TLP: GREEN

June 2023 Deep Web & Dark Web Threat Trend Report

Ransomware Groups & Cyber Crime Forums and Markets of June 2023

V1.0

AhnLab Security Emergency response Center (ASEC)

Jul. 7, 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 June 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) CLOP

The CLOP ransomware group claimed that they exploited the MOVEit vulnerability[1] (CVE-2023-34362) to infiltrate hundreds of companies and steal their data. Microsoft also officially announced that the MOVEit Transfer campaign is attributed to the CL0P (Lace Tempest, FIN11, TA505) threat group. [2]

MOVEit Transfer is a managed file transfer (MFT) solution developed by Ipswitch, a subsidiary of Progress Software Corporation based in the US. It allows companies to use SFTP, SCP, and HTTP-based uploads to safely transfer files between business partners and clients.

The CLOP ransomware group announced on their dedicated leak site (DLS) that they had stolen data from "hundreds of companies", and if the ransom is not paid, the group will begin to release the names and data from the infiltrated companies after June 14.

[1] https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

[2] https://twitter.com/MsftSecIntel/status/1665537730946670595

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - F[illegible]
STEP 3 - [illegible]

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

Figure 1. The threat uploaded to the CLOP DLS

The threat actor seems to have sent the threat as an announcement on their DLS instead of sending individual emails because there are too many victims. This is an unusual method that has not been used before. In their threat post, they claimed that they are only motivated by financial gain and are not interested in politics. The group also stated that they deleted all data related to the government, city, and police.

The CLOP ransomware group has a history of using the following vulnerabilities in similar cases to infect companies that use the affected services with ransomware or steal their data and demand ransom through threats.

Service Name	CVE Number
Accellion FTA	CVE-2021-27101 CVE-2021-27102 CVE-2021-27103 CVE-2021-27104
SolarWinds Serv-U	CVE-2021-35211
GoAnywhere MFT	CVE-2023-0669
PaperCut	CVE-2023-27350 CVE-2023-27351

MOVEit Transfer	CVE-2023-34362

Table 1. List of vulnerabilities used by the CLOP ransomware group for data leaks and ransomware infection

After the attacks with this malware type which resulted in many victims, the CLOP ransomware group tended to disclose data from the victims over a long period of time. It was also observed in the recent attacks that the names of the targeted companies were posted frequently on the DLS for a long time.[3]

Figure 2. List of victims uploaded to the CLOP DLS - As of June 30, 2023

Over 80 victims in total including a famous energy company in the US, a UK-based global accounting corporation, and a Japanese multinational conglomerate were uploaded in the month of June.

(2) LockBit

The LockBit ransomware group claimed that they breached a famous large Taiwanese semiconductor corporation in late June, which earned them much attention from security researchers and the media. This incident first became known when "Bassterlord" uploaded details on Twitter regarding a ransomware attack seemingly involving the corporation in

[3] https://atip.ahnlab.com/ti/contents/asec-notes?i=9c29fb3d-fe5b-4a8c-8517-00172c43b3e6

question. Bassterlord is a notorious initial access broker (IAB) leading the "National Hazard Agency", a group known to be affiliated with LockBit.[4]

The victim of the breach denied this fact, but the group requested a large sum of $70 million as ransom and uploaded the following details and proof to their DLS.

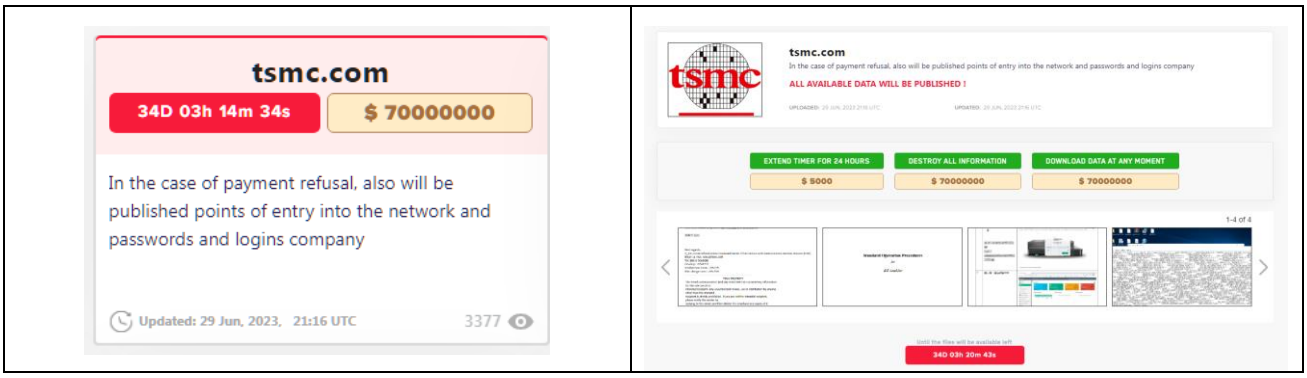


Figure 3. A large Taiwanese semiconductor corporation posted as a victim

Afterward, the corporation announced that a third party in a cooperative relationship with them became the target of a cyber attack by LockBit and information leakage occurred. It also stated that the operations of the semiconductor corporation were not affected by this incident and no harm was done to customer information. Moreover, the corporation claimed that they ceased exchanging data with the affected supplier immediately after the incident.

The ransom of $70 million suggested by LockBit is known to be in the top 5 ransom amounts until now. The top 5 ransom amounts in history are as follows.

Ransomware Group	Victim	Industry	Ransom
Hive	MediaMarkt	Electronics retailer	$240 million
REvil	Acer	Electronic parts manufacturer	$100 million
REvil	Kaseya	Software developer	$70 million
LockBit	TSMC	Semiconductor manufacturer	$70 million
LockBit	Pendragon	Car retailer	$60 million

Table 2. Top 5 demanded ransom amounts

[4] https://www.bleepingcomputer.com/news/security/tsmc-denies-lockbit-hack-as-ransomware-gang-demands-70-million/

The number of victims uploaded to the LockBit ransomware group's DLS decreased slightly in comparison to the CLOP ransomware this month, leading to CLOP taking the first place which had been continuously held by LockBit. Note that these figures and rankings may differ depending on the threat intelligence company monitoring the DLS of ransomware groups.

(3) Snatch

The Snatch ransomware group uploaded a Korean car manufacturer as a victim in early June, but aside from the name and a description of the organization, no evidence of the breach was given. [5] No evidence has been given as of early July, a month following the update.

Figure 4. Korean car manufacturer uploaded as a victim

It seems this group has been active since the summer of 2018, and this has been confirmed through a blog post by security company "Sophos".[6] The group also uploaded a post on a Russian cyber crime forum recruiting affiliates, with the condition that they are only hiring Russian speakers. Based on this fact, we assume that the operators of the Snatch ransomware are based in Russia.

In the early stages of their activities, Snatch used ransomware developed in Go which only

[5] https://atip.ahnlab.com/ti/contents/asec-notes?i=b59c0138-1c83-4a79-a243-c6156407a231

[6] https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/

runs in Windows environments. The recent notice on the Snatch ransomware's DLS claims that the group does not use ransomware. This seems like the group has changed their tactics to only practice data theft, but this is only a one-sided claim of a cyber criminal and its legitimacy has not been ascertained.

The Snatch ransomware group performs attacks against a variety of industries. In late November 2021, the first victim was uploaded to their DLS where they reveal their victims and disclose leaked data. As of June 2023 present, over 80 victims are posted on the DLS.

(4) RA Group

Around 13:00 on Saturday, June 17 (KST), the RA Group posted a victim they named "Target-8" on their DLS and claimed that data totaling 923 GB in size was leaked from this organization.

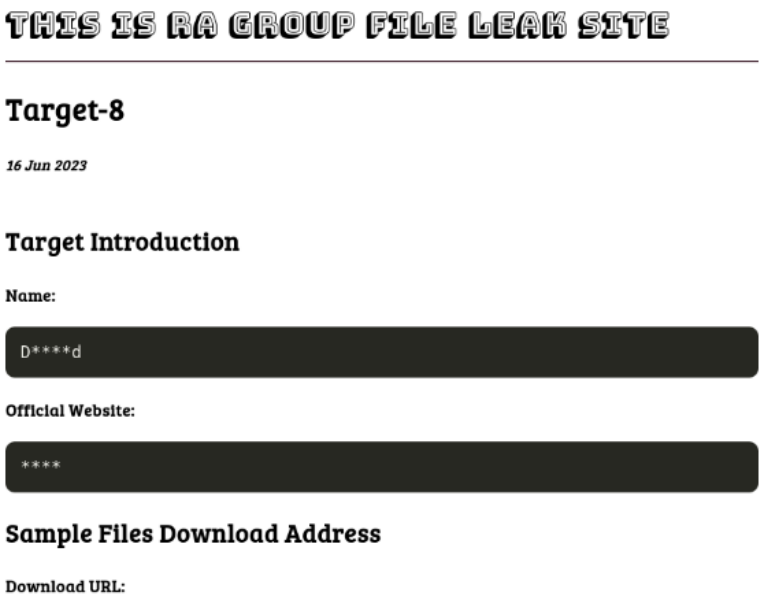


Figure 5. The victim posted to the RA group's DLS

Some ransomware groups conceal the names of their victims with asterisks (*) to hinder threat analysis of security companies that monitor their DLS and as a part of their threat tactics on the victim. It seems that the RA group renders their victims indistinguishable by referring to them as "Target-(number)" and when negotiations fail, changes it to the actual name of the organization.

This group uploaded "Target-8" and "Target-9" to their DLS on June 21 and 28 respectively and included a sample of the leaked data as well. The victim named "Target-8" was identified to be a Korean AI solutions provider. This group also breached a Korean pharmaceutical

research and development company and disclosed the leaked data last month. Additionally, "Target-9" was found to be a Thai reinsurance company.

(5) Ransomware Groups' Affiliate Recruitment Ads

The Trigona and Everest ransomware groups each uploaded the following ad for affiliate recruitment. Trigona uploaded the ad on a cyber crime forum while Everest uploaded it to their DLS.

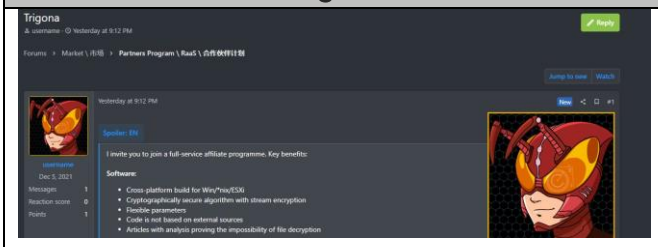
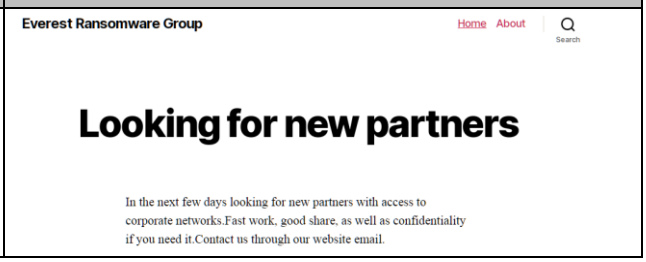
Trigona	Everest
	

Figure 6. Affiliate recruitment ads uploaded by ransomware groups – Trigona source: Twitter @FalconFeedsio

The following are reasons why ransomware operators recruit affiliates.

- They can expand the scale and scope of attack targets. The more affiliates there are, the more victims they can attack, meaning that they can earn ransom from the leaked data.

- The operator can hide their identity and disperse liabilities. As the operator of the ransomware is not directly involved in any attacks launched by an affiliate, they become more difficult to track.

- Human and material resources needed for attacks can be procured, increasing the chances of success. Affiliates may have more knowledge of the attack target than the ransomware operator and perform attacks more effectively.

2) Forum & Black Market

(1) Monopoly Market's Operator Arrested

This is a continuation of the "Monopoly Market" and the results of Operation SpecTor covered in AhnLab's May 2023 Deep Web & Dark Web Threat Trend Report.[7] 33-year-old Milomir Desnica, a Serbian male who is the operator of the market, was arrested in November 2022 in Austria and repatriated to the US.[8]

United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
DISTRICT of COLUMBIA

HOME ABOUT NEWS MEET THE U.S. ATTORNEY DIVISIONS PROGRAMS

U.S. Attorneys » District of Columbia » News

Department of Justice
U.S. Attorney's Office
District of Columbia

SHARE

FOR IMMEDIATE RELEASE — Friday, June 23, 2023

Citizen of Croatia and Serbia Charged with Running Monopoly Drug Market on the Darknet

Defendant Facilitated $18 Million in Illegal Drug Transactions Using Cryptocurrency

WASHINGTON –Milomir Desnica has been extradited from Austria to face charges of running a criminal darknet narcotics marketplace. The charges, unsealed on May 25, 2023, were announced today by United States Attorney Matthew M. Graves and Acting Special Agent in Charge Sarah Linden, of the FBI Washington Field Office's Criminal and Cyber Division.

Desnica, 33, of Smederevska Palanka, Serbia, was indicted on July 26, 2022, by a grand jury in the U.S. District Court for the District of Columbia on charges of conspiracy to distribute and possess with intent to distribute 50 grams or more of methamphetamine and one count of conspiracy to launder monetary instruments. The indictment also includes a forfeiture allegation seeking all proceeds of the alleged crimes. Desnica will be arraigned on the charges on a date to be determined by the Court.

Figure 7. A part of the bill of indictment for suspect Milomir Desnica[9]

He was charged with operating a drug market on the darknet called "Monopoly Market".

[7] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=ca975693-f4f5-4c89-bd99-0ad195e7a27f

[8] https://www.bleepingcomputer.com/news/security/man-charged-in-us-for-running-monopoly-darknet-drug-market/

[9] https://www.justice.gov/usao-dc/pr/citizen-croatia-and-serbia-charged-running-monopoly-drug-market-darknet

According to the United States Department of Justice, through an analysis of the seized server, the law enforcement authority was able to identify and analyze records of drug sales instigated by Monopoly, financial records which document the payment of cryptocurrency in said market, and communications records and statements of commission payment that the Monopoly operator sent to vendors. With this, they were able to identify the suspect.

The operator is charged with instigating illegal drug trades totaling $18 million by running the "Monopoly Market". He was given a life sentence, the maximum penalty for the distribution of a particular drug, and was sentenced to an additional maximum of 20 years for cryptocurrency laundering.

The apprehension of a cyber criminal can act as a warning to other criminals, dissuading them from their activities. However, such influence differs case by case and may be temporary.

(2) Suspension of ExposedForums

"ExposedForums" earned much attention and saw an explosive increase in the number of its members last month when it leaked the database of "RaidForums". However, the operator of this new forum uploaded a short message saying that they do not have enough time to maintain and manage the forum and was looking for a new owner to look after the forum, before disappearing completely.

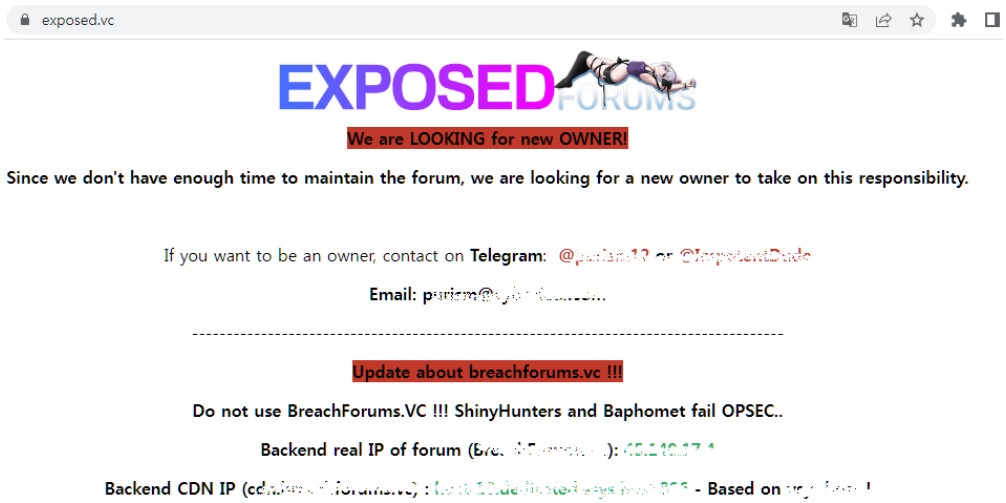


Figure 8. Post from the Exposed forum's operator announcing the closing of the website

Additionally, "BreachForums", a new version of "BreachedForums" which was closed down by law enforcement authorities in March of this year suffered operational security (OPSEC) failure. A post was uploaded saying that the actual IP of the forum was disclosed and that this forum should not be used.

Ordinarily, the reasons that cyber crime forums close are as follows.

- Surveillance and inspection by law enforcement authorities
- High levels of attention and criticism from the outside regarding illegal data sales
- OPSEC failure

While the specific reason is unknown, it seems that the closing of "ExposedForums" would be of help in part to responding to cyber crime. With the closing of the forum, cyber criminals will find it difficult to share and sell illegal data. It is expected that this will also increase awareness of some forum users on cyber crime and help prevent harm from cyber crime.

(3) Rebirth of BreachForums

"Baphomet" and "ShinyHunters", former admins of "BreachedForums" which had been closed by law enforcement, announced that they are commencing service for "BreachForums", a new data leak forum to replace BreachedForums and RaidForums.

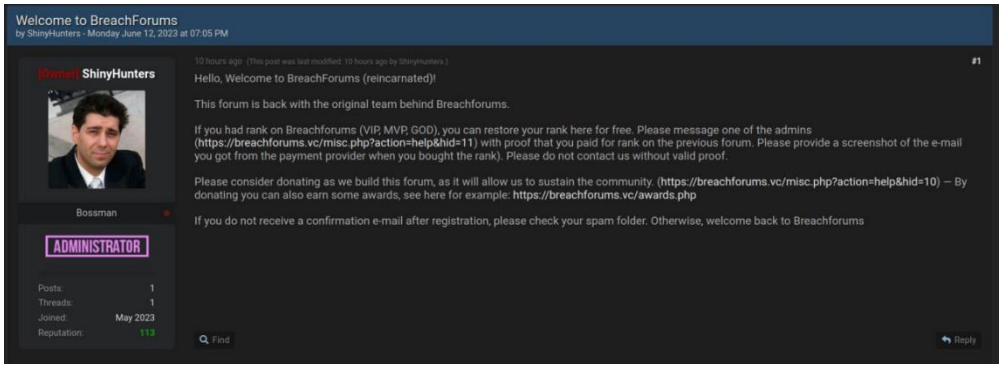


Figure 9. BreachForums operator notifying the opening of the forum

Similar to the forums that closed down, this forum was also built based on MyBB, an open-source forum software. Other features are also the same as the previous forums but with enhanced security.

The new "BreachForums" is becoming a popular forum for cyber criminals. As in the past, the forum is being used as a place to share information on hacking, data leak, and other cyber crimes, and this is becoming a concern for companies and researchers who study cyber security.

3) Threat Actor

(1) LockBit Ransomware Group's Affiliate

The US Department of Justice announced that Russian citizen Ruslan Magomedovich Astamirov was arrested in Arizona, US, and that he is prosecuted for distributing the LockBit ransomware.[10] This suspect from the Chechen Republic in their 20s is known to have been involved in LockBit ransomware attacks between August 2020 and March 2023.

Figure 10. Press data from the US Department of Justice regarding the prosecution of Astamirov

[10] https://www.justice.gov/opa/pr/russian-national-arrested-and-charged-conspiring-commit-lockbit-ransomware-attacks-against-us

The suspect is charged with extorting tens of millions of dollars from over 1,400 victims using the LockBit ransomware and is facing up to 20 years of imprisonment.

According to the announcement from the US Department of Justice, Astamirov is the third individual affiliated with LockBit who has been prosecuted by the US since November 2022. The following is the status information on individuals affiliated with LockBit affiliates who have been prosecuted and/or apprehended thus far.

Name (Nickname)	Status
Mikhail Vasiliev	Prosecuted and arrested
Mikhail Pavlovich Matveev (Wazawaka)	Prosecuted
Ruslan Magomedovich Astamirov	Prosecuted and arrested

Table 3. LockBit affiliates who have been prosecuted and/or arrested

The prosecution or apprehension of a known cyber criminal can have a positive effect on cyber security. This is because such measures place legal liabilities on the criminals and send a warning message to other criminals.

(2) Bjorka

Bjorka is known to have leaked many databases in Indonesia since 2020. This threat actor specializes in database leaks from the Indonesian government and companies.

Figure 11. Bjorka's own database leakage portal

They recently became active on the newly opened "BreachForums" and more recently, opened their own database leakage portal. This could have a negative effect on cyber security because sensitive information may be posted on this forum which may become another market where the said information can be sold to cyber criminals who abuse the data.

(3) Anonymous Sudan

In mid-June, Anonymous Sudan warned that they have joined forces with groups such as KillNet and REvil to launch a large-scale attack on the financial systems of the US and Europe within the next 48 hours. This is likely a new attack campaign on the financial sectors of Western countries, and it is notable that the ransomware group "REvil" is participating.

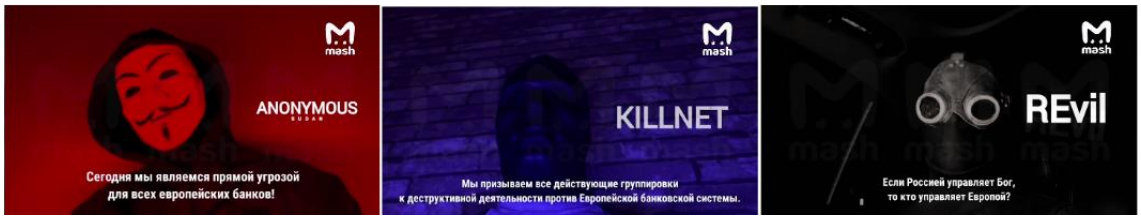


Figure 12. Each group appearing in the video regarding the attack campaign against Western financial sectors

Hacktivists are known to launch cyber attacks to express their opposition to governments, organizations, and individuals, or to raise awareness on certain issues. Some security researchers conclude that the news of REvil's participation and the attack threats against the financial systems of the US and Europe are absurd and groundless because there have been no past cases of REvil forewarning their attacks before a camera.

Afterward, KillNet and Anonymous Sudan posted a Telegram message saying that they have launched the attack campaign against the financial sector, starting with the European Investment Bank (www.eib.org).

Figure 13. Telegram message forewarning the attack on the European Investment Bank

The threat groups then launched a DDoS attack on the website of the International Finance Corporation (IFC) and posted a Telegram message regarding the details. Unlike their initial claim that they would attack the Society for Worldwide Interbank Financial Telecommunication (SWIFT), their DDoS attack was launched against a different target.

Besides the campaign above, Anonymous Sudan also launched a DDoS attack on Microsoft's web services in June. The DDoS attack technique employed at this time was found to be the following attack type targeting layer 7.[11]

Attack Type	Details
HTTP(S) flood attack	A method that uses the HTTP(S) protocol to send large volumes of legitimate requests to the server, expending the server's resources and degrading its response capabilities
Cache bypass	A method where requests are sent directly to the server by bypassing the web cache, consuming resources of the actual server instead of cached contents
Slowloris	A method of maintaining a connection to the server and sending requests very slowly, taking up the maximum number of simultaneous connections and preventing other users from connecting to the server

Table 4. Types of DDoS attacks launched by Anonymous Sudan

Layer 7 DDoS attacks refer to attacks against the target system using application layer protocols such as HTTP, HTTPS, and SMTP. Microsoft announced that they believe Anonymous Sudan is capable of enlisting large numbers of botnets and tools to start DDoS attacks from multiple cloud services and open proxy infrastructure.

[11] https://msrc.microsoft.com/blog/2023/06/microsoft-response-to-layer-7-distributed-denial-of-service-ddos-attacks/

Conclusion

A key takeaway from the incident where the CLOP ransomware group exploited a MOVEit vulnerability would be that the top priority is to reduce the attack surface. Threat actors are known to have abused zero-day vulnerabilities to exfiltrate sensitive data and threaten victims with it. Unfortunately, perfect prevention of zero-day vulnerabilities is not possible, but by reducing the attack surface, even if harm is caused, the damage can be minimized.

In the case of the incident examined in this report, visibility must be procured first by checking all internet-based applications running in the organization, as well as understanding and identifying the attack surfaces that are exposed externally. Afterward, risk management and minimization must be practiced through strong security policies and auditing for products and systems that are inappropriately exposed or managed externally.

Cyber crime forums are places where cyber criminals mutually share information and provide cooperation. The closing and re-emergence of these forums may greatly impact the activities of cyber criminals. For the purpose of attracting users of existing forums, some new forums even inherit user tiers and give compensation in "credit" which can be used as currency in the forums. With enhanced operation security and access to more illegal data, the forums also stimulate the curiosity of users.

The cooperation of Pro-Russian hacktivists Anonymous Sudan and KillNet with REvil, a ransomware group based in Russia was quite unusual, and alliance presented their plans of DDoS attacks against the Western financial sector and put them to action. The reason why these groups are cooperating is not clear, but we know that in order to protect Russia, KillNet added to their member roster hacktivist group Anonymous Sudan who usually launches DDoS attacks against Western or anti-Russian countries.

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