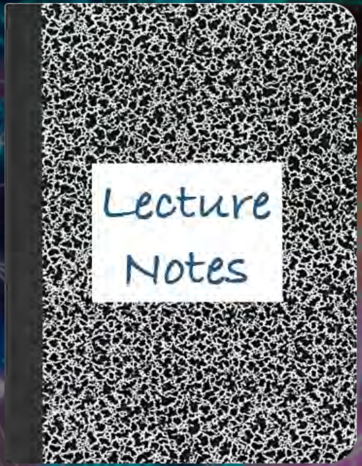


CS 419: Computer Security

Week 1: Part 1

Introduction

Paul Krzyzanowski

What is security?

security

noun se·cu·ri·ty \si-ˈkyu̇r-ə-tē\

the quality or state of being secure: such as

a **:** freedom from danger **:** safety

b **:** freedom from fear or anxiety

c **:** freedom from the prospect of being laid off
<job *security*>

What is computer security?

Keeping systems, programs, and data “safe”

The CIA Triad[*]:

1. **Confidentiality**
2. **Integrity**
3. **Availability**

[*]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 other's 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
Secrecy: hide the existence of information

Privacy is increasingly harder to attain

- **“Free” services**
  - Facebook, Google, X, LinkedIn, Instagram, TikTok, …
  - Information collection, browser cookies to track web access
- **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*

This can be both good and bad

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 espionage:**
  - Strategy, schedules, employees, 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

Some 2024 Breaches

- **National Public Data (NPD) — 2.9 billion records**
- **Financial Business and Consumer Solutions (FBCS) — 4.2 million records**
- **Ticketmaster — 560 million records**
- **Change Healthcare – 190 million records**
  (largest breach of medical data in U.S. history – months of outages)
- **AT&T — 110 million records**
- **Dell — 49 million records**
- **Snowflake** (May): Exposed customer data due to weak authentication.
  Affected customers included AT&T, Lending Tree, Santander Group, Ticketmaster, and Advance Auto Parts.

Some 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 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

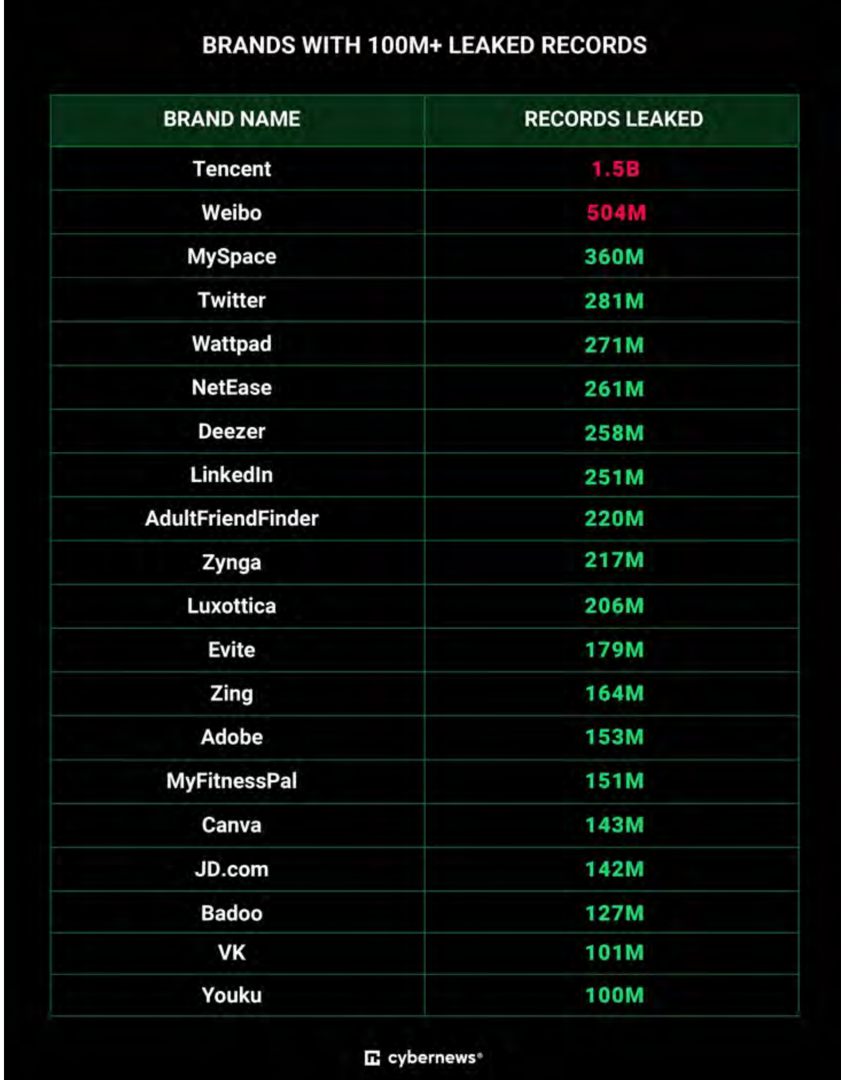
cybernews

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/



BRANDS WITH 100M+ LEAKED RECORDS

BRAND NAME	RECORDS LEAKED
Tencent	1.5B
Weibo	504M
MySpace	360M
Twitter	281M
Wattpad	271M
NetEase	261M
Deezer	258M
LinkedIn	251M
AdultFriendFinder	220M
Zynga	217M
Luxottica	206M
Evite	179M
Zing	164M
Adobe	153M
MyFitnessPal	151M
Canva	143M
JD.com	142M
Badoo	127M
VK	101M
Youku	100M

cybernews®

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!

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

Sometimes it’s human error

Bill Toulas • December 30, 2021

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/

Baltic Sea data cable damaged in latest case of potential sabotage

FINANCIAL TIMES

Disruption of line between Sweden and Latvia follows earlier incidents linked to Russia and China

Richard Milne • January 26, 2025

An underwater data cable between Sweden and Latvia was damaged early on Sunday, in at least the fourth episode of potential sabotage in the Baltic Sea that has caused concern in Nato about the vulnerability of critical infrastructure.

Latvian Prime Minister Evika Siliņa said damage to the cable between the Latvian coastal town of Ventspils and Fårösund on the Swedish island of Gotland was significant and thus was probably caused by an external force.

Criminal investigations have started in Latvia and Sweden, according to Swedish prosecutors, and the Malta-flagged Vezhen has been seized as part of the probes. Previous incidents have been linked to Russian and Chinese ships.

Ulf Kristersson, Sweden's prime minister, said that "at least one" data cable had been damaged and that he had been in touch with Siliņa, and was co-operating closely with Nato.

https://www.ft.com/content/b8765ad0-3e72-41b8-9915-da86b25de033

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

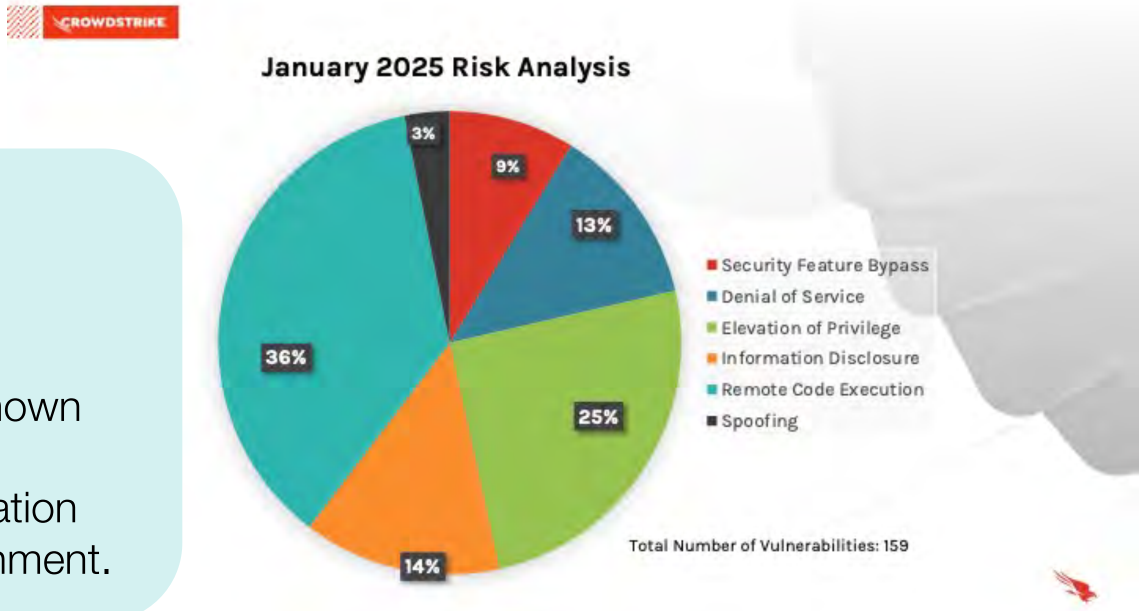
The human factor

- People make mistakes: coding, configuration, usage

Microsoft's January 2025 Patch Tuesday:
10 Critical Vulnerabilities and Eight Zero-Days Among 159 CVEs

January 14, 2025

- 132 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.

Examples:
A few recent security attacks

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

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

SecurityIntelligence

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

arstechnica

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

arstechnica

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 paper to replace digital displays after cyberattack

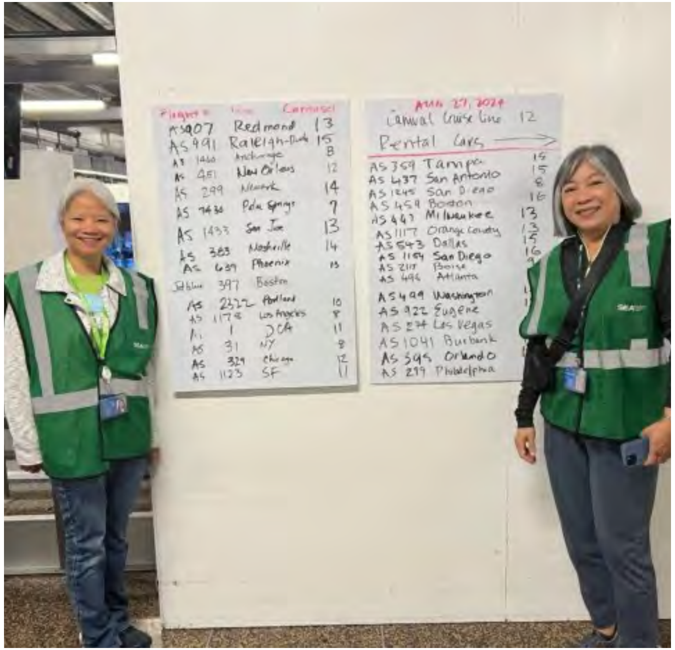
GeekWire

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.



Flight #	[illegible]	Carousel
AS907	Redmond	13
AS491	Raleigh-Durh	15
AS 1460	Anchorage	8
AS 451	New Orleans	12
AS 299	Newark	14
AS 7438	Palm Springs	7
AS 1433	San Jose	13
AS 383	Nashville	14
AS 639	Phoenix	13
Jetblue 397	Boston	
AS 2322	Portland	10
AS 1178	Los Angeles	8
AA 1	DCA	11
AS 31	NY	8
AS 329	Chicago	12
AS 1123	SF	11

AUG 27, 2024

Carnival Cruise Line 12

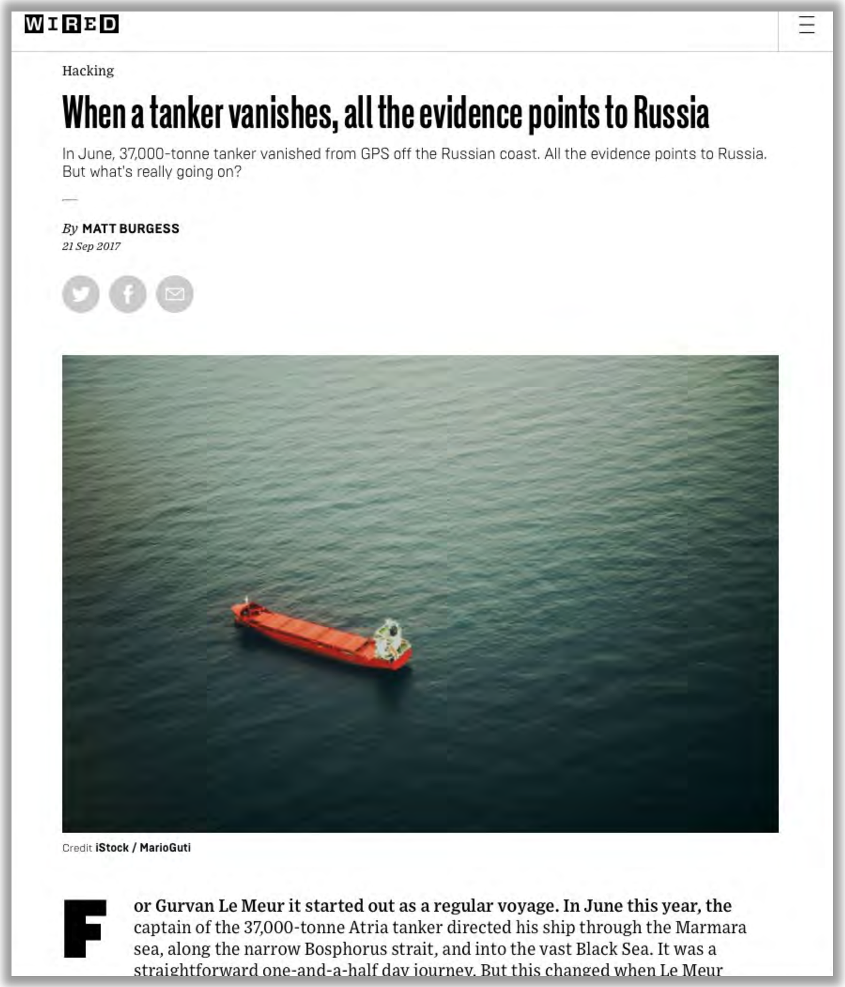
Rental Cars →

AS 359	Tampa	15
AS 437	San Antonio	15
AS 1245	San Diego	8
AS 459	Boston	16
AS 447	Milwaukee	13
AS 1117	Orange County	13
AS 543	Dallas	15
AS 1154	San Diego	16
AS 2117	Boise	9
AS 496	Atlanta	
AS 499	Washington	
AS 922	Eugene	
AS 274	Las Vegas	
AS 1041	Burbank	
AS 595	Orlando	
AS 219	Philadelphia	

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



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.

…

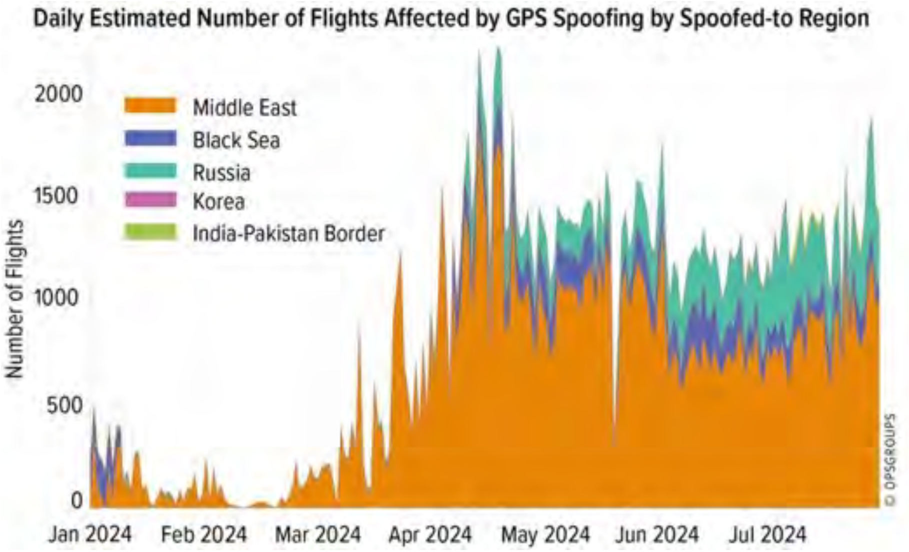
The operators eventually figured out what was going on. The drones had been fooled into thinking they were in a no-fly zone, and had ceased operating. Drone makers like DJI and others employ a method known as geofencing to ensure their drones are not flown in prohibited areas such as around airports: 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/

GPS attacks on the rise: jamming & spoofing

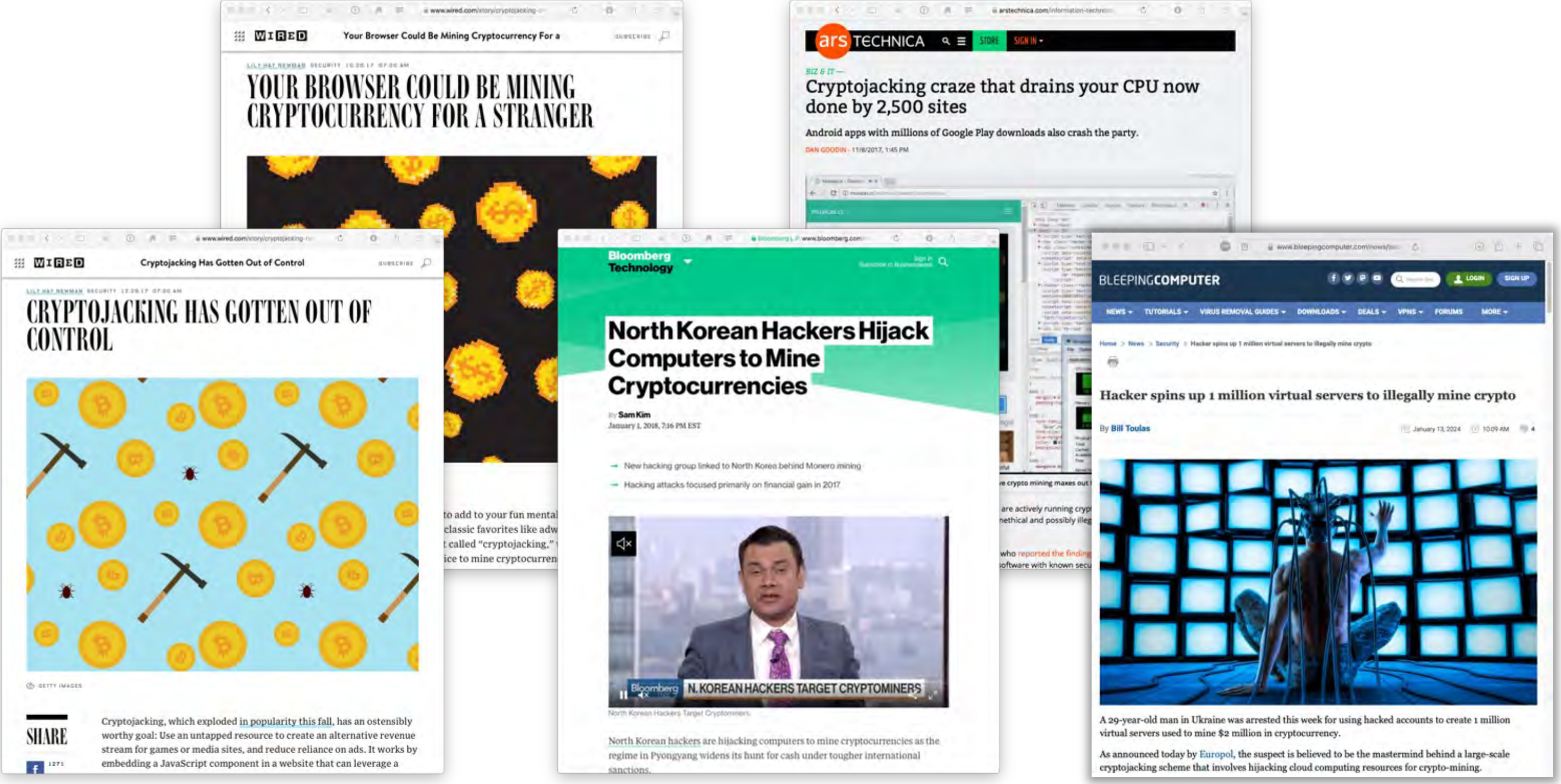
- **500% increase by the end of 2024**
  - Average of 300 flights per day affected in Q1/Q2 2024
  - Average of 1500 flights per day affected in by the end of the year

- **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



Source: https://ops.group/dashboard/wp-content/uploads/2024/09/GPS-Spoofing-Technical-Guide-WG2024-OG2.pdf

Fall 2018-now – Cryptojacking



www.wired.com/story/cryptojacking-

WIRED — Your Browser Could Be Mining Cryptocurrency For a

LILY HAY NEWMAN SECURITY 10.20.17 07:00 AM

YOUR BROWSER COULD BE MINING CRYPTOCURRENCY FOR A STRANGER

to add to your fun mental
classic favorites like adw
t called "cryptojacking,"
ice to mine cryptocurren

arstechnica.com/information-techno

ars TECHNICA — STORE — SIGN IN

BIZ & IT —

Cryptojacking craze that drains your CPU now done by 2,500 sites

Android apps with millions of Google Play downloads also crash the party.

DAN GOODIN - 11/8/2017, 1:45 PM

e crypto mining maxes out

are actively running cryp
nethical and possibly illeg

who reported the finding
oftware with known secu

www.wired.com/story/cryptojacking-

WIRED — Cryptojacking Has Gotten Out of Control

LILY HAY NEWMAN SECURITY 12.26.17 07:00 AM

CRYPTOJACKING HAS GOTTEN OUT OF CONTROL

GETTY IMAGES

SHARE

1271

Cryptojacking, which exploded in popularity this fall, has an ostensibly worthy goal: Use an untapped resource to create an alternative revenue stream for games or media sites, and reduce reliance on ads. It works by embedding a JavaScript component in a website that can leverage a

Bloomberg L.P. www.bloomberg.com

Bloomberg Technology

North Korean Hackers Hijack Computers to Mine Cryptocurrencies

By Sam Kim
January 1, 2018, 7:16 PM EST

- New hacking group linked to North Korea behind Monero mining
- Hacking attacks focused primarily on financial gain in 2017

North Korean Hackers Target Cryptominers

North Korean hackers are hijacking computers to mine cryptocurrencies as the regime in Pyongyang widens its hunt for cash under tougher international sanctions.

www.bleepingcomputer.com/news/sec

BLEEPINGCOMPUTER — LOGIN — SIGN UP

NEWS — TUTORIALS — VIRUS REMOVAL GUIDES — DOWNLOADS — DEALS — VPNS — FORUMS — MORE

Home > News > Security > Hacker spins up 1 million virtual servers to illegally mine crypto

Hacker spins up 1 million virtual servers to illegally mine crypto

By Bill Toulas — January 13, 2024 — 10:09 AM — 4

A 29-year-old man in Ukraine was arrested this week for using hacked accounts to create 1 million virtual servers used to mine $2 million in cryptocurrency.

As announced today by Europol, the suspect is believed to be the mastermind behind a large-scale cryptojacking scheme that involves hijacking cloud computing resources for crypto-mining.

Supercomputers hacked across Europe to mine cryptocurrency

ZDNet

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

Catalin Cimpanu • May 16, 2020

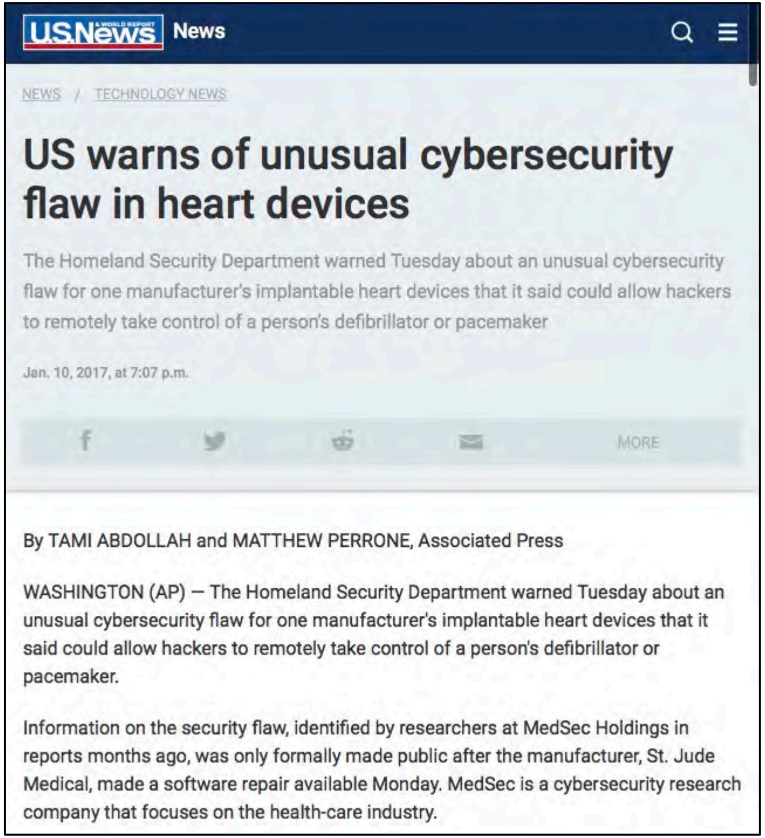
Multiple supercomputers across Europe have been infected this week with cryptocurrency mining malware and have shut down to investigate the intrusions.

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



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.

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

arstechnica

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

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.

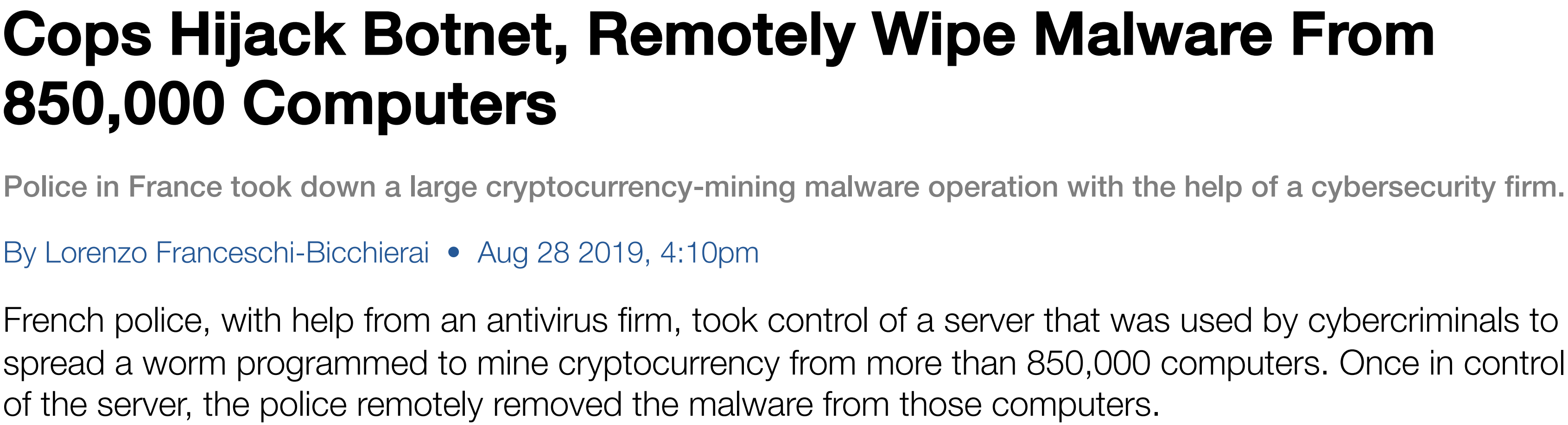
Most disturbing for Curry, though, was that they found they could also track the Subaru's location—not merely where it was at the moment but also where it had been for the entire year that his mother had owned it.

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 hijacked 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