AhnLab Cyber Threat Intelligence Report

TLP: GREEN

Deep Web & Dark Web Threat Trend Report

Ransomware Groups & Cybercrime Forums and Markets of September 2023

V1.0

AhnLab Security Emergency response Center (ASEC)

Oct. 6, 2023

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can only be accessed by the recipient or the recipient department** Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	**Can be copied and distributed within the recipient organization (company) of reports** Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	**Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training** Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded, meaning that the sum of each item may not match the total.

This report is a work of authorship protected by the Copyright Act.
Unauthorized copying or reproduction for profit is strictly prohibited under any circumstances.

Seek permission from AhnLab in advance if you wish to use a part or all of the report.

If you reprint or reproduce the material without the permission of the organization mentioned above, you may be held accountable for criminal or civil liability.

Contents

Note 5

Major Issues 5

1) Ransomware 5

(1) Akira 5

(2) ALPHV (BlackCat) 6

(3) LockBit 11

(4) RansomedVC 13

2) **Forum & Black Market** 17

(1) Data Breach Affecting 7 Million Users 17

(2) Personal Information of Police Officers Leaked 17

3) **Threat Actor** 20

(1) Prosecution of Individuals Associated with the Trickbot Cybercrime Group 20

(2) About USDoD 23

(3) Mastermind of #OpCanada Campaign 25

(4) Indonesian Hacktivist Groups Attacked the Digital Infrastructure of India 28

Conclusion 31

CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Note

This trend report on the deep web and dark web of September 2023 is sectioned into Ransomware, Forums & Black Markets, and Threat Actors. We would like to state beforehand that some of the content has yet to be confirmed to be true.

Major Issues

1) Ransomware

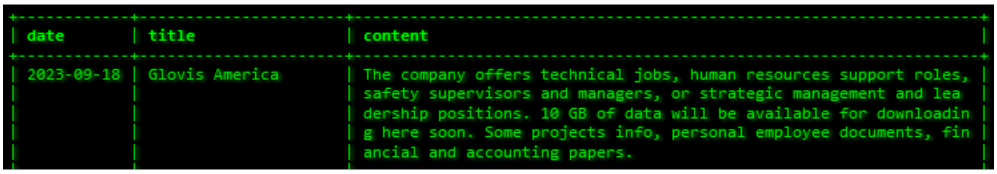
(1) Akira

The Akira ransomware gang was first discovered in March 2023, and as of September 2023, it has posted information from over 130 victim organizations on its Dedicated Leak Site (DLS) and is actively engaging in aggressive ransomware activities. According to the US cybersecurity company Arctic Wolf, it is believed that this group has a deep connection with the Conti ransomware gang (disbanded in mid-2022) as there were striking similarities found in its ransomware code as well as insights gained from the blockchain analysis.[1]

Arctic Wolf reported that it was able to discover additional wallet addresses by analyzing the known cryptocurrency wallet addresses and their transaction patterns. In some cases, the company observed the threat actors reusing cryptocurrency wallet addresses, which suggests that the individual controlling these wallet addresses may have split from the original group or is simultaneously cooperating with other groups.

The primary victims of Akira appear to be from the US and Canada, with a focus on small to medium-sized enterprises. Medical institutions and schools have also been designated as victims on the gang's DLS. Most recently, the gang designated the US subsidiary of a South Korean global logistics and distribution company as a victim.

[1] https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/



```
+------------+----------------------+-------------------------------------------------------------------+
| date       | title                | content                                                           |
+------------+----------------------+-------------------------------------------------------------------+
| 2023-09-18 | Glovis America       | The company offers technical jobs, human resources support roles, |
|            |                      | safety supervisors and managers, or strategic management and lea  |
|            |                      | dership positions. 10 GB of data will be available for downloadin |
|            |                      | g here soon. Some projects info, personal employee documents, fin |
|            |                      | ancial and accounting papers.                                     |
|            |                      |                                                                   |
```

Figure 1. South Korean global logistics and distribution company designated as a victim

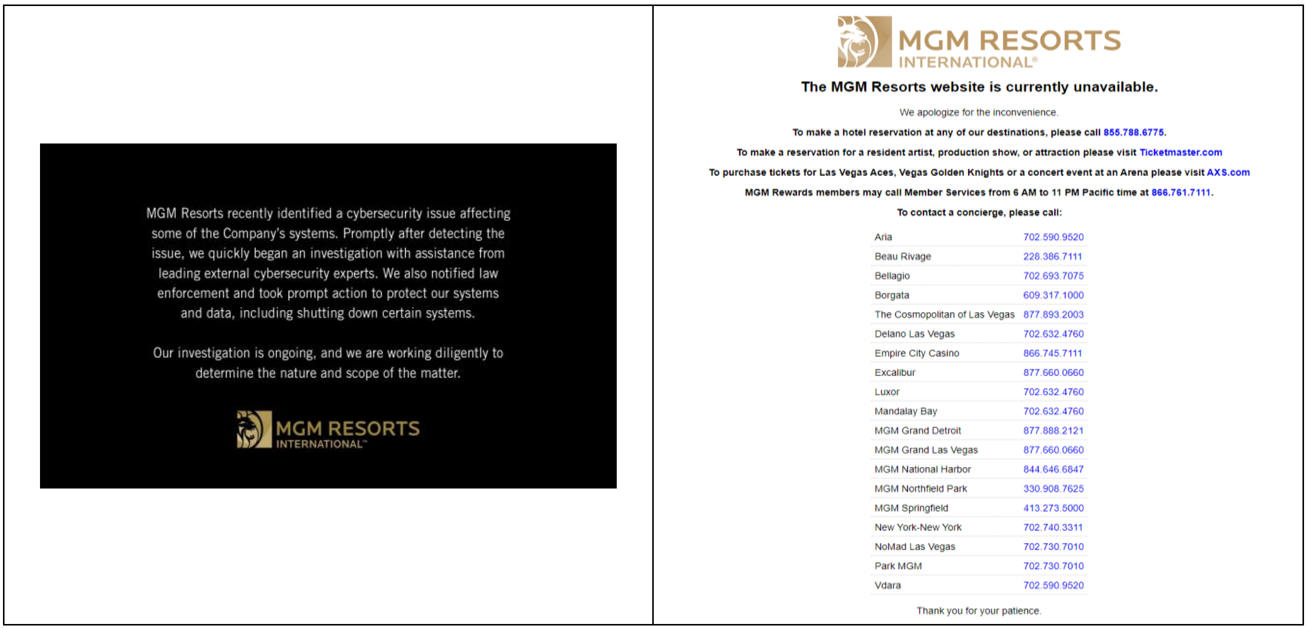
The gang claimed to have exfiltrated 10 GB of data including some project information, personal documents of employees, and financial and accounting records.

Among the recent victims of this gang are a Chicago-based automotive aftermarket parts catalog manufacturing company, a city redevelopment agency in San Diego, and a non-profit welfare organization called the Polish American Association.

(2) ALPHV (BlackCat)

MGM Resorts is the world's second largest casino hotel chain, following Caesars Entertainment in the US. The BlackCat ransomware gang designated MGM Resorts International as a victim on its DLS a week after its attack. Although the incident was initially reported as a cybersecurity issue on September 10th, the full scope of the matter was revealed a week later once the gang designated MGM Resorts International as a victim on its website.

MGM Resorts International announced through X (formerly Twitter) and its website that it temporarily shut down its IT systems due to a cybersecurity issue that began on Sunday night, September 10th.



MGM Resorts recently identified a cybersecurity issue affecting some of the Company's systems. Promptly after detecting the issue, we quickly began an investigation with assistance from leading external cybersecurity experts. We also notified law enforcement and took prompt action to protect our systems and data, including shutting down certain systems.

Our investigation is ongoing, and we are working diligently to determine the nature and scope of the matter.

The MGM Resorts website is currently unavailable.

We apologize for the inconvenience.

To make a hotel reservation at any of our destinations, please call 855.788.6775.

To make a reservation for a resident artist, production show, or attraction please visit Ticketmaster.com

To purchase tickets for Las Vegas Aces, Vegas Golden Knights or a concert event at an Arena please visit AXS.com

MGM Rewards members may call Member Services from 6 AM to 11 PM Pacific time at 866.761.7111.

To contact a concierge, please call:

Aria	702.590.9520
Beau Rivage	228.386.7111
Bellagio	702.693.7075
Borgata	609.317.1000
The Cosmopolitan of Las Vegas	877.893.2003
Delano Las Vegas	702.632.4760
Empire City Casino	866.745.7111
Excalibur	877.660.0660
Luxor	702.632.4760
Mandalay Bay	702.632.4760
MGM Grand Detroit	877.888.2121
MGM Grand Las Vegas	877.660.0660
MGM National Harbor	844.646.6847
MGM Northfield Park	330.908.7625
MGM Springfield	413.273.5000
New York-New York	702.740.3311
NoMad Las Vegas	702.730.7010
Park MGM	702.730.7010
Vdara	702.590.9520

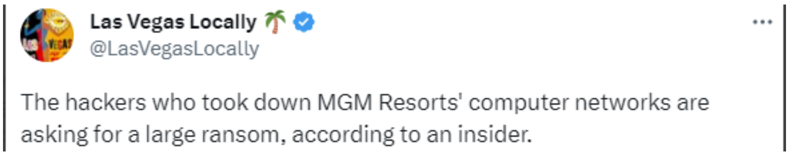
Thank you for your patience.

Figure 2. Notices of IT systems being shut down temporarily due to cybersecurity issues

At that time, the specific details of the issue were not disclosed, but the temporary shutdown of the following IT systems was confirmed.

- Main website
- Online room reservation
- Some parts of the casino's in-house services such as ATMs, slot machines, and credit card machines
- Smartphone application

Meanwhile, speculative posts suggesting that the incident may have been caused by ransomware were also circulating on social media.



Las Vegas Locally 🌴
@LasVegasLocally

The hackers who took down MGM Resorts' computer networks are asking for a large ransom, according to an insider.

Figure 3. News of MGM Resorts being affected by ransomware

This security incident is known as the second security breach experienced by MGM Resorts. The first one occurred in 2019 when its cloud services were compromised with the threat actors leaking records of over 10 million customers.

This incident was only discovered in 2020, and the exposed data reportedly included customer names, birth dates, email addresses, phone numbers, and addresses.

The reasons why cybercriminals target casinos, hotels, and entertainment resorts vary, but generally include the following reasons:

- Monetary benefits
  - ■ Casinos, hotels, and entertainment resorts value the availability and confidentiality of their customer data, making them more likely to negotiate for its recovery in case of damage

- Data value
  - ■ Sensitive information like customer details, credit card information, and reservation information can be illegally sold or used for other criminal purposes

- System vulnerabilities
  - ■ Casinos, hotels, and entertainment resorts operate complex IT systems, and since there is a chance for various vulnerabilities to exist, they are easy targets for threat actors

- Social impact
  - ■ Cybersecurity incidents at well-known casinos, hotels, and entertainment resorts can damage their reputation and the trust of victims while also garnering attention for the threat actors

According to a post made on September 14th Thursday by the individual who owns the vx-underground account on X (formerly Twitter), the ALPHV (BlackCat) ransomware gang was responsible for MGM's cybersecurity issue.[2]
Although it was initially reported that the gang collaborated with a cybercriminal group known as "Scattered Spider" for this attack, the BlackCat ransomware gang later denied this claim.

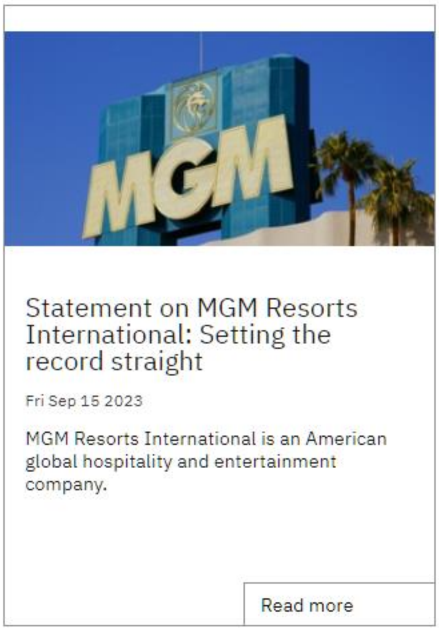
According to the press release, this group found an MGM Resorts employee's information on LinkedIn and posed as that employee to call the IT help desk and obtain system access privileges.[3]
The group is comprised of individuals from the US and the UK and the members are known to mainly employ the following tactics with their proficiency in their native language (English):

[2] https://twitter.com/vxunderground/status/1701758864390050145

[3] https://www.engadget.com/hackers-claim-it-only-took-a-10-minute-phone-call-to-shutdown-mgm-resorts-143147493.html

gaining credential information by using vishing (voice phishing) attacks to carry out sophisticated and effective social engineering techniques or coaxing victims to download malware and gain access privileges.[4]

On Friday, September 15th, the ALPHV (BlackCat) ransomware gang designated MGM Resorts as a victim on its DLS and also published a lengthy statement.



Statement on MGM Resorts International: Setting the record straight

Fri Sep 15 2023

MGM Resorts International is an American global hospitality and entertainment company.

Figure 4. MGM designated as a victim on the BlackCat ransomware DLS

The summary of the statement they provided in chronological order is shown below. Note that these are claims made by cybercriminals and may differ from the truth.

Date	Details
Sept. 8, Friday	● Attack begins with a network intrusion ● Administrator privileges gained in Okta SSO and Azure cloud tenant
Sept. 9, Saturday	● Network access interruptions occur ● A statement is made attributing the interruptions to an internal MGM issue and not an external attack
Sept. 10, Sunday	● MGM Resorts switches its critical infrastructure as offline ● Negotiations are attempted via a private link, but MGM does not respond
Sept. 11, Monday	● Successful ransomware attacks are conducted on approximately 100 ESXi hypervisors

[4] https://atip.ahnlab.com/ti/contents/threat-actor/detail?tagSeq=27672

	● The ransom is not paid
Sept. 12, Tuesday	● News of the cyberattack on MGM Resorts emerge ● Speculative posts about a ransomware attack are confirmed on social media
Sept. 14, Thursday	● Reports emerge that ALPHV (BlackCat) and Scattered Spider cooperated to attack MGM Resorts
Sept. 15, Friday	● ALPHV (BlackCat) designates MGM Resorts as a victim on its DLS

Table 1. A reorganized timeline of the information disclosed by BlackCat

Meanwhile, the gang countered some media reports that claimed it had cooperated with "Scattered Spider" by arguing that the threat actors' tactics, procedures, and indicators can be easily imitated by anyone.

Following MGM Resorts, Caesars Entertainment also experienced a cybersecurity incident in the same month, and it is presumed that this incident may have occurred before the MGM incident. The characteristics of this incident are summarized below.

Type	Details
Data breach	It was revealed that customer data was stolen during the cyberattack. Hackers stole a copy of the company's loyalty program database, which included the driver's license number and social security number information for a "significant number of members."
Social engineering attack	It was revealed that hackers used social engineering techniques to infiltrate the computer systems of an outsourced IT support company.
Response measure	Caesars confirmed that they paid the ransom when the (ransomware) threat actors threatened to release the data.[5]
Legal issue	Following this incident, Caesars faced at least four class-action lawsuits related to the data breach.[6]

Table 2. Characteristics of Caesars Entertainment's cybersecurity incident

Caesars' and MGM's cybersecurity incidents provide the following important implications:

[5] https://www.bleepingcomputer.com/news/security/caesars-entertainment-confirms-ransom-payment-customer-data-theft/

[6] https://www.cybersecuritydive.com/news/caesars-lawsuits-database-hack/694915/

- Severity of ransomware attacks
  - These two incidents illustrate how destructive ransomware attacks can be. A majority of MGM's systems were shut down, causing various inconveniences for its customers. Ransomware attacks are generally well-known, constantly occurring, and receive more attention than other cybersecurity incidents, so they are a constant threat.

- Effectiveness of social engineering attacks
  - In the case of Caesars, hackers infiltrated through social engineering techniques aimed at an external IT outsourcing company. This serves as a reminder that social engineering techniques remain as effective intrusion measures.

- Risk of data breaches
  - Both Caesars and MGM suffered massive customer data breaches. This led to the exposure of personal information, posing a serious threat to customers and significantly undermining the companies' trustworthiness.

- Importance of response measures
  - Caesars and MGM are reported to have taken measures to respond to the incidents. However, such measures may not be always effective. In Caesars' case, it paid the ransom to have the data deleted.

- Need for enhanced security
  - The two cases highlight the importance for businesses to strengthen their security measures to protect their systems. Businesses like casinos, which handle significant amounts of money and customer data, especially need to enhance their security measures.

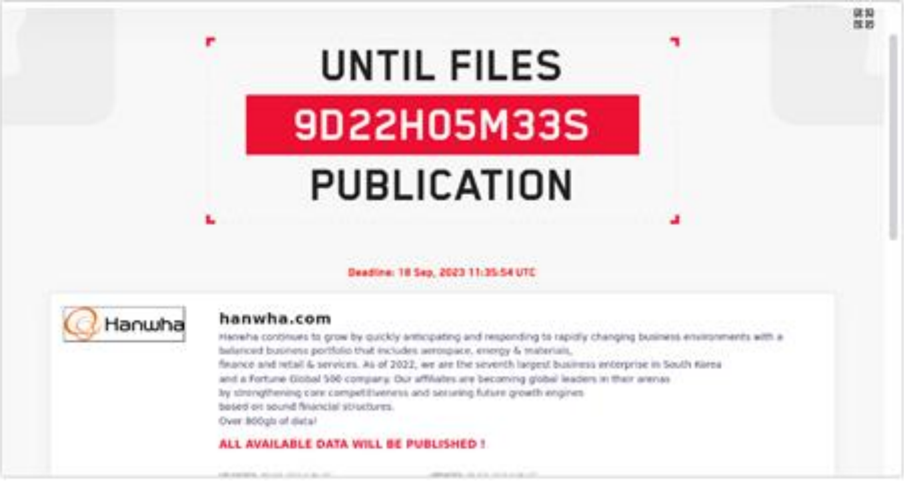
(3) LockBit

LockBit is known to have unofficially posted about 2,000 victims on its DLS as of this point. Known for its aggressive activities, LockBit started to face internal issues within its DLS operations and subsidiaries in 2023.

According to a report prepared by Analyst1, several important operational issues have been revealed, which are summarized below:[7]

- Absence of ransomware developers
  - Unable to release a new version in June 2023
  - Release/leakage of incorrectly coded LockBit Mac
- Data leakage and DLS posting issues
  - Inappropriate posts on DLS with random characters and fake victim companies
- Subsidiary-related issues
  - Surge in complaints due to delays in the response time from management
  - Arrests/prosecutions against some subsidiaries
  - Withdrawal of subsidiaries

Despite the above operational issues, the LockBit ransomware gang continues to demonstrate its resilience by posting numerous victims on its DLS, having even designated a South Korean conglomerate as a victim.



UNTIL FILES

9D22H05M33S

PUBLICATION

Deadline: 18 Sep, 2023 11:35:54 UTC

hanwha.com

Hanwha continues to grow by quickly anticipating and responding to rapidly changing business environments with a balanced business portfolio that includes aerospace, energy & materials, finance and retail & services. As of 2022, we are the seventh largest business enterprise in South Korea and a Fortune Global 500 company. Our affiliates are becoming global leaders in their arenas by strengthening core competitiveness and securing future growth engines based on sound financial structures.
Over 800gb of data!

ALL AVAILABLE DATA WILL BE PUBLISHED !

Figure 5. South Korean conglomerate designated as a victim on LockBit's DLS

LockBit introduced the targeted company as being the seventh largest in South Korea and selected as one of the Fortune Global 500 companies. It claimed to have exfiltrated 800 GB of data and also shared a sample of the leaked data.

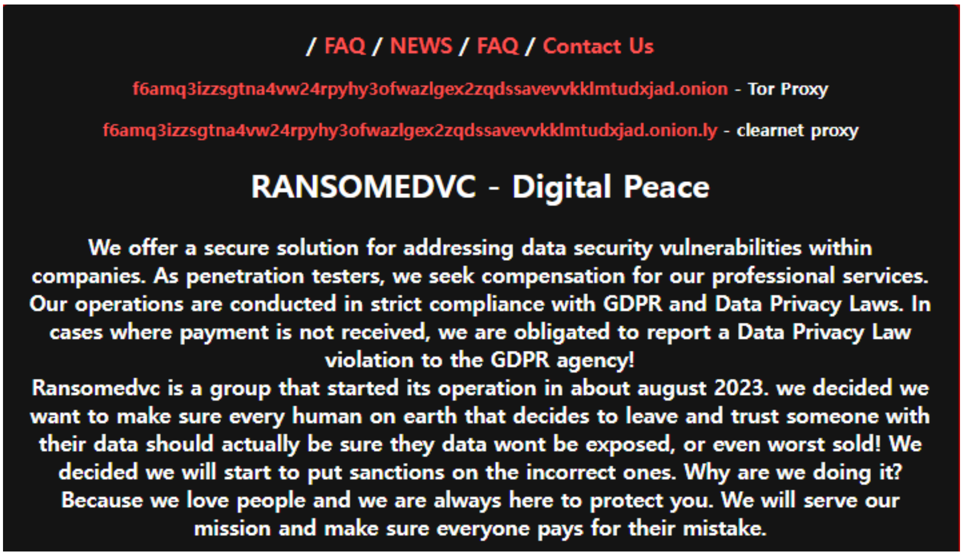
Upon examining a portion of the disclosed data sample, it can be inferred that it was the subsidiary records of the company that operated in China and involved in the solar energy business. With this data in hand, LockBit asserted on its DLS that the records were exfiltrated

[7] https://analyst1.com/ransomware-diaries-volume-3-lockbits-secrets/

from the conglomerate.
It seems that the operator in charge of managing the DLS or the subsidiary that attacked the company to leak the data had listed the incorrect information. While this is a specific case, it suggests that the operational issues related to data leakage and DLS listing mentioned earlier still persist.

(4) RansomedVC

RansomedVC is a new ransomware gang that came to the surface in August 2023. Initially, it primarily focused on data leaks, initial infiltration brokers, and exploits in cybercrime forums. However, it later transformed into a ransomware gang and started focusing on generating profits from leaked data.[8] Since a majority of the operators on the DLS it manages are of Russian and Ukrainian origin, the gang stated that it will restrict its subsidiaries from carrying out attacks on those countries.



/ FAQ / NEWS / FAQ / Contact Us

f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvkklmtudxjad.onion - Tor Proxy

f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvkklmtudxjad.onion.ly - clearnet proxy

RANSOMEDVC - Digital Peace

We offer a secure solution for addressing data security vulnerabilities within companies. As penetration testers, we seek compensation for our professional services. Our operations are conducted in strict compliance with GDPR and Data Privacy Laws. In cases where payment is not received, we are obligated to report a Data Privacy Law violation to the GDPR agency!
Ransomedvc is a group that started its operation in about august 2023. we decided we want to make sure every human on earth that decides to leave and trust someone with their data should actually be sure they data wont be exposed, or even worst sold! We decided we will start to put sanctions on the incorrect ones. Why are we doing it? Because we love people and we are always here to protect you. We will serve our mission and make sure everyone pays for their mistake.

Figure 6. RansomedVC DLS

Dark web threat intelligence researcher @DailyDarkWeb, who operates on X (formerly Twitter), conducted an interview with RansomedVC and summarized some of the contents as follows:[9]

[8] https://www.resecurity.com/blog/article/ransomedvc-in-the-spotlight-what-is-known-about-the-ransomware-group-targeting-major-japanese-businesses

[9] https://linkedin.com/pulse/inside-mind-ransomware-operator-ransomedvc-gang-interview

Question	Answer
Brief introduction	The team is composed of several groups that have established partnerships with 77 subsidiaries
Motive for attack	The primary attack motive is financial gain, but there are occasionally political reasons as well
Target selection	Targets are selected based on the gang's minimum requirement of $5 million dollars in profit, with its primary targets belonging to the US, Canada, Italy, and the EU
Any feeling of guilt	The interviewee stated that it is the fault of those who set up the vulnerable systems, indicating no guilt about the damages caused by the attacks
Attack technique	Seeing that the interviewee redirected the question about attack techniques to their subsidiaries suggests the gang has a basic ransomware group structure (initial access brokers, developers, subsidiaries, etc.) It is speculated that the gang uses more than publicly available scripts and mostly engages in coding for zero-day vulnerabilities
Ethical aspects of attacks	While the interviewee mentioned occasional attacks on plastic surgery hospitals, the group claims to not attack regular hospitals
About collaboration with Everest Ransomware	Assumed to have maintained a long relationship and will continue to do so
Relationship between Exposed Forum and RansomedVC	No connections whatsoever

Question	Answer
What happens to the money received through ransom	Laundered through a few businesses the gang legally owns, which include exchangers and carders

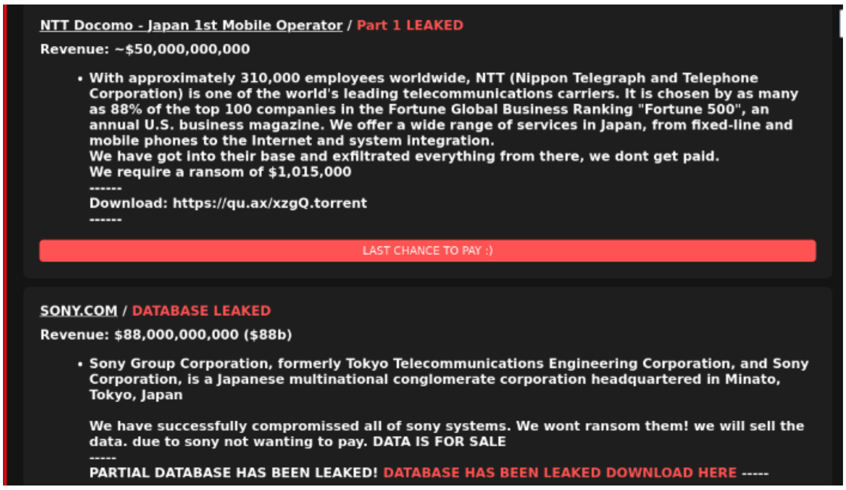
Table 3. Interview with the operator of RansomedVC

This gang employs a unique pressure tactic by abusing the General Data Protection Regulation (GDPR) of the EU. If affected companies refuse to pay the ransom, the gang discloses the exfiltrated information. By doing so, the companies need to pay the fine under the GDPR. This approach contrasts with the typical method used by most ransomware gangs where data is encrypted and a ransom is demanded for decryption.

Item	RansomedVC	Typical ransomware group
Pressure Tactic	Abuses the GDPR to make companies receive fines Discloses the exfiltrated data on a cybercrime forum and tries to sell it there	Only discloses a sample of the exfiltrated data on a DLS

Table 4. Comparison between RansomedVC and other typical ransomware gangs

RansomedVC gained attention for targeting major Japanese companies. In particular, the gang claimed to have attacked SONY and Japan's largest telecommunications company, NTT Docomo.



NTT Docomo - Japan 1st Mobile Operator / Part 1 LEAKED

Revenue: ~$50,000,000,000

- With approximately 310,000 employees worldwide, NTT (Nippon Telegraph and Telephone Corporation) is one of the world's leading telecommunications carriers. It is chosen by as many as 88% of the top 100 companies in the Fortune Global Business Ranking "Fortune 500", an annual U.S. business magazine. We offer a wide range of services in Japan, from fixed-line and mobile phones to the Internet and system integration.
  We have got into their base and exfiltrated everything from there, we dont get paid.
  We require a ransom of $1,015,000

  Download: https://qu.ax/xzgQ.torrent

SONY.COM / DATABASE LEAKED

Revenue: $88,000,000,000 ($88b)

- Sony Group Corporation, formerly Tokyo Telecommunications Engineering Corporation, and Sony Corporation, is a Japanese multinational conglomerate corporation headquartered in Minato, Tokyo, Japan

  We have successfully compromissed all of sony systems. We wont ransom them! we will sell the data. due to sony not wanting to pay. DATA IS FOR SALE

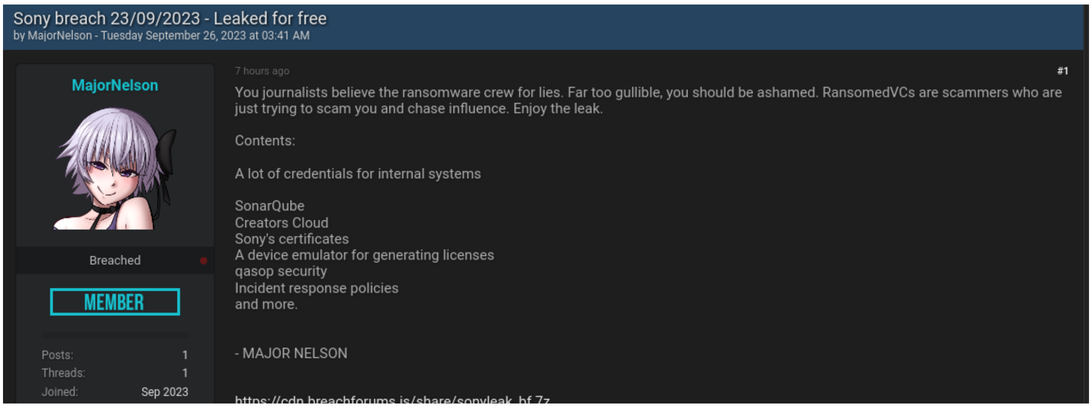
  PARTIAL DATABASE HAS BEEN LEAKED! DATABASE HAS BEEN LEAKED DOWNLOAD HERE -----

Figure 7. NTT Docomo and SONY posted on RansomedVC's DLS

In the attack against SONY, RansomedVC claimed to have successfully breached all of the company's systems and attempted to sell the exfiltrated data instead of demanding a ransom. In the attack on NTT Docomo, RansomedVC demanded a ransom of $1,015,000 for not releasing the stolen data.

The sale of the leaked data from SONY is interpreted as part of the gang's pressure tactic, aimed at causing maximum damage to the reputation of this technology and media conglomerate. Typically, ransomware gangs target the reputation of victims to gain leverage during negotiations.

However, a hacker with the nickname MajorNelson, who is known in a cybercrime forum infamous for data leaks, stepped forward and claimed responsibility for the SONY breach. This hacker alleged that RansomedVC's data leak claims were false and accused the gang of being scammers only chasing the influence of breaching a conglomerate. MajorNelson then posted the exfiltrated data for free download on the forum.



Sony breach 23/09/2023 - Leaked for free
by MajorNelson - Tuesday September 26, 2023 at 03:41 AM

MajorNelson

Breached

MEMBER

Posts: 1
Threads: 1
Joined: Sep 2023

7 hours ago #1

You journalists believe the ransomware crew for lies. Far too gullible, you should be ashamed. RansomedVCs are scammers who are just trying to scam you and chase influence. Enjoy the leak.

Contents:

A lot of credentials for internal systems

SonarQube
Creators Cloud
Sony's certificates
A device emulator for generating licenses
qasop security
Incident response policies
and more.

- MAJOR NELSON

https://cdn.breachforums.is/share/sonyleak_bf.7z

Figure 8. The SONY-related exfiltration posted by a hacker on a cybercrime forum

As of now, it is unclear which party's claim regarding the source of the exfiltrated data related to SONY is accurate, RansomedVC or MajorNelson. The affected party, SONY, is reportedly conducting an investigation into the data leak.[10]

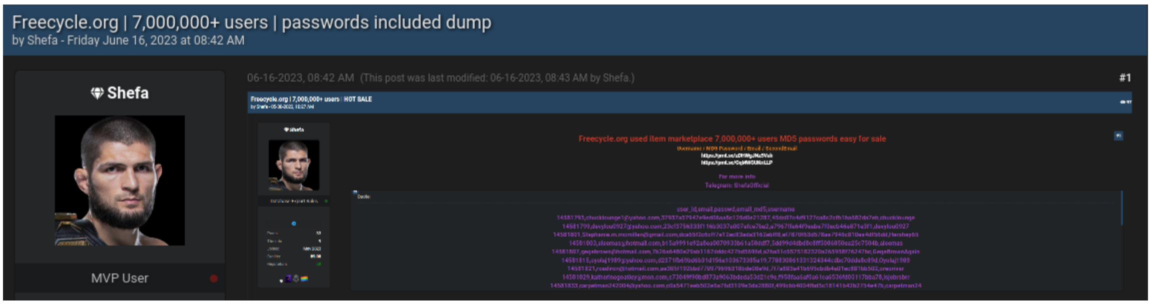
[10] https://www.bleepingcomputer.com/news/security/sony-investigates-cyberattack-as-hackers-fight-over-whos-responsible/

2) Forum & Black Market

(1) Data Breach Affecting 7 Million Users

Freecycle.org is a non-profit online marketplace where members engage in the practice of giving away and receiving items for free in their respective cities. The website's goal is to prevent good items from ending up in landfills by promoting recycling.

Recently, a data breach occurred on this website, affecting the information of approximately 7 million members. The breach occurred on September 5th, 2023, and it was only discovered later even though the information had already been compromised.



Freecycle.org | 7,000,000+ users | passwords included dump
by Shefa - Friday June 16, 2023 at 08:42 AM

Shefa

MVP User

06-16-2023, 08:42 AM (This post was last modified: 06-16-2023, 08:43 AM by Shefa.)

#1

Freecycle.org | 7,000,000+ users | HOT SALE

Freecycle.org used item marketplace 7,000,000+ users MD5 passwords easy for sale

Username / MD5 Password / Email / SecondEmail

For more info
Telegram: ShefaOfficial

```
user_id,email,passwd,email_md5,username
[illegible]
```

Figure 9. A post selling the Freecycle member information uploaded to a cybercrime forum

The leaked information includes user names, unhashed user passwords, email addresses, and secondary email addresses. An increase in spam emails has been reported due to this leak, and users were affected as a result.[11] Freecycle.org has recommended that all its members change their passwords in response to this incident.

(2) Personal Information of Police Officers Leaked

The two personal information breaches that occurred in September are similar in the fact that they both targeted the police. On September 14th, the personal information of hundreds of individuals associated with the Greater Manchester Police in the UK was leaked in a ransomware attack. The group behind the attack remains unclear. The targeted company Digital-ID produces ID cards and is located in Stockport, United Kingdom. It is known to

[11] https://www.bleepingcomputer.com/news/security/freecycle-confirms-massive-data-breach-impacting-7-million-users/

possess the information of several UK organizations including the Greater Manchester Police.

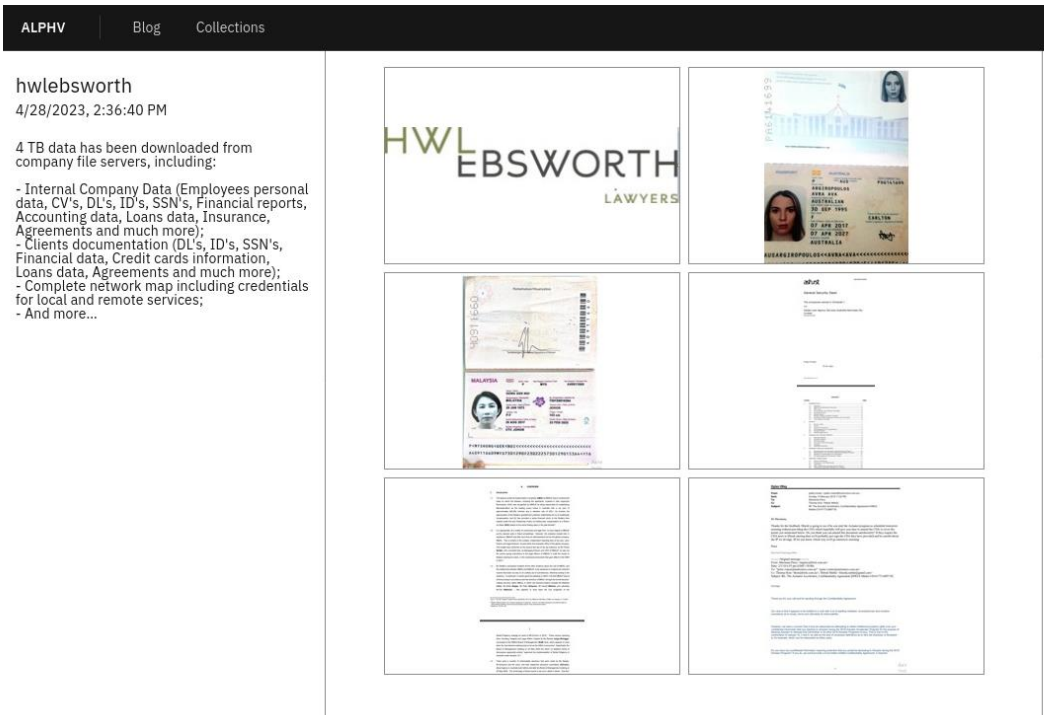
This incident appears to be similar to a breach that happened about a month earlier involving a third-party supplier for the Police Service of Northern Ireland. As for that case, personally identifiable information (PII), ranks, and locations of approximately 10,000 police officers were leaked. Around the same time, the Metropolitan Police also reported that a hacker had illegally accessed their third-party IT supplier's systems, resulting in the exposure of names, ranks, photos, assessment grades, and salary information of around 47,000 police officers and staff.[12]

These incidents in the UK are being treated with great seriousness and various agencies including the National Crime Agency are reportedly investigating the matter.[13]

The second case involves the Australian Federal Police (AFP) and the exposure of its members' personal information, which occurred on September 15th. The company that was targeted in this attack was a law firm named HWL Ebsworth, which had previously been designated as a victim of the Russia-based ransomware gang ALPHV (BlackCat) DLS in late April. As a result of this breach, data from government department agencies was posted on a DLS. The Australian Federal Police was one of the many government agencies that were clients of this firm. The leaked information included the identities and email addresses of Australian Federal Police officers.

[12] https://www.bleepingcomputer.com/news/security/manchester-police-officers-data-exposed-in-ransomware-attack/

[13] https://www.theguardian.com/uk-news/2023/sep/14/greater-manchester-police-officers-data-hacked-in-cyber-attack



hwlebsworth
4/28/2023, 2:36:40 PM

4 TB data has been downloaded from company file servers, including:

- Internal Company Data (Employees personal data, CV's, DL's, ID's, SSN's, Financial reports, Accounting data, Loans data, Insurance, Agreements and much more);
- Clients documentation (DL's, ID's, SSN's, Financial data, Credit cards information, Loans data, Agreements and much more);
- Complete network map including credentials for local and remote services;
- And more...

Figure 10. HWL Ebsworth uploaded as a victim to ALPHV (BlackCat)'s DLS

The leakage of police officers' personal information can lead to the following potential damages and impacts:

- Impact on criminal investigations
  - When the personal information of police officers is exposed, it can allow criminals to access information about police investigation methods, operations, and other critical details. This could be used by the criminals to evade or obstruct police investigations.

- Threat to personal and family safety
  - If leaked information includes officers working undercover in dangerous areas (e.g., surveillance and intelligence), it can potentially endanger the safety of these officers and their families.

- Decreased trustworthiness
  - Data breaches within law enforcement agencies can erode public trust in these institutions, potentially affecting public safety.

- Operational security breach
  - Operational security may be compromised while threat actors are assessing the stolen information, potentially resulting in data corruption. Hence, the police will

be considered negligent in its efforts to consistently monitor and update its security infrastructure.

- Financial loss
  - The process of recovering from data breaches can be costly.

3) Threat Actor

(1) Prosecution of Individuals Associated with the Trickbot Cybercrime Group

The US and the UK announced the prosecution and sanctions against 11 members of a Russia-based cybercrime group known as Trickbot.[14] The Trickbot group developed the Trickbot malware and initially used it to exfiltrate banking information and other credentials. The group later expanded its features to create a modular malware ecosystem.

This cybercrime group was also involved in the creation and distribution of the Ryuk and Conti ransomware and used the Trickbot malware as the initial method of infiltration for these ransomware infections. Its attacks have led to the shutdown of critical social infrastructures. The malware known as Emotet also installs Trickbot. According to some sources, the group has links to Russian intelligence agencies and targeted US and UK companies as well as the critical social infrastructure of these countries.

Conti ransomware, which has attacked more than 900 victims worldwide including the US, was responsible for targeting a greater amount of critical infrastructures in 2021 than any other ransomware variant according to the FBI.
In the UK, the group was responsible for extorting at least £27 million from 149 victims, targeting hospitals, schools, and businesses. This group is known to have been involved in global extortion attacks totaling at least $800 million.[15]

[14] https://www.justice.gov/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware

[15] https://www.nationalcrimeagency.gov.uk/news/russian-ransomware-group-hit-with-new-sanctions

Figure 11. Some of the individuals known as Trickbot members - <Source> nationalcrimeagency.gov.uk

The sanctions are enforced by the US Department of Treasury's Office of Foreign Assets Control (OFAC) and the US Department of Justice (DOJ) announced its intent to prosecute these individuals. These measures are the result of the joint effort between the US and the UK, aiming to respond to ransomware attacks and combat cybercrime. The individuals being prosecuted will face asset freezes and financial transaction restrictions in the US and the UK.

The information of the individuals who have been prosecuted and sanctioned this time is as follows:

Name	Nickname	Role
Andrey Zhuykov	Defender, Dif, Adam	Core senior manager of the group
Maksim Galochkin	Bentley, Volhvb, Max17	Tester group leader responsible for test development, supervision, and implementation
Maksim Rudenskiy	Buza, Silver, Binman	Core member of the Trickbot group, also a coder and team leader
Mikhail Tsarev	Mango, Frances, Khano	Intermediate manager responsible for supporting the group's finances and overseeing HR features
Dmitry Putilin	Grad, Staff	Involved in Trickbot infrastructure purchases
Maksim Khaliullin	Kagas	HR manager for the group

Name	Nickname	Role
		involved in the Trickbot infrastructure purchases including the procurement of virtual private servers (VPS)
Sergey Loguntsov	Begemot, Begemot_Sun, Zulas	Developer of the group
Alexander Mozhaev	Green, Rocco	Member of the management team responsible for general administrative tasks
Vadym Valiakhmetov	Weldon, Mentos, Vasm	Worked as a coder with responsibilities including backdoor and loader projects
Artem Kurov	Naned	Worked as a coder responsible for development tasks within the Trickbot group
Mikhail Chernov	Bullet, m2686	Member of the internal utility group

Table 5. Information of the 11 prosecuted Trickbot group members[16]

The prosecution and sanction of the Trickbot group members provide the following implications:

- Enhanced international cooperation
  - The joint action taken by the US and the UK demonstrates a close collaboration between the two countries to combat cybercrime. This act signifies that both nations are taking leading roles in the global fight against cybercrimes.

- Strong responses to cybercrimes
  - These sanctions illustrate that the US and UK governments are responding strongly to cybercrimes. In particular, such measures against a Russia-based cybercrime organization reflect concerns about Russia's role as a safe haven for cybercrimes.

- Freezing of assets and profits
  - Due to the sanctions, the personal assets and profits of these individuals within the US have been frozen. Moreover, anyone who does transactions with

[16] https://www.nationalcrimeagency.gov.uk/news/russian-ransomware-group-hit-with-new-sanctions

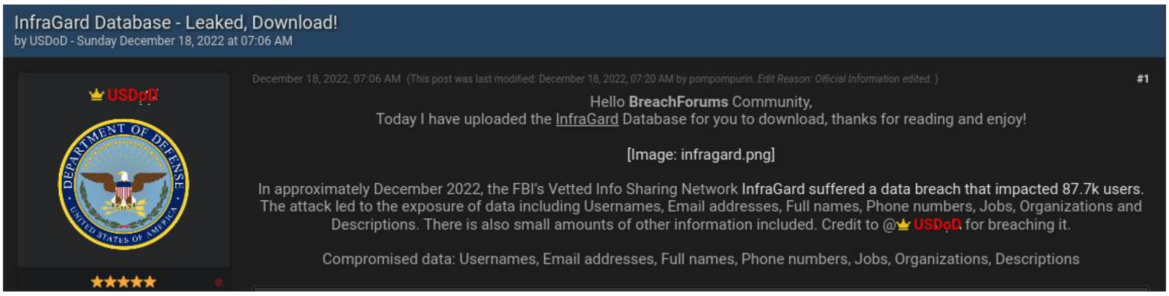
sanctioned individuals could also face sanctions. This is likely to make the activities of Trickbot members more difficult.

- Warning to cybercriminals
  - These measures also serve as a warning to other cybercriminals, indicating that their actions are under international scrutiny and could face legal consequences as a result.

Therefore, these prosecutions and sanctions show that the global society is increasingly responding more forcefully to cybercrimes, sending a message that individuals and groups engaging in such criminal activities can face serious consequences.

(2) About USDoD

In December 2022, the cybercriminal known as USDoD gained attention for hacking into the FBI's information-sharing network, Infragard.
This breach resulted in the leakage of information belonging to over 80,000 individuals.



InfraGard Database - Leaked, Download!
by USDoD - Sunday December 18, 2022 at 07:06 AM

USDoD

December 18, 2022, 07:06 AM (This post was last modified: December 18, 2022, 07:20 AM by pompompurin. *Edit Reason: Official Information edited.*) #1

Hello **BreachForums** Community,
Today I have uploaded the InfraGard Database for you to download, thanks for reading and enjoy!

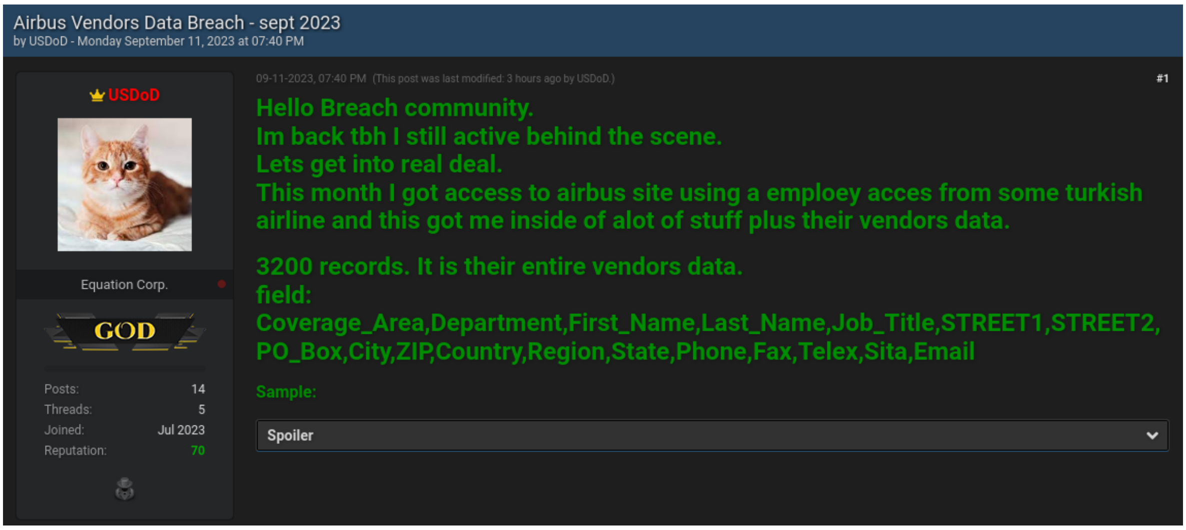
[Image: infragard.png]

In approximately December 2022, the FBI's Vetted Info Sharing Network **InfraGard suffered a data breach that impacted 87.7k users.** The attack led to the exposure of data including Usernames, Email addresses, Full names, Phone numbers, Jobs, Organizations and Descriptions. There is also small amounts of other information included. Credit to @USDoD for breaching it.

Compromised data: Usernames, Email addresses, Full names, Phone numbers, Jobs, Organizations, Descriptions

Figure 12. InfraGard database being posted on a cybercrime forum by USDoD

Recently, this cybercriminal abused the account of a Turkish airline employee to breach the database of the global aviation manufacturer Airbus.
Approximately 3,000 individuals' information (names, job titles, addresses, phone and fax numbers, email addresses, etc.) was confirmed to have been exposed in this incident.



Airbus Vendors Data Breach - sept 2023
by USDoD - Monday September 11, 2023 at 07:40 PM

USDoD

Equation Corp.

GOD

Posts:	14
Threads:	5
Joined:	Jul 2023
Reputation:	70

09-11-2023, 07:40 PM (This post was last modified: 3 hours ago by USDoD.) #1

Hello Breach community.
Im back tbh I still active behind the scene.
Lets get into real deal.
This month I got access to airbus site using a employe acces from some turkish airline and this got me inside of alot of stuff plus their vendors data.

3200 records. It is their entire vendors data.
field:
Coverage_Area,Department,First_Name,Last_Name,Job_Title,STREET1,STREET2,PO_Box,City,ZIP,Country,Region,State,Phone,Fax,Telex,Sita,Email

Sample:

Spoiler

Figure 13. Airbus database being posted on a cybercrime forum by USDoD

USDoD is known as a hacker who infiltrates companies and leaks sensitive data, and recently, he disclosed some of his background information and his ongoing activities in an interview. The following is a summary of the key points.[17]

- Background

USDoD is a man in his mid-30s who holds dual citizenship in Brazil and Portugal and currently resides in Spain. He is fluent in Portuguese, English, and German and has recently started learning Russian.

He started to learn hacking after joining a Brazilian gaming community in 1999. He revealed that he drew inspiration from a mentor he met in the community and Kevin Mitnick. According to him, he at the age of 11 used social engineering techniques to help catch a child predator.

He had apparently attacked less-known companies to gain experience and enhance his hacking skills. He was active as "NetSec" on the now-closed RaidForums and was classified as a Russian threat actor by Cyble Research Lab in February 2022 due to the #RaidAgainstTheUS campaign targeting the US military and defense companies.[18] However, he claimed to not be pro-Russia in the interview.

[17] https://www.databreaches.net/im-not-pro-russia-and-im-not-a-terrorist-infragard-and-airbus-hacker-usdod-unveils-his-new-campaigns/

[18] https://cyble.com/blog/u-s-armed-forces-and-defense-industrial-base-under-cyber-attack/

- Ethical stance

Due to moral and personal reasons, USDoD does not attack specific countries, including Russia, China, South and North Korea, Israel, and Iran. He expressed a dislike for governments and politics and emphasized that his hacking activities are not politically motivated. USDoD revealed that his primary motivations vary, going beyond just personal challenges and financial gain.

- Notable incidents

When infiltrating InfraGard, USDoD gained access by using social engineering techniques to impersonate the CEO of a major US financial company. He is active on BreachForums under the name "USDoD" and has posted the data he exfiltrated. Recently, he stole a Turkish airline employee's authentication information to access the Airbus data and has hinted at future hacking attempts targeting Lockheed Martin and Raytheon.

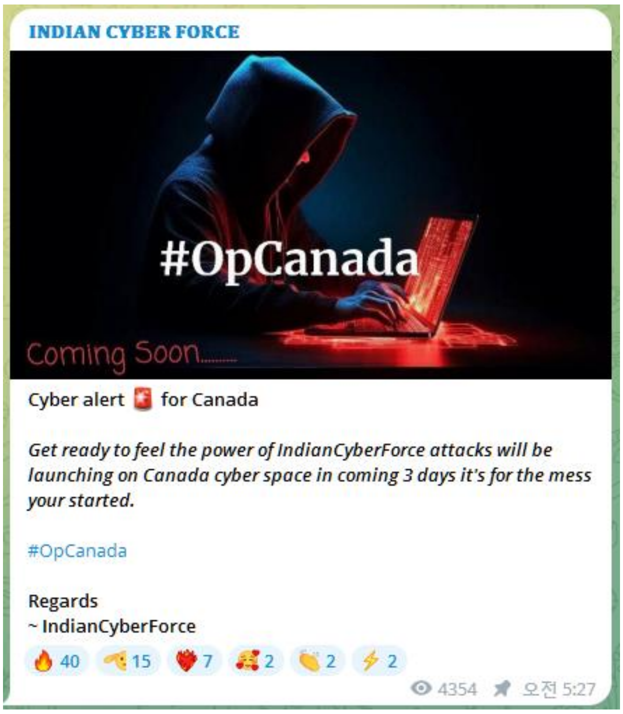
- Current activities and future plans

USDoD has revealed his ongoing operation targeting Deloitte, NATO, CEPOL, Europol, and Interpol. He claimed that he already has access to NATO and CEPOL, and is aiming to establish a company on the dark web to sell military information. He showed a particular interest in European endpoints and military data.

USDoD is a skilled hacker with complex motivations, including the desire to challenge himself and test his abilities. He targets various organizations and plans to expand his influence further, particularly in the military information field. Military organizations in the future should be prepared for potential threats from hackers like USDoD.

(3) Mastermind of #OpCanada Campaign

The India-based hacktivist group known as "Indian Cyber Force" or "ICF" set its sights on the cyber-based facilities of Canada and announced the #OpCanada campaign.



INDIAN CYBER FORCE

Cyber alert 🚨 for Canada

Get ready to feel the power of IndianCyberForce attacks will be launching on Canada cyber space in coming 3 days it's for the mess your started.

#OpCanada

Regards
~ IndianCyberForce

🔥 40 🫡 15 ❤️‍🔥 7 🥰 2 👏 2 ⚡ 2

👁 4354 📌 오전 5:27

Figure 14. #OpCanada warning posted on Indian Cyber Force's Telegram channel

According to BBC News, the relations between India and Canada have recently deteriorated.[19] This conflict is known to be due to the murder of Hardeep Singh Nijjar (the leader of Sikh) that happened in Canada in June. Canadian Prime Minister Justin Trudeau announced that Canada is investigating the "credible allegations" which suggest the potential involvement of Indian government agents in this incident. In response, the Indian government has termed these allegations as "baseless" and stated that they "vehemently deny them." It is against this backdrop of conflict that the India-based hacktivist group "Indian Cyber Force" has declared the #OpCanada campaign.

The following is a timeline of the leader of Sikhism's murder in Canada and the subsequent developments:

- June 18th, 2023
  - Sikh leader Hardeep Singh Nijjar is killed in Surrey, British Columbia, Canada.
  - The Canadian police classify the incident as a "targeted attack."

- September 2023
  - Canadian Prime Minister Justin Trudeau announces that Canadian intelligence agencies have found "credible ties" that connect Indian government agents with

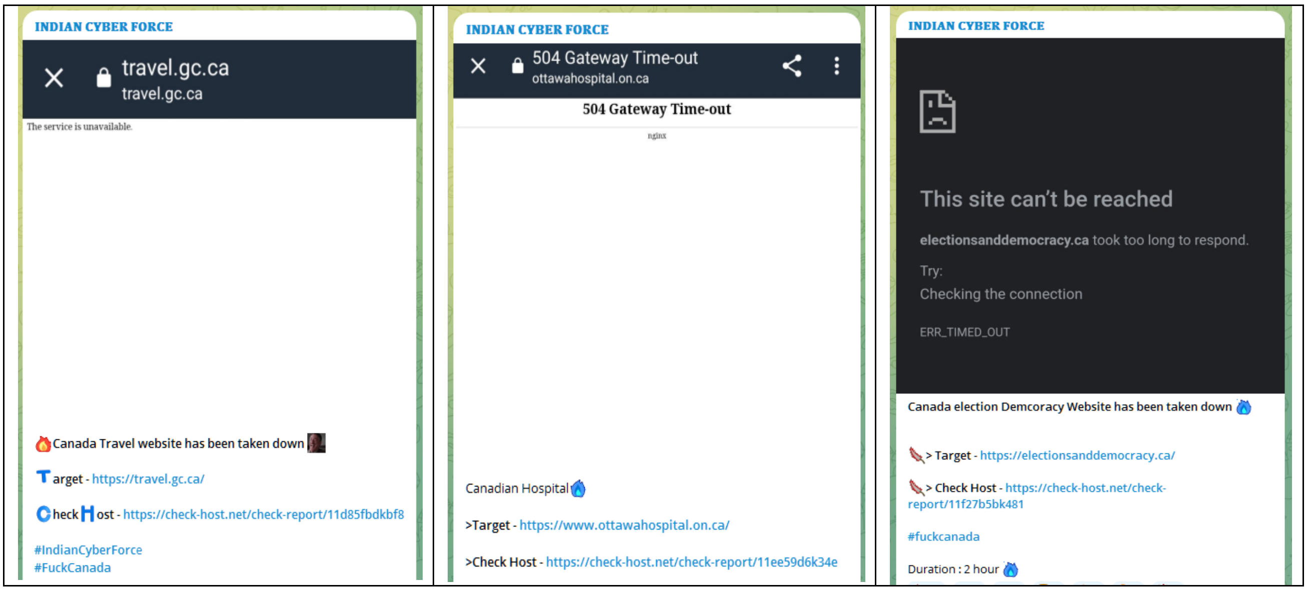
[19] https://www.bbc.com/korean/international-66865119 (This link is only available in Korean.)

Nijjar's death.

- In response, the Indian government denies all related claims.

- September 21st, 2023
  - The Indian hacktivist group named Indian Cyber Force declares the #OpCanada campaign.
  - The group states its intention to launch attacks against Canada's cyber assets through this campaign.

- September 27th to 28th, 2023
  - Indian Cyber Force carries out DDoS attacks against the official Canadian travel site, the Ottawa Hospital, Elections Canada, and military websites, as well as defacement attacks against numerous official government websites.



INDIAN CYBER FORCE

travel.gc.ca
travel.gc.ca

The service is unavailable.

🔥Canada Travel website has been taken down

Target - https://travel.gc.ca/

Check Host - https://check-host.net/check-report/11d85fbdkbf8

#IndianCyberForce
#FuckCanada

INDIAN CYBER FORCE

504 Gateway Time-out
ottawahospital.on.ca

504 Gateway Time-out

nginx

Canadian Hospital🔥

>Target - https://www.ottawahospital.on.ca/

>Check Host - https://check-host.net/check-report/11ee59d6k34e

INDIAN CYBER FORCE

This site can't be reached

electionsanddemocracy.ca took too long to respond.

Try:
Checking the connection

ERR_TIMED_OUT

Canada election Demcoracy Website has been taken down 🔥

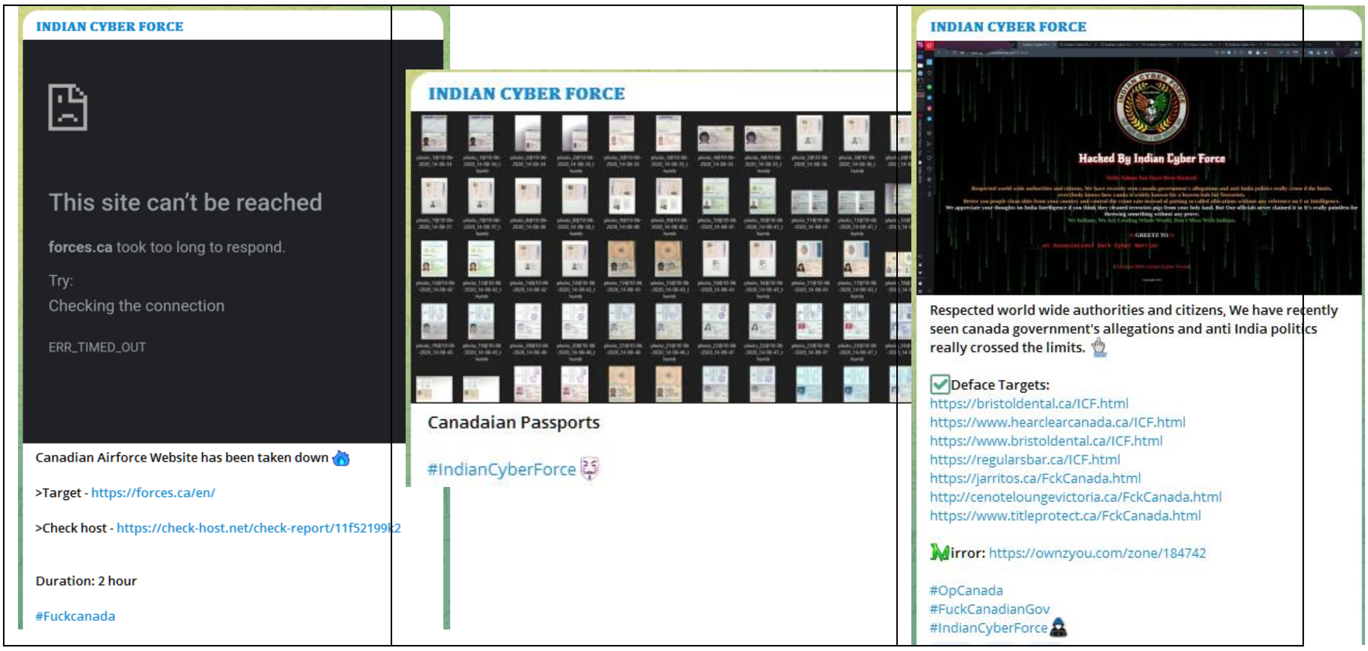
> Target - https://electionsanddemocracy.ca/

> Check Host - https://check-host.net/check-report/11f27b5bk481

#fuckcanada

Duration : 2 hour 🔥

Figure 15. Websites that had their services shut down due to Indian Cyber Force's DDoS attack



INDIAN CYBER FORCE

This site can't be reached

forces.ca took too long to respond.

Try:
Checking the connection

ERR_TIMED_OUT

Canadian Airforce Website has been taken down 🔥

>Target - https://forces.ca/en/

>Check host - https://check-host.net/check-report/11f52199k2

Duration: 2 hour

#Fuckcanada

INDIAN CYBER FORCE

Canadaian Passports

#IndianCyberForce

INDIAN CYBER FORCE

Respected world wide authorities and citizens, We have recently seen canada government's allegations and anti India politics really crossed the limits. 👆

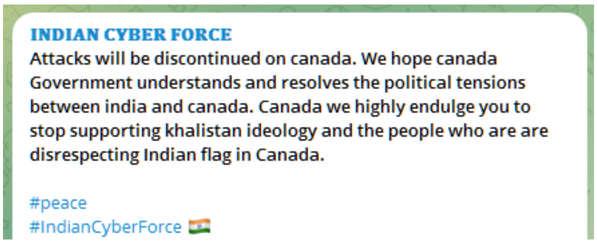
☑Deface Targets:
https://bristoldental.ca/ICF.html
https://www.hearclearcanada.ca/ICF.html
https://www.bristoldental.ca/ICF.html
https://regularsbar.ca/ICF.html
https://jarritos.ca/FckCanada.html
http://cenoteloungevictoria.ca/FckCanada.html
https://www.titleprotect.ca/FckCanada.html

Mirror: https://ownzyou.com/zone/184742

#OpCanada
#FuckCanadianGov
#IndianCyberForce

Figure 16. Website that had its service shut down due to Indian Cyber Force's DDoS attack, as well as lists of Canadian passports and websites that have been defaced

- September 29th, 2023
  - Indian Cyber Force ceases its cyberattack on Canada.



INDIAN CYBER FORCE

Attacks will be discontinued on canada. We hope canada Government understands and resolves the political tensions between india and canada. Canada we highly endulge you to stop supporting khalistan ideology and the people who are are disrespecting Indian flag in Canada.

#peace
#IndianCyberForce 🇮🇳

Figure 17. Indian Cyber Force announces the discontinuation of its cyberattack.

(4) Indonesian Hacktivist Groups Attacked the Digital Infrastructure of India

During the previous G20 Summit held in New Delhi, India, in September 9th-10th, 2023, hacktivist groups of Indonesian, Pakistani, and Bangladeshi origins launched a large-scale cyberattack on the Indian government's websites.

On September 5th, Indonesian hacktivist groups GanonSec Team, Jambi Cyber Team, and Team Insane Pk warned that they would carry out cyberattacks on India's digital infrastructure during the G20 Summit, which they subsequently did.

The participating hacktivist groups include the following. These attacks were part of a cyberattack operation known under the hashtag #OPINDIA, led by the group Team Insane Pk.

- 313 Team Ya MahdiGarnesia Team
- Ganosec Team
- Hizbullar Cyber Team
- Jambi Cyber team
- Team Insane Pk

Hacktivists carry out their attacks for political and religious reasons, and the hacktivists in this particular attack joined the #OPINDIA campaign under the religious message of "Stop harassing Muslims and Islamic people."

HACKTIVIST
INDONESIA
DATE AND TIME 9-10 SEPTEMBER 2023
#OPINDIA
TARGET ALL INDIAN WEBSITES
THE ATTACKS WILL GO ON FOR TWO DAYS WITHOUT STOPPING.

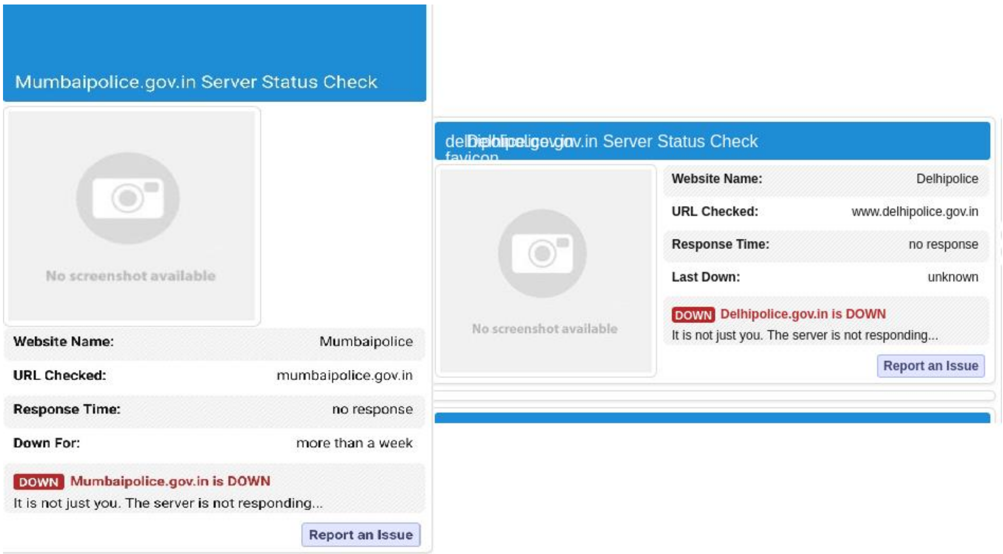
Figure 18. #OPINDIA campaign logo

According to news reports, they conducted around 2,450 cyberattacks under the name of #OpIndia campaign. More than half of these attacks were Distributed Denial of Service (DDoS) attacks, and roughly 370 of these attacks were directed at India's government digital infrastructure.[20]

Non-profit organization websites were targeted in 80 cases. The financial and banking sector faced 35 attacks, while approximately 15 attacks were reported against energy and petroleum

[20] https://www.timesnownews.com/technology-science/pakistan-indonesian-hackers-target-indian-govt-websites-g20-summit-2023-article-103537657/

sector websites. The websites of Delhi and Mumbai police departments experienced temporary outages, with Team Insane Pk claiming responsibility for taking them down.



Mumbaipolice.gov.in Server Status Check

No screenshot available

Website Name: Mumbaipolice
URL Checked: mumbaipolice.gov.in
Response Time: no response
Down For: more than a week

DOWN Mumbaipolice.gov.in is DOWN
It is not just you. The server is not responding...

delhipolice.gov.in Server Status Check

No screenshot available

Website Name: Delhipolice
URL Checked: www.delhipolice.gov.in
Response Time: no response
Last Down: unknown

DOWN Delhipolice.gov.in is DOWN
It is not just you. The server is not responding...

Figure 19. Web availability checker showing proof of websites being down

The #OpIndia campaign is part of the hacktivists' strategy to gain attention by leveraging social issues and major political events. These attacks have the following implications and impact:

- Vulnerability of digital infrastructure
  - From the shutdown of essential services, the risk of sensitive data exposure, and damage to a nation's image and reputation, various serious threats can come from DDoS attacks on digital infrastructures.

- The reality of digital threats
  - Although social, political, and geopolitical issues are used as a strategy to attract attention, these attacks actually emphasize the fact that a nation's digital infrastructure is indeed a major target for threats.

- Increase in hacktivist activities
  - Hacktivist attacks using social, political, religious, geopolitical issues, and events as leverage are expected to rise. Recent events such as the G20 Summit in India and the Sikh leader's murder in Canada made these countries major targets. Hacktivists employ DDoS attacks on major corporations and organizations, which, along with other means, can lead to serious consequences such as operational disruptions, financial losses, and reputation damage.

- Need for enhanced security
  - To counter these threats, enhanced cybersecurity measures and critical infrastructure monitoring are necessary. Cybersecurity experts recommend strengthening digital defenses through practices like software updates, powerful authentication methods, use of security software and threat intelligence services, and conducting security audits.

Conclusion

The ransomware attacks and data leaks at MGM Resorts and Caesars Entertainment had a significant impact on the casino industry. It highlighted the increased importance of cybersecurity and the need for greater vigilance. Both resorts failed to protect customer data, leading to large inconveniences in customer service such as being unable to access hotel rooms, kiosks, gaming consoles, etc. MGM Resorts suffered an estimated loss of around $80 million in revenue due to the ransomware attack, and its IT systems were down for 36 hours.[21] Caesars Entertainment is speculated to have experienced similar consequences.[22]

The recent attacks demonstrated that despite how long social engineering techniques have been around, they can still be used to manipulate people and bypass security measures. In the case of MGM, the threat actors utilized publicly available information and persuasive phone calls to gain access to MGM's systems. These incidents emphasize the importance of cybersecurity to the casino industry.

The data leak incidents involving the personal information of police officers in the UK and Australia underscore the significance of safeguarding such data. When this type of information is leaked, it can jeopardize the safety of police officers and potentially impact criminal investigations. As can be observed in this case, even if the data leak didn't directly originate from the respective departments, the leakage of police officers' personal information can erode trust in police departments and discredit them in the eyes of the public.

Hacktivists use DDoS attacks as a strategy to gain media attention. This is because they serve an important purpose of spreading their message, garnering support for their cause, or

[21] https://blog.morphisec.com/mgm-resorts-alphv-spider-ransomware-attack

[22] https://www.usatoday.com/story/tech/news/2023/09/11/mgm-cyber-attack-impact-resorts-hotels-us/70828503007/

expanding their influence. In other words, hacktivists' attacks expand their social influence. Their goal is to emphasize their technical capabilities by exaggerating the seriousness of their attacks. This can encourage support from other hacktivists, leading to further attacks and imitations, ultimately expanding their influence.

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
https://www.ahnlab.com
https://asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency response (ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoints, networks, and clouds, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.