

CYBER SECURITY INSIGHTS



Analysis By
PurpleSec's Experts

October 2022



A Veteran Owned & Led Cyber Security Company

1410 12th St NW #4, Washington, DC 20005 / sales@purplesec.us

About PurpleSec

PurpleSec is a veteran owned and led cyber security company based in Washington, DC. Our cyber security experts have received extensive experience and training from operations serving in:

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

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

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

Ultimately, our goal is to provide enterprise level security that goes beyond the typical compliance checkboxes at an affordable price.

[SPEAK WITH AN EXPERT](#)



A Veteran Owned & Led
Cyber Security Company

[Meet Our Experts >](#)
[Request A Free Consult >](#)




PurpleSec's Cyber Risk Management Platform


Accurately prioritize vulnerabilities based on your environment, understand your actual risk aligned to your business objectives, and adapt our analytics algorithms to fit your operating requirements.


[DOWNLOAD DATASHEET](#)


With PurpleSec You Can:

 Orchestrate and accelerate risk mitigation with automated playbooks


 Manage the cyber risk lifecycle for application, cloud and infrastructure in one place

 Get expert remediation insight for all CVEs with fixes and workarounds

 Intelligently analyze and prioritize vulnerabilities based on your organization's risk

 Access deep analytics based on your organizational processes and requirements

 Facilitate communication and collaboration between all departments

 Understand risk management activities with customizable dashboards and reports



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >



In this month's issue we cover:

- Killnet DDoS Target Airports
- Advocate Aurora Health Data Leak
- Microsoft 2.4 TB Data Leak
- Optus Exposes 2.1M Customers
- \$570M Binance Coin Hack
- TikTok Denies Cyber Attack
- NATO Data Leak
- Uber's Systems Compromised
- Cisco Cyber Attack
- Samsung Exposes PII



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

RUSSIAN HACKTIVISTS TAKE DOWN US AIRPORT WEBSITES

Summary Of The Attack

- In October of this year, a pro-Russian hacker group claimed responsibility for hacking several US airport websites.
- Although this was widely reported in our cyber circles, it was just another DDoS attack on US airport websites by the notorious “Killnet” hacking group.
- Killnet – a pro-Russia hacker group known for conducting DoS (denial of service) and DDoS (distributed denial of service) attacks on government institutions and private companies in several countries during the Russian invasion of Ukraine in 2022.



Analysis by:
Dalibor Gašić



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

What Happened?

In October 2022, a pro-Russian hacker group, Killnet, claimed responsibility for hacking several US airport websites.

As we know, the situation between Ukraine and Russia is not getting any better, and more and more countries are becoming involved in the overall situation.

As a result, cyber attacks are now a common occurrence between countries. Although this was widely reported in our cyber circles, it was just another DDoS attack on US airport websites by the notorious “Killnet” hacking group.

The TSA (Transport Security Administration) issued a statement emphasizing that the cyber attack did not disrupt airport operations and that, while hackers were able to take the websites offline, they did not gain access to airport systems.

What Was The Impact?

Airports in Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, and Missouri responded to the group’s call to action.



Who Is Killnet?

Killnet is a pro-Russia hacker group known for conducting DoS (denial of service) and DDoS (distributed denial of service) attacks on government institutions and private companies in several countries during the Russian invasion of Ukraine in 2022.

The group is thought to have formed around March 2022.

Killnet is not the same as Russia's highly skilled hackers working for its intelligence agencies' groups like **Fancy Bear** and **Sandworm**, which have gained notoriety through hacks of US government systems.

Democratic National Committee and the release of the devastating ransomware **NotPetya**, respectively.

Killnet, on the other hand, resembles an enraged, nationalist online mob armed with low-level cyber-offensive tools and tactics. Its main achievement is in establishing a narrative about the war.

This group is also popular on the Telegram network, where they have about 90k subscribers on their channel "**WE ARE KILLNET**."

There are memes that criticize Ukraine and the West in general, but they also post targets for their subscribers to attack – where we can also see a list of US airport websites that they targeted.



Killnet is the polar opposite of the “[IT Army of Ukraine](#),” which is a [Telegram channel](#) set up to direct people to attack Russian websites, though they have more than double the subscribers (200k) and a focus on DDoSing rather than memes.

Similar Attacks

Killnet has targeted a wide range of countries, including:

- Japan
- Estonia
- Lithuania

The goal of each attack is to side with Ukraine and engage in anti-Russian activities.

One of the more interesting attacks was on Lithuania’s largest gas and energy supplier in July of this year, called the “[biggest cyber-attack in a decade](#)”.

In retaliation for Lithuania’s embargo on sanctioned Russian goods, the hacker group had previously carried out DDoS attacks against Lithuanian military, government, private, and public internet services and websites.



Why Did Killnet Attack US Airports?

Based on some research through well-known networks and people who deal with hacking groups, we concluded that Killnet only wanted media attention in this attack, given that there was no serious impact other than the temporary destruction of US airport websites.

Many hacktivist groups act in this manner to express dissatisfaction and to inform the community that they are active.

From our side, you can consult with any of our cyber security experts who will help you defend against DDoS attacks and how to preemptively set up the infrastructure so that there are no unwanted consequences.



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

ADVOCATE AURORA HEALTH EXPOSES DATA OF 3M PATIENT

Summary Of The Attack

- Advocate Aurora Health, which a 26 hospital healthcare system in Wisconsin and Illinois suffered a data breach which exposed data of 3 million patients.
- The issue most likely occurred due to improperly implemented Meta Pixel tracker.
- AAh is currently under investigation from the federal government.
- The official advice to the users is to use web browsers' trackers-blocking features or to use the incognito mode of the browser when logging in on medical portals.



Analysis by:
Eva Georgieva



**A Veteran Owned & Led
Cyber Security Company**

**Meet Our Experts >
Request A Free Consult >**

What Happened?

Advocate Aurora Health, AAH, a 26-hospital healthcare system in Wisconsin and Illinois, is notifying its patients of a data breach that exposed the personal data of 3 million patients. The data leakage happened due to the improper usage of Meta Pixel on Advocate Aurora Health's websites, where patients could log in and enter sensitive medical and personal information.

What Is A Meta Pixel?

Meta Pixel is an analytical tool that allows you to track your website visitors activities. This tool informally is known as the Facebook retargeting pixel, which is basically a snippet of code you can insert into the backend of your website and it helps drive and decode key performance metrics generated by a particular platform.

The way it works is by loading a small library of functions that you can use whenever a site visitor takes an action that you want to track. You will also have options to reach those users again through future Facebook ads.

It might be quite surprising that a pixel which is a tiny area on the display screen can also be used for online advertising. A tracking pixel is basically a 1×1 graphic that is loaded each time a person checks the website that has the pixel implemented.

All this data should be encrypted and depersonalized if implemented correctly.



What Was The Impact?

This practice is against the data privacy rules of the United States and Aurora Advocate Health is already **under investigation and its breach is publicly disclosed** on the official site of the United States Department. This could also lead to AAH being heavily penalized via class action lawsuits.

How Did The Data Leak Happen?

Security researchers commenting on the data breach have stated that the main reason for the data breach of 3 million patient records was the poor implementation of the Meta Pixel.

They stated that generally, pixels do not collect the level of information that was disclosed in the data breach which indicates that the implementation must have been done quite poorly and without the approval of information security teams to cause sensitive PHI to be disclosed to third parties.

The initial analysis that was conducted by the Advocate Aurora Health's investigation team showed that data such as:

- IP address
- Dates and times of scheduled appointments
- Gist of patient's medical history
- Proxy account information



Advocate Aurora Health's Response

Currently, the Pixel tracker has been disabled on all systems as notified by Advocate Aurora Health and they have implemented safeguards to prevent something similar like this from happening again.

However, the damage from the current data breach has already been done and the 3 million patient data have already been exposed.

Their official advice to the users is to use web browsers' trackers-blocking features or to use the incognito mode of the browser when logging in on medical portals.

This should pose a wake-up call for organizations to comprehend the risk they are undertaking when powering their web applications with tracking tools, especially from third-party vendors.

They are not only exposing their patients' data but also are putting themselves in a situation to face class action lawsuits and fines.



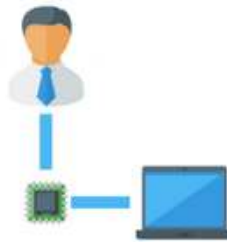


ENTERPRISE PENETRATION TESTING

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

SPEAK WITH AN EXPERT



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

MICROSOFT CAUSES 2.4 TB DATA LEAK

Summary Of The Attack

- On September 24, 2022 SOCRadar detected a misconfigured public bucket where Microsoft stored 2.4 TB of data.
- Impacted were 65,000 entities from 111 countries.
- The exposed data is dated from 2017 to August 2022.
- Microsoft stated that SOCRadar exaggerated the scope of the data leaked.



Analysis by:
Eva Georgieva



**A Veteran Owned & Led
Cyber Security Company**

**Meet Our Experts >
Request A Free Consult >**

What Happened?

Misconfiguration of an endpoint caused a leakage of 2.4 TB of data of Microsoft's customers. The issue stemmed from a misconfigured Azure Blob Storage and was spotted on September 24, 2022, by the [security company SOC Radar](#).

Who Was Impacted?

According to the SOCRadar statement, the data leaked was stored on a misconfigured Azure Blob Storage and the impact spanned 65,000 entities from 111 countries. Customer data was the entity that suffered in this Microsoft data leak, which included:

- Names
- Email addresses
- Email content
- Company name
- Phone numbers
- Proof of concept documents
- Sales data

In addition, attached files relating to business between a customer and Microsoft or an authorized Microsoft partner were also exposed. Per their statement, the exposed data is dated from 2017 to August 2022.



Added security | https://buckets.grayhatwarfare.com/bucket/507619/0

Home Filter Buckets Search Files Docs / API Top Keywords

Files in olympusv2.blob.core.windows.net

1 - 20 of 5382 results

#	Bucket	Filename	Container	Size
1	olympusv2.blob.core.windows.net	documents/100057-FW-Buy-E4-Now-promo-msg-54fadf27-58e5-4317-0236-0cc6b03694f6	documents	103.50kB
2	olympusv2.blob.core.windows.net	documents/100285-PGE-PD-97365307-for-409f8d95-90a1-4afe-ac30-5aff0e1ee962	documents	865.00kB
3	olympusv2.blob.core.windows.net	documents/100295-PGE-Buy-E4-Now-Offe-144d66b7-e495-42d3-b12c-a91497d4c0a7	documents	412.50kB
4	olympusv2.blob.core.windows.net	documents/100319-PGE-ABRIL-COMUNICAB-42024670-483b-429f-bda2-e133fb8a2e0	documents	149.50kB
5	olympusv2.blob.core.windows.net	documents/100321-ADIDAS-GROUP-PROD-F-90557631-43b5-4f32-a521-0d219c614ed	documents	477.02kB
6	olympusv2.blob.core.windows.net	documents/104337-FY16AGPGE123-docx-7651b385-2a85-43a4-eb36-3b895a173f3a	documents	31.51kB
7	olympusv2.blob.core.windows.net	documents/104337-FY16AGPGE123-docx-0200523f-bc27-49d6-a9fa-4cfe21a7d4e	documents	31.51kB
8	olympusv2.blob.core.windows.net	documents/104496-FY16AGPOEMilestone1-5db5a634-4e2e-4c6e-a703-4ffb73b00ba	documents	24.40kB

Researchers stated that the bucket was publicly indexed for months and it actively appeared in search engines.

The researchers named the leak “BlueBleed” referring to the exposed sensitive data from six misconfigured buckets.

SOCRadar even [set up a website called BlueBleed](#) where users can check if their data has been exposed.



What Is BlueBleed?

From the official SOCRadar website it is clearly stated that the term “BlueBleed” was created by Can Yoleri, who is a Threat and Vulnerability Researcher at SOCRadar.

The term refers to the sensitive information leaked by six misconfigured buckets collectively. In their blog post, it is clearly elaborated how they discovered BlueBleed Part I as it is referred to.

The issue they stated was clearly a misconfigured public bucket where they stored 2.4 TB of data inside one single bucket.

By their estimation, it can be considered maybe one of the most significant B2B leaks, considering the scope of it.

RE: ACTION REQUIRED: Final Proof of Execution (POE) document required for [redacted]

[redacted]

[redacted]

From: [redacted]
Sent: Tuesday, 17 July 2018 8:08 AM
To: [redacted]
Cc: [redacted]
Subject: RE: ACTION REQUIRED: Final Proof of Execution (POE) document required for [redacted]

Hi [redacted]

Same with this one, thanks for addressing the phone number and service description matter through the [redacted] comments.

With regards to the customer identifier issue, I am unable to retrieve the POE document from same email [redacted] as what is needed. Please send the email from customer with the POE attachment to this alias, [redacted] for my further review.

Cordially,
[redacted]

From the [redacted] support team
Hours of Operation: Business Days 8:00 a.m. to 5:00 p.m., local time, in all supported geo.
Standard Response Time on weekdays: within 24 hours based on posted hours of operation.

Please reach out to the appropriate alias below, should you have any further questions:

Geographical Region	Alias
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]



How Can The Information Be Used?

Third parties or threat actors that might have had access to the bucket can use this information in different ways.

The first and most obvious one is scraping the email addresses for targeting the companies affected by the breach utilizing social engineering techniques, however blackmailing and selling the information on the dark web or Telegram channels are also viable options.

Besides that, SOC Radar also stated that the information exposed included information about network configuration and infrastructure posture of potential customers.

This opens another vector of attack, where researchers or threat actors might start looking for vulnerabilities in those systems and network configurations based on the information from the exposed data.



Microsoft's Response

Microsoft in their statement elaborated that they do appreciate that SOCRadar informed them about the issue, however, following SOCRadar's blog post Microsoft stated that the security company has greatly exaggerated the scope.

Based on Microsoft Security Response Center's in-depth analysis and investigation they were able to conclude that a lot of the data that was exposed was duplicate information with multiple references to the same projects, email addresses and users.

They also expressed their disappointment in SOCRadar releasing a search tool where users can check if their data is exposed, since that does not follow best security practices and may even pose an additional security risk.

Actions Taken

In the official statement released towards the customers, Microsoft stated that they did notify every impacted customer directly and provided them with instructions on how they can further proceed to handle the incident.



OPTUS EXPOSES 2.1 MILLION CUSTOMERS IN DATA BREACH

Summary Of The Attack

- On October 3, 2022, Australian mobile company Optus confirmed that a cyberattack last month had exposed the government identification numbers of 2.1 million of its customers.
- The threat actor had first tried to blackmail Optus by demanding a \$1 million ransom in exchange for them not disclosing or selling the stolen data.
- The actual data breach appears to have been caused due to improperly configured security protections on an API endpoint, but still, there is no proper understanding in Optus of how the incident occurred.



Analysis by:
Dušan
Trojanović



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

What Happened?

On October 3, 2022, Australian mobile company Optus confirmed a cyber attack last month had exposed the government identification numbers of 2.1 million of its customers.

What Was The Impacted?

The Disclosure came following the leak of 10,000 Optus customer records, which included user information such as:

- Names
- Birthdates
- Home
- Email addresses
- Phone numbers
- Personal identification numbers

14,900 genuine Medicare ID numbers were also compromised as a result of the incident.



How The Attack Happened

The actual data breach appears to have been caused due to improperly configured security protections on an API endpoint, but still, there is no proper understanding in Optus of how the incident occurred or how to stop it from happening again. [Optus has hired Deloitte](#) to conduct an independent external review of the company's security systems and processes.

At least one number from a current, legitimate form of identification, along with personal data, has been compromised for about 1.2 million clients.

These customers have been contacted by Optus, and it has been suggested to take steps to update their identification documents.

Along with personal information, numbers related to expired IDs have been exposed to about 900,000 customers. Optus consults with authorities on what additional actions clients should take.

The Ransom Demand

The threat actor had first tried to blackmail Optus by demanding a \$1 million ransom in exchange for them not disclosing or selling the stolen data.

The hacker posted the personal information of 10,000 clients, including names, addresses, phone numbers, and dates of birth, on a hacking site after not being paid.



Optus Data will not be sold or leaked

by optusdata - Tuesday September 27, 2022 at 12:02 AM

optusdata



BreachForums User

MEMBER

Today, 12:02 AM

Too many eyes. We will not sale data to anyone. We cant if we even want to: personally deleted data from drive (Only copy)

Sorry too 10.200 Australian whos data was leaked.

Australia will see no gain in fraud, this can be monitored. Maybe for 10.200 Australian but rest of population no. Very sorry to you.

Deepest apology to Optus for this. Hope all goes well from this

Optus if your reading we would have reported exploit if you had method to contact. No security mail, no bug bountys, no way too message.

Ransom not payed but we dont care any more. Was mistake to scrape publish data in first place.

Optus can confirm for the 7.7 million clients for whom the leaked information did not contain valid or current document ID numbers after carefully analyzing the data for the company's 9.8 million customers with the assistance of government agencies.

Information like email addresses, birth dates, or phone numbers was included in the data. For these clients, it's critical to use caution.

What Is Optus's Response?

Customers whose current ID documents were affected by the cyberattack received emails or SMS messages from Optus informing them that their ID document information had been compromised and outlining what they should do. Additionally, Optus contacted clients whose IDs had expired to inform them that their IDs had been compromised.



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

Customers who have been informed that both their license number and card identification number have been compromised are urged to update their license number as soon as possible because the danger of identity fraud increases when this information is made public.

Customers are still advised to submit an application for a new license number even if only their license number was compromised.

More than 10,000 clients had their records put online, and the Australian Federal Police is currently conducting two investigations into who obtained and sought to sell the data and protections for those customers.

How Optus Could Have Prevented This Attack

If Optus had proper API monitoring in place, the transfer of sensitive data to the Internet, the lack of authentication, and the exposure of the testing API to public Internet traffic would have all been discovered, notified to, and addressed by Optus much earlier than a post to a data-leak forum.

The effects of the Optus data breach are still being felt, and a class action lawsuit is now a very real possibility.

Protecting a company and its clients from harmful data attacks requires a combination of technologies, training, and **building a culture of security awareness**.





\$570 MILLION IN CRYPTO STOLEN ON BINANCE BRIDGE

Summary Of The Attack

- In response to a cyberattack on October 4, 2022, which resulted in the theft of about two million BNB (Binance Coin) tokens, exchangeable for over \$570 million in fiat currency.
- The BSC Token Hub cross-chain bridge, which connects the BNB Beacon Chain/BEP2 and BNBChain/BEP20 chains, was exploited by the hacker.
- The hacker started distributing some of the funds around other liquidity pools in an effort to convert the BNB into other assets.
- Binance plans to hold on-chain governance votes to decide whether to offer a 10% bounty for finding the hacker and returning the funds and to set up a bug bounty program to award \$1 million to those who report serious bugs.



Analysis by:
Dušan
Trojanović



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

What Happened?

In response to a cyber attack on October 4, 2022, which resulted in the theft of about two million BNB (Binance Coin) tokens, exchangeable for over \$570 million, at the moment of article writing.

In order to conduct an investigation, Binance paused the BNB Smart Chain on October 6th, 2022, after acknowledging a security incident.



BNB Chain 
@BNBCHAIN



Due to irregular activity we're temporarily pausing BSC. We apologize for the inconvenience and will provide further updates here.

Thank you for your patience and understanding.

6:19 PM · Oct 6, 2022 · Twitter Web App

3,393 Retweets 2,151 Quote Tweets 9,705 Likes



Later that day, the CEO of Binance disclosed that an exploit was used in the BSC Token Hub to send BNB to the attacker, after which Binance had asked all validators to suspend the Binance Smart Chain, as well as that the issue is contained at the moment and that customers funds are safe.



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

What Was The Impact?

Initial estimates put the amount of money removed from the Binance Smart Chain at \$100M and \$110M.

However, an estimated \$7M was quickly frozen owing to the community, internal teams at Binance, and outside security partners.

The breach allowed hackers to get away with approximately \$570 million in digital assets, including:

- Ethereum
- Polygon
- BNB Chain
- Avalanche
- Fantom
- Arbitrum
- Optimism

In the wake of the breach, **BNB's price fell by about 3.7%**.



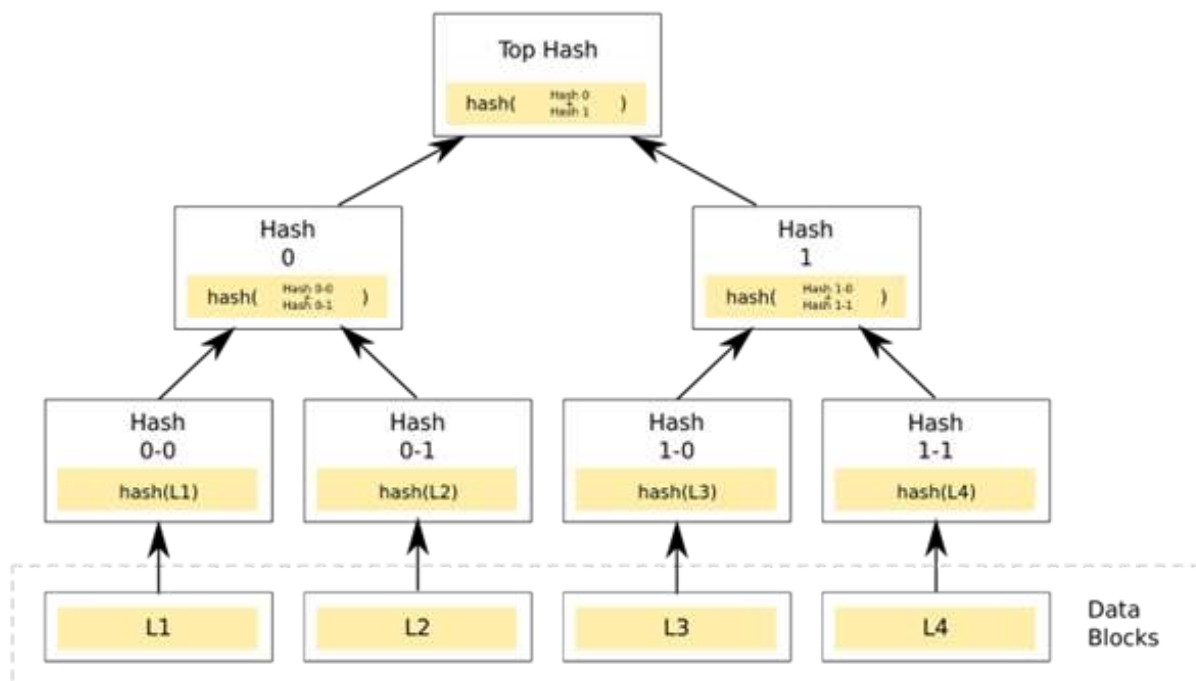
How The Attack Happened

BSC (Binance Smart Chain) was started out as a fork of Ethereum, which represents a protocol and decentralized blockchain.

In the world of cryptocurrencies, bridges function in a sense by locking funds on one side of the bridge and then receiving an equal amount of other funds on the other side of the bridge.

Bridges are beneficial for connecting blockchains, but because they frequently require a central storage location to lock deposited assets, they are generally seen as being less secure than base-layer networks like Bitcoin and Ethereum.

The BSC Token Hub cross-chain bridge, which connects the BNB Beacon Chain/BEP2 and BNBChain/BEP20 chains, was exploited by the hacker.



Data in smart contract blockchains are stored in trees. The Cosmos ecosystem's AVL tree implementation is used by the Binance Bridge. The data representation is known as the Merkle tree. Hash functions are used to validate these trees.

Hashes are proven up the tree from the leaf nodes to the root.

Who owns what can be altered if someone is able to manipulate the data in leaf nodes while still producing hashes that are validated as accurate by higher-up nodes.

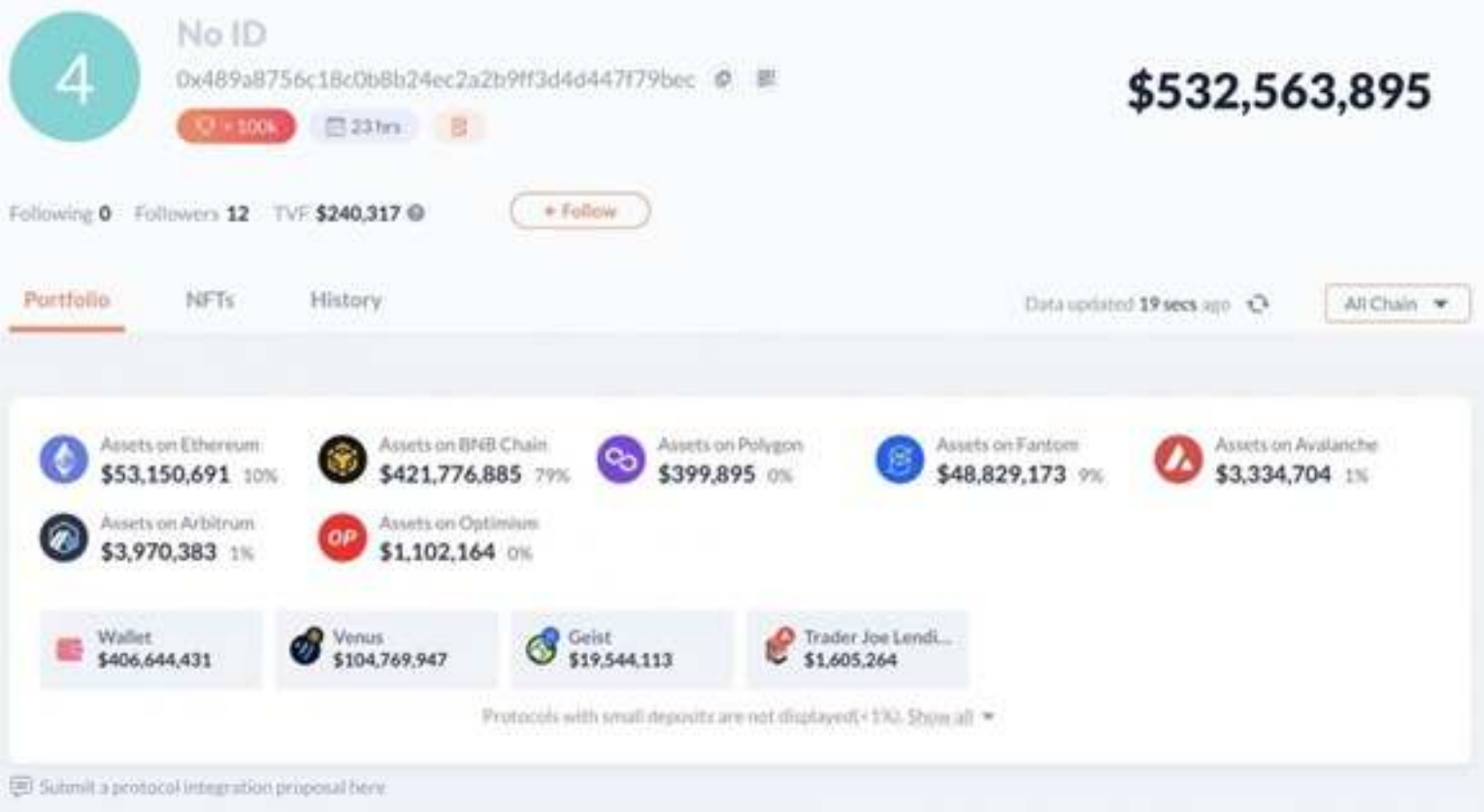
This suggests that someone might have been able to forge those proofs.

Who Is Responsible?

The attacker, now known as the "BNB bridge exploiter," appears to have registered as a relay for the BSC Token Hub bridge as the initial step in the attack so they could set up for the exploit.

The BSC Token Hub bridge was able to accept forged proof messages created by the attacker.





The bridge's failure to completely verify the Merkle tree to the root hash likely caused the problem, allowing the attacker to create forged proofs from an earlier, legitimate one and mint BNB directly to their wallet.

The attacker was able to forge proof messages which were accepted by the BSC Token Hub bridge.

The bug likely was a result of the bridge not fully verifying the Merkle tree to the root hash, which allowed the attacker to generate forged proofs from a previous, legitimate one and then mint BNB directly to their wallet. The attack proved to be unique because the attacker did not steal existing funds, but rather minted new ones.

As quickly as possible, the hacker started distributing some of the funds around other liquidity pools in an effort to convert the BNB into other assets.



Not Binance's First Hack

This is not Binance's first significant hack.

The hacker stole over 7,000 bitcoins from the exchange in 2019, costing Binance almost \$40 million.

Although the funds were never found, the business compensated customers for their losses.

The theft is the most recent in a string of attacks against blockchain bridges, which enable cross-blockchain transactions via so-called smart contracts.

The theft of Nomad for \$191 million happened in August. Prior to that, there was the:

- Poly Network Bridge (\$610 million that was reimbursed)
- Wormhole Bridge (\$320 million)
- Meter.io Bridge (\$4.4 million)
- Ronin Bridge (\$600 million)
- Qubit Bridge (\$80 million)
- Wormhole Bridge (\$320 million)



What Is Binance's Response?

Binance plans to hold on-chain governance votes to decide whether to:

- Offer a 10% bounty for finding the hacker and returning the funds.
- Set up a bug bounty program to award \$1 million to those who report serious bugs.
- Freeze the hacked funds.
- Use BNB auto-burn to restore the remaining hacked funds.

Cross-chain bridges have emerged as the most frequent target of ultra-high value hacks in recent years, in part because they constantly hold enormous amounts of cryptocurrency tokens.



**A Veteran Owned & Led
Cyber Security Company**

**Meet Our Experts >
Request A Free Consult >**

TIKTOK DENIES CYBER ATTACK

TikTok

Summary Of The Attack

- A hacker organization called “AgainstTheWest” posted a discussion on a forum and claims that this server contains 2.05 billion records in a vast 790GB database containing user data, platform statistics, software code, cookies, auth tokens, server info, and many more.
- Microsoft Corporation revealed on August 31 that it has discovered a high severity vulnerability in TikTok’s Android application that could have been used by attackers to quickly compromise user accounts.
- It is advised for users of the TikTok video platform to update their passwords and enable two-factor authentication.



Analysis by:
Dušan
Trojanović



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

What Happened?

Popular short-form social video platform TikTok denied reports that it had been compromised by the hacking group [AgainstTheWest](#) after they claimed to have gained access to an insecure cloud server and also mentioning the source code posted on hacking forums isn't part of its platform.

What Was The Impact?

The denial comes in response to suspected hacking reports that appeared on the breach forums message board on the 3rd of September. The threat actor claimed that the server holds 2.05 billion records in a massive 790GB database.

TikTok also mentioned that the leaked user data could not result from a direct scraping of its platform, as they have adequate security safeguards to prevent automated scripts from collecting user information.

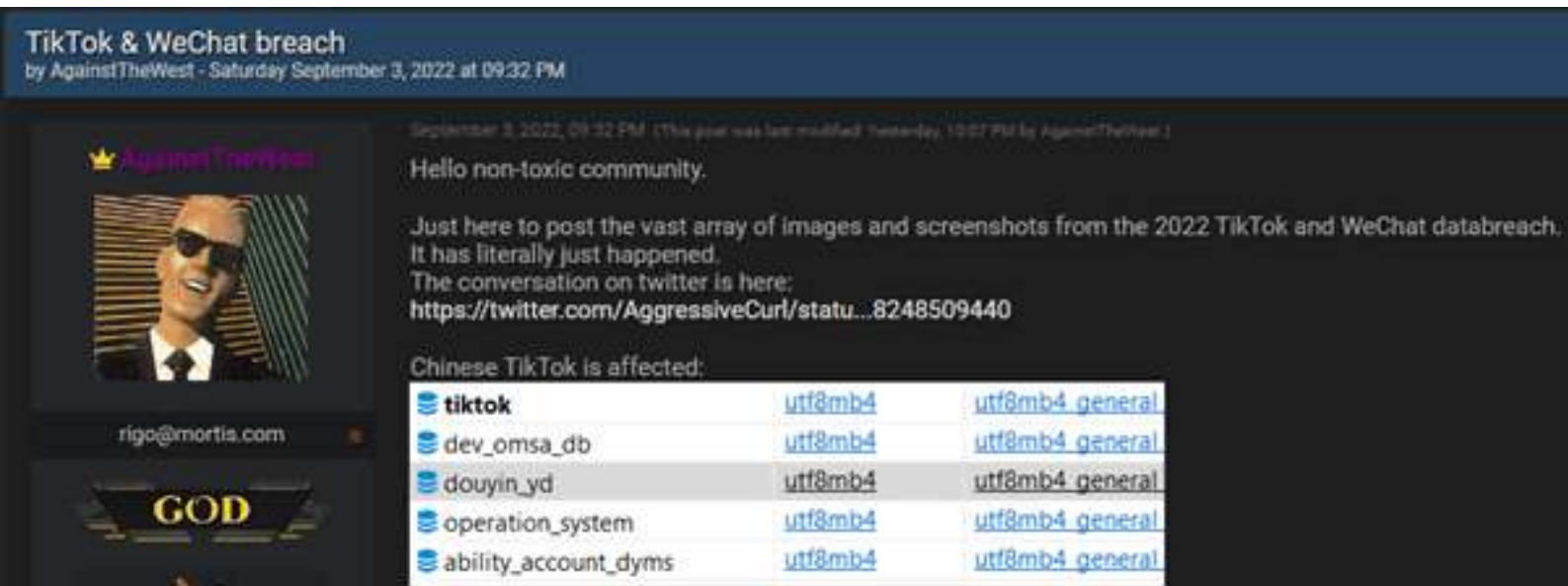
How This Attack Happened

A hacker organization called "AgainstTheWest" posted a discussion on a forum on the 3rd of September, a hacking group known as 'AgainstTheWest' created a topic on a hacking forum claiming to have breached both TikTok and WeChat.

The user shared images of what they claim to be screenshots of a database used by the companies, accessed on an Alibaba cloud instance, containing data for both TikTok and WeChat users.



The threat actor claims that this server contains 2.05 billion records in a vast 790GB database containing user data, platform statistics, software code, cookies, auth tokens, server info, and many more.



WeChat and TikTok are both Chinese companies, however, they are not owned by the same parent company. WeChat is owned by Tencent, while TikTok is owned by ByteDance. Thus, the fact that they were both found in the same database suggests that there was not a direct breach on each platform.

Most likely, the unprotected database from a third-party data scraper or broker who scraped publicly available data from both services and exported data into a single database.

Additionally, some security researchers verified the authenticity of the user data that was exposed, but they were unable to draw any firm conclusions regarding the data's origin.



Table Name
app_info
app_server_info
cookie
sys_user
tiktok_author_stats
tiktok_author_stats_his
tiktok_author_stats_yesterday
tiktok_category
tiktok_day_statistics
tiktok_user
tiktok_user_stats_daily
tiktok_video
tiktok_video_link_parse_record
tiktok_video_parse_record
tiktok_video_stats_daily
tiktok_video_username_parse_record

```

DROP TABLE IF EXISTS `user_friend`;
CREATE TABLE `user_friend` (
  `friend_sn` varchar(100) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  `operation_sn` varchar(100) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  `friend_wechat` varchar(50) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  `nick_name` varchar(150) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  `remark_name` varchar(150) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  `gender` char(1) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  `city_id` varchar(50) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  `province_id` varchar(50) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  `create_time` timestamp(0) NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `status` char(1) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  `group_id` tinyint(4) NULL DEFAULT -1 COMMENT '客服自定义分组',
  `tag_id_list` varchar(100) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  `show_user_level` tinyint(4) NULL DEFAULT -1 COMMENT '秀场等级',
  `show_royl_level` tinyint(4) NULL DEFAULT -1 COMMENT '秀场等级',
  `remark` varchar(500) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  `scene` varchar(10) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  `show_reply_cnt` smallint(6) NULL DEFAULT 0 COMMENT '秀场回复次数',
  `status_date` timestamp(0) NULL DEFAULT NULL COMMENT '状态日期',
  `marketing_num` smallint(6) NULL DEFAULT 0 COMMENT '营销套餐数',
  `marketing_cnt` tinyint(4) NULL DEFAULT 0 COMMENT '营销次数',
  `marketing_date` timestamp(0) NULL DEFAULT NULL COMMENT '营销日期',
  `show_reg_time` timestamp(0) NULL DEFAULT NULL COMMENT '秀场注册时间',
  `status_mode` varchar(2) CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL,
  PRIMARY KEY (`operation_sn`, `friend_sn`) USING BTREE,
  INDEX `create_time` (`create_time`) USING BTREE,
  INDEX `friend_sn` (`friend_sn`) USING BTREE
) ENGINE = InnoDB CHARACTER SET = utf8mb4 COLLATE = utf8mb4_0900_ai_ci

```

Personnel from TikTok confirmed that the data samples described are all publicly available and are not the result of any breach of TikTok systems, networks, or databases.

Microsoft Reveals Vulnerability

Microsoft revealed on August 31 that it has discovered a high severity vulnerability in TikTok’s Android application that could have been used by attackers to quickly compromise user accounts.

The vulnerability discovered by Microsoft is a more specific problem that may have affected Android-powered mobile devices and placed millions of accounts at risk. In February 2022, Microsoft informed TikTok of the issue, and less than a month later, the vulnerability was addressed.



For East and Southeast Asia, TikTok's Android app is available in two flavors: com.ss.android.ugc.trill for that region, and com.zhiliaoapp.musically for the rest of the world.

Microsoft conducted a vulnerability study on the TikTok Android app and found that the issues were affecting both versions of the app, which have over 1.5 billion installations through the Google Play Store.

As part of our responsible disclosure policy, a Microsoft security researcher informed TikTok of the flaws in February 2022 via [Coordinated Vulnerability Disclosure](#) (CVD) via [Microsoft Security Vulnerability Research](#) (MSVR).

Was TikTok Breached?

Even though TikTok has strongly denied a breach, the data in the database may have originated from other sources. If the further analysis reveals that the data is legitimate, TikTok will be required to take action to mitigate the leak's effects even if it wasn't penetrated.

How Can You Protect Yourself?

It is advised for users of the TikTok video platform to update their passwords and enable two-factor authentication.



SENSITIVE NATO DATA LEAKED AFTER CYBER ATTACK

Summary Of The Attack

- Diario de Noticias, a local Portuguese news organization, on September 8th reported that the Portuguese Government Department of Defense has been a subject of a cybersecurity data breach involving leakage of sensitive NATO documents that are published and sold on the dark web.
- After an investigation was performed, it was established that unsecure channels were used for transmission of data.
- The attack in which the data were exfiltrated was constructed in such a manner that it was undetectable and it was launched through a bot network that was primarily designed to obtain sensitive data.
- The Department which suffered the breach is under suspicion that they broke protocol which led to the incident.



Analysis by:
Eva Georgieva



**A Veteran Owned & Led
Cyber Security Company**

**Meet Our Experts >
Request A Free Consult >**

What Happened?

On September 8, Portuguese local news organization, Diario de Noticias reported that the Portuguese Government's Department of Defense has allegedly been a subject of a cyber security data breach involving exfiltration of confidential NATO documents.

The Anatomy Of The Attack

The General Staff of the Armed Forces (EMGFA) was the department that was attacked and hundreds of documents were found for sale on the dark web. The department that was attacked only found out about the incident after US intelligence informed them of it.

Portugal's Prime Minister António Costa was informed about the breach through the US embassy in Lisbon.

According to the report, a team of security experts from the National Security Office and also a team from Portugal's national cyber security center investigated the attack and the network and it was established that unsecured channels were used for sending and receiving classified documents.

Later on, they also came to the conclusion that the attack was constructed in such a manner that it was undetectable and it was launched through a bot network that was primarily designed to obtain sensitive data.



Human Error Or Breaking Protocol?

Since we should be talking about highly secure systems, in the General Staff of the Armed Forces (EMGFA), a government department that deals with highly confidential information, **we would assume that the computers are air gapped**, which reportedly it was the case, however, the exfiltration used standard non-secure lines.

From that, the initial conclusion of the investigation was that the top military body had broken the operational security rules at a certain point which led to the secret information being exposed, leaked and then sold on the dark web.

From the results of the investigation, it was also reported that **the exfiltration of documents that were sent from NATO to Portugal** took place on EMGFA computers, mainly those used by CISMIL, The Department for Military Secrets, and The General Directorate of Resources of National Defense.



Next Steps

The National Office of Security (GNS), External Secrets, and The Secret Services are involved in investigating the hack, however, allegedly NATO did demand an explanation from the Portuguese government even though they didn't want to make any official statements on the matter.

On the other hand, the Portuguese Prime Minister's office spokesperson gave a statement in which it was elaborated that the government is dedicated to maintaining and protecting its armed forces and the Defense Ministry's credibility as a founding member of NATO.

Furthermore, the spokesperson noted that they will continue to work daily, as they have so far, so that their credibility remains intact.



UBER'S INTERNAL SYSTEMS COMPROMISED BY AN 18 YEAR OLD

Summary Of The Attack

- On September 15th, Uber's internal systems were compromised.
- The attacker managed to hack the company's HackerOne account, gained access to a Slack account and obtained full admin on their AWS Web Services and GCP accounts.
- The entry attack targeted Uber's employees utilizing a social engineering campaign.
- Uber is still investigating the incident and some of their internal systems were temporarily disabled due to the hack.



Analysis by:
Eva Georgieva



Analysis by:
Dalibor Gašić



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

What Happened?

On September 15th, an 18 year old managed to hack Uber. The hacker reportedly gained control over the company's internal systems leveraging social engineering techniques that led to compromising an employee's Slack account.



From there on the hacker accessed their internal databases, and obtained control of the company's Amazon Web Services and Google Cloud accounts.



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

How The Attack Happened

Allegedly the attack was carried out by the hacker performing what it seems to be a classic social engineering play.

The hacker sent a text message to an Uber employee that seemed like it was coming from the Uber's IT department, the employee thought it was a legitimate message coming from their department and they shared their password.

Once the password was shared the hacker was in.

What Was The Impact?

On September 16th, Uber decided to give a statement on Twitter, claiming that they are responding to a cybersecurity incident without giving out too many details.

However, data coming in from different sources indicates that the hacker got access to Uber's HackerOne account and most likely all their reports.

 Uber staff posted a comment. Sep 15th (5 mins ago)

UBER HAS BEEN HACKED (domain admin, aws admin, vsphere admin, gsuite SA) AND THIS HACKERONE ACCOUNT HAS BEEN ALSO



Apart from that, [Sam Curry](#), a Bug Bounty Hunter, also shared on Twitter that the hacker claimed they've got full administrative rights on AWS and Google Cloud Platform.



From an Uber employee:

Feel free to share but please don't credit me: at Uber, we got an "URGENT" email from IT security saying to stop using Slack. Now anytime I request a website, I am taken to a REDACTED page with a pornographic image and the message "F*** you wankers."

9:19 PM · Sep 15, 2022 · Twitter for iPhone

282 Retweets 107 Quote Tweets 1,556 Likes

He also posted that an Uber employee shared that at Uber they got an urgent email stating that all employees should stop using Slack, which is the platform on which the hacker, after gaining access, posted a message from the compromised user's account saying "[I announce I am a hacker and Uber has suffered a data breach.](#)"

From the employee statements, the message initially was not taken seriously by the rest of the employees, until the IT team asked the employees to stop using Slack.



The Aftermath

Uber still hasn't disclosed the scope of the breach and how exactly they are dealing with it.

However, it does seem like the hackers were motivated by the hack by the low pay that Uber drivers receive as was seen in one of the messages that were posted on Slack, as reported by [The New York Times](#).

They haven't asked for a ransom and it does look like they have done this to affect Uber's reputation.

Concealing A Data Breach

This is not the first time Uber had to deal with a cyber security data breach. [In 2016, 57 million driver accounts were breached](#) and confidential information was stolen.

A deeper investigation was conducted into the current and now former and accused CISO [Joseph Sullivan](#).

This month, [Mr. Sullivan was found guilty of obstructing justice and actively concealing a felony for concealing the breach](#) from the Federal Trade Commission, which was investigating Uber's privacy protections at the time.

He faces up to five years in prison for obstruction and up to three years for the latter charge.



Based on our sources and information available online, Sullivan was made aware of a data breach that had occurred at Uber which happened on November 3, 2016.

A hacker had gained access to the personal information of 57 million Uber users, including their names, email addresses and phone numbers.

Rather than reporting the breach to the authorities, Mr. Sullivan hid it.

He then paid the hacker \$100,000 to destroy the evidence and keep quiet about what had happened.



**A Veteran Owned & Led
Cyber Security Company**

**Meet Our Experts >
Request A Free Consult >**



CISCO SUFFERS CYBER ATTACK BY UNC2447, LAPSUS\$, & YANLUOWANG

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 and that the actor tried to extort them under the threat of leaking stolen files online.
- During the investigation, it was determined that a Cisco employee's credentials were compromised.
- The attacker conducted a series of sophisticated voice phishing attacks under the guise of various trusted organizations.
- After obtaining initial access, the threat actor conducted a variety of activities to maintain access, minimize forensic artifacts, and increase their level of access to systems within the environment.



Analysis by:
Dušan
Trojanović



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

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.

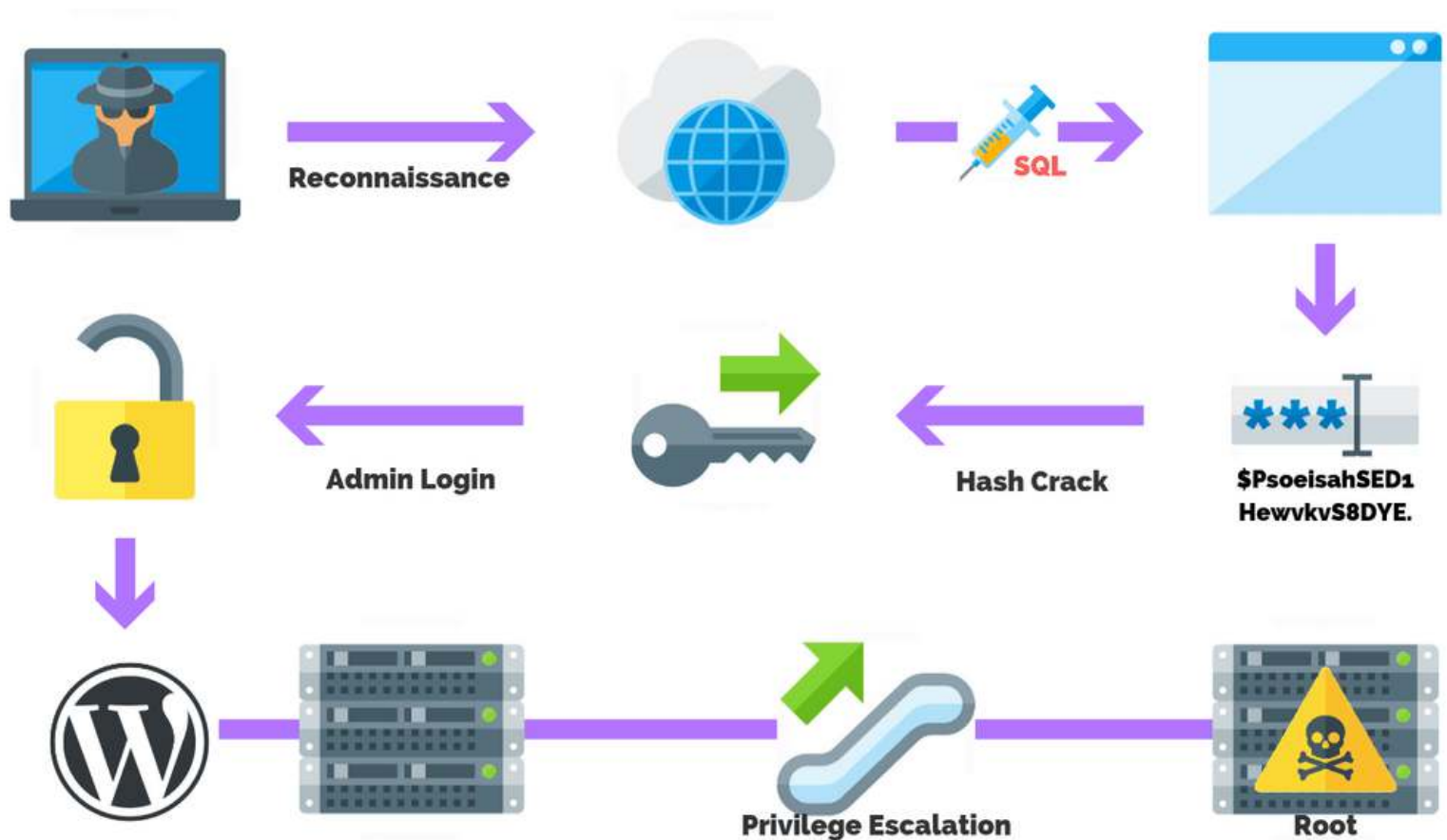
After obtaining the user's credentials attacker attempted to bypass MFA (Multi-Factor Authentication) with multiple bypass techniques, and with two of them, vishing (Voice phishing) and MFA fatigue attackers managed to gain access and enroll multiple new devices to authenticate to Cisco VPN service.



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 as performing a variety of activities for:

- Maintaining systems access
- Minimizing forensic artifacts
- Increase 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.



SAMSUNG EXPOSES PII IN RECENT DATA BREACH

Summary Of The Attack

- Samsung experienced a data breach back in late July and discovered the intrusion in early August.
- Samsung neglected its duty as a collector of personal information by not reporting the incident to affected customers in a timely manner.
- A proposed class action accuses Samsung of not warning customers of the breach in a reasonable amount of time.
- Names, contact and demographic details, dates of birth, and information related to product registration were all allegedly compromised, according to Samsung's statement. Although Samsung claims that neither social security numbers nor credit or debit card information was accessed.



Analysis by:
Dušan
Trojanović



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

What Happened?

Samsung experienced a data breach back in late July and discovered the incident in early August.

Cyber attacks can typically go undetected for weeks or months, and it would be wise for companies involved to make public these incidents, lest they face legal ramifications, as Samsung is about to.

The case, which was submitted to the U.S. District Court for Nevada, claims that Samsung neglected its duty as a collector of personal information by failing to notify impacted customers in a timely manner, until September.

What Was The Impact?

Samsung disclosed a data breach that it discovered on or about the 4th of August that compromised the personal data of more than 3,000 customers. Several Samsung US systems were compromised in late July 2022 after information was obtained by an unauthorized party.

Samsung stated that they determined through ongoing investigation that the personal information of certain customers was affected.

Samsung claims that it found out about the breach after conducting an investigation. The issue raised by the complaint, though, is that Samsung didn't contact its affected customers until the following month.



Personal Identifiable Information Exposed

Names, contact and demographic details, dates of birth, and information related to product registration were all allegedly compromised, according to Samsung's statement. They observed that depending on the client, the information changed.

Although Samsung claims that neither social security numbers nor credit or debit card information was accessed, however, the extent of the data that was compromised is alarming.

Important Notice Regarding Customer Information

September 2, 2022

At Samsung, security is a top priority. We recently discovered a cybersecurity incident that affected some customer information.

In late July 2022, an unauthorized third party acquired information from some of Samsung's U.S. systems. On or around August 4, 2022, we determined through our ongoing investigation that personal information of certain customers was affected. We have taken actions to secure the affected systems, and have engaged a leading outside cybersecurity firm and are coordinating with law enforcement.

We want to assure our customers that the issue did not impact Social Security numbers or credit and debit card numbers, but in some cases, may have affected information such as name, contact and demographic information, date of birth, and product registration information. The information affected for each relevant customer may vary. We are notifying customers to make them aware of this matter.

At Samsung, we value the trust our customers place in our products and services – trust that we have built up over many years. By working with industry-leading experts, we will further enhance the security of our systems – and our customers' personal information – and work to maintain the trust our customers have put into the Samsung brand for more than 40 years.

Below are FAQs about the incident and additional recommended actions our customers can take to help protect their information. If you'd like to check your credit report, you are entitled under U.S. law to one free credit report annually from each of the three major nationwide credit reporting agencies.

We regret any inconvenience this may cause our valued customers and appreciate their trust in us.

To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228

Equifax
www.equifax.com
1-800-525-6285
Equifax Information Services LLC
P.O. Box 740241
Atlanta, GA 30374

Experian
www.experian.com
1-800-397-3742
Experian Inc.
P.O. Box 9554
Allen, TX 75013

TransUnion
www.transunion.com
1-800-680-7289
TransUnion LLC
P.O. Box 2000
Chester, PA 19016



A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

In its privacy policy, Samsung's data breach notice includes a vague mention of demographic information that was stolen by the hackers.

Samsung mentioned that it collects this unspecified demographic information to help deliver the best experience possible with its products and services, which is another way of expressing targeted advertising.

Cybercriminals may be interested in the stolen data for subsequent phishing assaults. The business warned clients not to click on links in shady emails or open unsolicited messages.

Samsung Experienced A Breach In March 2022

In March, Samsung experienced yet another serious security breach that exposed sensitive corporate information, including the source code for its Galaxy smartphone line.

The business then clarified that while some source code related to the operation of Galaxy devices was compromised, neither customer nor employee personal data was exposed.

Although the precise number of people affected is still unknown, the March hack was thought to have exposed 190GB of user data.



Why Did Samsung Wait To Disclose The Breach?

It is unclear why Samsung would wait until September to inform its customers if the breach was discovered sometime around the 4th of August.

According to the business, Samsung started sending emails to consumers whose personal information had been taken earlier this month.

Samsung stated that it began an inquiry, which is currently ongoing, after hiring a reputable outside cybersecurity firm. Law enforcement has also been notified by Samsung.

Samsung released a new privacy statement and reported a data breach on the same day. The updated policy now clearly indicates that, with the user's permission, Samsung may use a customer's precise geolocation for marketing and advertising.

Additionally, the revised policy clearly specifies how long Samsung keeps user-shared data from the Quick Share feature. Samsung claims it might compile the materials you share, which will be accessible for three days.



You made it to the end! As a reward you get a bunch of free stuff:

- [Top 6 Cyber-attacks And How To Prevent Them](#)
- [30 Free Security Policy Templates](#)
- [Data Security Policy Template](#)
- [Sample Penetration Test Report](#)
- [Sample Web Application Assessment Report](#)
- [Sample Vulnerability Assessment Report](#)

Here's what I'd like to ask of you in return.

First, send an email to Jason@purplesec.us and give me your honest feedback. We want to improve the quality of this report.

Second, [connect with me on LinkedIn](#). I'd love to get an opportunity to learn from you and connect you with my very awesome network of security professionals.

Finally, if you got value from this report please [consider sharing the work with a friend or on socials](#). It's always appreciated!

- Jason Firch, CEO & Co-founder

