

TLP: GREEN

July 2023 Deep Web & Dark Web Threat Trend Report

Ransomware Groups & Cyber Crime Forums and Markets of July 2023

V1.0

AhnLab Security Emergency response Center (ASEC)

Aug. 8, 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
	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) ALPHV (BlackCat)	5
(2) Cactus	6
(3) CLOP	7
(4) Monti	10
2) Forum & Black Market	12
(1) The Sale of Genesis Market.....	12
(2) BreachedForums Database on Sale.....	14
(3) US Medical Institution's Database Breached	15
3) Threat Actor	16
(1) Operation OpSweden Carried Out by Multiple Hacker Groups	16
(2) DDoS Attacks by NoName057(16) Against Lithuania and NATO	17
(3) Scareware Developer Arrested.....	19
Conclusion	21



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 July 2023 is sectioned into Ransomware, Forums & Black Markets, and Threat Actor. We would like to state beforehand that some of the content has yet to be confirmed to be true.

Major Issues

1) Ransomware

(1) ALPHV (BlackCat)

The BlackCat ransomware group breached the data of a Highland Health Systems in Aniston, Alabama, US, who provides treatment for those with mental disorders, developmental disabilities, and substance abuse problems. The group added this hospital to their leak site, which raised serious issues. This group posted a different threat message than usual. They claimed they would contact all patients and employees by phone and offer to pay for their data removal from public leaks or darknet sales.

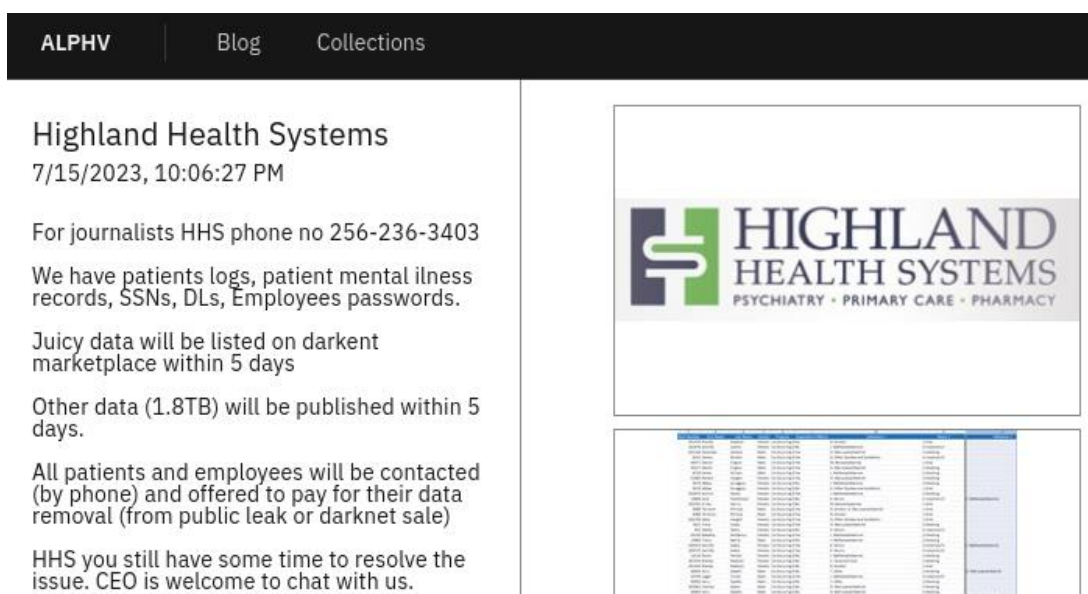


Figure 1. Victim's information uploaded to BlackCat's DLS

Security researchers monitoring BlackCat's dedicated leak site (DLS) condemned such actions of the BlackCat ransomware group. The group, having felt the gravity of situation, removed the Highland hospital from their leak site two days later, but it is unknown whether they had given any form of apology or decryption tools.

Some ransomware-as-a-service (RaaS) organizations claim to have internal standards such as prohibiting attacks against core social infrastructures like hospitals to avoid social criticism. For example, when the LockBit ransomware group infiltrated a children's hospital in Toronto, Canada late last year, they faced fierce criticism about the attack. As a result, the group removed this hospital from their victims list and apologized, promising to provide a decryption tool. However, the unilateral claim of such criminal organization cannot be trusted.



Figure 2. Apology from LockBit after breaching the data of a children's hospital

Security researchers deem the following to be the reasons behind RaaS groups claiming to have such standards and providing apologies and decryption tools upon the data breaches of medical infrastructure related to human lives.

- Avoiding attentions of law enforcement authorities that rises due to social criticism
- Means of enhancing their reputation to recruit affiliates

However, even with these reasons, RaaS organizations target and launch attacks against the easiest subjects to attack, regardless of moral and ethical standards.

(2) Cactus

The Cactus is an emerging ransomware group that recently uncovered in July, 2023. Details on their identity are not yet known, such as whether they have RaaS business model, the origin or country of residence of the threat actors, and their ties to other ransomware groups.

Because the ransomware payload itself is encrypted and requires a key to decrypt the encrypted binary for execution, some media outlets reported their ransomware bypasses the detection features of antivirus products.¹ It has been overserved that they began their activities between March and June 2023. and by the time their activities reached its peak in July, 18 victims were listed on their dedicated leak site (DLS).

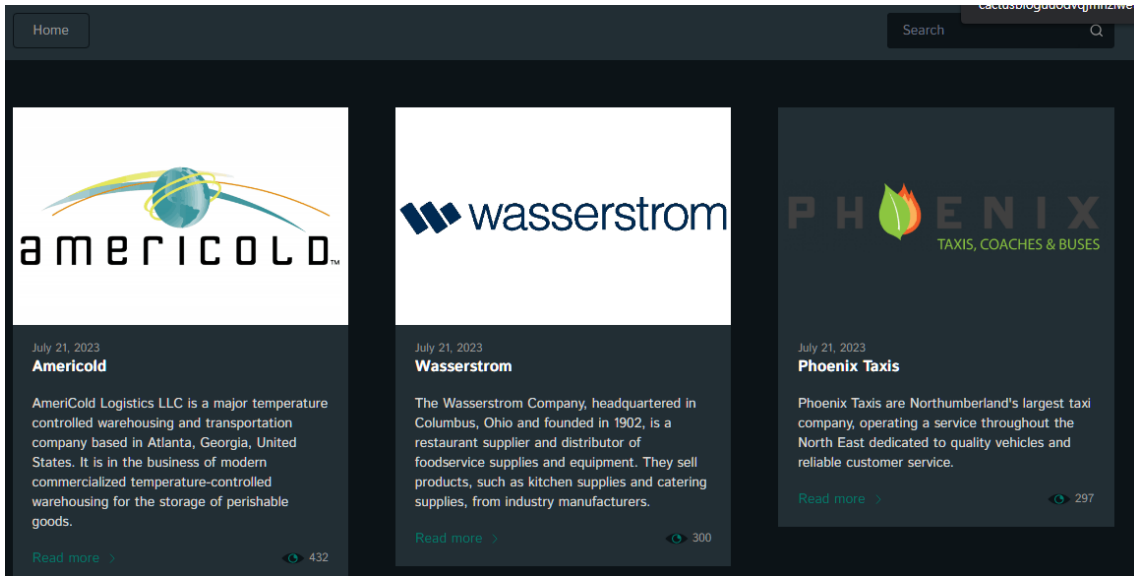


Figure 3. Some of the victims uploaded to Cactus's DLS

Most victims were in the US, and the manufacturing industry was targeted. Besides the US, there were victims in France, Portugal, Italy, the UK, and Switzerland as well.

(3) CLOP

Since the CLOP ransomware group launched their initial attacks by exploiting the MOVEit vulnerability (CVE-2023-34362) in June, they have been listing the infiltrated enterprises on their DLS and threatening them in July as well. Particularly, on July 27, they uploaded 69 victims, breaking the record for the most victims uploaded in a single day. It must be noted that this figure may be different depending on the date of collection and the method of calculation.

¹ <https://www.kroll.com/en/insights/publications/cyber/cactus-ransomware-prickly-new-variant-evades-detection>

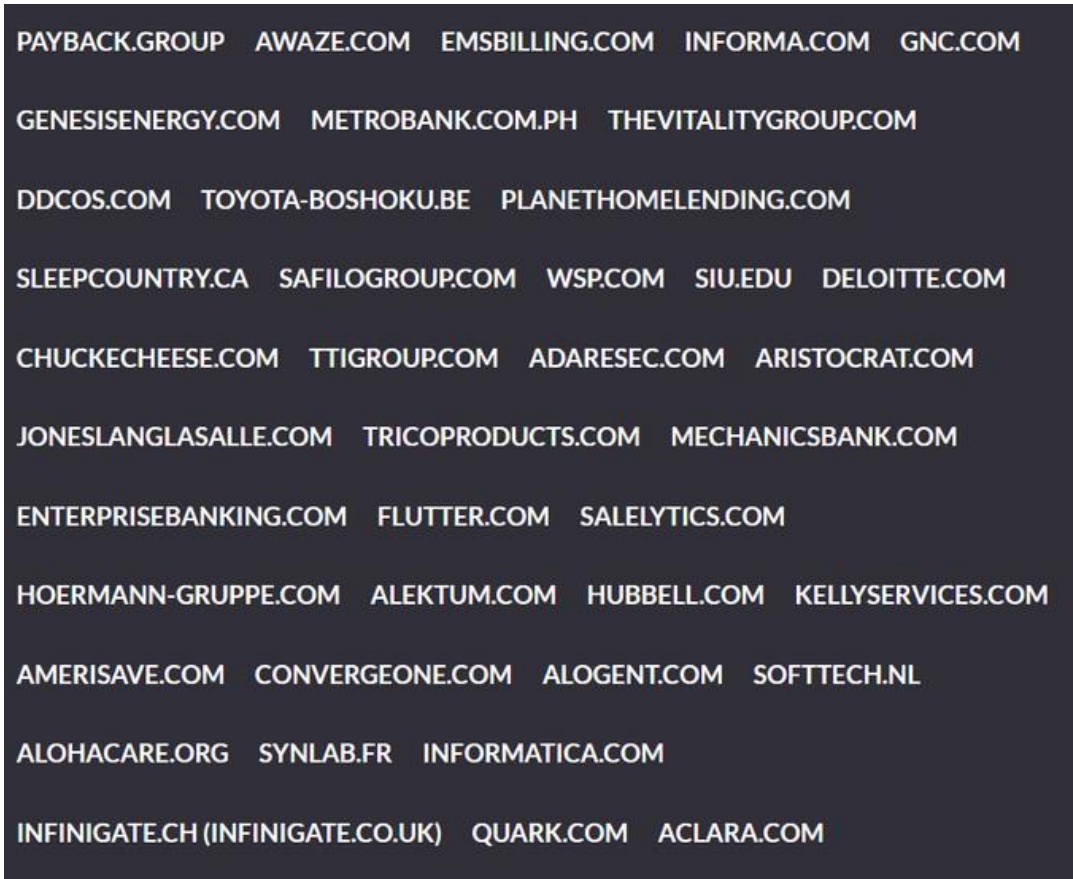


Figure 4. A portion of the victims uploaded to CLOP's DLS

On this day, one of the “Big Four” accounting firms also appeared on the group’s DLS. As a result, CLOP now lists three of the big four accounting giants as victims of the MOVEit vulnerability. CLOP also utilized the same threat tactic employed by the ALPHV (BlackCat) ransomware group in the past to leak data from one of the infiltrated accounting firms; they uploaded the leaked data on the surface web which is accessible by anyone.



Figure 5. A notice involving the uploading of the breached data on the surface web

However, such a tactic is a double-edged sword. While the tactic makes their postings easily accessible, blocking them can be easily done as well. Just a few days after their domain had become known, it was blocked.

Since this incident, the CLOP ransomware group created a separate Onion site to share the data from some of their victim enterprises via torrent.

Company	Logo	Magnet
klgates.com		FULL FILES dn=klgates
paycor.com		FULL FILES dn=paycor
caresource.com		FULL FILES dn=caresource
1stsource.com		FILES PART b&dn=1stsource-fp1
www.pwc.com		FULL FILES dn=pwc
ey.com		FILES PART b&dn=ey-fp1
paycom.com		FULL FILES dn=paycom

Figure 6. A post sharing the breached data via torrent

This is also not the first time a ransomware group leaked the data via torrent. Last July, US cyber security company Entrust was listed as a victim of LockBit and had their leaked data disclosed on the DLS. Afterward, for unknown reasons, LockBit's DLS fell victim to a DDoS attack. When the site became inaccessible, LockBit's operator shared the leaked data via torrent.

There are many speculations as to why RaaS groups leak the breached data on torrent networks, but the most rational is that the Tor network is not suitable for downloading large files.

The Tor network uses a unique Onion routing method where data is transmitted over various intermediary nodes (relay servers) to ensure user anonymity. This process can slow down the data transfer speed.

However, torrent sites can be shared among many users to accelerate the file download process, and such decentralized distribution method makes it harder for law enforcement authorities to shut them down. It is presumed that the torrent sites were used because it is the optimal way to reach larger number of people. This is interpreted as being another data breach threat tactic employed by ransomware groups.

(4) Monti

The Monti ransomware group first became known sometime between May and June 2022. They are known to have ties to the Conti ransomware group which disbanded in May of the same year.



Figure 7. Connections with the Conti ransomware group
<Source> - [OCD_WorldWatch_Ransomware-ecosystem-map_v23²](https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_WorldWatch_Ransomware-ecosystem-map_v23.pdf)

Thus, some researchers and security companies see Monti as a derivative or a subsidiary group of Conti. The Monti ransomware is assumed to have been created based on the Conti source code leaked in March 2022. Monti ransomware group deliberately imitated the tactics, techniques, and procedures (TTP) as well as Conti's tools and the ransomware encryption methods.

This group has been taking a toll on various countries and industries. As of July 2023, 11 victims were on their DLS. Recently, the group posted their data breach on the Hungarian Investment Promotion Agency. Out of the leaked data, a scan of the passport belonging to an employee of a Korean conglomerate was disclosed, along with the claim that there were many

² https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_WorldWatch_Ransomware-ecosystem-map_v23.pdf

more passport images like this.

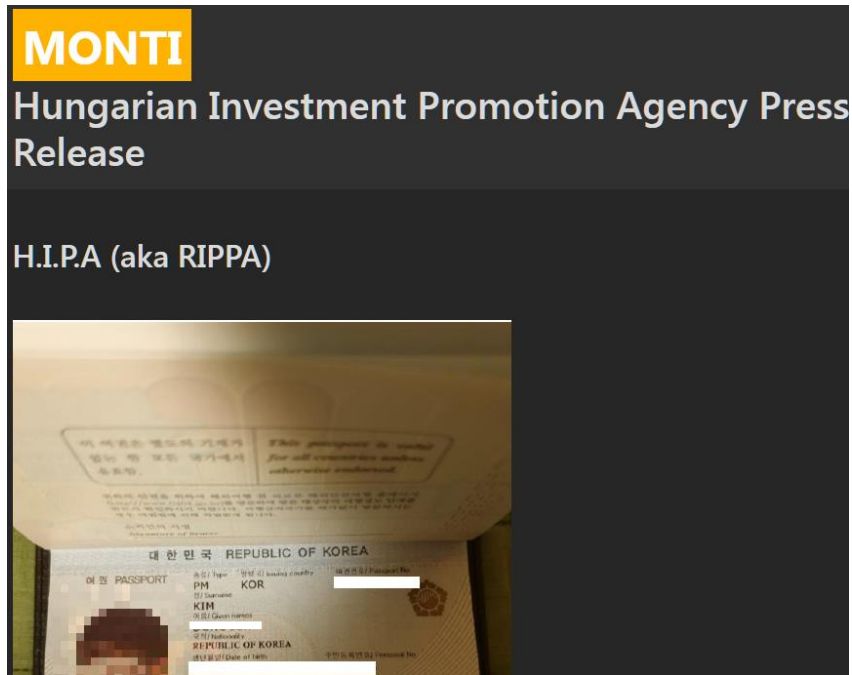


Figure 8. The scan of Korean passport leaked from Hungarian Investment Promotion Agency

As a proof of their activity, the group put forward a list of the leaked files. In the list of files found in a folder named "útlevel" (passport in Hungarian) was a list of scanned Korean passports that belong to 328 Korean who are presumed to work at the same conglomerate and their affiliates.

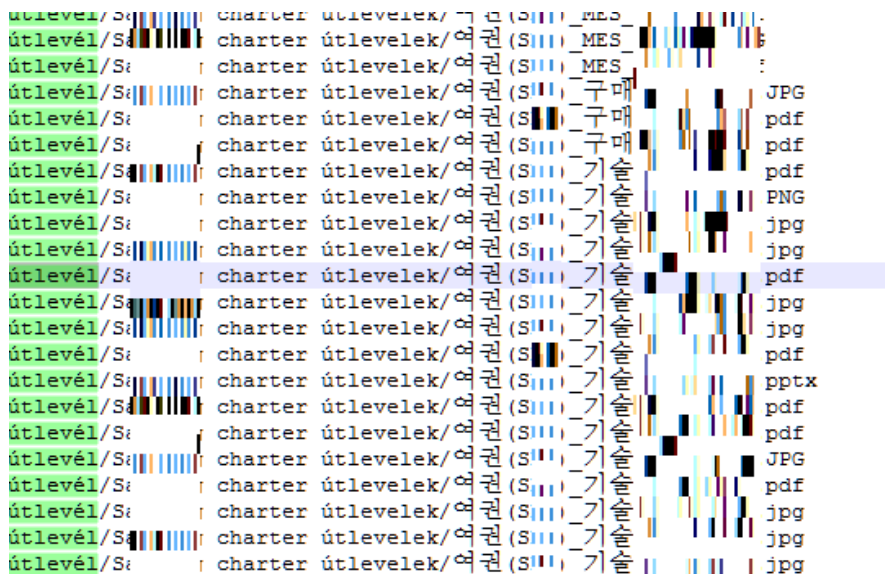


Figure 9. List of scanned Korean passports

Once passport data is leaked on the dark web, criminals can use this information for passport

forgery, so such incidents must be reported immediately to proper authorities who issue passports. Passport information is sold on the dark web in the following three forms.

- A digital scan;
- Template to make complete passports; and
- Actual physical passport (counterfeit or stolen passports)

When passport information is leaked secondary damages may occur, such as:

- Illegal immigration;
- Identity theft (abused for financial transactions);
- Fraud (abused for employment and real estate leasing); and
- Terrorism (terrorists masking their identity to board planes).

2) Forum & Black Market

(1) The Sale of Genesis Market

Genesis Market, a cybercrime marketplace set up in late 2017, was shut down last April after the coordinated global operation on the Genesis Market led by the Federal Bureau of Investigation (FBI).³ In late June, almost three months after its closure, the GenesisStore team posted on a Russia-based cybercrime forum to advertise the sale of their marketplace.



Figure 10. A post selling the market, uploaded by the Genesis team <Source> Twitter - @DailyDarkWeb

³ <https://therecord.media/genesis-market-takedown-cybercrime>

They claimed the items on sale include databases, source codes, scripts, and server infrastructure, excluding some user information. In early July, in another post they said a buyer has been found and a deposit had been made for the purchase of Genesis Market, adding all rights will be handed over to a new owner once the trade completes next month.



Figure 11. A post notifying that the market has been sold, uploaded by the Genesis team
<Source> Twitter - @DailyDarkWeb

Systematically collecting user profile information – consists of user credentials, cookies, device and behavior fingerprints, and other metadata – and selling them in a bundle is called impersonation-as-a-service (ImpaaS).

Regarding this, Bleepingcomputer commented that Genesis Market sold various pieces of leaked user profile information, and added a custom JavaScript code enabled the collection of all the data necessary to impersonate the victim machine and log into various service.⁴ This JavaScript code was distributed through Infostealers (AZORult, DanaBot, Raccoon, RedLine) that steal a variety of information.

The fact that Genesis Market has been sold is a significant issue in the dark web marketplace ecosystem, as it proves that there is still a demand for the ImpaaS market. This means that even after the Genesis Market shut down, small and big marketplaces operated and that stealing user profiles through Infostealers is still rampant.

Although law enforcement authorities continue their efforts to shut down the dark web marketplaces, cyber criminals still find these marketplaces profitable for reasons, such as:⁵

⁴ <https://www.bleepingcomputer.com/news/security/genisis-market-infrastructure-and-inventory-sold-on-hacker-forum/>

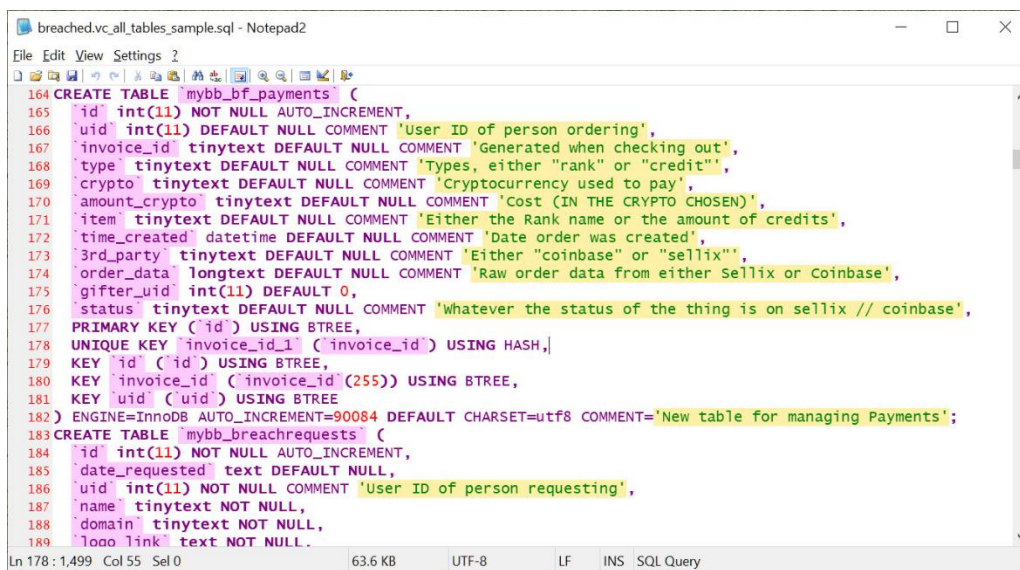
⁵ <https://www.forbes.com/sites/forbestechcouncil/2020/04/23/five-key-reasons-dark-web-markets-are-booming/>

- Anonymity of cryptocurrency
- Growth of anonymous network (Tor)
- Increase in the rate of ransom payments
- Increase in profitability of dark web markets
- Increase in the attack surface of organizations

(2) BreachedForums Database on Sale

BreachedForums was a famous cybercrime forum run by a man living in Peekskill, US, under the username "Pompompurin". In mid-March 2023, three months after the arrest of the forum operator, the US federal authorities seized the domain of BreachedForums.

This forum's database is currently being sold by a threat actor with the username of "breached_db_person", and they have shared the database with Have I Been Pwned, a data breach notification service, to prove the authenticity of the database.⁶



```
breached.vc_all_tables_sample.sql - Notepad2
File Edit View Settings 2
164 CREATE TABLE `mybb_bf_payments` (
165   `id` int(11) NOT NULL AUTO_INCREMENT,
166   `uid` int(11) DEFAULT NULL COMMENT 'User ID of person ordering',
167   `invoice_id` tinytext DEFAULT NULL COMMENT 'Generated when checking out',
168   `type` tinytext DEFAULT NULL COMMENT 'Types, either "rank" or "credit"',
169   `crypto` tinytext DEFAULT NULL COMMENT 'Cryptocurrency used to pay',
170   `amount_crypto` tinytext DEFAULT NULL COMMENT 'Cost (IN THE CRYPTO CHOSEN)',
171   `item` tinytext DEFAULT NULL COMMENT 'Either the Rank name or the amount of credits',
172   `time_created` datetime DEFAULT NULL COMMENT 'Date order was created',
173   `3rd_party` tinytext DEFAULT NULL COMMENT 'Either "coinbase" or "sellix"',
174   `order_data` longtext DEFAULT NULL COMMENT 'Raw order data from either Sellix or Coinbase',
175   `gifter_uid` int(11) DEFAULT 0,
176   `status` tinytext DEFAULT NULL COMMENT 'Whatever the status of the thing is on sellix // coinbase',
177   PRIMARY KEY (`id`) USING BTREE,
178   UNIQUE KEY `invoice_id_1` (`invoice_id`) USING HASH,
179   KEY `id` (`id`) USING BTREE,
180   KEY `invoice_id` (`invoice_id` (255)) USING BTREE,
181   KEY `uid` (`uid`) USING BTREE
182 ) ENGINE=InnoDB AUTO_INCREMENT=90084 DEFAULT CHARSET=utf8 COMMENT='New table for managing Payments';
183 CREATE TABLE `mybb_breachrequests` (
184   `id` int(11) NOT NULL AUTO_INCREMENT,
185   `date_requested` text DEFAULT NULL,
186   `uid` int(11) NOT NULL COMMENT 'User ID of person requesting',
187   `name` tinytext NOT NULL,
188   `domain` tinytext NOT NULL,
189   `looo link` text NOT NULL.
Ln 178 : 1,499 Col 55 Sel 0      63.6 KB   UTF-8   LF   INS   SQL Query
```

Figure 12. Leaked forum SQL table <Source> BleepingComputer

The sale of BreachedForums's database indicates that there is a risk of the personal information of this website's members being exposed. This database is known to contain the information, including usernames, IP addresses, email addresses, encoded passwords, and private messages between BreachedForums's members. Some of the data found is said to

⁶ <https://www.bleepingcomputer.com/news/security/breachforums-database-and-private-chats-for-sale-in-hacker-data-breach/>

include the members' level in the forum, their payment information regarding credit purchases, and messages that are useful in identifying cyber criminals.

Database leaks from normal websites can exacerbate concerns about the protection of personal data and security and can lead to secondary damage from personal information leakage. However, database leaks from cybercrime forums and their sales greatly help law enforcement authorities and cyber security researchers potentially identify the threat actors.

(3) US Medical Institution's Database Breached

A large-scale for-profit healthcare institution that operates 190 hospitals and clinics in the US and the UK suffered a major data breach that leaked the data of at least 11 million patients, and these data were being sold on a cybercrime forum. The data accessed includes the patients' names, cities, states, ZIP codes, email addresses, phone numbers, dates of birth, genders, patient service dates, locations, and next appointment dates. The healthcare institution announced the data breach took place at an external storage location and no malicious activities were identified in the hospital network or systems.⁷

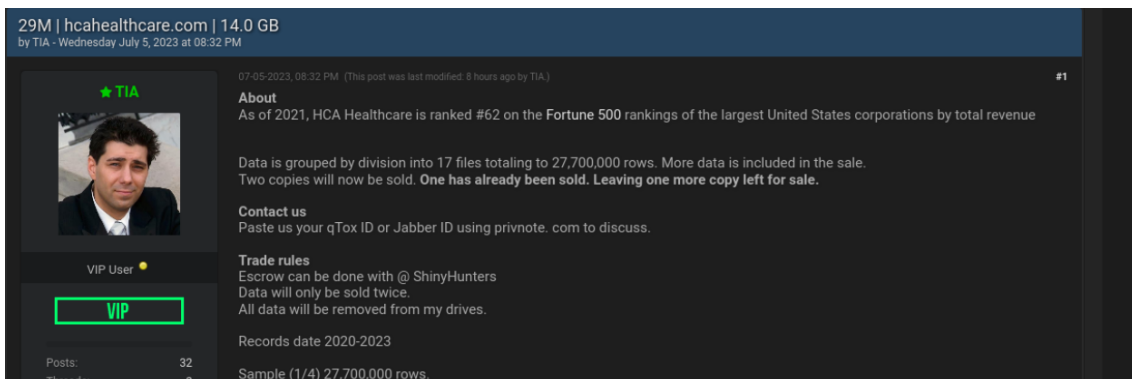


Figure 13. A post selling the database, uploaded to a cybercrime forum

This medical institution stated that the breached data did not include clinical information such as diagnosis, social security numbers, or payment details, but the breached data sample reportedly includes information on scheduled checkups and the examining department.⁸

⁷ <https://www.forbes.com/sites/alexknapp/2023/07/12/innovationrx-hca-healthcare-data-breach-affects-11-million-patients/>

⁸ <https://www.bleepingcomputer.com/news/security/hca-confirms-breach-after-hacker-steals-data-of-11-million-patients/>

A takeaway from this incident is that the protection of personal data and security are very important in the medical sector. Since healthcare services deals with sensitive data on patients, it is important to consider security and compliance with regulations from the development stage to build secure applications and systems. For this, the DevSecOps development-security-operations (DevSecOps) methodology must be adopted to minimize the risk of data breaches and protect sensitive patient data.

3) Threat Actor

(1) Operation OpSweden Carried Out by Multiple Hacker Groups

On June 28, an Iraqi protester burned the Quran (Qur'an, the religious text of Islam) near a mosque in Stockholm, Sweden. The burning of the Quran happened on the first day of Eid al-Adha, one of the important holidays in the Islamic calendar celebrated by Muslims around the world. Muslims view the Quran as the sacred words of God (the only god) and consider intentional damage on or expression of scorn towards the book very offensive.

As a protest against the Quran burning, in cyberspace, the pro-Russian hacktivist group Noname057(16) initiated cyber-attacks against Sweden on June 28, citing Sweden supported Ukraine. Other hacker groups including Anonymous Sudan, Mysterious Team Bangladesh, Türk Hack Team, and GANOSEC TEAM also joined the protest and cyberattacks.

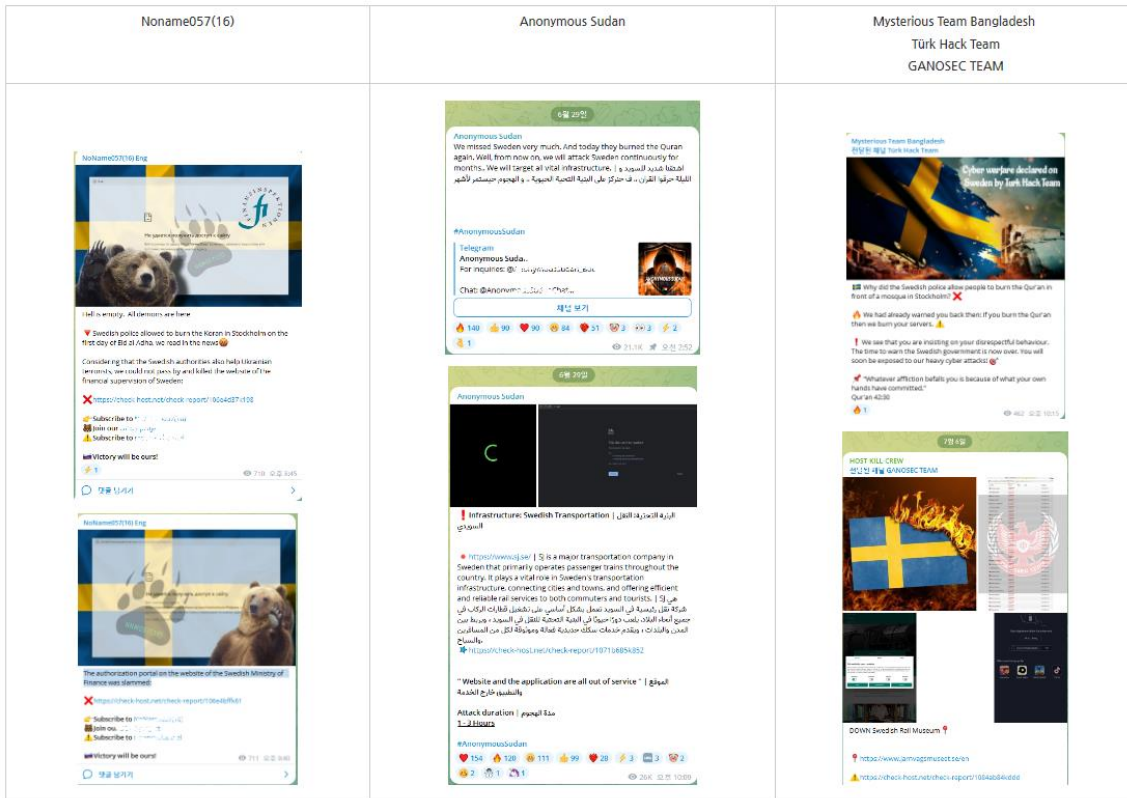


Figure 14. Images from hacktivist groups proving their DDoS attacks against the Swedish IT infrastructure

Then, it was followed by multiple pro-Islamic hacktivists including Anonymous Sudan which supports the Muslim community criticized the Quran burning in Sweden and launched distributed denial-of-service (DDoS) attacks against many Swedish organizations (government organizations) and major infrastructure (railways) using the hashtag #OpSweden.

Some threat intelligence researchers and companies believe that some of the hacktivist groups participating in #OpSweden are a part of Russia's intelligence tactics.

(2) DDoS Attacks by NoName057(16) Against Lithuania and NATO

The North Atlantic Treaty Organization (NATO) summit was held in Vilnius, the capital of the Republic of Lithuania between July 11-12.

It was an important event to have in-depth discussion on ongoing Russia-Ukrainian war and

the future of NATO.⁹ The most prominent pro-Russian hacktivist group NoName057(16) launched DDoS attacks against Lithuanian government organizations, transportation and electricity infrastructure, media outlets, finance and NATO-related websites during the period between July 10 to 13.

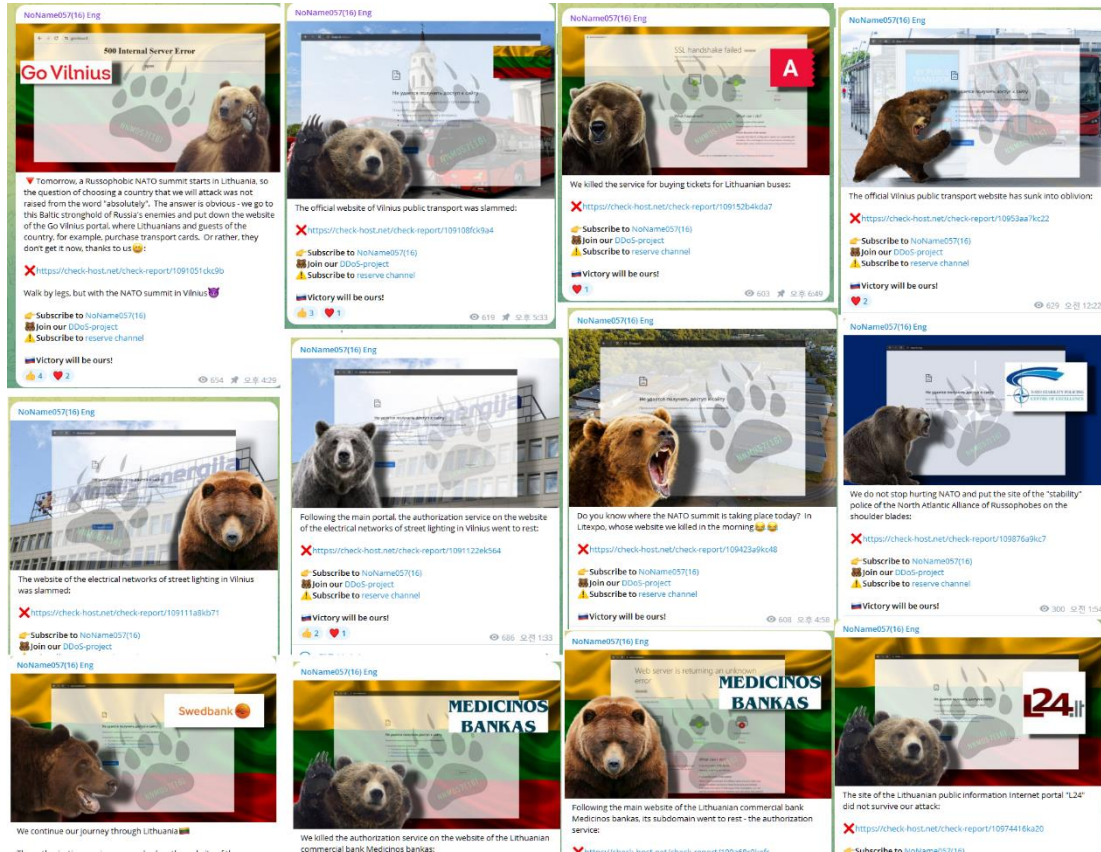


Figure 15. Images from NoName057(16) proving their DDoS attacks against Lithuania and NATO

NoName057(16) created the images above as proof of their attacks and posted them on their Telegram channel. The post includes the flag of the targeted country, the brown bear (Russia's mascot and symbol), descriptions of the affected website, and a link to an external service where one can check the website availability status at the time of the attack.

Victims of DDoS attacks between July 10-13 are as follows, and some websites were attacked more than once.

Target	Number of Affected Websites	Website Type
Lithuania	25	Government organizations,

⁹ <https://www.bbc.com/korean/articles/c9r1yexyllro>

		water/electricity infrastructure, media, finance
NATO	13	Science and Technology Organization, security and technology, Maritime Development Division, Multimedia AEW&C Programme Management Agency, Allied Command Transformation, Cooperative Cyber Defence Centre of Excellence Centre for Maritime Research and Experimentation, information exchange portal

Table 1. Websites affected by NoName057(16)'s DDoS attacks against Lithuania and NATO

(3) Scareware Developer Arrested

The Spanish police arrested the scareware developer who had been on the run from law enforcement authorities for over a decade at El Prat Airport in Barcelona.¹⁰

This person, whose identity remains undisclosed, is a Ukrainian national who has been participating in the development of scareware between 2006 and 2011 and was wanted internationally.¹¹

Scareware is a type of malware disguised as a legal antivirus program that claims to detect and resolve actually non-existent problems in PCs, smartphones, and tablets.

¹⁰ <https://therecord.media/scareware-developer-arrested-in-spain>

¹¹ https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=15824#

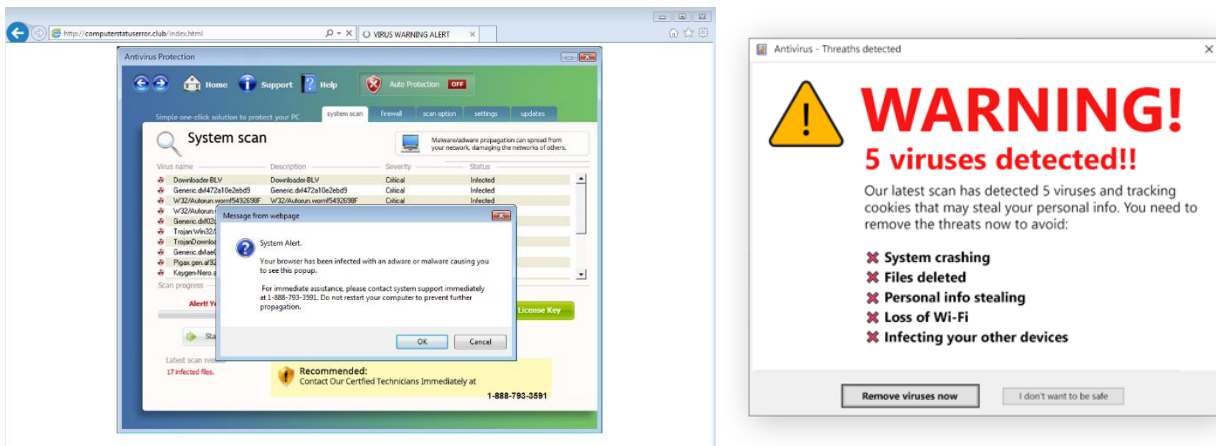


Figure 16. Scareware's detection alert <Source> (Left) malwarebytes.com¹² / (Right) avast.com¹³

The malware continuously exposes fake notifications that scare victims and stress urgency, prompting users to pay to clean their devices from viruses. As a note, AhnLab's V3 products detect this malware as "FakeAV" or "FakeAlert".

According to therecord.media which wrote an article about the arrest of the scareware developer, though the press release from the Spanish police did not include much information about the developer, the suspect appears to have engaged in Operation Trident Tribunal¹⁴ which happened in the past.

In 2011, the Operation Trident Tribunal was conducted by the US Department of Justice and the FBI to target international scareware cybercrime organizations. The operation resulted in the indictment of two individuals from Latvia and the seizure of more than 40 computers, servers, and bank accounts.

One of the targeted criminal groups caused more than \$74 million in total from over 1 million computer users through the sale of fraudulent computer security software known as "scareware".

¹² <https://www.malwarebytes.com/blog/news/2016/04/tech-support-scammers-bring-back-fakeav>

¹³ <https://www.avast.com/c-scwareware>

¹⁴ <https://archives.fbi.gov/archives/news/pressrel/press-releases/departement-of-justice-disrupts-international-cybercrime-rings-distributing-scwareware>

Conclusion

ALPHV (BlackCat) was the first ransomware group to breach data and leak this not on the dark web but on the surface web. An individual DLS was set up on the surface web and the breached data was provided in a format that is easily accessible and searchable by anyone. Such actions distress victims and make other victims feel uneasy as well.

The CLOP ransomware group used the same tactic as the one employed by the BlackCat and LockBit groups and posted the breached data from certain victims both on the surface web and the torrent network. Such a phenomenon is a threat tactic used by ransomware groups following a data breach that serves the purpose of putting more pressure on the victims. Therefore, it is highly likely for other ransomware groups to copy this method in the future.

Cybercrime marketplaces being traded and their databases being sold pose a great challenge to threat intelligence. In response to such threat activities, threat intelligence companies continuously monitor the dark web to collect information on new threats and trends and inform their clients through various media contents.

Activities of pro-Russian hacktivists are on the rise. The cause each activity may vary. In increasing number of incidents, the attacks are launched because of religious or geopolitical reasons or to disrupt countries who support for Ukraine or sanction Russia. This indicates that religious and geopolitical tensions can lead to cyberattacks. Thus, national organizations must enhance cyber security to protect the country's data and systems from such attacks.

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>

© AhnLab, Inc. All rights reserved.

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 endpoint, network, and cloud, 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.