TLP: GREEN

May 2023 Deep Web & Dark Web Threat Trend Report

Ransomware Groups & Cyber Crime Forums and Markets of May 2023

V1.0

AhnLab Security Emergency response Center (ASEC)

Jun. 9, 2023

AhnLab

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.

Contents

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 May 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)

ALPHV (BlackCat) showed an unusual activity by infiltrating two Korean companies simultaneously and designating them as victims. One is a famous Korean confectionary company[1] and the other is a company well known for global localization services for Korean and overseas companies.[2]

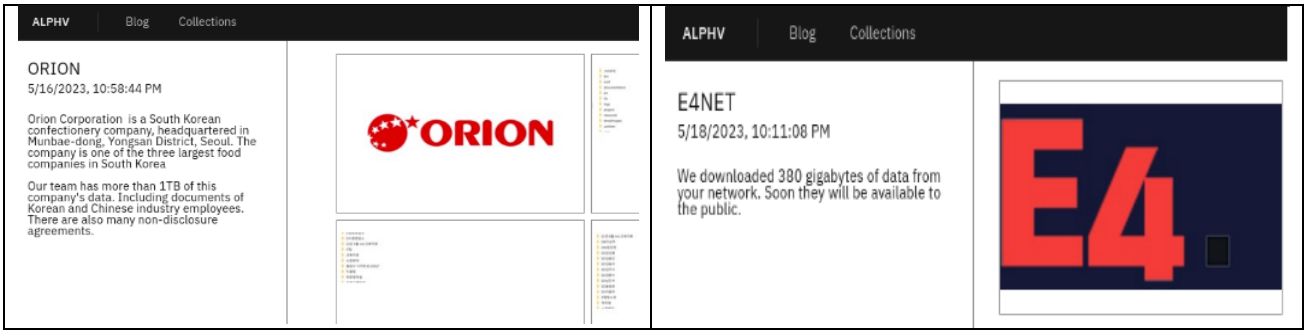

Figure 1. Korean victim companies uploaded
on the ALPHV (BlackCat)'s dedicated leak site (DLS)

This ransomware group had launched attacks against targets in various industries worldwide, with a focus on manufacturing and technology-related organizations and

[1] https://atip.ahnlab.com/ti/contents/asec-notes?i=7e058d8f-898d-493d-af07-bfdc72f2afef

[2] https://atip.ahnlab.com/ti/contents/asec-notes?i=2cbe61c8-3f7e-4581-bdc9-1a5e90ecfcab

companies in the US and Australia. Aside from the aforementioned regions, organizations and companies based in Europe and the Asia Pacific region also became attack targets. According to the data from Trend Micro, ALPHV (BlackCat) preferred to target companies based in the US for their attacks, and organizations based in Europe and the Asia Pacific region were the biggest targets.[3]

Seeing from the cases of threats against Western Digital and McDermott which were recently uploaded as ALPHV victims, the group's level of intimidation is becoming more bold and threatening, and the reasons behind this are deemed to be as follows.

- The bolder the threat, the higher the possibility of the victim paying the ransom
- ALPHV is known to be a highly skilled group and aims to show off their levels of technique and influence
- Data disclosure through threats can cause serious harm to the victim, and this is for the purpose of disturbing the victim's business

Like other ransomware groups, ALPHV also employs a double extortion tactic where they steal and disclose data from the victim company, forcing them to pay a ransom. The group often severely pressures victims into paying their ransom by uploading their data not on the dark web but on a public website accessible by anyone. Their ransom demands range from $400,000 to $3 million, and asked for even larger sums to some large companies that were infiltrated.

While their targets include a variety of industries, they mainly attack the financial, manufacturing, legal, and professional services industries, and it has been confirmed that over 400 victims have been uploaded on the group's DLS where the victim companies and stolen data are disclosed since 2021 when this group first became known.

[3] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat

(2) Akira

The US subsidiary of a Korean pharmaceutical company was listed as a victim on the DLS of the Akira group, which is known to be a relatively new ransomware group.[4] Akira usually attacks companies and organizations in the US and Canada, and it is deemed that they did not specifically target the local subsidiary of a Korean pharmaceutical company. After the group became known in early April, 29 companies have been uploaded to their DLS as of late May present.

date	title	content
2023-05-30	SK Life Science	SK Life Science is a subsidiary of SK Biopharmaceuticals, Co., Ltd., and a part of SK Group—a large conglomerate global corporation. SK Life Science is a CNS-focused pharmaceutical company. You will see their corporate data soon.
2023-05-30	The National Association of Home Builders	The National Association of Home Builders represents the largest network of craftsmen, innovators and problem solvers dedicated to building and enriching communities. "Building Homes, Enriching Communities, Changing Lives" is the motto of the company. They really change lives because of a neglecting attitude to their own security, so you will be able to do whatever you want with their clients, employees and others info soon. Stay tuned.
2023-05-30	Lewis Young Robertson & Burningham	Lewis Young Robertson & Burningham is an independent, fully registered municipal financial advisor. As this firm played an active role as financial advisor and consultant to local governments in Utah, Wyoming, Idaho, Oregon, Washington, and American Samoa, you will be able to take a look at the details of their cooperation and other corporate data of the Lewis Young firm here in our blog .
2023-05-29	Brokers Trust Insurance Group	Brokers Trust is a family insurance company with eyes on the future. This highly experienced team provides expertise for both personal and business insurance coverage. And we, in our turn, will provide both personal and business customer information of this company in our blog soon, if we fail to agree with them. We want to underline that the data is pretty much detailed.
2023-05-29	Computer Information	Computer Information Concepts Inc provides information technology

Figure 2. Victims uploaded to the Akira ransomware group's DLS

Including this case, there was a total of three Korean pharmaceutical-related companies that suffered infiltration and data leakage by ransomware this month. While the incidents were all caused by different ransomware groups, they share the fact that the attacks were against Korean pharmaceutical-related companies. This will be covered in more detail below while examining the trends of the BianLian and RA Group ransomware.

(3) BianLian

BianLian has shown a high level of activity this month, placing third in the number of victims sorted by ransomware group (40 victims uploaded). The group targets organizations in a variety of industries, which are usually organizations and private corporations of major

[4] https://atip.ahnlab.com/ti/contents/asec-notes?i=abfa84f2-6cbf-466e-8030-349f4871e050

infrastructure sectors of the US and Australia.[5] A well-known Korean pharmaceutical company was the first Korean company to be listed as a victim.[6]

This group is known to have accessed the victims' systems through valid Remote Desktop Protocol (RDP) credentials, used open-source tools and command line scripting for credential theft, and extracted the victims' data using File Transfer Protocol (FTP), Rclone, or Mega.[7]

Figure 3. Victim companies listed on the BianLian ransomware's DLS

At the time of writing this document in early June, the name, and personal information of executives in upper management, and data exfiltrated from a Korean pharmaceutical company that fell victim to their information theft were disclosed.

(4) RA Group

The RA Group is a ransomware group that was newly discovered this month. Through security company Cisco Talos, it became known that this group uses the leaked source code of the

[5] https://www.bleepingcomputer.com/news/security/fbi-confirms-bianlian-ransomware-switch-to-extortion-only-attacks/

[6] https://atip.ahnlab.com/ti/contents/asec-notes?i=3a7e9907-b07b-4a72-8772-333de91e7836

[7] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a

Babuk ransomware. As of late May 2023, a total of five victim companies were uploaded to the DLS where the ransomware groups disclose information on their victims as well as their stolen data. This list contained three American, one Korean, and one Taiwanese companies in the electrical parts, investment consulting, insurance, pharmaceutical research and development, and freight shipping, showing that the group targets a variety of industries. Being a new ransomware group, their connection to other groups, their infiltration methods, or data theft processes have not yet been identified.

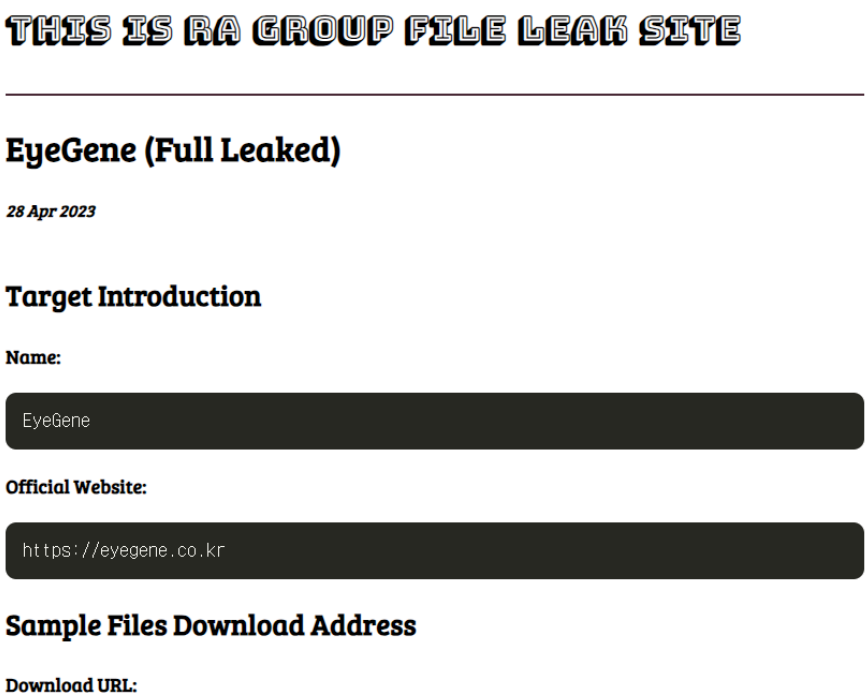

Figure 4. Companies listed as victims on the RA Group's DLS

One of the victims of this group is a Korean pharmaceutical research and development company, and a portion of the leaked data was disclosed. They stated that they would regularly disclose additional data, threatening that all data would be disclosed within a year. This signifies that negotiations for ransom have likely resulted in a failure, and it is forecasted that the threat actor, having put forward a time frame of one year, will continue to pressure the victim with the data they have leaked.

(5) Royal

The Royal ransomware group is a cyber crime organization based in Russia and has been active since September 2022. It is presumed to be a group derived from the Conti ransomware group which has currently been disbanded. The Royal group used the BatLoader malware for initial

infiltration in late 2022, and like normal ransomware groups, employed a double extortion tactic of stealing data and attacking with ransomware.

On May 3, Wednesday, it became known that the official website of Dallas, TX, US, as well as the computer support systems of the city's police and fire departments had their services suspended due to the Royal ransomware attacks.[8] It is said that due to these attacks, the IT systems of the city hall and the court had also been affected, which led to the cancellation of most of the scheduled events at the court. The city of Dallas announced that they are doing their best to mitigate the effects of this cyber attack and that it may take some time to restore the city's IT system.[9]

The city of Dallas was uploaded on the Royal ransomware group's DLS as a victim two weeks after the incident.[10] The city announced that there were no circumstances of personal information leakage as of yet, but the Royal ransomware group stated that they had exfiltrated the personal data of city officials as well as tens of thousands of citizens including their court cases, inmate data, and medical information, of which they are planning to disclose.

Figure 5. The city of Dallas listed as a victim on the Royal ransomware's DLS

[8] https://www.bleepingcomputer.com/news/security/city-of-dallas-hit-by-royal-ransomware-attack-impacting-it-services/

[9] https://www.dallasnews.com/news/politics/2023/05/11/ransomware-full-recovery-could-take-months-dallas-officials-say/

[10] https://atip.ahnlab.com/ti/contents/asec-notes?i=cce41c9d-1d4e-48fc-ba29-b2982d1f04fa

Security researcher Callow from Emsisoft, a company well known for their ransomware analysis and free decryption tool, stated in an interview with Bleeping Computer that "incidents involving US local governments happen at a rate of more than 1 per week". This year, at least 29 small and large local US governments were affected by ransomware, and it has been said that data from at least 16 local governments had been stolen.[11] It has also been said that the recent ransomware attack against the city of Dallas is on the larger side in terms of the scale of damage.

2) Forum & Black Market

(1) Drug-related Criminals Apprehended Through Information Collected Following the Shutdown of Monopoly Market

In December 2021, Monopoly Market, a popular marketplace on the dark web for selling mainly drugs, was suddenly shut down. A variety of suspicions surrounding such an abrupt shutdown arose, some of which are given below.

- Tracking and investigations of law enforcement
- Exit scam where the administrator embezzled the entrusted cryptocurrency
- The administrator retired voluntarily after reaching their financial goals

[11] https://www.bleepingcomputer.com/news/security/city-of-dallas-hit-by-royal-ransomware-attack-impacting-it-services/

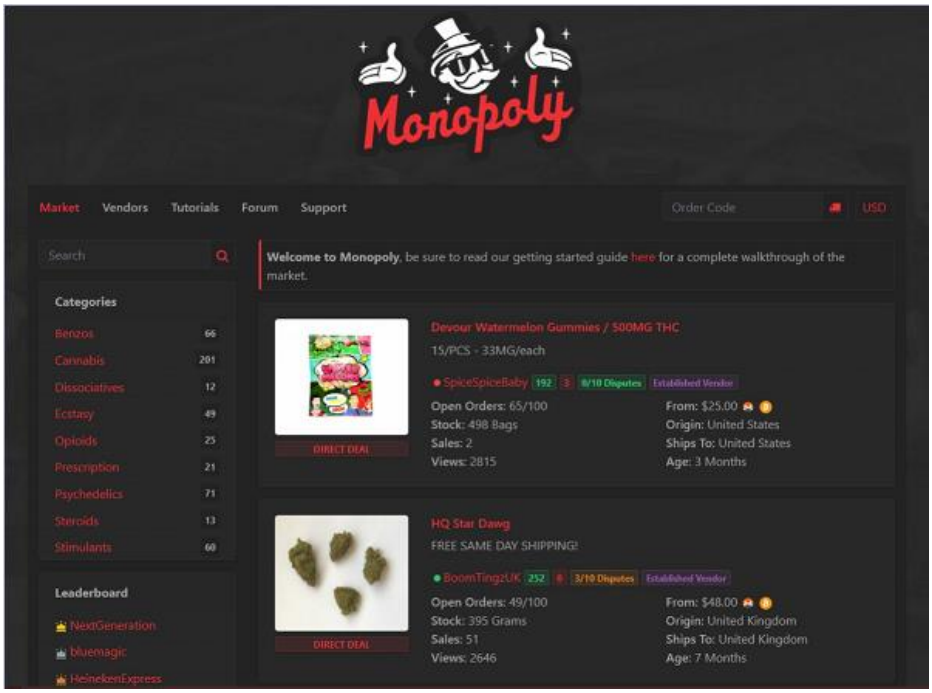

Figure 6. Monopoly Market before shutdown

On May 2, 2023, Europol announced that they have apprehended 288 drug dealers and buyers on the dark web through their Operation SpecTor.[12] Dealers traded with buyers worldwide in BitCoin and Monero cryptocurrency. Aside from Monopoly Market, the apprehended suspects were also known to have been active in other illegal marketplaces and some were regarded as “high-value targets” by Europol.

Monopoly Market was shut down in December 2021 by German law enforcement authorities. Evidence of drug trade was collected from this marketplace, and Europol was able to use the “target package” made based on this evidence in their operation and apprehend the suspects.

[12] https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure

Figure 7. Results of Operation SpecTor – <Source> Europol

Europol stated that investigations are still ongoing to identify the additional individuals still active on the dark web and uncover the parties behind them. As law enforcement authorities became able to access the vast list of buyers held by drug dealers, thousands of drug buyers worldwide are now at risk of being prosecuted.

(2) RaidForums's Database Leaked

A new cyber crime forum known as ExposedForums made its appearance. This forum uses MyBB, free open-source forum software developed by the MyBB Group which is also used by BreachedForums; it also has the same design. However, "Purism", known to be the owner of the forum, argued that they had no connection to BreachedForums.

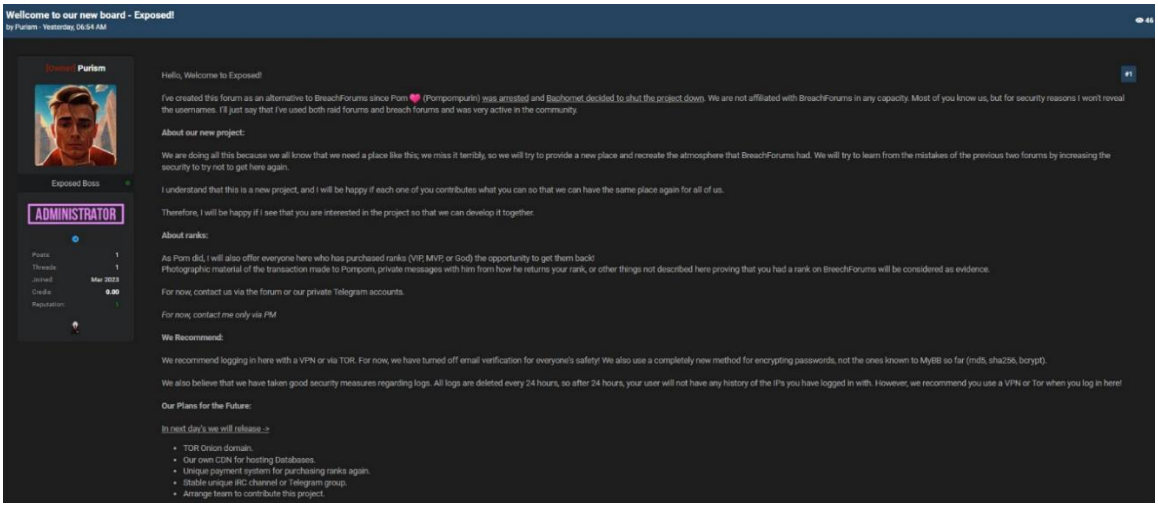

Figure 8. Welcome message from an administrator of ExposedForums

"Impotent", an administrator of ExposedForums, disclosed the member database of RaidForums in late May on their forum. This database leakage occurred two years after the US Department of Justice seized "RaidForums", a notorious cyber crime forum; a database containing details of almost 500,000 users was disclosed online. The leaked data includes usernames, email addresses, hashed passwords, and registration dates.

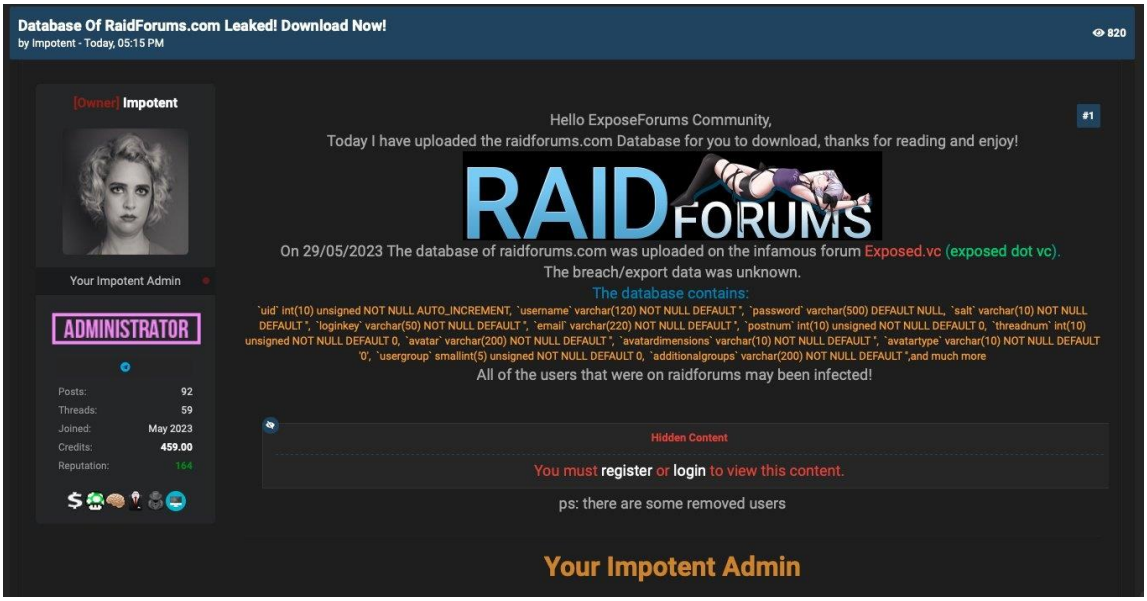

Figure 9. Post on ExposedForums regarding the RaidForums database leakage

Forum admin "Impotent" stated that the data of some RaidForums members had been removed from the database and that it is unknown when and why this dump was created. After the RaidForums database leakage, the user count of ExposedForums increased from about 900 users on the day before the leakage to 3,200 users after the leakage, about a threefold increase.

3) Threat Actor

(1) Wazawaka on the Wanted List

Wazawaka is known to be a male Russian individual named Mikhail Pavlovich Matveev. The US Department of Justice unsealed a bill of indictment on the grounds that this Russian citizen launched attacks using three different ransomware variants on victims all across the US, particularly law enforcement authorities of Washington and New Jersey as well as a variety of sectors including medical organizations, schools, and police departments, causing them harm.[13] Based on this, the FBI uploaded the following wanted poster of this individual.[14]

WANTED BY THE FBI

MIKHAIL PAVLOVICH MATVEEV

Computer Intrusion; Conspiracy; Intentional Damage to a Protected Computer; Threats Relating to a Protected Computer; Aiding and Abetting

DESCRIPTION

Aliases: "Wazawaka", "Boriscelcin", "m1x", "Uhodiransomwar"	
Date(s) of Birth Used: August 17, 1992	**Hair:** Brown
Eyes: Blue / Gray	**Sex:** Male
Race: White	**Languages:** Russian
Scars and Marks: Matveev has a full-sleeve tattoo on his right arm which includes celestial objects such as moons, planets, and meteors, and sea creatures such as a large fish and sting rays. He only has four fingers on his left hand, where he is missing his left ring finger.	

REMARKS

Matveev has ties to both Kaliningrad, Russia, and St. Petersburg, Russia, and is known to travel between the two locations. In addition, Matveev has previously traveled to Thailand.

CAUTION

Mikhail Pavlovich Matveev, a Russian National, is allegedly a prolific ransomware affiliate currently based in Russia. Matveev has been linked to numerous ransomware variants including Lockbit, Babuk, and Hive. He has allegedly conducted significant attacks against both United States and worldwide businesses, including critical infrastructure. Matveev has also been identified as one of the alleged developers/administrators behind the Babuk ransomware variant. Matveev has been charged with multiple Lockbit attacks to include a police department located within New Jersey. He has also been charged with multiple Babuk attacks to include the attack against the Washington D.C. Metropolitan Police Department. In addition, Matveev has been charged with Hive-related counts of conspiracy and intentional damage to a protected computer, including an attack against a New Jersey-based company.

On December 6, 2022, Matveev was charged with Intentional Damage to a Protected Computer; Threats Relating to a Protected Computer; and Aiding and Abetting in the United States District Court for the District of Columbia, Washington, D.C., and a federal warrant was issued for his arrest. On December 8, 2022, Matveev was charged with Computer Intrusion and Conspiracy in the United States District Court for the District of New Jersey, Newark, New Jersey, and a federal warrant was issued for his arrest.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Newark

Figure 10. FBI's wanted list - Mikhail Pavlovich Matveev <Source> - FBI

Mikhail Pavlovich Matveev is known under the aliases “Wazawaka” and “Boriselcin” and also uses the nicknames "m1x" and "Uhodiransomwar". Matveev is connected to Hive, LockBit, and Babuk ransomware created by ransomware-as-a-service (RaaS) based in Russia and is known to have been tracked by law enforcement authorities for using the ransomware to cause harm

[13] https://www.justice.gov/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure

[14] https://www.fbi.gov/wanted/cyber/mikhail-pavlovich-matveev

and significant financial losses worldwide. Matveev was active as a member or an affiliate of the above ransomware group and performed ransomware attacks against organizations and corporations of the key infrastructure in the US.

Following the fugitive warrant issued by the FBI, in an interview with a security company, Matveev stated that [15]"Being placed on the wanted list will not change my actions or influence what I do". The US Department of Justice offered a $10 million reward for information leading to the arrest of Matveev.

Conclusion

This month, there was an unusual listing of five Korean companies as ransomware victims. The fact that three of these victims were in the same industry of pharmaceuticals also drew attention. It seems that some pharmaceutical companies recorded the highest sales during the COVID-19 pandemic, and cyber criminals likely took note of this fact and actively targeted pharmaceutical companies.

According to some studies, ransomware attacks do not begin with the selection of attacks but with the purchasing of network access permissions of a company that seems promising for extorting ransom from, out of those sold by an initial access broker (IAB) before performing the attack.[16] There can be more attacks from IAB and RaaS against medical institutes and pharmaceutical companies which had been blessed with increased demands due to COVID-19, so these industries must heighten their interest and sense of awareness in cyber crime including ransomware and data leakage.

Following the disclosure of the RaidForums database, ExposedForums is quickly gaining popularity and notoriety and is assessed as having the means to secure its identity as a replacement for the Breached forum. The leaked database of RaidForums will possibly be useful for law enforcement authorities and security researchers to profile the forum users and link them to other malicious activities.

While the fugitive warrant on Wazawaka increased awareness in cyber crime, it is not

[15] https://therecord.media/wazawaka-cyber-most-wanted-interview-click-here

[16] https://atip.ahnlab.com/ti/contents/issue-report/trend?i=baa21824-5f80-405f-9304-158609e00c8d

expected to have a great influence on the activities of cyber criminals. It is not yet known whether the event will be of help in restraining the activities of ransomware groups he was a part of or instead spur their attacks even more. However, the news of the fugitive warrant will be somewhat helpful for companies around the world preparing defenses against ransomware 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

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

AhnLab