TLP: GREEN

March 2023 Deep Web & Dark Web Threat Trend Report

V1.0

AhnLab Security Emergency response Center (ASEC)

Apr. 07, 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.

The version information of this report is as follows:

Version	Date	Details
1.0	2023-04-07	First release

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 March 2023 is sectioned into Ransomware, Forum & Black Market, 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 Ransomware

The ransomware group known as Clop or CL0P is also known by the name TA505. This group exploited the file transfer tool GoAnywhere's administrator console zero-day vulnerability (CVE-2023-0669) to steal data from more than 130 groups over 10 days.[1] GoAnywhere is a web-based managed file transfer (MFT) solution, mainly used by companies. The company that created this tool is Fortra, formerly known as HelpSystems. Ironically, this company is the same company that created Cobalt Strike, a well-known legitimate commercial penetration testing tool.

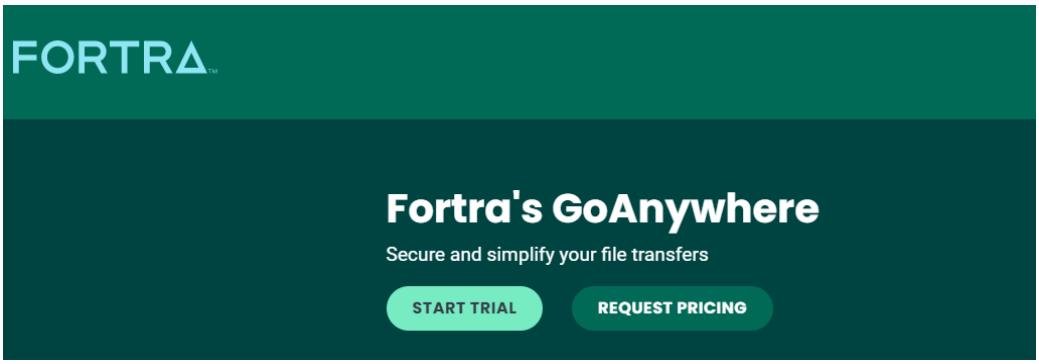

Figure 1. GoAnywhere product introduction page (www.fortra.com)

Although Fortra was known to have only leaked data without distributing ransomware through vulnerability exploitation, a month later on March 12, the threat group began to reveal multiple victim organizations that had been attacked through the GoAnywhere zero-day

vulnerability on their dedicated leak site (DLS).

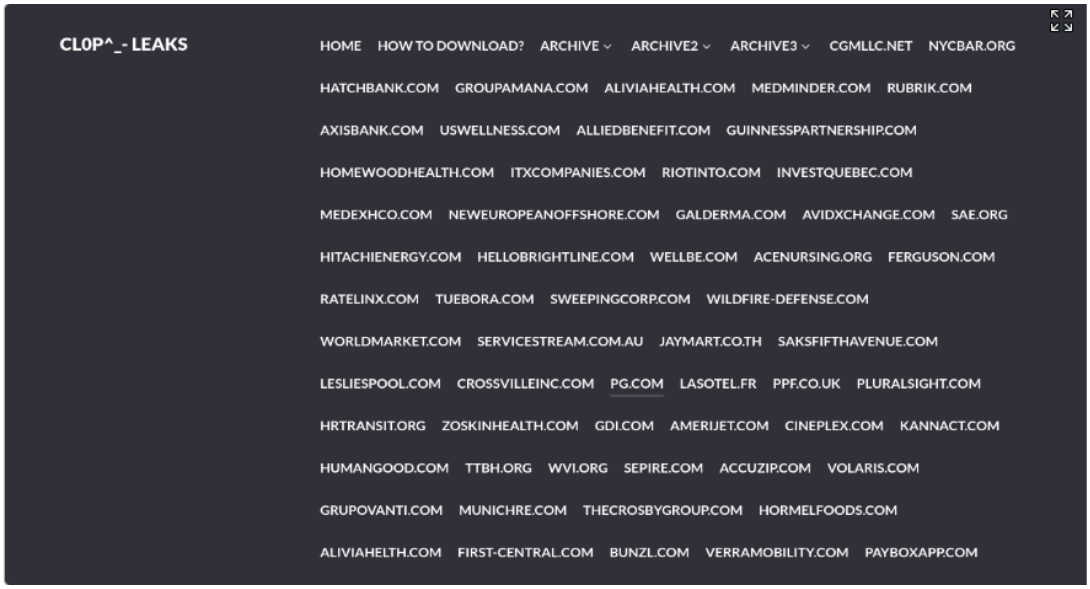

Figure 2. Victims announced on the Clop Ransomware DLS

The number of attacked companies increased continuously throughout March, reaching over 100. Among the victims was the American multinational company Procter & Gamble (P&G), a manufacturer and distributor of various consumable items such as soup, shampoo, toothbrushes, diapers, etc.[2] The company announced that there was a data leak that affected some of its employees after the GoAnywhere MFT security file-sharing platform had been damaged. It was formerly posted on the DLS that the city of Toronto, Canada had also been attacked, but for unknown reasons, the post was deleted. The state of Tasmania, Australia was also posted as a victim, and the state government announced that it is investigating this matter.[3]

(2) BlackCat (Alphv) Ransomware

The BlackCat (Alphv) ransomware group showed off a vicious method to pressure the victims this month. This group invaded the Lehigh Valley Health Network (LVHN) in Pennsylvania, US, and leaked its data. Afterward, they revealed clinical test pictures of female participants' faces and bodies, along with their personal information as sample data.

Figure 3. Information on LVHN posted on the BlackCat (Alphv) ransomware group's DLS

Many security researchers criticized this incident, saying that it was a shameless crime that took advantage of cancer patients receiving care. The hospital in question refused to submit to the ransomware group's threats and did not pay the ransom. As a note, the Federal Bureau of Investigation (FBI) advises not to pay the ransom when involved in a ransomware attack because doing so will only encourage additional attacks and there is no guarantee that the leaked data will be deleted.

Before the hospital refused to pay the ransom, they had to endure the pressure of additional data leaks every week. Currently, all of the data has been revealed. Afterward, the patients whose clinical pictures and personal information had been leaked filed a lawsuit against the hospital through a representative attorney.[4] If proper precautions are not taken against cyber attacks like breaches via ransomware, then it could lead to unexpected collateral damage. As shown in this case, individuals whose personal information is leaked can experience embarrassment and are prone to identity theft and fraud. Solving these problems takes up personal cost and time.

The US FBI and Cybersecurity and Infrastructure Security Agency (CISA) had released multiple warnings against ransomware group attacks that target American medical facilities. In other words, it is crucial to prepare adequate and reasonable actions to prevent ransomware attacks. However, this hospital failed to secure its management and thus had to face dire

consequences.

(3) LockBit Ransomware

The LockBit ransomware group posted Korea's National Tax Service as its victim. This was the first known case of a Korean government facility being posted on a ransomware DLS. The post was uploaded on March 29, 2023, and it announced that the data would be leaked on April 1. However, the data was not revealed even after the announced date had passed.

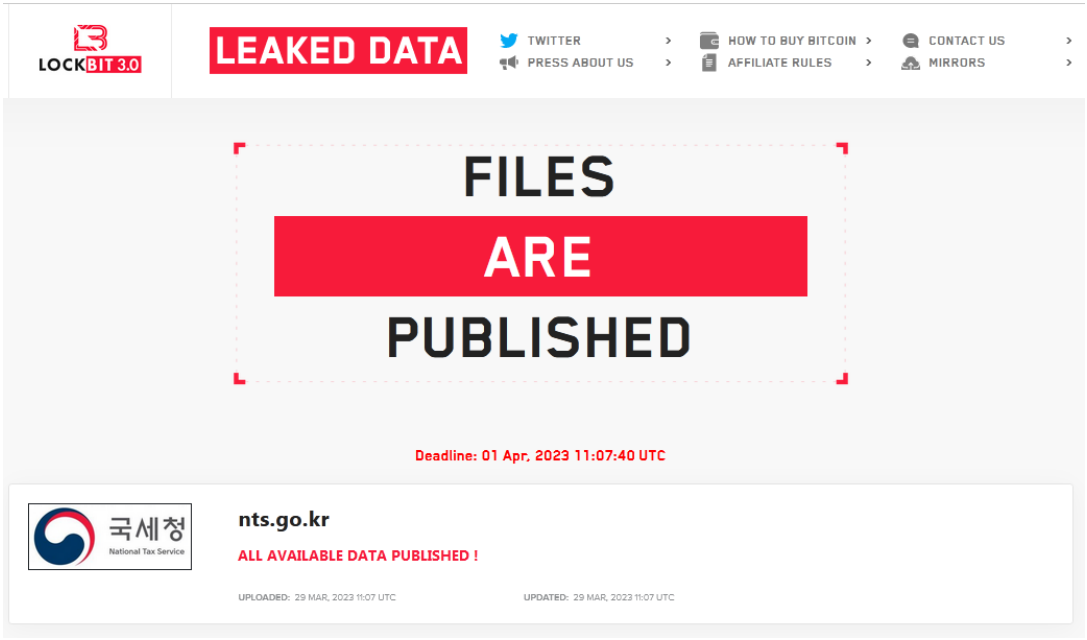

Figure 4. The Korean National Tax Service posted on LockBit DLS

The LockBit ransomware group attacks both private enterprises and government facilities, with no specific industry in mind. The government organizations that have been recently announced as victims are as follows.

Domain	Date	Organization Name
nts.go.kr	Mar. 29, 2023	National Tax Service, Korea
medellin.gov.co	Mar. 27, 2023	Medellin, Columbia

ksrsac.karnataka.gov.in	Mar. 21, 2023	Karnataka Geospatial Center, Indonesia
oaklandca.gov	Mar. 21, 2023	Oakland, CA, US
agenziaentrate.gov.it	Jan. 27, 2023	National Tax Service, Italy
dof.ca.gov	Dec. 12, 2022	California State Treasurer's Office, US
railway.gov.tw	Oct. 30, 2022	Taiwan Railways Administration
frederickco.gov	Sep. 7, 2022	Town of Frederick, CO, US

Table 1. Government organizations posted on the LockBit DLS as ransomware attack victims (from the past 8 months)

(4) Medusa Ransomware

The Medusa ransomware group first became known in 2021, but it is becoming more active in 2023. This group is different from the MedusaLocker ransomware. In other words, Medusa and MedusaLocker are two different groups. This means the TOR addresses of the two groups are different as well.[5] The Medusa ransomware adds the extension .MEDUSA to the encrypted files.

Figure 5. Minneapolis Public Schools posted as a victim

Medusa breached Minneapolis Public Schools in early March and demanded a ransom of one million dollars along with the post of a video containing data suspected to have been leaked on their DLS, drawing interest from the public. Such threat is a newly-seen strategy as previous ransomware groups presented screenshots and lists of files as proof of data breach.

2) Forum & Black Market

(1) Breached Forums Closed

Breached Forums is a cyber crime forum that gained its notoriety for leaking databases of Korean companies of all sizes. Conor Brian Fitzpatrick, the administrator of said forum, was arrested by the US FBI in Peekskill, New York on March 15.[6] He was known as "Pompompurin" on the forum.

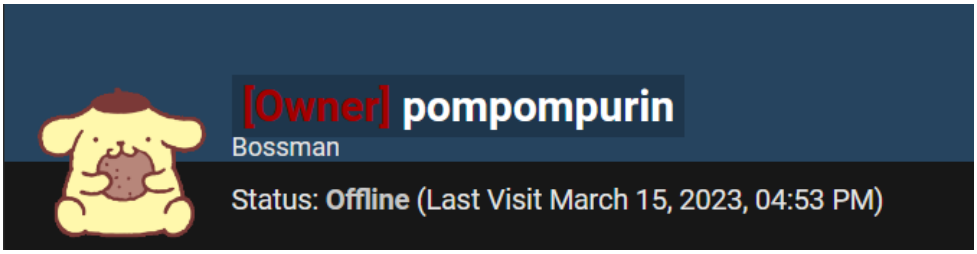

Figure 6. Conor Brian Fitzpatrick's Breached Forums ID

Breached Forums is known as the alternative site to Raid Forums, which was taken down after its administrator had been arrested last year. After being arrested, his parents paid bail and he has been released. He appeared in court on Mar 24, and has been prosecuted for his crimes of stealing and selling sensitive personal information and is facing up to five years in prison if found guilty. He earned 1,000 dollars' worth of profit every day by selling "Credits" that can be used in the forum, and it is speculated that he used this money to maintain the forum and purchase other domains.

After the arrest of its administrator, the ownership of Breached Forums was transferred to one of the remaining administrators, who was a user with the nickname "Baphomet". They attempted to stabilize the forum but found that an unknown party (suspected to be a federal agent of a law enforcement agency) had already logged in as an administrator and searched and changed the server settings. Following this, the manager gave up on normalizing the

forum and posted about their discovery on their own website and Telegram channel.

After Breached Forums closed down, multiple imitations of it were found. Some claim that they are able to succeed the privileges of Raid Forums and Breached Forums. However, there has not been a noticeable increase in the number of their members due to DDoS attacks from unknown parties and because the forums failed to earn the trust of their users. Some imitators failed at management security or had their management data leaked, causing their web services to be extremely unstable.

3) Threat Actor

(1) Netwire RAT Malware Infrastructure Confiscated and Administrator Arrested

The administrator of NetWire Remote Access Trojan (RAT) was arrested, and the service's web domain and hosting server were confiscated.[7] This operation was carried out as an international law enforcement operation by the FBI and international police departments.

Figure 7. Confiscated NetWire RAT domain - <Source> https://www.bleepingcomputer.com

NetWire RAT is a subscription-based commercial RAT tool, distributed as a Malware-as-a-

Service (MaaS) model. It can take remote screenshots, download and upload files, execute commands, download and execute additional files in infected systems.

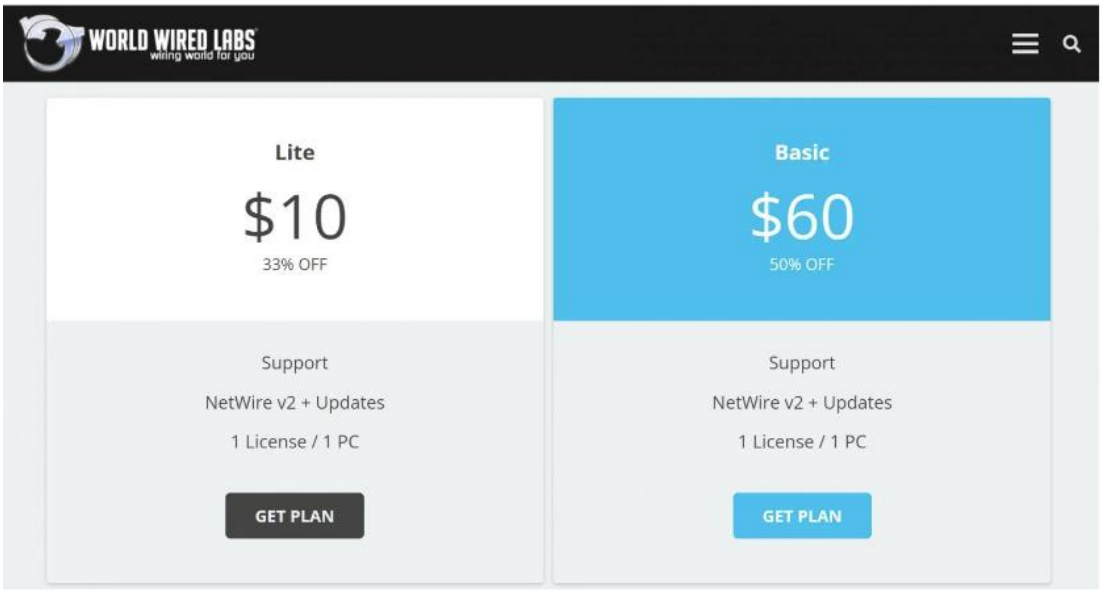

Figure 8. Subscription-based NetWire RAT - <Source> https://www.bleepingcomputer.com

However, the creators of the malware abused this service for phishing attacks and malicious spam emails. More importantly, it has been used on a wide scale of malicious activity, such as breaching corporate networks. A Croatian citizen suspected to be the manager of the NetWire website has been apprehended by the Croatian authorities and is scheduled to be prosecuted.

(2) DoppelPaymer Ransomware Group Suspects Arrested

An international law enforcement operation took place to investigate the "key members" of the DoppelPaymer ransomware group.[8] This operation was overseen by Europol. The German and Ukrainian police forces conducted a simultaneous seizure and search in each country on February 28. The investigators analyzed the seized devices and are working on figuring out the structure of the ransomware group and the exact roles of the suspects.[9] Additionally, arrest warrants for three additional suspects have been issued. They are presumed to be key suspects.

Name	Role
Igor Garshin/Garschin	Estimated to have been responsible for

	reconnaissance, violation, and distribution of DoppelPaymer ransomware to target networks.
Igor Olegovich Turashev	Estimated to have been the admin of the infrastructure and malware used for infiltration, and to have played a key role in attacks against German companies.
Irina Zemlianikina	Responsible for sending malicious emails in the early stage of the attacks. Also took care of the DLS and chat system, and posted data stolen from the victims online.

Table 2. The names and roles of key DoppelPaymer ransomware suspects

The DoppelPaymer ransomware first emerged in June 2019, and it was infamous for its indiscriminate ransomware attacks against American, English, German government agencies, medical and educational facilities, and manufacturers until April 2021. It is estimated that their members are mostly from Russia and Eastern Europe. DoppelPaymer is a rebranded version of the known ransomware BitPaymer. DoppelPaymer has been rebranded to Grief once more. Currently, the ransomware group's activities have been suspended for a long time.

(3) Hacktivist Group's Activity

Hackers with political motives are called "hacktivists", and their hacking attempts, website modulations, and DDoS attacks against web services with the purpose of fulfilling a political, social, or religious objective are called acts of hacktivism. Hacktivists have mainly carried out DDoS attacks against government agencies or private enterprises in countries that are either critical of Russia or are offering Ukraine military or financial support. This sort of hacktivism showed a sharp increase in March due to the following hacktivist groups becoming more active.

- Anonymous Sudan

Anonymous Sudan is known to have no relation to the actual Anonymous group.[10] They claim to be hacktivists based in Sudan. Some threat intelligence companies believe that the group was created as a part of Russia's intelligence operations in order to complicate the process of Sweden joining the North Atlantic Treaty Organization (NATO).[11] Recently, they established a partnership with the pro-Russia KillNet hacktivist group.[12]

Figure 9. Anonymous Sudan's Telegram channel profile image

Below are the countries that were targeted by the group's DDoS attacks during March.

- Denmark
- France
- Sweden
- Australia

Private enterprises, educational facilities (universities), and airport websites (Australia) of the countries above suffered DDoS attacks.

- NoName057(16)

NoName057(16), also known as 05716nnm, Nnm05716, or NoName05716, is a pro-Russia hacktivist group that has been active since March 2022.[13] They mainly conduct DDoS attacks. Below are the countries that were targeted by the group's DDoS attacks during March.

- Japan
- Norway
- Czech Republic
- Lithuania
- Slovakia
- Italy
- Lithuania
- Germany
- Poland
- Estonia

- Ukraine
- North Macedonia

The group conducted DDoS attacks against private enterprises (transport and warehousing businesses, finance and insurance, communications, shipping, banks) and government branch (administration, diplomacy, defense) websites of the countries listed above.

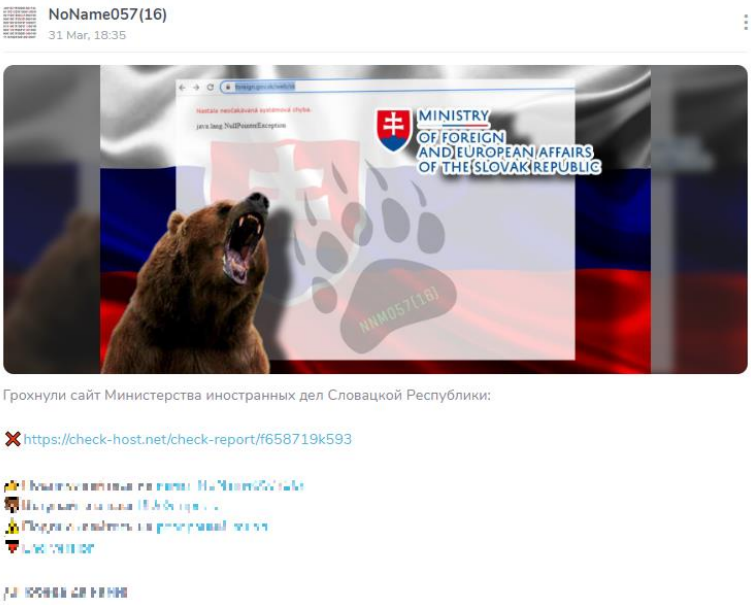

Figure 10. Image claiming to have performed a DDoS attack against the Slovakian Department of Foreign Affairs

The tactics and techniques possessed by NoName057(16) are assessed to be considerably limited due to the fact they have only carried out DDoS attacks. Additionally, they are more focused on alerting others of the process before and after the DDoS attacks through Telegram and social media.

Conclusion

Law enforcement agencies of countries worldwide worked together to actively track ransomware groups and investigate cyber crime forums. In January, the FBI and the US Department of Justice succeeded in closing the Hive ransomware group and confiscating related infrastructure. Additionally, the US government confiscated the REvil ransomware group's cryptocurrency funds and succeeded in identifying the owner of the funds. Even among the efforts of such law enforcement agencies, new ransomware groups calling

themselves DarkPower, Abyss, and Money Message emerged. They all posted multiple victims in a short period of time, so they seem to be highly active.

Additionally, the administrator of Breached Forums, known for its data leaks, was arrested and prosecuted. Following that, the web service was also terminated. It is estimated that with Breached Forums shut down, there will be major changes to threats against cyber crime forums. Active members of the forum will move to different places to avoid being tracked, and there is a high possibility that with the tracking and crackdowns, new cyber crime communities will be met with distrust. No matter what kind of community emerges to replace Breached Forums, unless it proves that is not a honeypot of a law enforcement agency and that it possesses powerful management security, success seems unlikely. It is also speculated that threat activities will increase in other social media and messaging platforms such as Telegram and Discord. Accordingly, the uncertainty and unpredictability of new cyber crime forums will likely continue.

Hacktivists like Anonymous Sudan and NoName057(16) are conducting DDoS attacks, website modification attacks, and many different types of cyber attacks. They post statements claiming responsibility for these attacks, notably on platforms such as Telegram and Twitter. It is difficult to pinpoint what the hacktivists' motivations and goals are, but it seems they are trying to raise awareness for political, social, and religious issues through their actions. The hacktivists mentioned above are especially supportive of Russia ever since the breakout of the Russo-Ukrainian War, and they sometimes cooperate with other pro-Russian hacktivists to conduct cyber attacks against Ukrainian targets.

References

[1] https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/

[2] https://www.bleepingcomputer.com/news/security/procter-and-gamble-confirms-data-theft-via-goanywhere-zero-day/

[3] https://therecord.media/tasmania-added-to-clop-ransomware-list/

[4] https://news.yahoo.com/proposed-class-action-lawsuit-filed-001300610.html/

[5] https://www.bleepingcomputer.com/news/security/medusa-ransomware-gang-picks-up-steam-as-it-targets-companies-worldwide/

[6] https://www.justice.gov/opa/pr/justice-department-announces-arrest-founder-one-world-s-largest-hacker-forums-and-disruption/

[7] https://www.bleepingcomputer.com/news/security/police-seize-netwire-rat-malware-infrastructure-arrest-admin/

[8] https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets/

[9] https://www.bleepingcomputer.com/news/security/core-doppelpaymer-ransomware-gang-members-targeted-in-europol-operation/

[10] https://socradar.io/hacktivism-on-the-rise-killnet-anonymous-sudans-cyber-campaign-targets-australia/

[11] https://cyesec.com/blog/what-you-need-to-know-about-the-anonymous-sudan-hacker-group/

[12] https://www.truesec.com/hub/blog/what-is-anonymous-sudan/

[13] https://socradar.io/dark-web-profile-noname05716

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