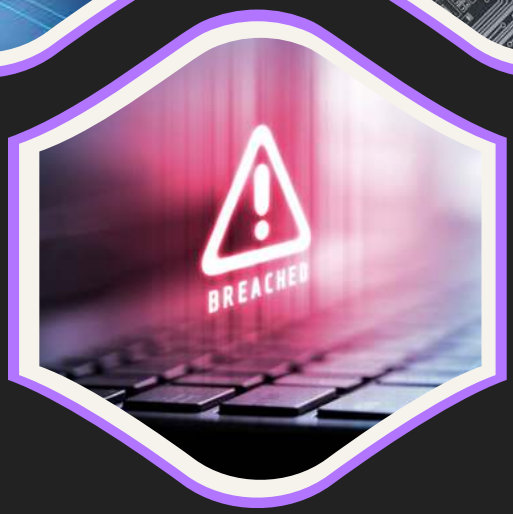
CYBER SECURITY INSIGHTS

PURPLESEC

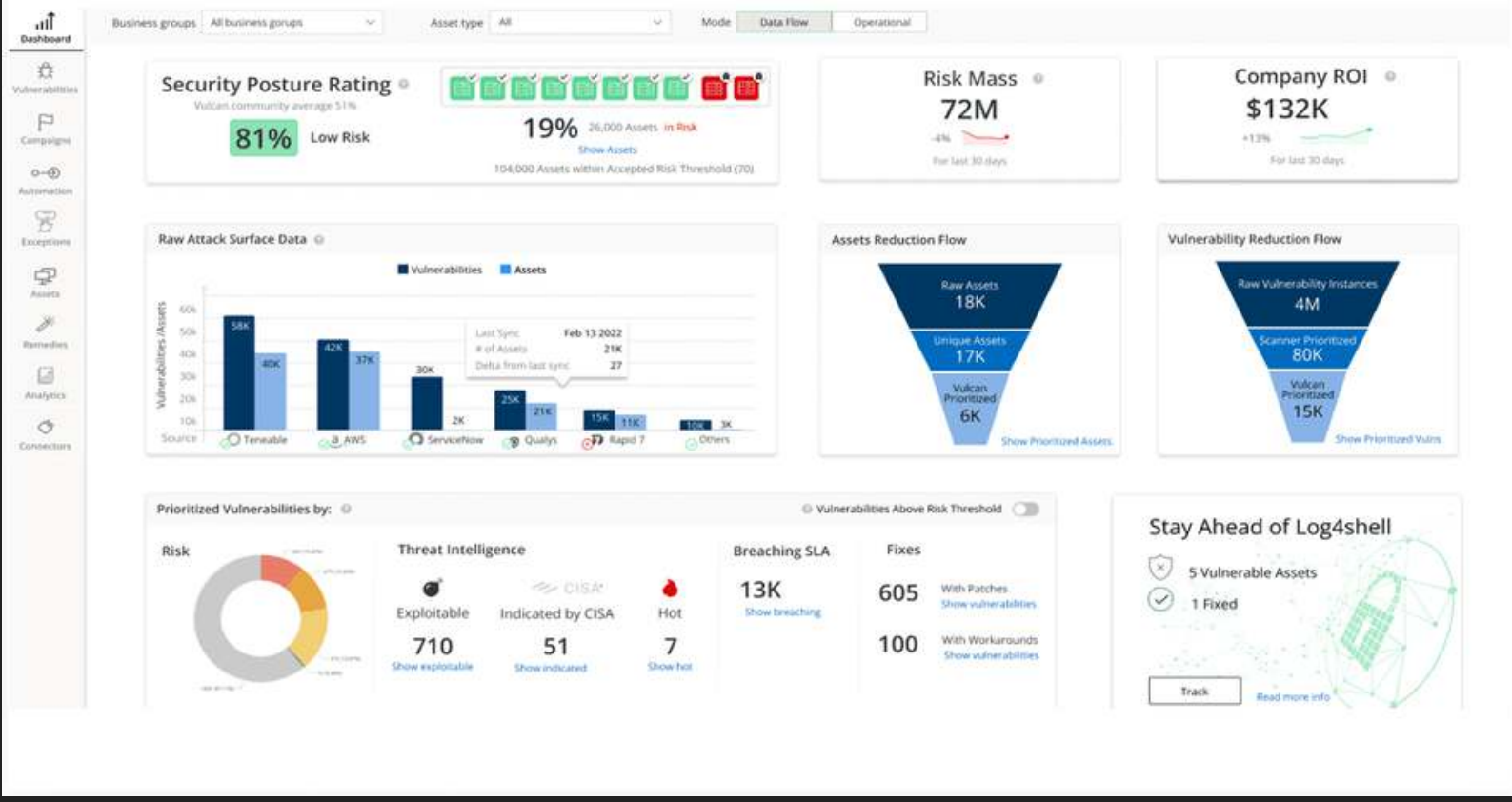
Analysis By PurpleSec's Experts

August 2022



A Veteran Owned & Led Cyber Security Company

purplesec.us / 2151 Tannin PL, Vienna, VA 22182 / sales@purplesec.us



AI POWERED VULNERABILITY MANAGEMENT

Automatically manage and analyze vulnerabilities and risk in one place

A rapid time-to-value solution that's easy to use and has minimal requirements for implementation, configuration or training.

Expert-defined Remediation library that immediately delivers the right fix for any vulnerability to speed up risk remediation.

Easy to configure with the ability to automate as much or as little of the vulnerability management lifecycle as you need.

LEARN MORE

PURPLESEC

A Veteran Owned & Led Cyber Security Company

Meet Our Experts >
Request A Free Consult >

RECENT CYBER ATTACKS

As **data breaches** become more pervasive in our interconnected world so must our understanding of modern day cyber attacks.

In this series, our security researchers provide their analysis of the most recent and relevant cyber attacks and breaches. No fluff - just the facts.

In this month's issue we cover:

- **Twitter Zero-Day Exposed Data Of 5.4 Million Accounts >**
- **Cloudflare And Twilio Targets Of A Sophisticated Smishing Attack >**
- **Cisco Suffers Cyber Attack By UNC2447, Lapsus$, & Yanluowang >**
- **How The Largest European DDoS Attack Was Blocked >**

Summary Of The Attack

- Twitter suffered a zero-day vulnerability which allowed the attackers access to personal information of 5.4 million accounts.
- The vulnerability was being exploited in December 2021, but reported to Twitter through HackerOne's bug bounty platform in January 2022.
- The security researcher was awarded $5,040 for his findings.
- The vulnerability allows any party without any authentication to obtain a Twitter ID of any user by submitting a phone number/email even though the user has prohibited this action in the privacy settings.
- The vulnerability is now patched and recommended precautionary measures are enabling 2FA and refraining from linking personal information to your Twitter account.

Analysis by:
Eva Georgieva

What Happened?

Social media platform **Twitter confirmed they suffered a now-patched zero-day vulnerability**, used to link email addresses and phone numbers to users' accounts, which allowed attackers to gain access to the personal information of 5.4 million users.

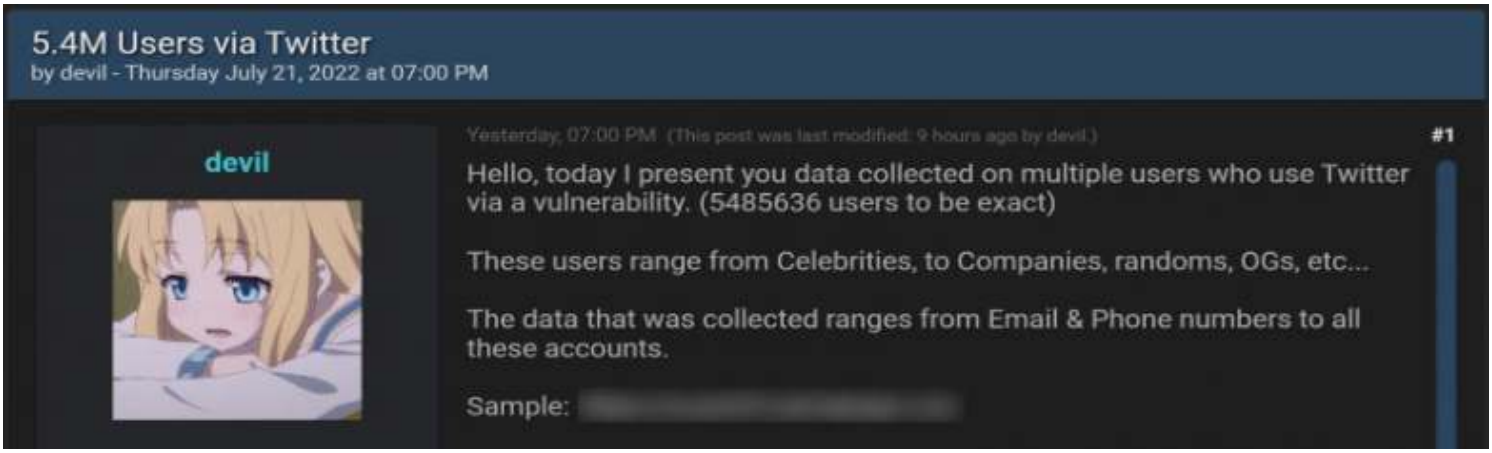
What Is A Zero-Day?

A zero-day vulnerability is **a weakness in software that has been discovered by a threat actor** but is still unknown to the developer. It's called "zero-day" because once a threat actor detects the vulnerability, the software vendor essentially has "zero time" to patch it before it's exploited.

Zero-day vulnerabilities can stem from software bugs, weak passwords, or lack of authorization and encryption.

How Does The Twitter Zero-Day Attack Work?

The vulnerability allowed anyone to submit an email address or phone number, verify if it was associated with a Twitter account, and retrieve the associated account ID.



More technically, what **the security researcher zhirinovsky reported** on **HackerOne's bug bounty platform** is that this vulnerability allows any party without any authentication to obtain a twitter ID (which is almost equal to getting the username of an account) of any user by submitting a phone number/email even though the user has prohibited this action in the privacy settings.

As he stated, the bug exists due to the process of authorization used in the Android Client of Twitter, specifically in the process of checking the duplication of a Twitter account. The security researcher reported the vulnerability in January 2022 and the company awarded a $5,040 bounty for his findings.

Prior to that, the attackers created profiles of 5.4 million Twitter users in December 2021 and scraped public information, such as follower counts, screen name, login name, location, profile picture, URL, and other information.

Scope Of The Threat

The researcher in its report expressed that this is a very serious threat, as people can not only find users who have restricted the ability to be found by email/phone number, but any attacker with a basic knowledge of scripting/coding can enumerate a big part of the Twitter user base unavailable to enumeration prior.

Such bases can be sold to malicious parties for advertising purposes or malicious activities.

A redacted example of one of the generated Twitter profiles.

Mitigation Steps Being Taken

In their official statement released on August 5, 2022, the tech giant pointed out that no passwords were exposed, but **they encouraged their users to enable two-factor authentication apps** or hardware security keys to protect their accounts from unauthorized logins.

AI POWERED PENETRATION TESTING

Bring agility and automation into your penetration testing

Deliver immediate ROI with an agile, efficient, and inexpensive solution

Skilled pen testers are equipped with tools up to date with the latest exploits

Simple exploits or high/critical findings can be quickly reported and remediated

LEARN MORE

PURPLESEC

A Veteran Owned & Led Cyber Security Company

Meet Our Experts >
Request A Free Consult >

CLOUDFLARE & TWILIO ARE TARGETS OF SMISHING ATTACK

Summary Of The Attack

- Twilio and Cloudflare were targets of a sophisticated smishing attack.
- Both companies' employees phished and credentials were stolen.
- Twilio's security team also revoked access to the compromised employee accounts to mitigate the attack.
- Cloudflare's security systems in place stopped the attack from being successful, credentials weren't enough to allow access to the company's systems.

Analysis by:
Eva Georgieva

What Happened?

Cloudflare revealed on Tuesday, August 9th that they were also targeted by the **threat actors who breached Twilio** and gained unauthorized access to some of its systems on August 4th.

The threat actor sent phishing text messages to Twilio employees to trick them into entering their credentials on a malicious website.

How Does The Attack Work?

Twillio became aware of unauthorized access to information related to a limited number of Twilio customer accounts through a sophisticated social engineering attack with a goal to steal employee credentials.

The format of the attacks was that the messages informed the recipients that they had expired passwords, schedule changes, and pointed to domains that included the words 'Twilio', 'Okta' and 'SSO'.

Phishing messages sent to Twilio employees.

The Cloudflare version was that similarly crafted messages were sent to their employees on July 20th.

The company, **in their official statement**, said that more than 100 SMS messages were sent to its employees and their families.

The messages were pointing to domains that appeared that they belonged to Cloudflare.

Twilio VS Cloudflare Take On The Attack

The threat actors that targeted the companies' employees managed to fool some employees from both companies into providing their credentials.

Twilio, confirmed that the attackers used the credentials to gain access to some of their internal systems, where they were able to access certain customer data.

From what they stated, they worked with the U.S. carriers to shut down the actos and worked with the hosting providers serving the malicious URLs to shut those accounts down.

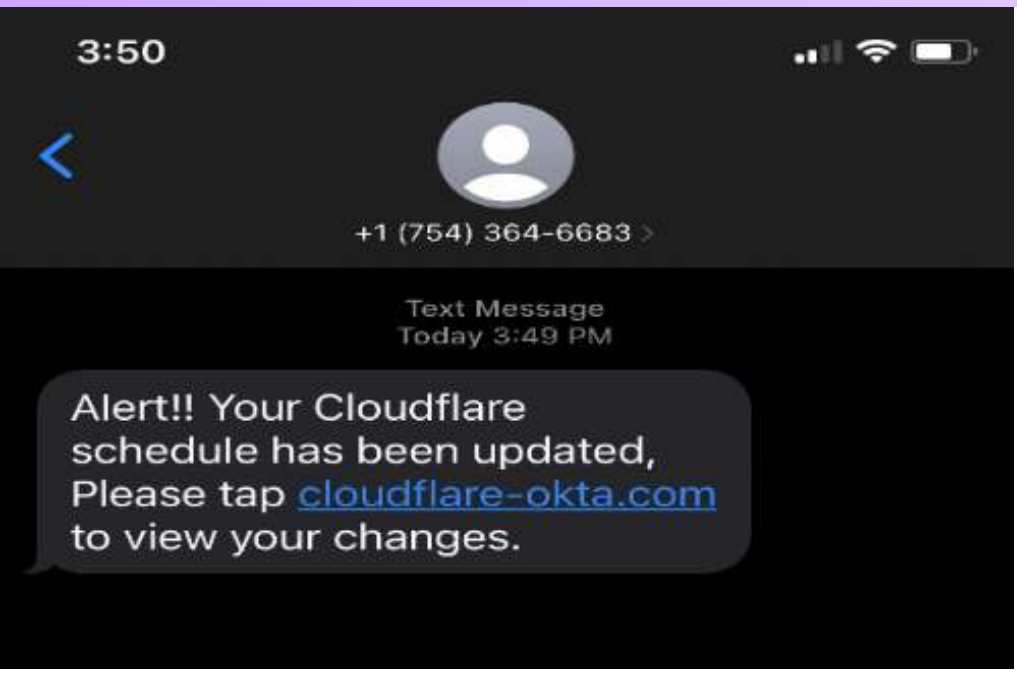
Twilio's security team also revoked access to the compromised employee accounts to mitigate the attack and engaged a leading forensic firm to aid their ongoing investigation.

While Twilio is taking remediation steps, Cloudflare, on the other hand, were able to stop the attack while it was running.

They did state that individual employees did fall for the phishing messages but they were able to thwart the attack through use of their **Cloudflare One Products** and physical security keys that they issued to every employee that are required to access all of their applications.

Every employee at the company is issued a FIDO2-compliant security key from a vendor like **YubiKey**.

Since the hard keys are tied to users and implement origin binding, even a sophisticated, real-time phishing operation like this one cannot gather the information necessary to log in to any of the Cloudflare systems.



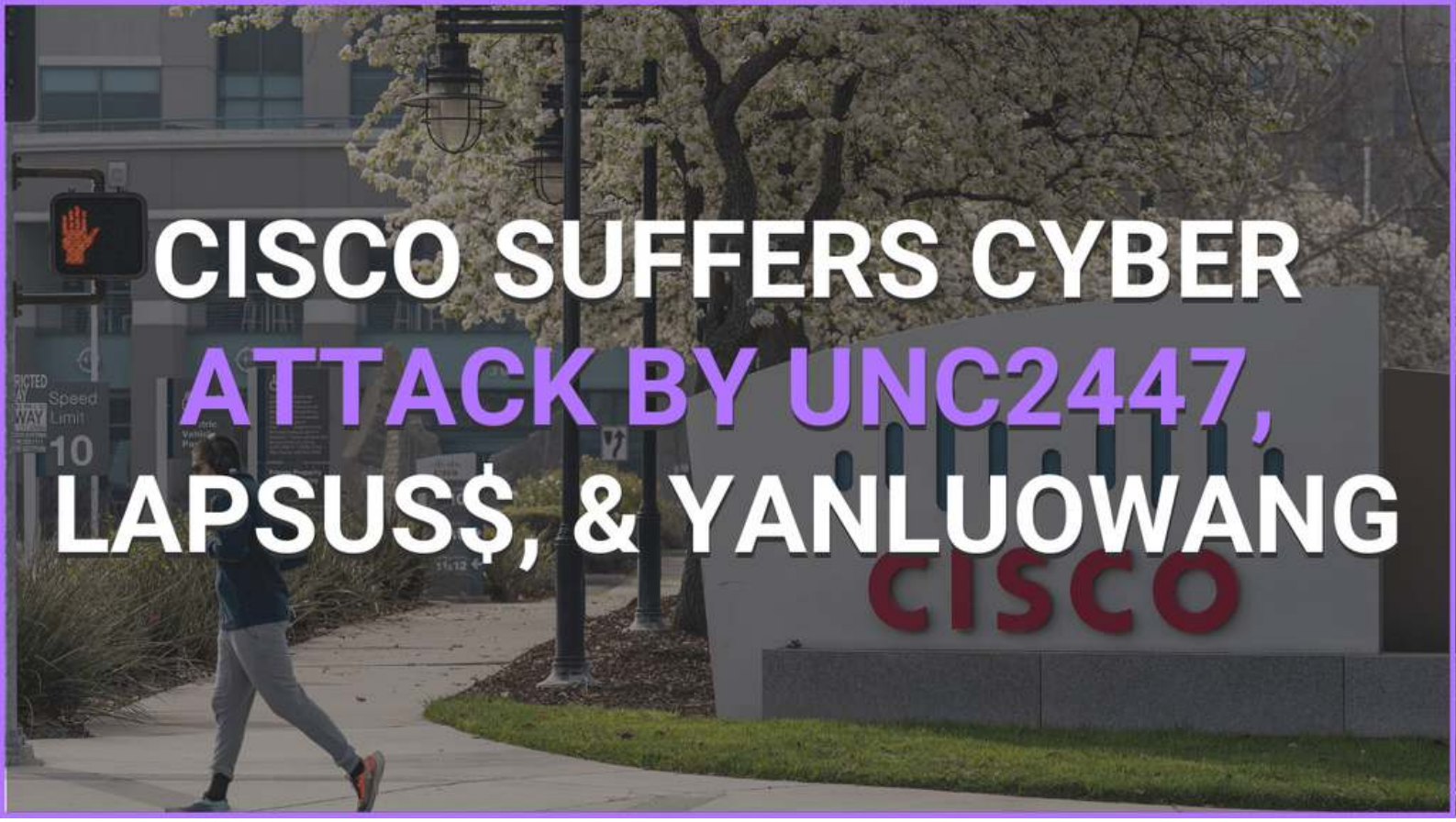
The phishing messages sent to Cloudflare employees.

While the attacker attempted to log in to their systems with the compromised username and password credentials, they could not get past the hard key requirement.

In their official statement, they expressed that no Cloudflare systems were compromised.

Next Steps

The attacks have not yet been linked to a known threat actor, but **Cloudflare has shared some indicators of compromise** as well as information on the infrastructure used by the attacker.



Summary Of The Attack

- Cisco confirmed that the UNC2447 cybercrime gang, Lapsus$ threat actor group, and Yanluowang ransomware operators breached its corporate network in late May.
- During the investigation, it was determined that a Cisco employee's credentials were compromised after an attacker gained control of a personal Google account where credentials.
- The attacker conducted a series of sophisticated
- Voice phishing attacks under the guise of various trusted organizations attempting to convince the victim to accept multi-factor authentication (MFA) push notifications initiated by the attacker. The attacker ultimately succeeded in achieving an MFA push acceptance.

Analysis by:
Dušan Trojanović

What Happened?

Cisco has confirmed that Yanluowang ransomware operators, UNC2447 and Lapsus$ groups have breached their local network on the May 24, 2022, described their actions and it has resulted that human is still supposed to be the security weakest link.

After further breach impact analysis on Cisco business, there was no impact on any Cisco services, sensitive customer or employee data, Cisco intellectual property, or supply chain operations.

What Is The Impact?

Ransomware operators Yanluowang claimed that they manage to steal a total of 2.75 GB including 3100 files that were published on the Dark web on the 10th of August.

Cisco shared technical details with the public and they claimed that they took additional measures to get their network and systems safe from potential similar attacks in the future.

How Did This Attack Happen?

According to **Talos analysts**, the attackers started by gaining control of a Cisco employee's personal Google account.

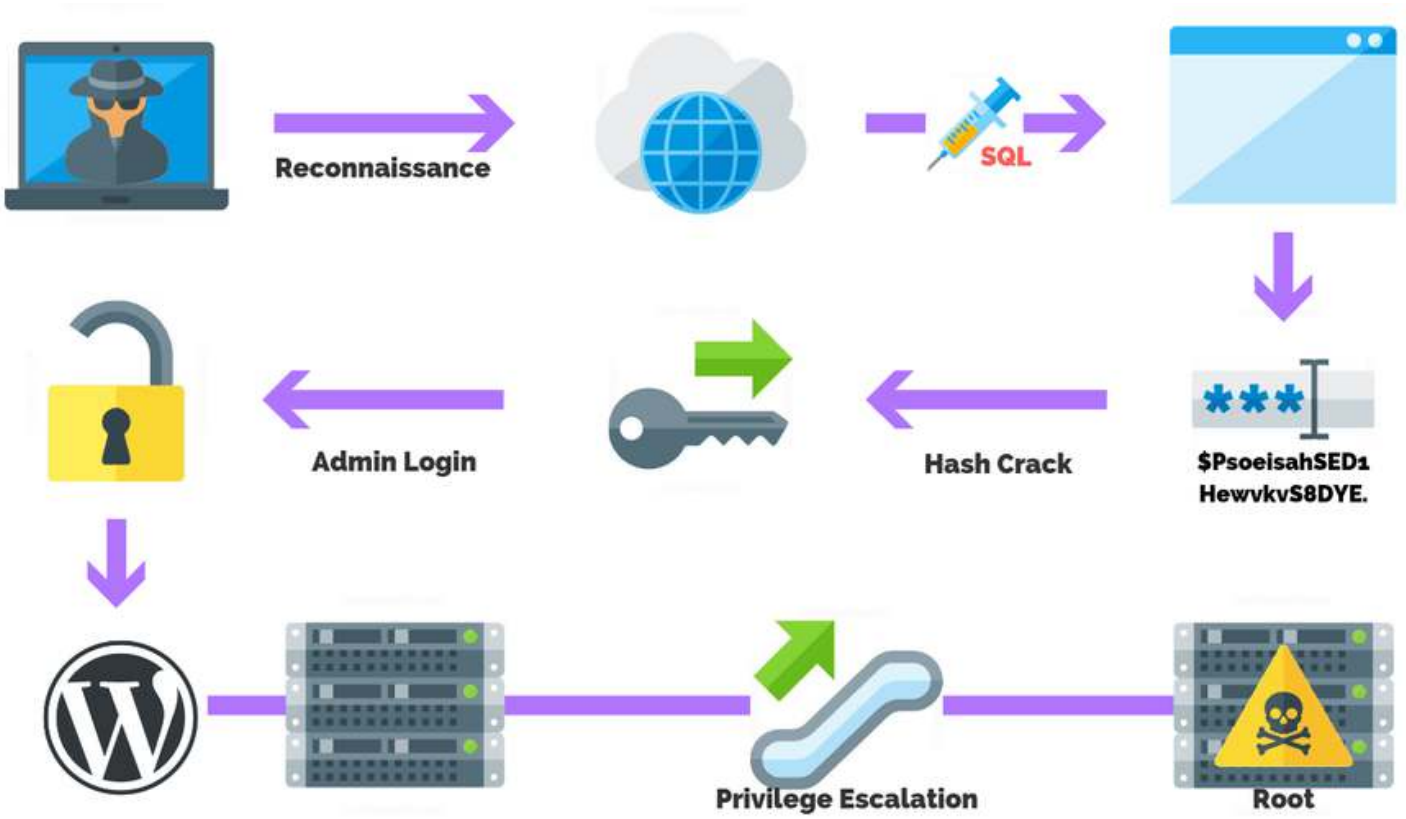
Cisco compromise started when one of their employees had enabled password syncing and had stored its Cisco corporate credentials in the Google Chrome web browser, allowing credentials to synchronize to the Google account.

After obtaining the user's credentials attacker attempted to bypass MFA (Multi-Factor Authentication) with multiple bypass techniques, and with two of them, **vishing (Voice phishing)** and MFA fatigue attackers managed to gain access and enroll multiple new devices to authenticate to Cisco VPN service.

Vishing is a **common social engineering technique** where attackers try to trick employees into disclosing sensitive information over the phone.

MFA fatigue is an attack where criminals target a user's MFA application for account access by sending multiple push requests to the target device until user accidentally or on purpose allow one of the repeated push notifications they are receiving.

After attackers successfully authenticated to Cisco VPN service, **they had escalated from regular user privilege to administrative privileges**, which allowed them to log in to multiple systems inside Cisco's corporate network.



For remote accessing systems attackers have used tools similar to **LogMeIn** and **TeamViewer**.

Once attackers gain access to a system, they began to enumerate the local environment. They do this by using built-in Windows utilities to enumerate the targeted system, user, and group membership configuration.

This results in obtaining details about the operating user's account context.

Offensive Security Tools Used

In order to accomplish privilege escalation, they have used offensive security post-exploitation tools such:

- Cobalt Strike
- PowerSploit
- Mimikatz
- Impacket

They then added their backdoor accounts as well as persistence mechanisms.

Maintaining Access

Attackers gained access to credential databases, registry information, and memory that contained credentials and deleted accounts they created.

Next, they cleared system logs to cover their tracks, as well performing a variety of activities for:

- Maintaining systems access
- Minimizing forensic artifacts
- Increasing access level to systems within the local environment

Attackers managed to drop multiple payloads onto systems.

One of them was a simple backdoor payload that takes commands from a command and control (C2) server and executes them on the end system via an active terminal session.

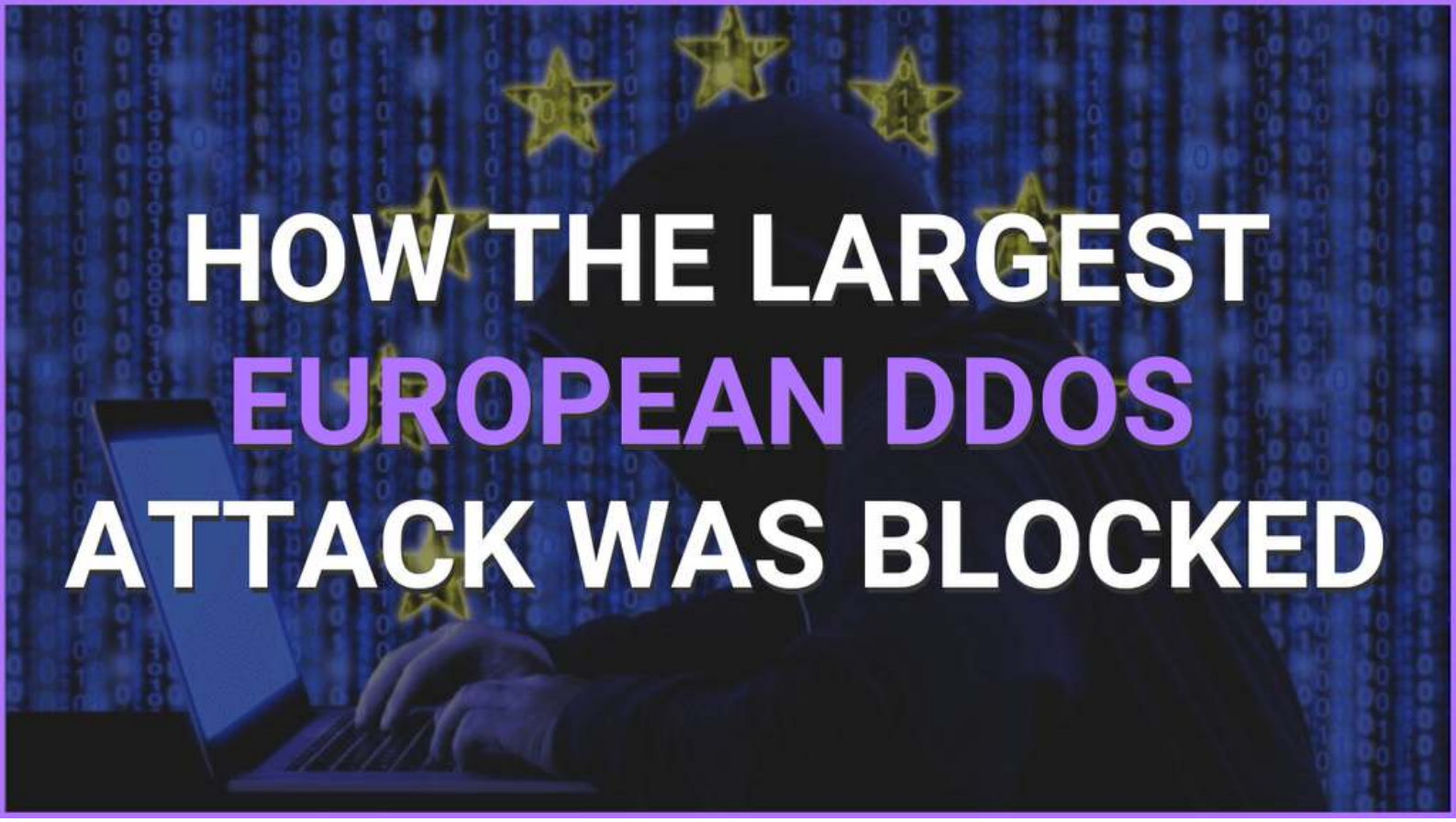
How To Mitigate These Types Of Attacks

Attackers were not successful at deploying ransomware, but there were able to deploy backdoor payload communicating with C2 server.

Cisco added two new **ClamAV detections** for the backdoor and a Windows exploit used for privilege escalation Win.Exploit.Kolobko-9950675-0 and Win.Backdoor.Kolobko-9950676-0, which were created to help other organizations to detect similar attacks.

The best way to mitigate this type of attack is to:

- Implement strong device verification for MFA solution by enforcing stricter device controls to manage enrollments and access from unmanaged or unknown devices.
- **Check endpoint security posture** before allowing VPN connections from remote endpoints.
- Implement network segmentation to **improve network performance and security**.
- **Implement a SIEM solution** to have greater visibility and real-time analysis of security alerts that happens inside the network.



Summary Of The Attack

- On July 21, 2022, Akamai detected and mitigated the largest DDoS attack up to this point, which has been launched against a publicly unknown Akamai European customer.
- The attack lasted over 14 hours and traffic was peaking at 853.7 Gbps and 659.6 Mpps which was targeting Akamai European customers.
- The most significant DDoS attack type was UDP flood in which a large number of UDP packets are sent to a target with the aim to overwhelm the target device's ability to process and respond.
- Chose the proper DDoS solution, identify what assets should be protected, identify what business impact, and define the procedure and dedicated team to respond to the attack.

Analysis by:
Dušan Trojanović

What Happened?

Cisco has confirmed that Yanluowang ransomware operators, UNC2447 and Lapsus$ groups have breached their local network on the May 24, 2022, described their actions and it has resulted that human is still supposed to be the security weakest link.

After further breach impact analysis on Cisco business, there was no impact on any Cisco services, sensitive customer or employee data, Cisco intellectual property, or supply chain operations.

What Is The Impact?

Ransomware operators Yanluowang claimed that they manage to steal a total of 2.75 GB including 3100 files that were published on the Dark web on the 10th of August.

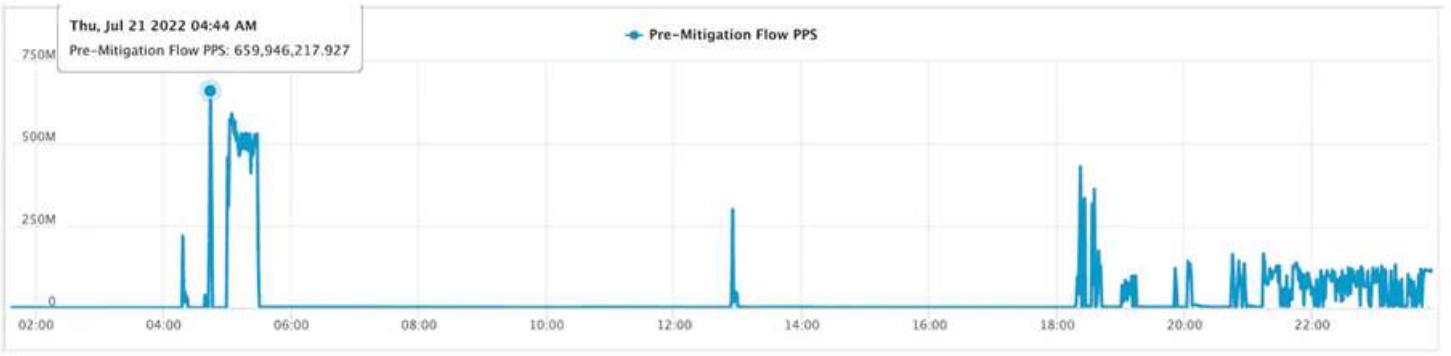
Cisco shared technical details with the public and they claimed that they took additional measures to get their network and systems safe from potential similar attacks in the future.

How This Attack Happened

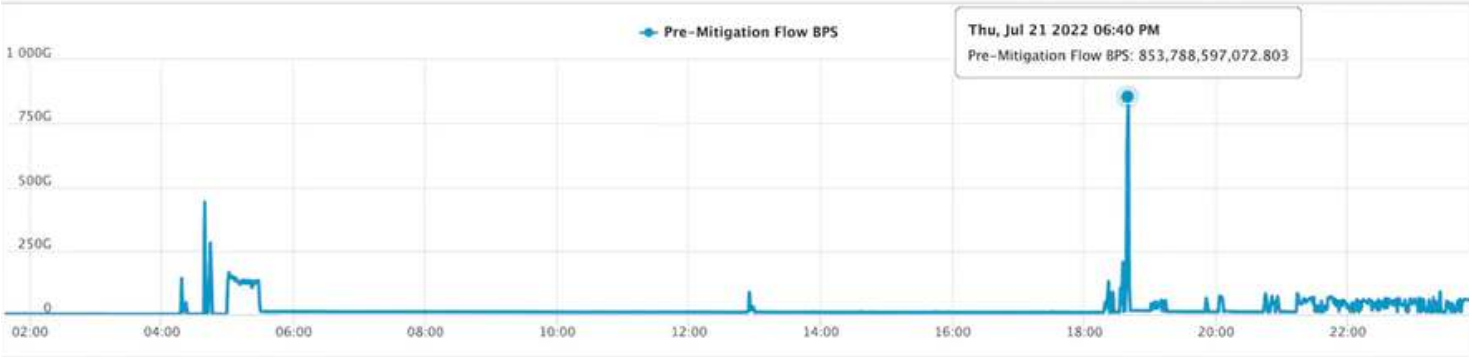
The attack lasted over 14 hours and traffic was peaking at 853.7 Gbps (Gigabit per second) and 659.6 Mpps (Maximum packets per second) which was targeting Akamai European customer large scope of IP addresses which resulted in the largest horizontal attack mitigated on the Prolexic platform.

The most significant DDoS attack type was UDP flood in which a large number of UDP (User Datagram Protocol) packets are sent to a target with the aim to overwhelm the target device's ability to process and respond. In the following figures, UDP flood was observed in both record spikes.

The first figure represents the maximum number of packets per second was reached 659.6 Mpps during the attack.



The second figure represents the highest attack peak which reached 853.7 Gbps.



Other noticed DDoS attack types were UDP fragmentation, ICMP flood, RESET flood, SYN flood, TCP anomaly, TCP fragment, PSH ACK flood, FIN push flood, and PUSH flood.

Mitigating This Attack

Today without proper automated DDoS defenses, primarily for critical business operations, it would likely collapse under a similar attack scale, making online business completely inaccessible and causing financial and reputational loss.

Recommendations for mitigating DDoS risk include:

- Chose the proper DDoS solution based on your business scale to keep service up and running.
- Identify what assets should be protected from DDoS attacks, which can include web applications, APIs, DNS servers, origin servers, data centers, and network infrastructure.
- Identify what business impact and operational, financial, regulatory, and reputational costs would incur from loss.
- Design robust architecture by separating data servers on separate networks, and review critical IP subnets to prevent a single point of failure.
- Define procedure and dedicated team to respond to attack on short notice.
- Identify an acceptable time to respond to an attack a do proper mitigation.
- Maintain a DDoS runbook, which allows the organization in case of need to experience a controlled, streamlined response to an attack.

SECURITY RESEARCH

With hundreds of publications being published on a weekly basis, it can be difficult to know what research needs to be kept top of mind.

In this series, our experts sift through the noise and analyze only **the top security research** you need to know.

In this month's issue we cover:

- **Space X's Starlink Dish Hacked >**
- **The No More Ransomware Project >**

Summary Of The Research

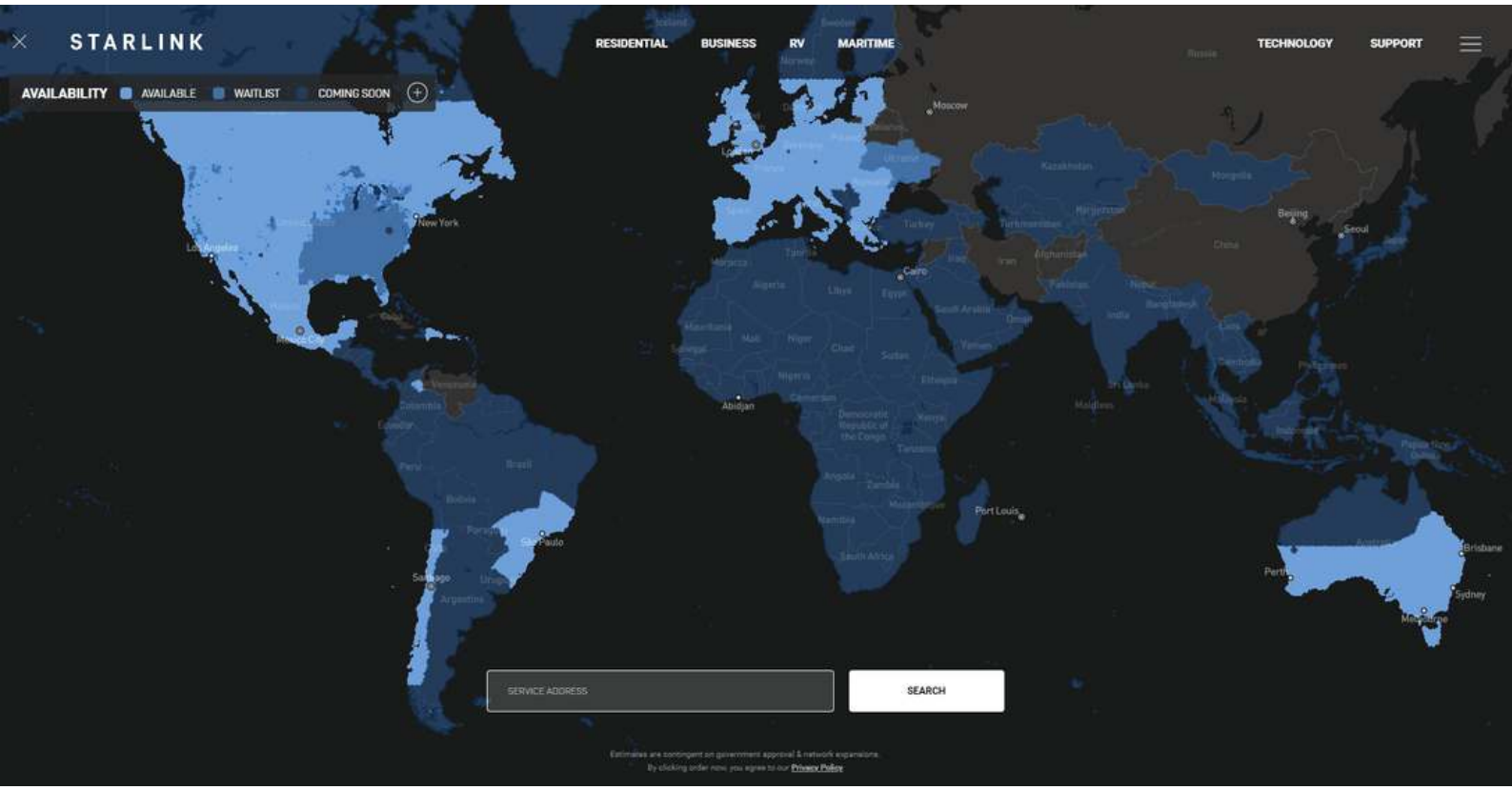
- At this year's BlackHat USA, held Aug. 6-11 in Las Vegas, a Belgian security researcher stunned the crowd by hacking Starlink Dish with a $25 device, gaining major notoriety worldwide.
- The researcher in question disassembled his terminal, or as SpaceX calls it, "Dishy McFlatface," and managed to perform a "Voltage Fault Injection Attack," also known as "glitching," to load modified firmware, after which he gained full access to the antenna.
- Starlink could not fix this problem with a software update but would have had to release new hardware.

Analysis by:
Dalibor Gašić

What is Starlink?

Starlink is a satellite internet provider owned and overseen by SpaceX. It currently provides access to 39 countries and plans to cover the entire globe with around 42,000 satellites in a few years.

This amazing project was launched in 2019, with the first satellites launched over the surface of the Earth to cover some of the remote parts of the country where there is little electricity and water, and now they have already started to cover them massively.



On the map above you can see the current area covered and the one where it is planned, and on the page where you can check if you can order the equipment.

The equipment is pretty much plug and play.

A satellite dish, as well as a pre-configured router from Starlink and a high-quality cable that connects the router and the antenna, is also included.

From there you'll be able to expand your network, configure the subnet and your devices, as well as set up additional protections, whether you are a business or for your home.

What Happened?

At this year's BlackHat Lennert Wouters, a Belgian security researcher stunned the crowd by hacking Starlink Dish with a $25 device, gaining major notoriety worldwide.

- **BlackHat Presentation**
- **Presentation Slides**

With just $25 in off-the-shelf hardware, Lennert was able to gain root access to a Satellite Dish terminal, which allowed him to explore the broader Starlink network – a capability that could enable the exploitation of Starlink satellites themselves.

How The Attack Works

Starlink terminals are very hardened and quite locked, it is very difficult to run any code in the form of plugins or applications on them, this device will only run firmware from Starlink and no one else.

The researcher in question disassembled his terminal, or as SpaceX calls it, "**Dishy McFlatface**," and managed to perform a **"Voltage Fault Injection Attack," also known as "glitching,"** to load modified firmware, after which he gained full access to the antenna.

"Glitching" works by interrupting power to the antenna's central processing unit (CPU) for a very short period of time to disrupt certain processor instructions.

The goal of this part of the attack is to bypass the "secure boot" code that confirms that the firmware on SpaceX's memory chip is signed and has not been tampered with.

The Lennert managed to bypass this mechanism "secure boot" in such a way that he loaded the modified firmware and in that way got full root access to the dish.

He wasn't satisfied with the hardware he used when he first succeeded in hacking the antenna because it was expensive.

So he took it a step further by ditching the expensive lab equipment and repeating the attack with a Raspberry PI Pico, before going one step further and making a custom circuit board that can be soldered directly to the dish.

This circuit board, commonly called a modchip, contains all the electronics needed for hacking and costs less than $25, plus it's open source.

Starlink Remediation Solution

Starlink could not fix this problem with a software update but would have had to release new hardware.

However, SpaceX can make it harder to exploit the vulnerability by releasing a firmware update that blows a fuse in the dish and permanently disables the serial output, as Modchip uses this to trigger the hack.

Learn more about **Starlink's Bug Bounty program**.

THE NO MORE RANSOMWARE PROJECT

Summary Of The Research

- In mid-July 2016, several cybersecurity companies pooled their resources and knowledge to launch the “No More Ransom” platform.
- The No More Ransom project includes 188 partners worldwide, including some well-known companies: Amazon Web Services, Barracuda Networks, CheckPoint, Cisco, Emsisoft, Bitdefender, ESET, Interpol, and other law enforcement, public and private entities.
- No More Ransom’s Crypto Sheriff Tool helps you find a free decryption program by uploading two encrypted files and the ransomware note and tries to match them with a list of available tools.

Analysis by:
Dalibor Gašić

What Is The No More Ransomware Project?

In mid-July 2016, several cybersecurity companies, and public and private organizations, pooled their resources and knowledge to launch the “No More Ransom” platform to help people affected by ransomware malware.

In the beginning, it was a partnership between law enforcement agencies (Europol and the Dutch police) and IT security companies (Kaspersky and McAffee).

At the time, there were only four decryption tools on the platform that could decrypt different types of ransomware, and it was only available in English.

For the part of the audience that doesn’t know what ransomware is, ransomware is still one of the most dangerous malware today, locks files, and cyber criminals demand a certain amount of money to send you the keys.

Today, the No More Ransom project includes 188 partners worldwide, including some well-known companies: Amazon Web Services, Barracuda Networks, CheckPoint, Cisco, Emsisoft, Bitdefender, ESET, Interpol, and other law enforcement, public and private entities, which can be found at the link above: **https://www.nomoreransom.org/en/partners.html**.

How Does It Work?

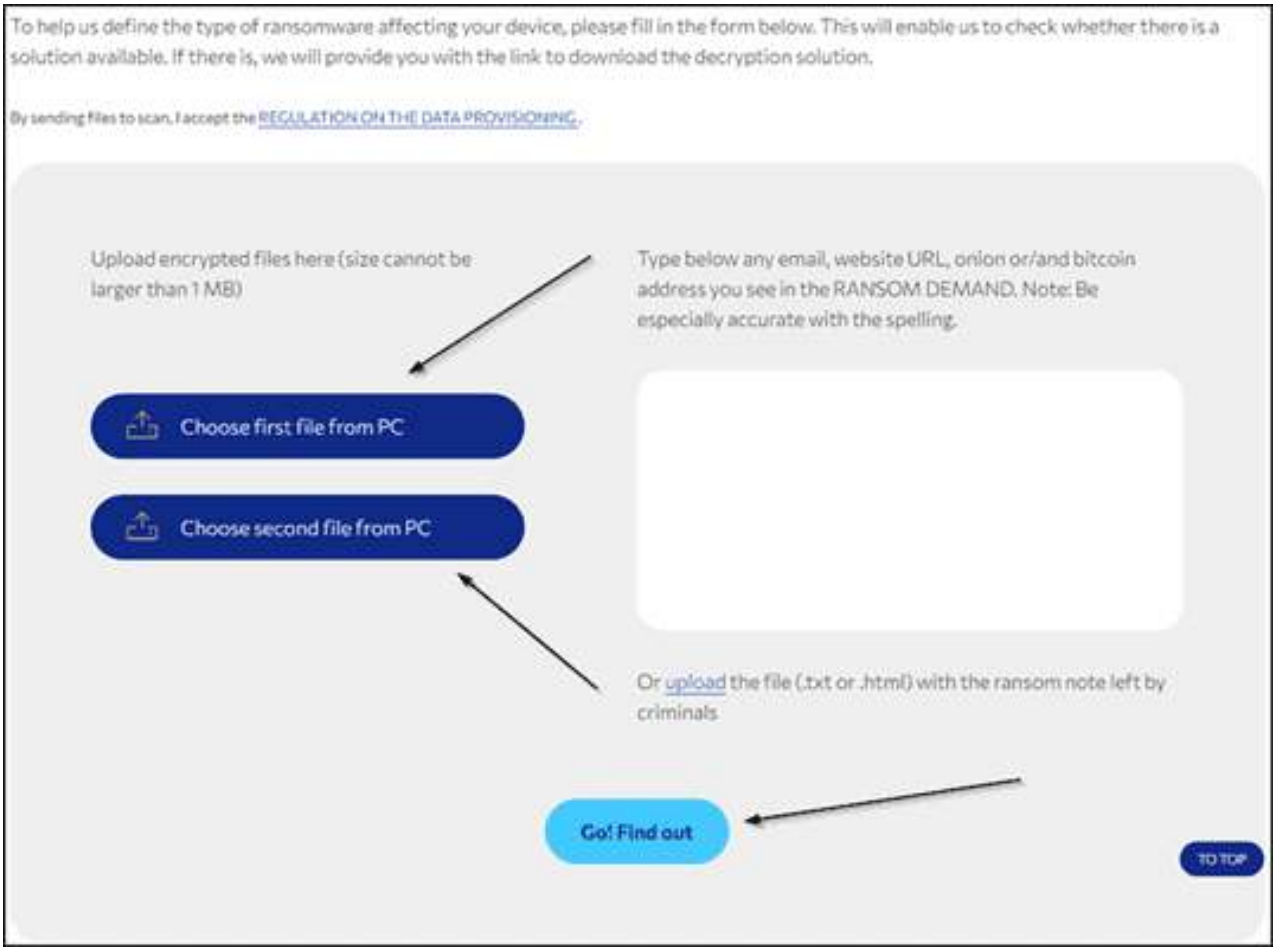
Apart from the fact that on this website we can find all the necessary information about what ransomware is, all the latest types of this malware, we can also find tool Crypto Sheriff.

No More Ransom's Crypto Sheriff Tool helps you find a free decryption program by uploading two encrypted files and the ransomware note and tries to match them with a list of available tools.

If it finds a match, it will tell you about a suitable ransomware decryption program for your encrypted files, along with detailed instructions on how to unlock them.

If no decryption program is found, you are advised to search for a match again in the future, as new decryption tools are added regularly.

This platform regularly provides new decryption tools for the latest malware strains.



To date, this platform has helped over 1.5 million people successfully decrypt their devices without the criminals having to pay for it. The portal is available in 37 languages to better help ransomware victims around the world.

Prevention Is Still The Key

The best cure against ransomware remains diligent prevention. On our side, we have advice for regular users and mitigation steps for business:

For Regular Users >

For Businesses >

GOVERNMENT POLICY & REGULATION

Many of the toolkits, processes, strategies, and technologies that enter the commercial sectors come down from the U.S. government and its military branches.

Our experts have over 30 years of combined experience working firsthand for U.S. Cyber Command, DoD, Special Operations, and Defense Industries to bring their **analysis on the latest regulations, departments, and techniques**.

In this month's issue we cover:

- **NIST Updates Guidance For Healthcare Security >**

Summary Of The Research

- NIST's updated cyber security related guidance is timely as the U.S. Department of Health and Human Services reported a significant increase in cybersecurity attacks affecting healthcare organizations.
- One of the NIST cybersecurity frameworks most important collection is Security and Privacy Controls (NIST SP 800-53) which can help organizations with a better approach to the risk management process.
- The new draft provides more than 400 unique responses NIST received from the community in its pre-draft stage last year.
- The new draft is intended to ensure the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits.
- NIST is seeking comments on the draft publication until Sept. 21, 2022.

Analysis by:
Dušan Trojanović

What Happened?

NIST has updated its cyber security guidance intended for the healthcare industry, in an effort to help healthcare organizations to protect patient's personal health information.

Download The Updated Guidance >

U.S. federal law Health Insurance Portability and Accountability Act of 1996 (HIPAA) intention is to improve the efficiency and effectiveness of the health care system by the creation of national standards to protect patient sensitive health information from being disclosed without the patient's consent or knowledge.

Under HIPAA, any information that can be used to identify a patient is considered to be Protected Health Information (PHI), and Electronic protected health information (ePHI) represents data that including:

- Patient data
- Names
- Dates
- Location
- Contact information
- Physical identity information
- Prescriptions
- Lab Results

NIST intention is not to create regulations to enforce HIPAA, but to revise the draft to align with its mission to provide and improve cyber security guidance.

The original NIST's cyber security guidance was published in 2008, and the updated guidance is meant to integrate into the NIST cyber security framework and other resources that were developed after the original guidance.

One of the NIST cyber security framework's most important collections is Security and Privacy Controls (**NIST SP 800-53**), which can help organizations with a better approach to the **risk management process**.

NIST has released a new draft publication, for improving cyber security resources guide titled Health Insurance Portability and Accountability Act 5 Security Rule (NIST Special Publication 800-66, Revision 2), which is designed to help the industry maintain security CIA triad (Confidentiality, Integrity and Availability) for ePHI.

The new draft provides more than 400 unique responses NIST received from the community in its pre-draft stage last year.

NIST's Guidance At A Glance

The publication guidance provides all entities and their business associates of all sizes throughout the world that store, process, or transmit ePHI.

NIST recommended the following guidelines for practices:

- Ensure the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats and hazards to the security or integrity of ePHI.
- Develop a list of **vulnerabilities** for which there is a higher probability be exploited.
- Investigate the probable consequences of a malicious attacker exploiting a vulnerability.
- Discuss methods in which PHI could be wrongly released.
- Define the risk level of an attacker.
- Document the outcomes of the **risk assessment**.

The revised draft was not intended to be a checklist for healthcare organizations to follow, it should present a guide to improving risk management to ePHI.

NIST is seeking comments on the draft publication until Sept. 21, 2022, which can be emailed to **sp800-66-comments@nist.gov.**

Healthcare Remains A Top Target

The number of ransomware attacks on U.S. healthcare organizations increased 94% from 2021 to 2022.

More than two-thirds of U.S. healthcare organizations reported that they had experienced a ransomware attack in 2021.

In terms of a large increase of attacks in past years healthcare providers and the companies that support them operate in an elevated cyber security risk environment.

When cyber security related incident occurs, during regulatory inquiries or litigation in most cases focus was on whether the organization and to what extent was aligned with security best practices and recommendations.

NIST's updated cyber security related guidance is timely as the U.S. Department of Health and Human Services reported a significant increase in cyber security attacks affecting healthcare organizations.

ABOUT PURPLESEC

PurpleSec is a veteran owned and led cyber security company based in Vienna, Virginia just outside of Washington, DC.

Our cyber security experts have received extensive experience and training from operations serving in:

- **U.S. Cyber Command**
- **Department of Defense**
- **Special Operations**
- **Private Industries**
- **Healthcare IT**

Now we're bringing the best of breed practices to the commercial marketplace.

Our proven methods backed by experts work to seamlesslessly integrate security into your existing business processes.

Ultimately, our goal is to provide enterprise level security for SMBs that go beyond the typical compliance checkboxes.

SPEAK WITH AN EXPERT