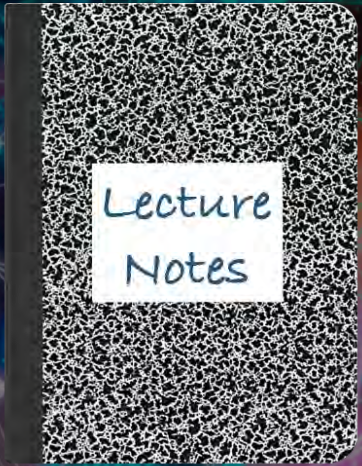


CS 419: Computer Security

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 vs. privacy

Privacy

- Limit what information can be shared with others
- Ability to send messages anonymously
- 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

Secrecy: hiding the existence of information; the ability to conceal messages or exchange messages without anyone else seeing them

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 hall 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, …

This can be 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 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

- **UNESCO adopted a Recommendation on the Ethics of AI in 2021**
  - "AI systems should not be used for social scoring or mass surveillance purposes"

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**
  - Authentication
- **System integrity**
  - The ability of a system to perform its intended function, free from deliberate or inadvertent manipulation

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

government technology

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

Thinking about security

Security is not

- 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: ~36M lines of code across 66,492 files
    - Linux kernel in 2021: 73,700 commits from 4,421 different authors
    - 3.2 million lines of new code were added and 1.3 million lines removed

Try to find the bugs!

- **Systems are complex**
  - Lots of layers: microcode + firmware + OS + libraries + apps + devices
  - Lots of elements: clients, servers, networks, embedded devices
  - Interaction with cloud services
  - Third-party components
  - Complex interaction models
  - All parts are not always under the control of one administrator
- **Human factor**
  - People make mistakes

Some big data breaches

Exfiltration

Some big data breaches

- **CAM4** – March 2020
  - Adult video site – 10.88 billion user accounts; 11 million email addresses
  - Full names, email, chat transcripts, payment logs, IP addresses
- **India Govt – Aadhaar database** – July 2023
  - 810 billion+ billion user accounts
  - Full names, chat transcripts, payment logs
- **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
- **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
- **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
  - *And 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
- **Adult Friend Finder** – October 2016
  - 412.2 million accounts from 20 years of data from six databases
  - Names, email addresses, passwords

COMB: largest breach of all time leaked online with 3.2 billion records

cybernews

Bernard Meyer • February 12, 2021

It’s being called the biggest breach of all time and the mother of all breaches: COMB, or the Compilation of Many Breaches, contains more than 3.2 billion unique pairs of cleartext emails and passwords. While many data breaches and leaks have plagued the internet in the past, this one is exceptional in the sheer size of it. To wit, the entire population of the planet is at roughly 7.8 billion, and this is about 40% of that.

However, when considering that only about 4.7 billion people are online, COMB would include the data of nearly 70% of global internet users (if each record was a unique person). For that reason, users are recommended to immediately check if their data was included in the leak. You can head over to the CyberNews personal data leak checker now.

…

So how did the COMB data leak happen?

On Tuesday, February 2, COMB was leaked on a popular hacking forum. It contains billions of user credentials from past leaks from Netflix, LinkedIn, Exploit.in, Bitcoin and more. This leak is comparable to the Breach Compilation of 2017, in which 1.4 billion credentials were leaked.

However, the current breach, known as “Compilation of Many Breaches” (COMB), contains more than double the unique email and password pairs. The data is currently archived and put in an encrypted, password-protected container.

https://cybernews.com/news/largest-compilation-of-emails-and-passwords-leaked-free/

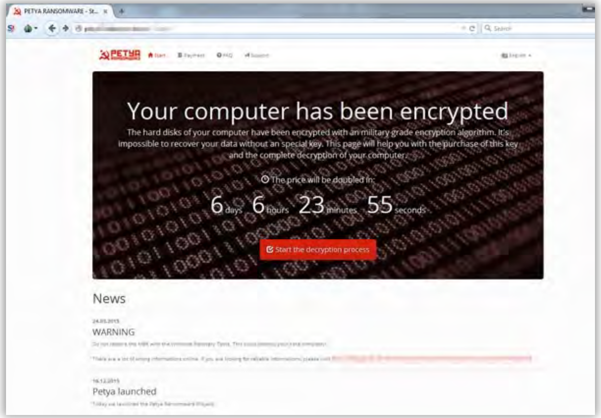
Ransomware attacks

- Colonial Pipeline – May 2021 — Stopped fuel delivery – $4.4M
- Costa Rican govt – April 2022 – shut down multiple govt systems - $30M/day
- JBS Meats – May 2021 – Stopped meat delivery – $11M
- Kronos – December 2021 – workforce mgmt software affected numerous companies
- Maersk – June 2017 – shipping company suffered ~$300M in losses – 2 weeks to recover
- Acer – March 2021 – demanded $50M
- Brenntag – chemical distribution – $4.4M
- Kaseya – IT monitoring – 800-1500 businesses – demanded $70M
- Quanta – contract manufacturing (Apple) – demanded $50M

Large-scale ransomware: 2016 – Petya

Encrypting malware that targets Microsoft Windows systems

- Ransom ~$400 & doubles after each week
- Infected millions of computers



Your computer has been encrypted

The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.

The price will be doubled in:

6 days 6 hours 23 minutes 55 seconds

News

WARNING

Petya launched

June 2017 – NotPetya – new variant of Petya launched

- Spread via software update mechanism of a Ukrainian tax preparation program
- Disguised as ransomware
- Damages estimated to be over $10 billion – Maersk was heavily hit
- Russian government blamed
  - Used EternalBlue exploit, believed to have been developed by the U.S. NSA

Just a few recent security attacks

Chinese Spies Exploited Vmware vCenter Server Vulnerability Since 2021

CVE-2023-34048, a vCenter Server vulnerability patched in October 2023, had been exploited as zero-day for a year and a half.

Ionut Arghire • January 22, 2024

The flaw, tracked as CVE-2023-34048 (CVSS score of 9.8), is an out-of-bounds write bug in VMware's implementation of the DCERPC protocol that could allow an attacker with network access to execute arbitrary code remotely.

VMware released patches for the vulnerability in October, noting that, due to the severity of the bug and the lack of workarounds, it had decided to make the fix available for product versions that reached end-of-life (EoL) status as well.

Last week, the virtualization technology company updated its advisory to warn that it was aware of in-the-wild exploitation of CVE-2023-34048, without providing specific information on the observed attacks.

On Friday, cybersecurity firm Mandiant, which is part of Google Cloud, revealed that the exploitation of CVE-2023-34048 likely started a year and a half ago, and that a sophisticated China-linked espionage group tracked as UNC3886 is responsible for it.

https://www.securityweek.com/chinese-spies-exploited-vmware-vcenter-server-vulnerability-since-2021/

A Flaw in Millions of Apple, AMD, and Qualcomm GPUs Could Expose AI Data

Patching every device affected by the LeftoverLocals vulnerability—which includes some iPhones, iPads, and Macs—may prove difficult.

Lily Hay Newman, Matt Burgess • January 16, 2024

As more companies ramp up development of artificial intelligence systems, they are increasingly turning to graphics processing unit (GPU) chips for the computing power they need to run large language models (LLMs) and to crunch data quickly at massive scale. Between video game processing and AI, demand for GPUs has never been higher, and chipmakers are rushing to bolster supply. In new findings released today, though, researchers are highlighting a vulnerability in multiple brands and models of mainstream GPUs—including Apple, Qualcomm, and AMD chips—that could allow an attacker to steal large quantities of data from a GPU's memory.

The silicon industry has spent years refining the security of central processing units, or CPUs, so they don't leak data in memory even when they are built to optimize for speed. However, since GPUs were designed for raw graphics processing power, they haven't been architected to the same degree with data privacy as a priority. As generative AI and other machine learning applications expand the uses of these chips, though, researchers from New York–based security firm Trail of Bits say that vulnerabilities in GPUs are an increasingly urgent concern.

https://www.wired.com/story/leftoverlocals-gpu-vulnerability-generative-ai/

Microsoft Executives’ Emails Hacked by Group Tied to Russian Intelligence

The New York Times

The hackers appeared to be trying to learn what the company knew about them, a regulatory filing said.

Karen Weise • January 19, 2024

An elite hacking group sponsored by Russian intelligence gained access to the emails of some of Microsoft’s senior executives beginning in late November, the company disclosed in a blog post and regulatory filing on Friday.

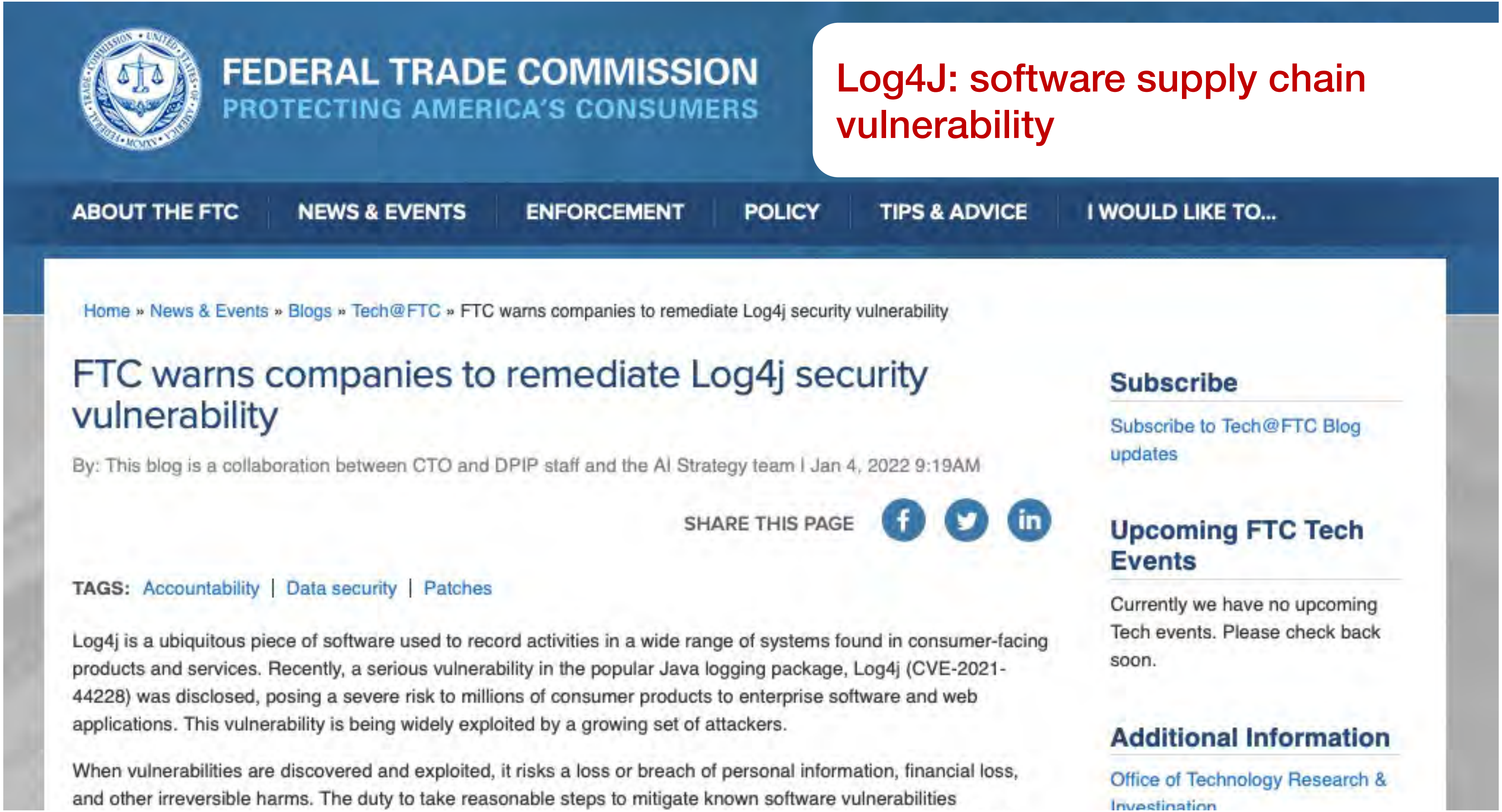
Microsoft said it had discovered the intrusion a week ago and was still investigating. The hackers appeared to focus on combing through Microsoft’s corporate email accounts to look for information related to the hacking group, which Microsoft’s researchers called Midnight Blizzard.

The hackers looked through emails from Microsoft’s senior leadership team as well as employees in cybersecurity, legal and other groups, and took some emails and attachments, the company said. The company, which had worked with cybersecurity firms and governments to investigate previous attacks by the hacking group, did not name the executives whose emails were targeted.

The Russian Foreign Intelligence Service has run the hacking group since at least 2008, according to the U.S. Cybersecurity and Infrastructure Security Agency. The group is known by a variety of nicknames, including Cozy Bear, the Dukes and A.P.T. 29, and has been behind a number of high-profile hacks, according to previous U.S. government investigations.

https://www.nytimes.com/2024/01/19/technology/microsoft-executive-emails-hacked.html

Log4J: software supply chain vulnerability



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

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

The past few days…

LoanDepot discloses that hackers breached personal data of 16 million customers

engadget

A ransomware attack against the mortgage lender slowed down the business for over a week.

Katie Malone • January 22, 2024

As mortgage lender LoanDepot continues recovery efforts from a ransomware attack, it revealed on Monday that hackers stole data from more than 16 million customers. A Securities and Exchange Commission filing from the mortgage lender did not detail what kind of information the hackers breached, only that "an unauthorized third party gained access to sensitive personal information."

LoanDepot first revealed it has fallen victim to attack on January 8. The company took some IT systems offline, but it faced a slow recovery. Customers took to social media to complain payment issues, struggles to access their accounts and even trouble closing deals on mortgages. By Friday, about two weeks since LoanDepot first came forward about the incident, systems like customer portals and other internal sites returned back online.

https://www.engadget.com/loandepot-discloses-that-hackers-breached-personal-data-of-16-million-customers-172702402.html

Backdoored Pirated Applications Targets Apple MacOS Users

Researchers warned that pirated applications have been employed to deliver a backdoor to Apple macOS users.

Pierluigi Paganini • January 22, 2024

Jamf Threat Labs researchers warned that pirated applications have been utilized to distribute a backdoor to Apple macOS users.

The researchers noticed that the apps appear similar to ZuRu malware, they allow operators to download and execute multiple payloads to compromise machines in the background.

The pirated applications discovered by Jamf Threat Labs are being hosted on Chinese pirating websites.

During their investigation, the researchers detected an executable name .fseventsd. The executable attempts to avoid detection by starting with a period and using the name of a process built into the operating system. It's not signed by Apple, however, at the time of the research it was not detected by any anti-virus on VirusTotal.

https://securityaffairs.com/157835/malware/backdoored-pirated-applications-targets-macos.html

Subway Data Breach: LockBit Ransomware Gang Claims Responsibility

THE CYBER EXPRESS BY CYBLE®

The Subway data breach announcement from the threat actor was made public through a post on its Tor data leak site.

Ashish Khaitan • January 22, 2024

The renowned American multinational fast-food chain, Subway, finds itself in an alleged cyber catastrophe. The LockBit ransomware gang has asserted responsibility for the Subway data breach, targeting the internal database, and leading to the compromise of sensitive information, including employee salaries, franchise royalty payments, master franchise commission payments, restaurant turnovers, and more.

The Subway data breach announcement from the threat actor was made public through a post on its Tor data leak site, setting a deadline for action: “Deadline: 02 Feb 2024 21:44:16 UTC.”

The message implies a significant security lapse on Subway’s part, accusing the sandwich giant of downplaying the severity of the situation.

https://thecyberexpress.com/subway-data-breach/

Google: Russian FSB hackers deploy new Spica backdoor malware

BLEEPINGCOMPUTER

Sergiu Gatlan • January 18, 2024

Google says the ColdRiver Russian-backed hacking group is pushing previously unknown backdoor malware using payloads masquerading as a PDF decryption tool.

The attackers send PDF documents that seem to be encrypted via phishing emails impersonating individuals affiliated with their targets (a tactic first observed in November 2022).

When the recipients reply that they can't read the 'encrypted' documents, they're sent a link to download what looks like a PDF decryptor executable (named Proton-decrypter.exe) to view the contents of the lure documents.

"COLDRIVER presents these documents as a new op-ed or other type of article that the impersonation account is looking to publish, asking for feedback from the target. When the user opens the benign PDF, the text appears encrypted," Google TAG said.

However, even though this fake decryption software will display a decoy PDF document, it will backdoor the victims' devices using a malware strain dubbed Spica by security researchers with Google's Threat Analysis Group (TAG), who spotted the attacks.

https://www.bleepingcomputer.com/news/security/google-russian-fsb-hackers-deploy-new-spica-backdoor-malware/

Attackers can steal NTLM password hashes via calendar invites

Zeljka Zorz • January 22, 2024

A recently patched vulnerability in Microsoft Outlook (CVE-2023-35636) that can be used by attackers to steal users' NTLM v2 hashes can be exploited by adding two headers to an email carrying a specially crafted file, security researcher Dolev Taler has shared on Friday.

…

While CVE-2023-35636 has been fixed, the other two vulnerabilities are considered by Microsoft to be of "moderate" severity and remain unpatched.

NTLM v2 – the most current iteration of the NTLM cryptographic protocol – is used by Microsoft Windows to authenticate users to remote servers via password hashes.

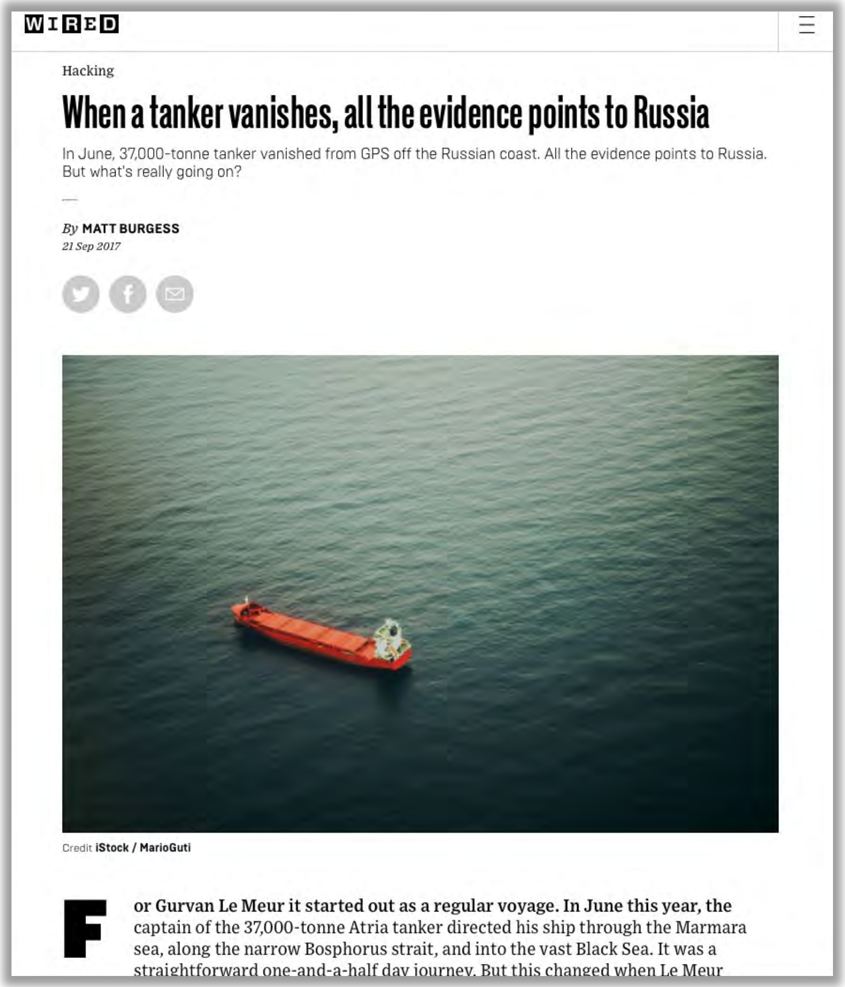
Compromised NTLM v2 password hashes can be used in authentication relay attacks or can be brute-forced (offline, on an attacker's machine) to reveal the hashed password.

In both cases, the threat actor can authenticate as the user and access sensitive enterprise systems and resources.

https://www.helpnetsecurity.com/2024/01/22/attackers-steal-ntlm-hashes/

Some more things to worry about

2017 – GPS hacking



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.

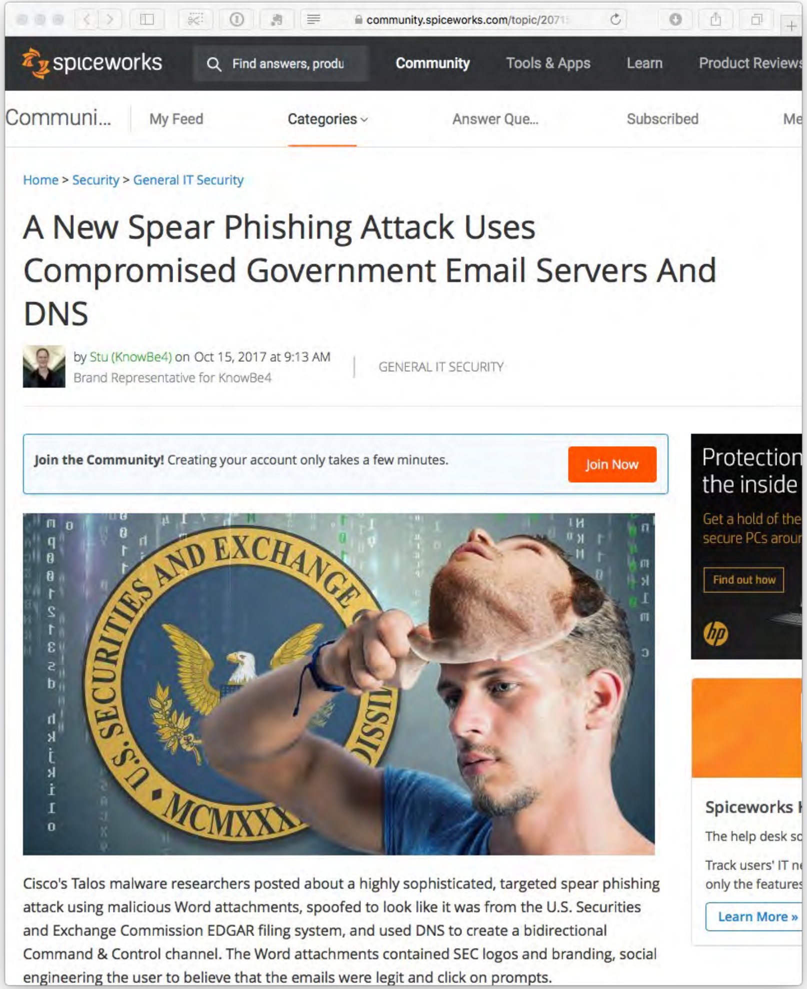
Radio-frequency jamming has become ubiquitous in Ukraine as both sides seek to prevent the other from using drones. Typically two type of electronic warfare are employed: generating radio noise to interfere with the control signal, making it impossible to pilot the drone, and blasting interference on 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/

2017 – Spear Phishing Coming From Government Servers



A New Spear Phishing Attack Uses Compromised Government Email Servers And DNS

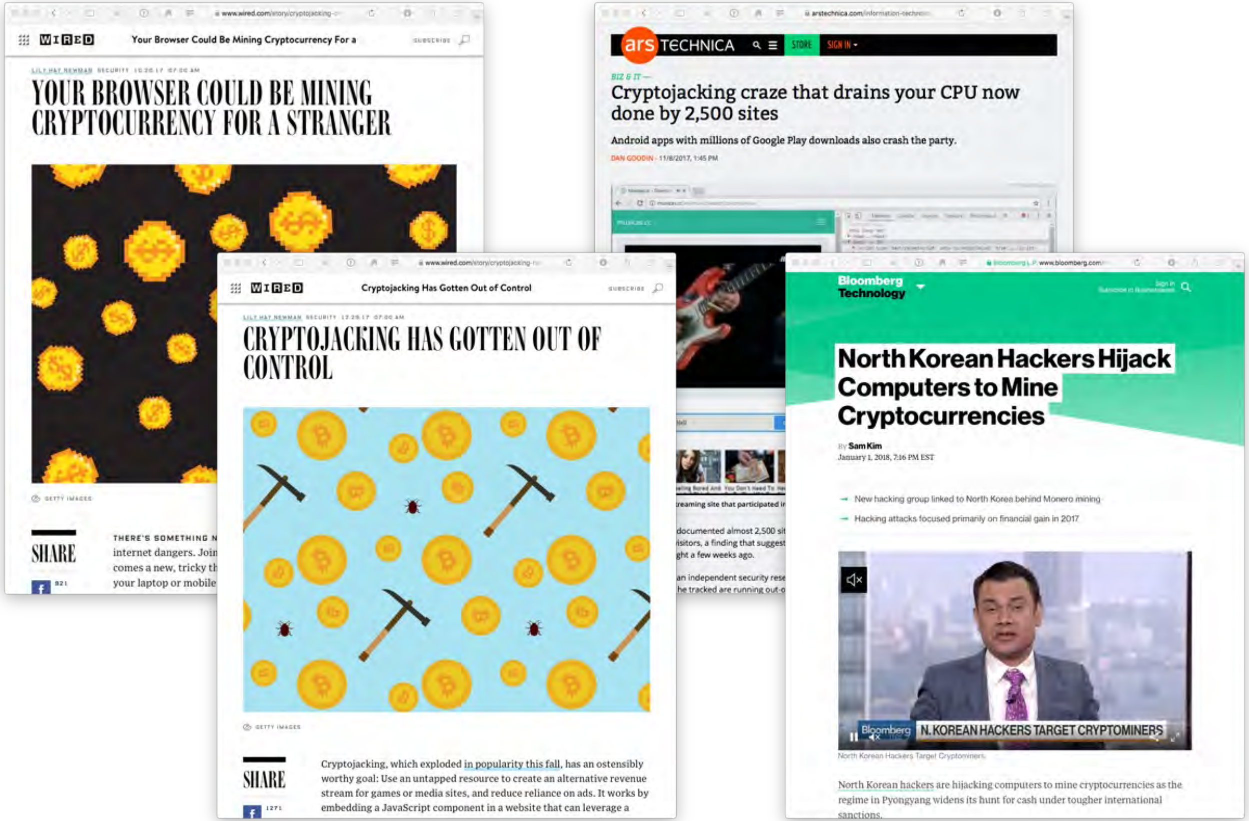
by Stu (KnowBe4) on Oct 15, 2017 at 9:13 AM
Brand Representative for KnowBe4

GENERAL IT SECURITY

Join the Community! Creating your account only takes a few minutes. Join Now

Cisco's Talos malware researchers posted about a highly sophisticated, targeted spear phishing attack using malicious Word attachments, spoofed to look like it was from the U.S. Securities and Exchange Commission EDGAR filing system, and used DNS to create a bidirectional Command & Control channel. The Word attachments contained SEC logos and branding, social engineering the user to believe that the emails were legit and click on prompts.

Fall 2018-now – Cryptojacking



www.wired.com/story/cryptojacking-

WIRED Your Browser Could Be Mining Cryptocurrency For a SUBSCRIBE

LILY HAY NEWMAN SECURITY 10.26.17 07:00 AM

YOUR BROWSER COULD BE MINING CRYPTOCURRENCY FOR A STRANGER

GETTY IMAGES

SHARE

921

THERE'S SOMETHING N
internet dangers. Join
comes a new, tricky th
your laptop or mobile

arstechnica.com/information-technol

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

treaming site that participated in

documented almost 2,500 sit
isitors, a finding that suggest
ght a few weeks ago.

an independent security rese
he tracked are running out-o

www.wired.com/story/cryptojacking-

WIRED Cryptojacking Has Gotten Out of Control SUBSCRIBE

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

Bloomberg N. KOREAN HACKERS TARGET CRYPTOMINERS

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.

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

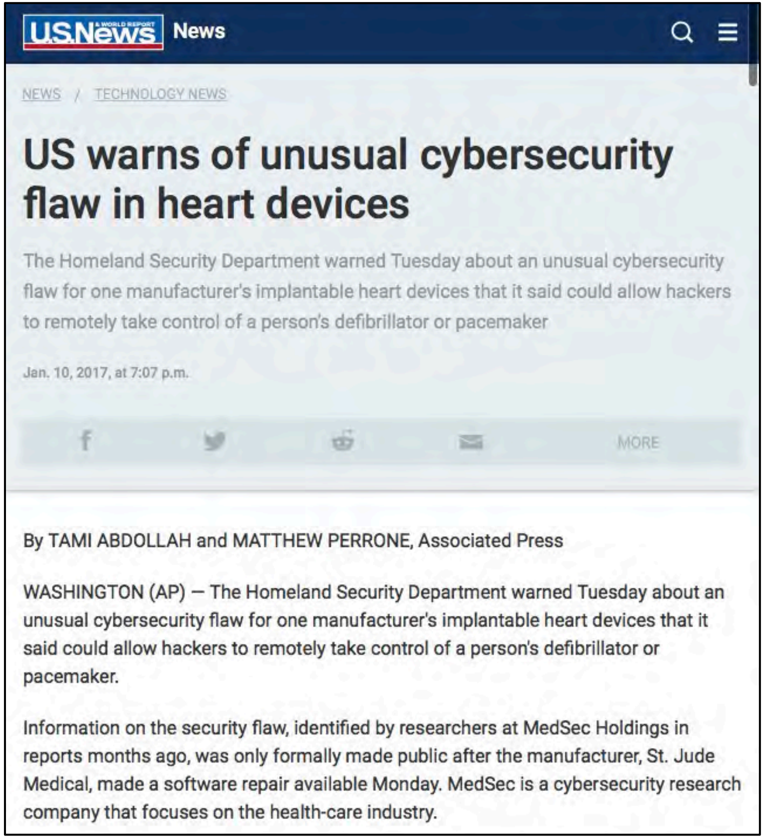
Multiple supercomputers across Europe have been infected this week with cryptocurrency mining malware and have shut down to investigate the intrusions.

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.

Link

Potential for physical harm



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

The Big Tesla Hack: A hacker gained control over the entire fleet, but fortunately he’s a good guy

electrek

Fred Lambert • August 27, 2020

A few years ago, a hacker managed to exploit vulnerabilities in Tesla’s servers to gain access and control over the automaker’s entire fleet.

In July 2017, Tesla CEO Elon Musk got on stage at the National Governors Association in Rhode Island and confirmed that a “fleet-wide hack” is one of Tesla’s biggest concerns as the automaker moves to autonomous vehicles.

He even presented a strange scenario that could happen in an autonomous future:

> *“In principle, if someone was able to say hack all the autonomous Teslas, they could say – I mean just as a prank – they could say ‘send them all to Rhode Island’ [laugh] – across the United States… and that would be the end of Tesla and there would be a lot of angry people in Rhode Island.”*

What Musk knew that the public didn’t was that Tesla got a taste of that actually happening just a few months prior to his talk.

https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/

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

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.

…

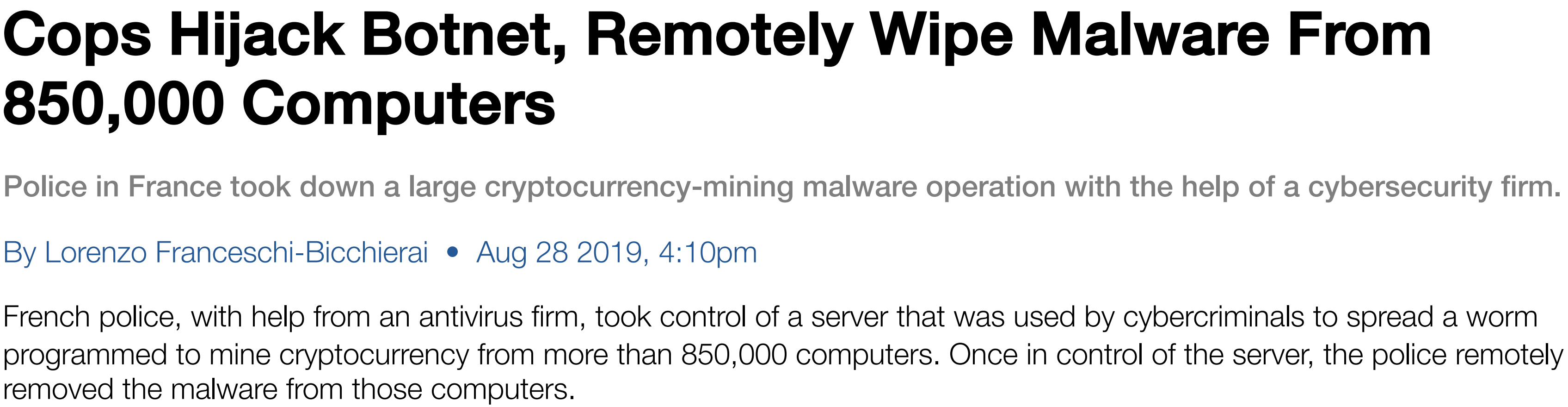
This class of hack is known as a relay attack, a close cousin of the person-in-the-middle attack. In its simplest form, a relay attack requires two attackers. In the case of the locked Tesla, the first attacker, which we'll call Attacker 1, is in close proximity to the car while it's out of range of 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/

Hack-backs

Attack the computers of the hackers

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

ZDNet

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/

US military has reportedly acted against ransomware groups

Action came after a series of crippling attacks raised concerns about vulnerabilities in the nation's critical infrastructure.

Steven Musil • December 5, 2021

The US military has gone on the offensive against ransomware groups as US companies increasingly become targets of malware attacks, the nation's top cyber defender acknowledged on Saturday.

Up until about nine months ago, reining in ransomware attacks was seen as the responsibility of law enforcement agencies, Gen. Paul M. Nakasone, the head of US Cyber Command and director of the National Security Agency, told the New York Times. But attacks like the ones on Colonial Pipeline and JBS beef plants have been "impacting our critical infrastructure," Nakasone said, leading federal agencies to ramp up the gathering and sharing of intelligence on ransomware groups.

"The first thing we have to do is to understand the adversary and their insights better than we've ever understood them before," Nakasone said in an interview at the Reagan National Defense Forum, a gathering of national security officials.

Nakasone didn't describe the action taken or identify the groups targeted, but said one of the goals is to "impose costs" for ransomware groups.

https://www.cnet.com/tech/services-and-software/us-military-has-reportedly-acted-against-ransomware-groups/

The End