

Major Backdoor in Millions of RFID Cards Allows Instant Cloning

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

A significant backdoor in contactless cards made by China-based Shanghai Fudan Microelectronics allows instantaneous cloning of RFID cards used to open office doors and hotel rooms around the world.

Ryan Naraine • August 20, 2024

French security services firm Quarkslab has made an eye-popping discovery: a significant backdoor in millions of contactless cards made by Shanghai Fudan Microelectronics Group, a leading chip manufacturer in China.

The backdoor, documented in a research paper by Quarkslab researcher Philippe Teuwen, allows the instantaneous cloning of RFID smart cards used to open office doors and hotel rooms around the world.

Although the backdoor requires just a few minutes of physical proximity to an affected card to conduct an attack, an attacker in a position to carry out a supply chain attack could execute such attacks instantaneously at scale, Teuwen explained in the paper.

...

Security vulnerabilities that allow "card-only" attacks (attacks that require access to a card but not the corresponding card reader) are of particular concern as they may enable attackers to clone cards, or to read and write their content, just by having physical proximity for a few minutes.

https://www.securityweek.com/major-backdoor-in-millions-of-rfid-cards-allows-instant-cloning/

Microsoft macOS Apps Vulnerability Allows Hackers to Record Audio/Video

Cyber Security News

Balaji N • August 19, 2024

Cisco Talos has identified eight security vulnerabilities in Microsoft applications running on the macOS operating system, raising concerns about potential exploitation by adversaries.

These vulnerabilities, if exploited, could allow attackers to hijack the permissions and entitlements of Microsoft applications, leading to unauthorized access to sensitive resources such as microphones, cameras, and user data.

...

Cisco Talos discovered that these Microsoft applications could be manipulated to bypass this permission model, allowing attackers to use existing app permissions without user verification.

...

All these apps are vulnerable to library injection attacks because they have the com.apple.security.cs.disable-library-validation entitlement set to true, allowing an attacker to inject any library and run arbitrary code within the compromised application.

https://cybersecuritynews.com/microsoft-macos-apps-vulnerability/

Unpatchable 0-day in surveillance cam is being exploited to install Mirai

ars technica

Vulnerability is easy to exploit and allows attackers to remotely execute commands.

Dan Goodin • August 28, 2024

Malicious hackers are exploiting a critical vulnerability in a widely used security camera to spread Mirai, a family of malware that wrangles infected Internet of Things devices into large networks for use in attacks that take down websites and other Internet-connected devices.

The attacks target the AVM1203, a surveillance device from Taiwan-based manufacturer AVTECH, network security provider Akamai said Wednesday. Unknown attackers have been exploiting a 5-year-old vulnerability since March. The zero-day vulnerability, tracked as CVE-2024-7029, is easy to exploit and allows attackers to execute malicious code. The AVM1203 is no longer sold or supported, so no update is available to fix the critical zero-day.

Akamai said that the attackers are exploiting the vulnerability so they can install a variant of Mirai, which arrived in September 2016 when a botnet of infected devices took down cybersecurity news site Krebs on Security. Mirai contained functionality that allowed a ragtag army of compromised webcams, routers, and other types of IoT devices to wage distributed denial-of-service attacks of record-setting sizes.

https://arstechnica.com/security/2024/08/unpatchable-0-day-in-surveillance-cam-is-being-exploited-to-install-mirai/

Unpatchable vulnerability in Apple chip leaks secret encryption keys

Fixing newly discovered side channel will likely take a major toll on performance

Dan Goodin • March 21, 2024

A newly discovered vulnerability baked into Apple's M-series of chips allows attackers to extract secret keys from Macs when they perform widely used cryptographic operations, academic researchers have revealed in a paper published Thursday.

The flaw—a side channel allowing end-to-end key extractions when Apple chips run implementations of widely used cryptographic protocols—can't be patched directly because it stems from the microarchitectural design of the silicon itself. Instead, it can only be mitigated by building defenses into third-party cryptographic software that could drastically degrade M-series performance when executing cryptographic operations, particularly on the earlier M1 and M2 generations. The vulnerability can be exploited when the targeted cryptographic operation and the malicious application with normal user system privileges run on the same CPU cluster.

The threat resides in the chips' data memory-dependent prefetcher, a hardware optimization that predicts the memory addresses of data that running code is likely to access in the near future. By loading the contents into the CPU cache before it's actually needed…

https://arstechnica.com/security/2024/03/hackers-can-extract-secret-encryption-keys-from-apples-mac-chips/

Plane English: Sea-Tac Airport turns to pen and pap to replace digital displays after cyberattack

GeekWire

Taylor Soper • August 28, 2024

Pen and paper to the rescue.

The photo above illustrates what life has been like at Sea-Tac Airport this week in the aftermath of a suspected cyberattack on the Port of Seattle that sparked an outage Saturday and continued through Wednesday.

The outage impacted many digital displays throughout Sea-Tac Airport, including information about flight times and where arriving passengers can find their luggage.

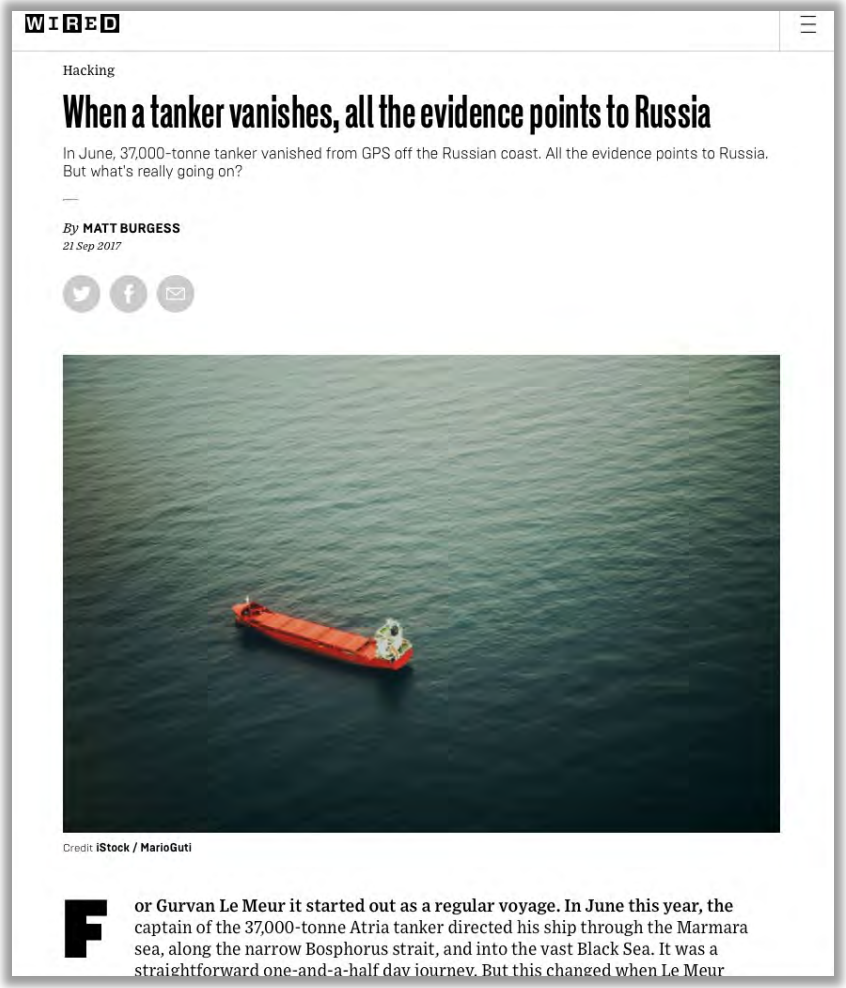
https://www.geekwire.com/2024/sea-tac-airport-resorts-to-handwritten-posters-to-replace-digital-displays-in-aftermath-of-cyberattack/

Some more things to worry about

2017 – GPS hacking

Multiple global navigation satellite systems (GNSS) are deployed:

- US: GPS
- Europe: Galileo
- Russia: GLONASS
- China BeiDou



WIRED

Hacking

When a tanker vanishes, all the evidence points to Russia

In June, 37,000-tonne tanker vanished from GPS off the Russian coast. All the evidence points to Russia. But what's really going on?

By **MATT BURGESS**
21 Sep 2017

Credit **iStock / MarioGuti**

For Gurvan Le Meur it started out as a regular voyage. In June this year, the captain of the 37,000-tonne Atria tanker directed his ship through the Marmara sea, along the narrow Bosphorus strait, and into the vast Black Sea. It was a straightforward one-and-a-half day journey. But this changed when Le Meur

Ukraine Is Spoofing Russian Drones Out Of The Sky

Forbes

David Hambling • April 21, 2023

A new type of electronic warfare is bringing Russian drones crashing to the ground by fooling their guidance systems.

Radio-frequency jamming has become ubiquitous in Ukraine as both sides seek to prevent the other from using drones. Typically two type of electronic warfare are employed: generating radio noise to interfere with the control signal, making it impossible to pilot the drone, and blasting interference on GPS frequencies so the drone's satellite navigation fails. Now a third technique has been observed: navigation spoofing.

...

The operators eventually figured out what was going on. The drones had been fooled into thinking they were in a no-fly zone, and had ceased operating. Drone makers like DJI and others employ a method known as geofencing to ensure their drones are not flown in prohibited areas such as around airports: a virtual fence surrounds every defined no-fly zone and the drone will not fly inside it. Ukrainian electronic warfare had tricked the Russian drones into crashing.

https://www.forbes.com/sites/davidhambling/2023/04/21/ukraine-is-spoofing-russian-drones-out-of-the-sky/

Plane carrying EU’s top leader targeted by alleged Russian GPS jamming

Ivana Kottasová • September 1, 2025

A plane carrying the European Commission President Ursula von der Leyen was targeted by GPS navigation jamming while trying to land inBulgaria on Sunday, a spokesperson for the commission told CNN.

The commission received “information from Bulgarian authorities that they suspect this blatant interference was carried out by Russia,” said European Commission Deputy Chief Spokesperson Arianna Podestà.

The Kremlin has denied the allegation, with Russian foreign ministry spokeswoman Maria Zakharova saying claims of Moscow’s involvement were “fake,” calling it “paranoia” from Europe during a press conference on Thursday.

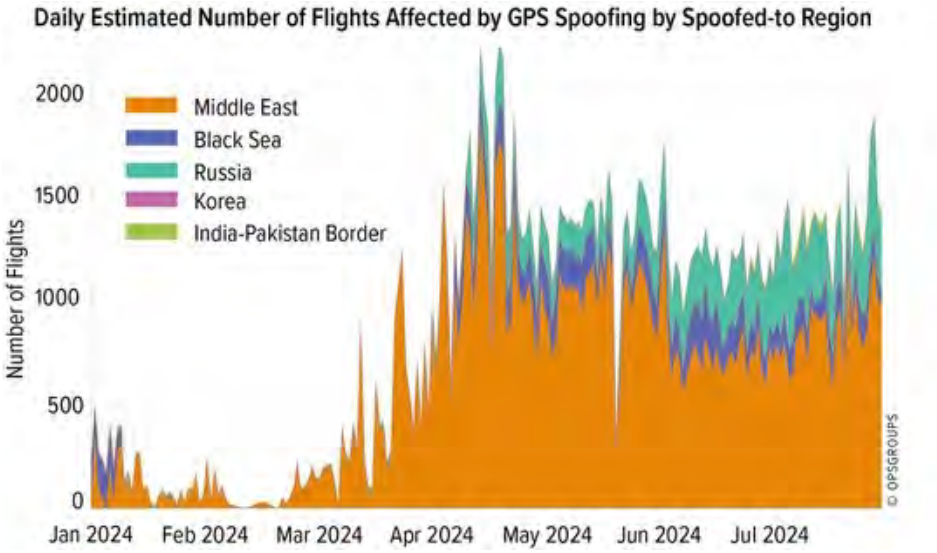
The plane landed safely, the European Commission spokesperson said. A source familiar with the situation told CNN the pilots landed the plane using paper maps.

https://www.cnn.com/2025/09/01/world/plane-ursula-von-der-leyen-intl

GPS attacks on the rise: jamming & spoofing

- **500% increase by the end of 2024**
  - Average of 300 flights per day affected in Q1/Q2 2024
  - Average of 1500 flights per day affected in by the end of the year
- **Mostly because of wide-area GPS attacks in conflict zones:**
  - Eastern Europe, Mideast, South China Sea
  - North Korea disrupted GPS signals along the South Korea border for at least 10 days in Nov. 2024

The Swedish Transport Agency (STA) recorded 733 incidents through August in 2025, up from 55 across the whole of 2023.

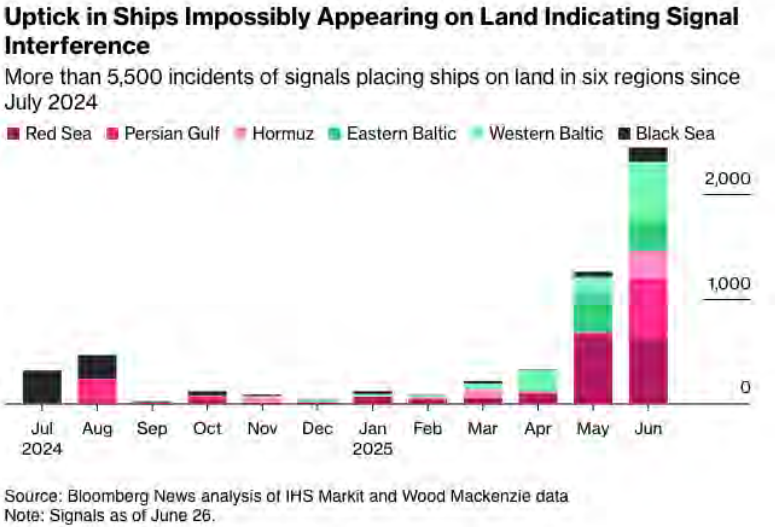


Source: https://ops.group/dashboard/wp-content/uploads/2024/09/GPS-Spoofing-Technical-Guide-WG2024-OG2.pdf
https://www.bbc.com/news/articles/clyx3ly54veo

GPS attacks on the rise: jamming & spoofing

Israel-Iran war – June 2025

- **Iran's communications ministry confirmed deliberate GPS jamming**
  - Exploring switching to alternative systems, like China's BeiDou
- **Impacted navigation of an average of 972 ships daily in the Persian Gulf & Gulf of Oman**
  - June 17, 2026: two oil tankers collided in the Gulf of Oman, possibly due to GPS jamming
- **Also affected terrestrial navigation apps, like Waze**

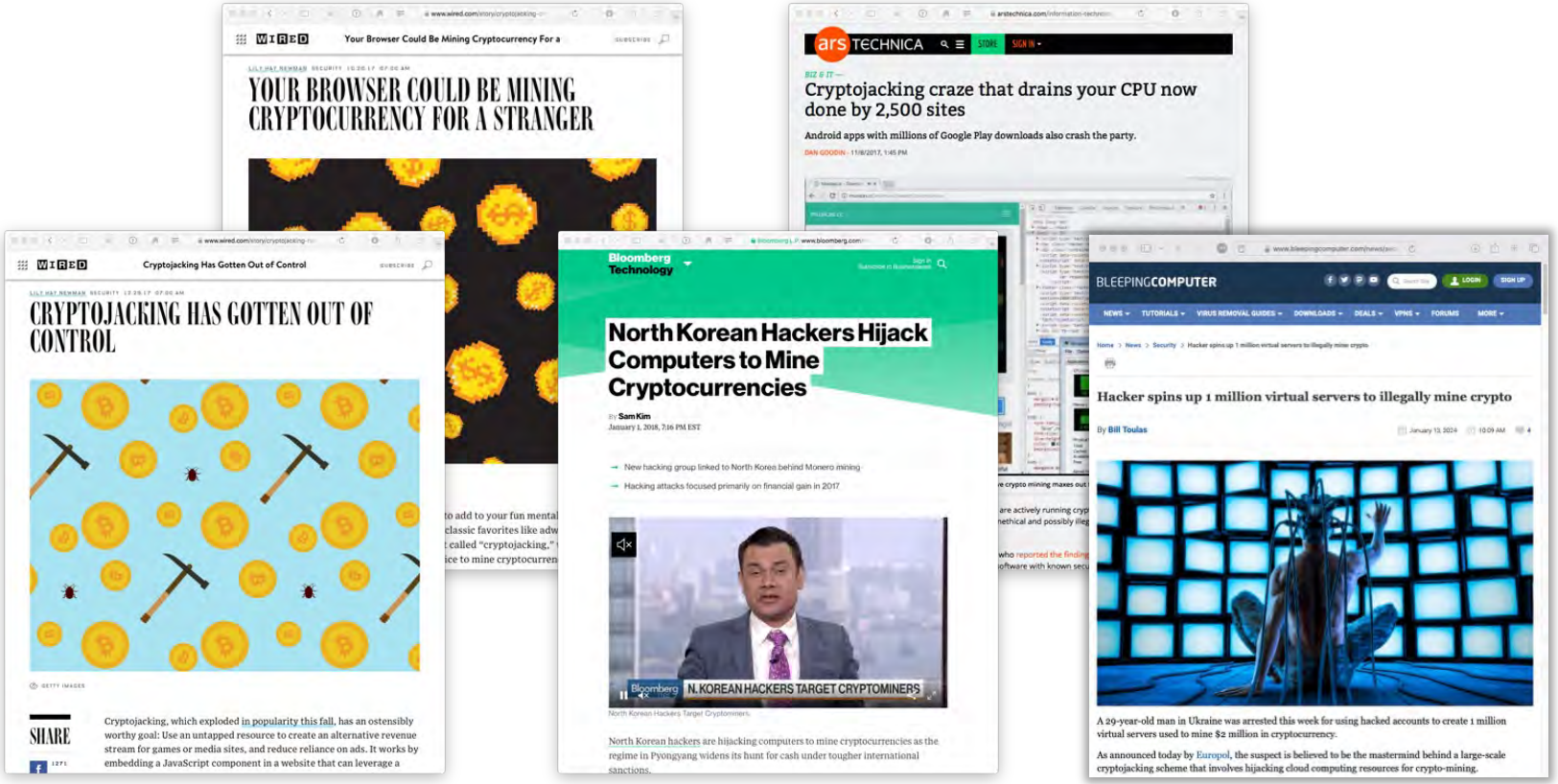


https://www.bloomberg.com/news/features/2025-06-29/iran-israel-conflict-worsens-global-shipping-navigation-problems

https://www.iranintl.com/en/202507149948

https://www.steptoe.com/en/news-publications/stepwise-risk-outlook/gps-jamming-during-israel-iran-war-demonstrates-risks-to-civilian-operations.html

Fall 2018-now – Cryptojacking



Supercomputers hacked across Europe to mine cryptocurrency

Confirmed infections have been reported in the UK, Germany, and Switzerland. Another suspected infection was reported in Spain.

Catalin Cimpanu • May 16, 2020

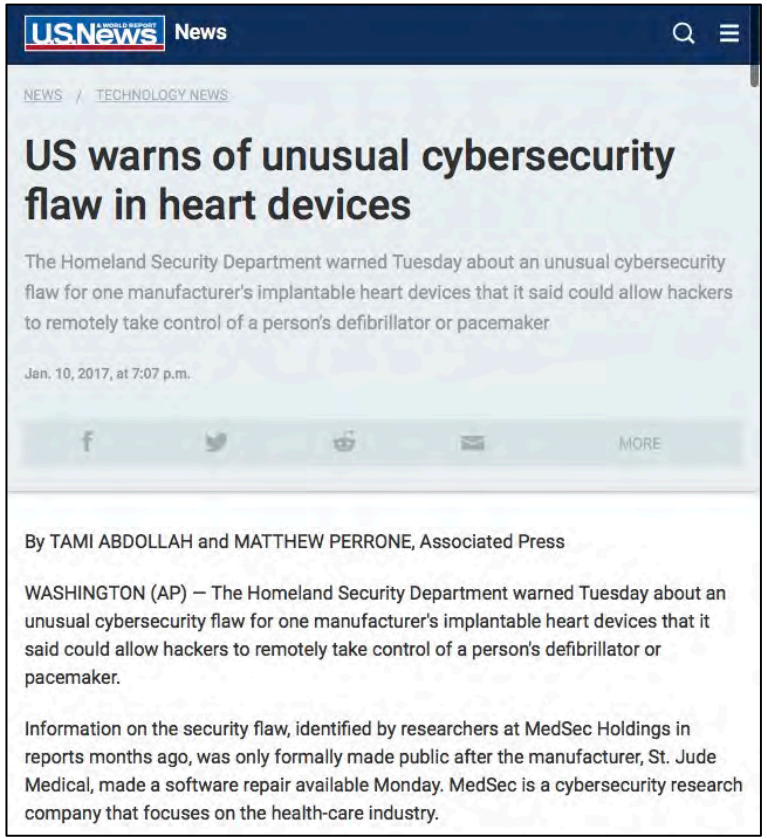
Multiple supercomputers across Europe have been infected this week with cryptocurrency mining malware and have shut down to investigate the intrusions.

Security incidents have been reported in the UK, Germany, and Switzerland, while a similar intrusion is rumored to have also happened at a high-performance computing center located in Spain.

The first report of an attack came to light on Monday from the University of Edinburgh, which runs the ARCHER supercomputer. The organization reported "security exploitation on the ARCHER login nodes," shut down the ARCHER system to investigate, and reset SSH passwords to prevent further intrusions.

https://www.zdnet.com/article/supercomputers-hacked-across-europe-to-mine-cryptocurrency/

Medical devices: potential for physical harm



U.S.News News

NEWS / TECHNOLOGY NEWS

US warns of unusual cybersecurity flaw in heart devices

The Homeland Security Department warned Tuesday about an unusual cybersecurity flaw for one manufacturer's implantable heart devices that it said could allow hackers to remotely take control of a person's defibrillator or pacemaker

Jan. 10, 2017, at 7:07 p.m.

MORE

By TAMI ABDOLLAH and MATTHEW PERRONE, Associated Press

WASHINGTON (AP) — The Homeland Security Department warned Tuesday about an unusual cybersecurity flaw for one manufacturer's implantable heart devices that it said could allow hackers to remotely take control of a person's defibrillator or pacemaker.

Information on the security flaw, identified by researchers at MedSec Holdings in reports months ago, was only formally made public after the manufacturer, St. Jude Medical, made a software repair available Monday. MedSec is a cybersecurity research company that focuses on the health-care industry.

Their research discovered 993 vulnerabilities within 966 medical products and devices, revealing a 59% increase from 2022. The majority of these vulnerabilities, 64%, were found in software, while 16% have been weaponized.

– 2023 State of Cybersecurity for Medical Devices and Healthcare Systems

https://www.nature.com/articles/s41598-023-45927-1

Medical devices: potential for physical harm

A 2023 Claroty study found:

- 63% of known exploited vulnerabilities can be found on health networks
- 23% of medical devices have at least one known exploited vulnerability
- 14% of connected medical devices are running an unsupported or end-of-life operating system
  - 1/3 of these are imaging devices, including X-ray and MRI systems
  - 23% of IoT devices and 20% of hospital IT systems running legacy systems that can have vulnerabilities with no supported patches
- Remotely accessible:
  66% of imaging devices, 54% of surgical devices, and 40% of patient devices

https://claroty.com/resources/reports/state-of-cps-security-report-healthcare-2023

https://shorturl.at/1wBIC

New Bluetooth hack can unlock your Tesla—and all kinds of other devices

ars technica

All it takes to hijack Bluetooth-secured devices is custom code and $100 in hardware.

Dan Goodin • May 18, 2022

When you use your phone to unlock a Tesla, the device and the car use Bluetooth signals to measure their proximity to each other. Move close to the car with the phone in hand, and the door automatically unlocks. Move away, and it locks. This proximity authentication works on the assumption that the key stored on the phone can only be transmitted when the locked device is within Bluetooth range.

Now, a researcher has devised a hack that allows him to unlock millions of Teslas—and countless other devices—even when the authenticating phone or key fob is hundreds of yards or miles away. The hack, which exploits weaknesses in the Bluetooth Low Energy standard adhered to by thousands of device makers, can be used to unlock doors, open and operate vehicles, and gain unauthorized access to a host of laptops and other security-sensitive devices.

...

This class of hack is known as a relay attack, a close cousin of the person-in-the-middle attack. In its simplest form, a relay attack requires two attackers. In the case of the locked Tesla, the first attacker, which we'll call Attacker 1, is in close proximity to the car while it's out of range of the authenticating phone. Attacker 2, meanwhile, is in close proximity to the legitimate phone used to unlock the vehicle. Attacker 1 and Attacker 2 have an open Internet connection that allows them to exchange data.

https://arstechnica.com/information-technology/2022/05/new-bluetooth-hack-can-unlock-your-tesla-and-all-kinds-of-other-devices/

Subaru Security Flaws Exposed Its System for Tracking Millions of Cars

WIRED

Now-fixed web bugs allowed hackers to remotely unlock and start millions of Subarus. More disturbingly, they could also access at least a year of cars' location histories—and Subaru employees still can.

Andy Greenberg • January 23, 2025

About a year ago, security researcher Sam Curry bought his mother a Subaru, on the condition that, at some point in the near future, she let him hack it.

It took Curry until last November, when he was home for Thanksgiving, to begin examining the 2023 Impreza's internet-connected features and start looking for ways to exploit them. Sure enough, he and a researcher working with him online, Shubham Shah, soon discovered vulnerabilities in a Subaru web portal that let them hijack the ability to unlock the car, honk its horn, and start its ignition, reassigning control of those features to any phone or computer they chose.

Most disturbing for Curry, though, was that they found they could also track the Subaru's location—not merely where it was at the moment but also where it had been for the entire year that his mother had owned it.

https://www.wired.com/story/subaru-location-tracking-vulnerabilities/

Hack-backs and shutdowns

Attacking the attackers

Hacking against the hackers

Cops Hijack Botnet, Remotely Wipe Malware From 850,000 Computers

Police in France took down a large cryptocurrency-mining malware operation with the help of a cybersecurity firm.

By Lorenzo Franceschi-Bicchierai • Aug 28 2019, 4:10pm

French police, with help from an antivirus firm, took control of a server that was used by cybercriminals to spread a worm programmed to mine cryptocurrency from more than 850,000 computers. Once in control of the server, the police remotely removed the malware from those computers.

https://www.vice.com/en_us/article/wjwd7x/cops-hijack-retadup-botnetwipe-malware-from-850000-computers

A ransomware gang shut down after Cybercom hija its site and it discovered it had been hacked

The Washington Post

Ellen Nakashima, Dalton Bennett • November 3, 2021

A major overseas ransomware group shut down last month after a pair of operations by U.S. Cyber Command and a foreign government targeting the criminals' servers left its leaders too frightened of identification and arrest to stay in business, according to several U.S. officials familiar with the matter.

The foreign government hacked the servers of REvil this summer, but the Russian-speaking criminal group did not discover it was compromised until Cybercom last month blocked its website by hijacking its traffic, said the officials who spoke on the condition of anonymity because of the matter's sensitivity.

Cybercom's action was not a hack or takedown, but it deprived the criminals of the platform they used to extort their victims — businesses, schools and others whose computers they'd locked up with data-encrypting malware and from whom they demanded expensive ransoms to unlock the machines, the officials said.

In the hours after the Cybercom operation, which has not been previously reported, one of REvil's leaders saw the site's traffic had been redirected.

"Domains hijacked from REvil," wrote 0_neday, an REvil leader, on a Russian-language forum popular with cyber criminals, on Oct. 17.

https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html

For six months, security researchers have secretly distributed an Emotet vaccine across the world

Binary Defense researchers have identified a bug in the Emotet malware and have been using it to prevent the malware from making new victim

Catalin Cimpanu • August 14, 2020

Most of the time, fighting malware is a losing game. Malware authors create their code, distribute payloads to victims via various methods, and by the time security firms catch up, attackers make small changes in their code to quickly regain their advantage in secrecy. ...

However, not all malware operations can be hurt this way. Some cyber-criminals either reside in countries that don't extradite their citizens or have a solid knowledge of what they're doing.

Emotet is one of the gangs that check both boxes. Believed to operate from the territories of the former Soviet States, Emotet is also one of today's most skilled malware groups, having perfected the infect-and-rent-access scheme like no other group.

The malware, which was first seen in 2014, evolved from an unimportant banking trojan into a malware swiss-army knife that, once it infects victims, it spreads laterally across their entire network, pilfers any sensitive data, and turns around and rents access to the infected hosts to other groups.

https://www.zdnet.com/article/for-six-months-security-researchers-have-secretly-distributed-an-emotet-vaccine-across-the-world/

FBI Shuts Down Botnet Run by Beijing-Backed Hackers That Hijacked Over 200,000 Devices

GIZMODO

"The government's malware disabling commands, which interacted with the malware's native functionality, were extensively tested prior to the operation," according to the DOJ.

Matt Novak • September 19, 2024

U.S. authorities have dismantled a massive botnet run by hackers backed by the Chinese government, according to a speech given by FBI director Christopher Wray on Wednesday. The botnet malware infected a number of different types of internet-connected devices around the world, including home routers, cameras, digital video recorders, and NAS drives. Those devices were used to help infiltrate sensitive networks related to universities, government agencies, telecommunications providers, and media organizations.

https://gizmodo.com/fbi-shuts-down-botnet-run-by-beijing-backed-hackers-that-hijacked-over-200000-devices-2000500627

The End