TLP: GREEN

April 2023 Deep Web & Dark Web Threat Trend Report

Ransomware Groups & Cyber Crime Forums and Markets of April 2023

V1.0

AhnLab Security Emergency response Center (ASEC)

May 04, 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.

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 liabilities.

The version information of this report is as follows:

Version	Date	Details
1.0	2023-05-04	First release

Contents

Note 5
Major Issues 5
1) Ransomware 5
(1) ALPHV (BlackCat) 5
(2) Akira 6
(3) CipherLocker 7
(4) LockBit 9
(5) Money Message 10
2) **Forum & Black Market** 12
(1) Closing of Genesis Market 12
(2) After the Closing of Breached Forums 14
3) **Threat Actor** 15
(1) Bassterlord's Retirement 15
(2) Hacktivist Group's Activity 17
Conclusion 19

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 April 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)

Western Digital fell victim to a data leak incident due to the ALPHV (BlackCat) ransomware attack. Consequently, a wide range of services including My Cloud were suspended. The victim is a global company that provides hard disk drive and data storage solutions. My Cloud is a personal cloud storage service provided by Western Digital.

Figure 1. Western Digital posted on the ALPHV (BlackCat) Dedicated Leak Site (DLS)

The threat actor of the ALPHV (BlackCat) ransomware pressured Western Digital by threatening the company two times with the data leaked on the DLS. Their pressure tactics resemble REvil's threat against MediBank, Australia's health insurance giant, which occurred in the fall of 2022. Using the leaked data, ALPHV is pressuring the victim and driving it to the brink by discovering the victim's internal process of response to breach incidents and uploading it to the DLS for anyone to see.

ALPHV (BlackCat)'s tactics did not stop with this company. A few days after the above incident, the threat group breached McDermott, a global supplier based in the US that provides engineering and construction solutions for the energy industry. ALPHV forewarned the release of this company's confidential documents and proof of their corruption, placing a lot of pressure on the victim.

(2) Akira

The Akira ransomware DLS first became known in early April of 2023. No information has been discovered about their identity regarding whether they are a new ransomware group or a rebranding of an existing ransomware group. One security researcher put forward their opinion that the string obfuscation code of Akira is similar to a variant of LockBit. Additionally, ransomware with the same name was reported to be in development in August 2017.[1] This ransomware became known as the Akira ransomware at the time because it changed the file extension of the encrypted file to .akira.

The word Akira has the same spelling as the title of a Japanese SF anime. When the Akira ransomware DLS first became known, there was no data on the victim list, and the victims only began being updated as of mid-April. Ten companies were added to this list until late April, and they were concentrated in the North American region. The victims were from a variety of industries, such as manufacturing, construction, real estate, service, investment companies, and educational institutes.

[1] https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-1st-2017-locky-exploit-kits-and-more/

Figure 2. Akira ransomware group's DLS

Unlike the DLS of typical ransomware groups, Akira used jQuery to create an interface resembling a terminal. jQuery is a JavaScript library mainly used in web development. It offers various features such as selecting and manipulating elements in the Document Object Model (DOM), event handling, animation effects, AJAX support, and many more. This DLS seems to have used the terminal plugin of jQuery. In order to view the list of victims, the given command must be entered on the DLS. General ransomware DLS must attract as many visitors as possible to view the list of victims and their data, and this is where the Akira DLS differs from the DLS run by other ransomware groups.

(3) CipherLocker

Recently, ads for CipherLocker, Ransomware as a Service (RaaS), was found on the cyber crime forum "nulled". The post claimed that CipherLocker exfiltrates passwords, system information, cryptocurrency wallet addresses, and more, but it was actually a RaaS recruitment ad that redirected the reader to a link on the Dark Web. The author of the post also gave a guide on how to use the TOR browser to connect to the CipherLocker DLS.

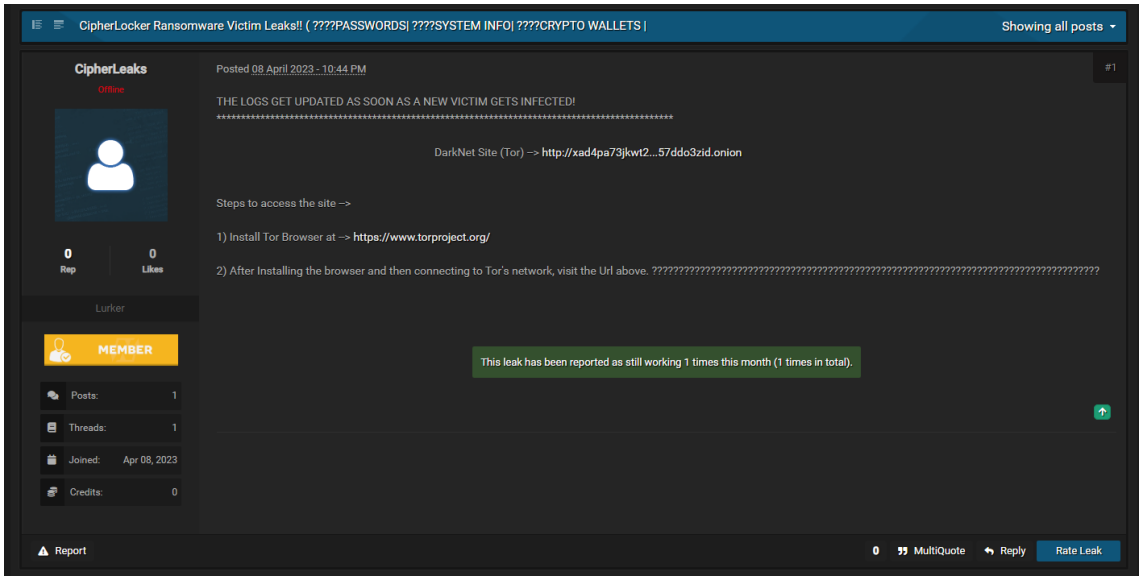


Figure 3. CipherLocker advertised on "nulled"

Accessing the DLS using the TOR browser as guided by the post revealed a recruitment ad for RaaS affiliates, as shown below.

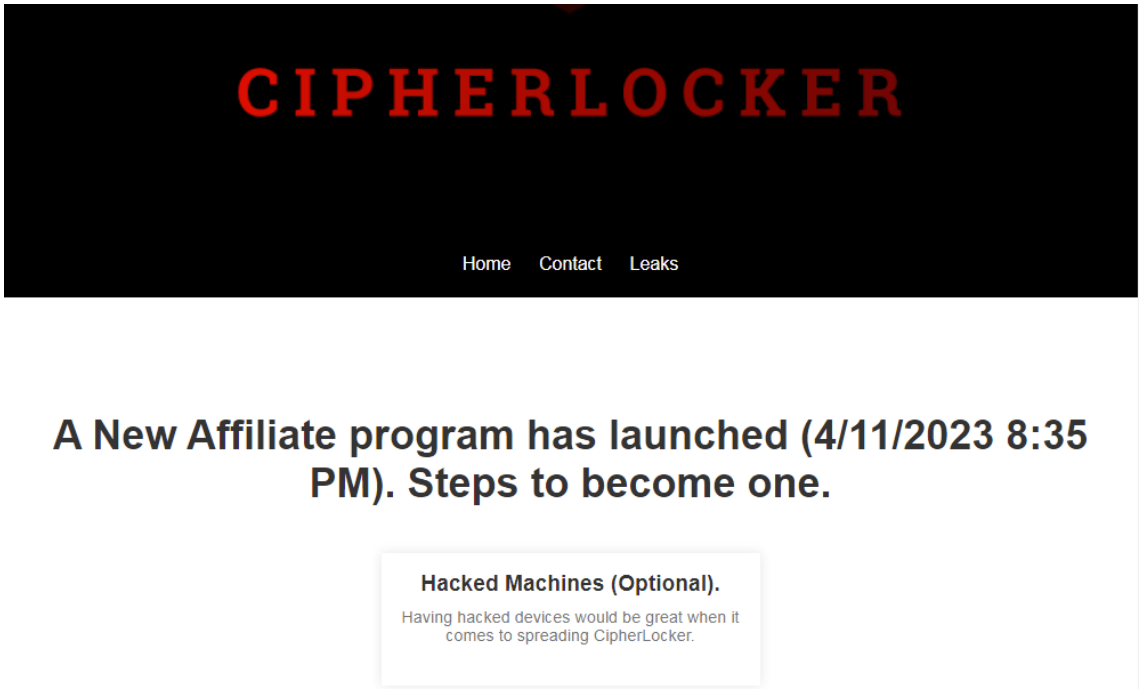


Figure 4. CipherLocker RaaS advertisement

CipherLocker's rules for RaaS affiliates included the following details.

- Must have many hacked systems for the spread of ransomware
- A set sum must be paid in Bitcoin to become an affiliate
- Must possess social engineering knowledge/technology

• 25% of any ransom received must be paid to the ransomware operator • Ransomware infection through deceiving users not familiar with the system is forbidden

Table 1. Rules for CipherLocker RaaS affiliates

Some cyber crime forums such as XSS forbid publicly advertising RaaS organizations. This is because when problems involving ransomware arise in the future, the forums can become a target of investigation by law enforcement authorities. In addition, the DLS founded on the Dark Web is inaccessible as of late April, present. This is presumed to be because the hosting server information (IP, OS, web server software name) of the DLS has been disclosed in cyber security communities.

(4) LockBit

LockBit breached the Korean National Tax Service on April 1 and threatened to disclose their data, but the data has not been disclosed as of yet. Around the same time period, the group showed signs of neglectful management, such as uploading multiple non-existent victims to the DLS.

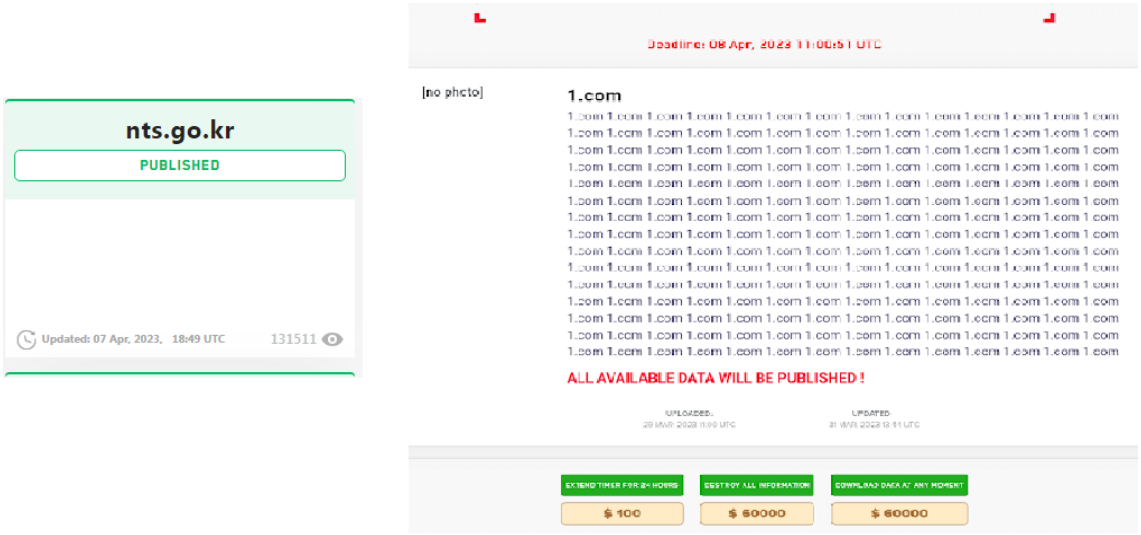


Figure 5. nts.go.kr (left) / nonexistent victim organization 1.com (right)

There was a tweet update from a security company pointing out the issue of LockBit's poor management. However, the threat actor uploaded a company with a similar name as the tweeter's company as a victim, leaving a message that seemed to mock both companies.

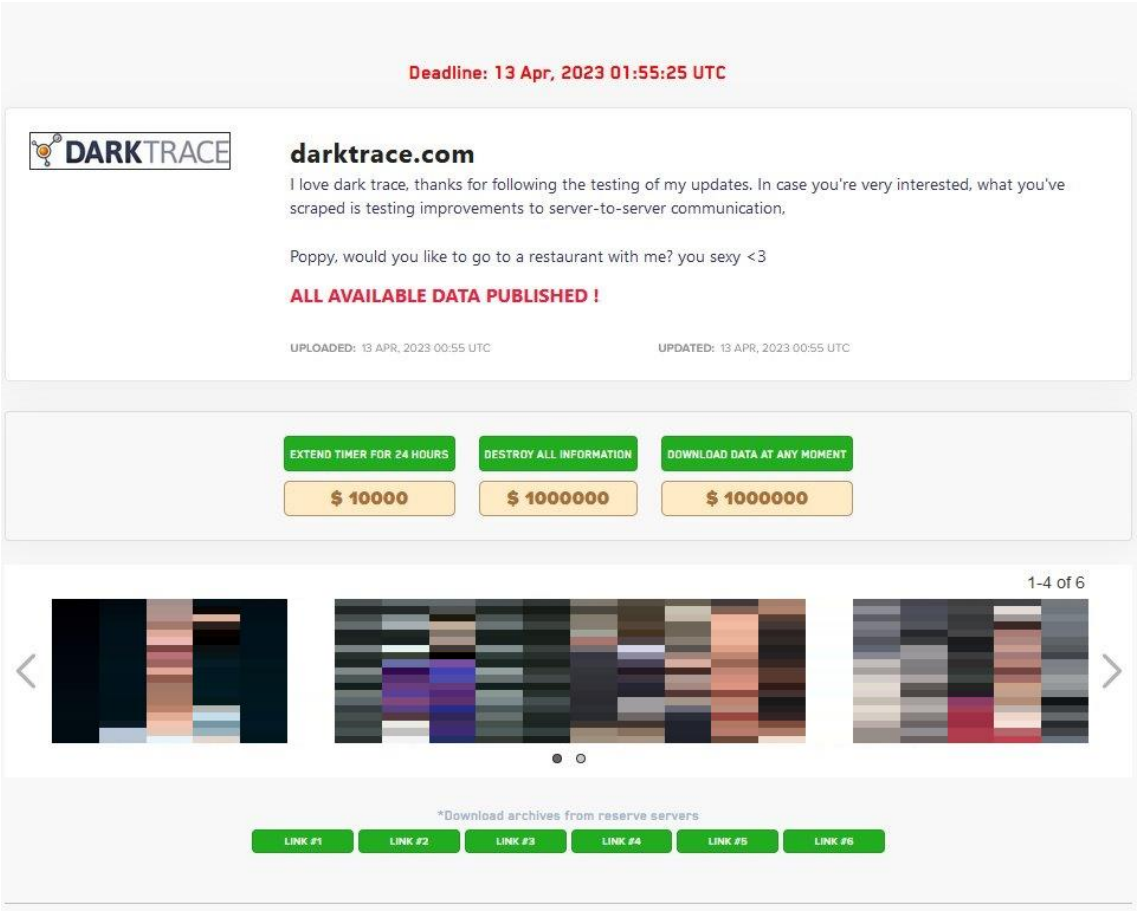


Figure 6. Security company uploaded as a fake victim

Some security researchers gave somewhat vague opinions, saying that this is not poor management of the DLS by LockBit, but rather a process of testing an update on communications security between servers. LockBit also breached a childcare service company and uploaded a post apologizing for this act and that they would provide a decryption tool. Multiple security researchers put forward critical opinions on this event, saying that such responses do not mean that they take LockBit's responsibility for ransomware breaches lightly.

(5) Money Message

Money Message is a ransomware group first reported in March 2023, and the group conducts ransomware attacks on targets worldwide.[2] However, most of their victims are identified to be based in the US, from a variety of industrial sectors, including banks, financial services, insurance, transportation and logistics, and manufacturing. This group encrypts both

[2] https://www.bleepingcomputer.com/news/security/new-money-message-ransomware-demands-million-dollar-ransoms/

Windows and Linux systems. They also employ the double extortion technique, which involves exfiltrating the victims' data before encrypting it, and uploading this data on their ransomware DLS if the ransom is not paid. Like the BianLian ransomware group, Money Message was also found concealing the identity of the victim when they are first revealed. While it is normal for the names of targeted organizations to be uploaded on a ransomware DLS, this group marked the target as "Guess Who!" instead of immediately exposing their names. This is understood to be for the purpose of evading threat intelligence companies' monitoring which study and track threats on the Deep Web and Dark Web, or to pressure the victim slowly.

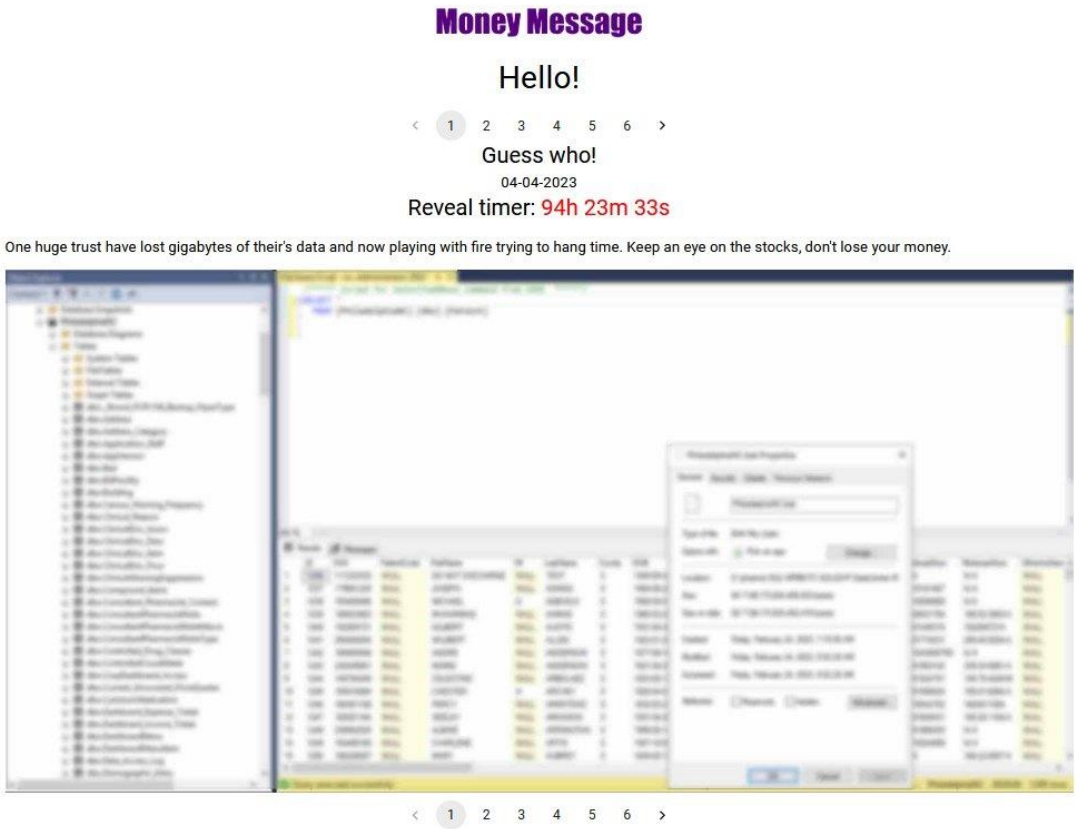


Figure 7. Money Message ransomware's victim whose identity could not be identified at first

The victim, whose identity was initially unknown, was found to be a Fortune 1,000 pharmacy services company based in the US. The Money Message ransomware group also posted multiple victims afterward. One of these victims included Micro-Star International (MSI), a Taiwanese motherboard and graphics card manufacturing company well-known in Korea as well as around the world. After breaching MSI, the threat group uploaded the company as a victim on the DLS.

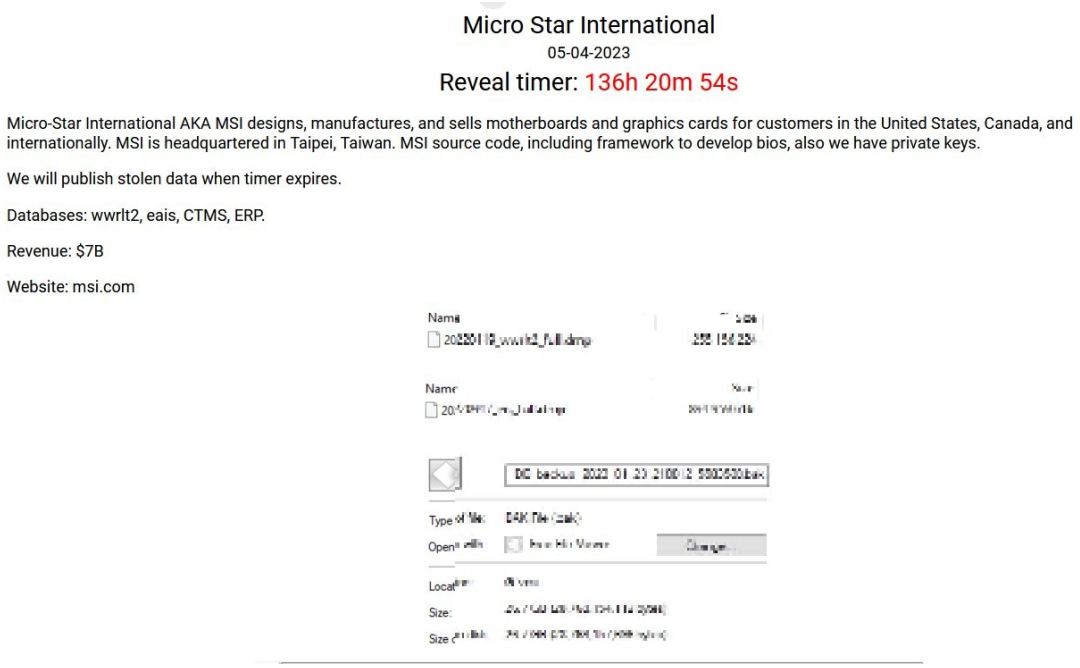


Figure 8. Micro-Star International uploaded as a victim

The threat actor demanded ransom, stating that they possess the BIOS development framework, source codes, and personal keys they have stolen from the victim. The Money Message group, which was comparatively lesser known in the past, became better known to security companies and the general public through this incident. Recent updates warn that MSI had not paid its ransom, and the data leaked from this company will be disclosed in the future.

2) Forum & Black Market

(1) Closing of Genesis Market

Genesis Market is a cyber crime market established in late 2017. It was famous for its user-friendly interface, including a clear product list and automated payment. This type of market became known as "autoshop" and Genesis Market was the largest and most popular cyber crime marketplace on the Internet. Through international cooperation, the Federal Bureau of Investigation (FBI) investigated Genesis Market and shut it down.[3] The operation code was

[3] https://therecord.media/genesis-market-takedown-cybercrime

"Cookie Monster". The investigation was led by the FBI, and they announced that they had received support from over 12 countries. Currently, Genesis Market cannot be accessed, and visiting the site displays an image seized by the FBI instead.

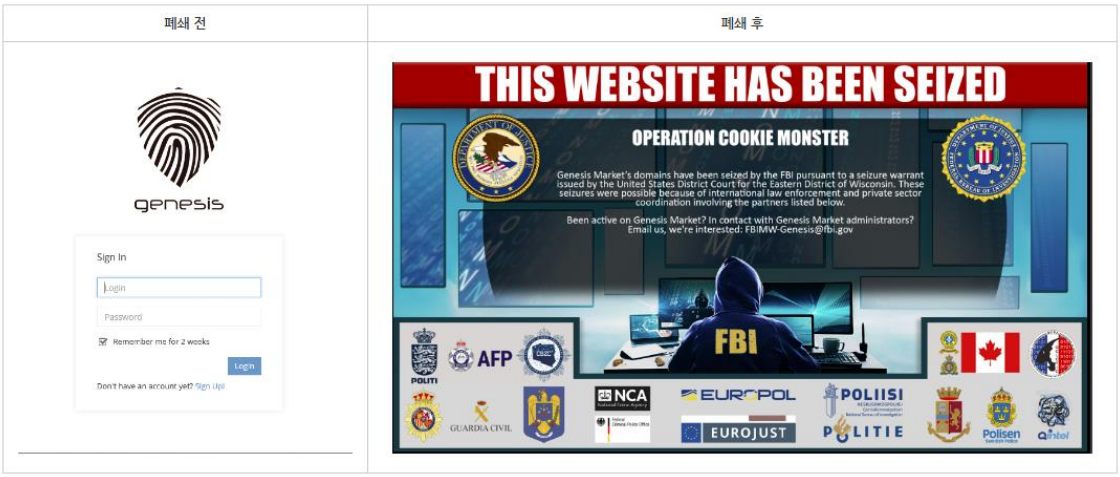


Figure 9. Before the shutdown of Genesis Market website (Left) / After the shutdown (Right)

Genesis Market is presumed to have been created by hackers based in Russia, and it only allows people with invitation codes to join. Browser cookie information collected by Infostealers such as RedLine and Raccoon is the mainly sold item. The cookies contain the session information of the currently logged-in web service. Activated session information can be used to bypass account authentication and multi-factor authentication mechanisms. Thus, this information can be used to disguise the user identity and use web services as the owner of the account. Genesis Market also provided an exclusive Chromium-based browser and plugins to exploit this.[4]

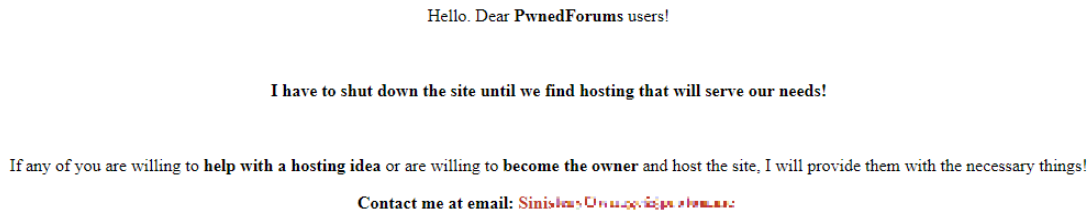
A recently conducted study calls such systematic collection of user profile information (user credentials, cookies, device and behavioral fingerprints, and other metadata) and batch-selling them as an "Impersonation-as-a-Service (ImpaaS)".[5] Genesis Market sold a variety of stolen user profile information, a large portion of which were non-financial service accounts from Amazon, Cloudflare, Ebay, Facebook, Gmail, LinkedIn, Netflix, PayPal, Reddit, Spotify, Twitter, WordPress, and Zoom.

[4] https://www.trellix.com/en-us/about/newsroom/stories/research/genesis-market-no-longer-feeds-the-evil-cookie-monster.html

[5] https://arxiv.org/abs/2009.04344

(2) After the Closing of Breached Forums

Breached Forums was the most active cyber crime forum for a year until the apprehension of its chief administrator by the FBI in March 2023. According to unconfirmed press data from an unknown source, the 19-year-old hacker who ran this forum, Connor Fitzpatrick, a.k.a. Pompompurin, attempted to take his life. On a side note, this forum is famous for being the replacement for RaidForums which was shut down in 2022 and had its chief administrator apprehended. Following the shutdown of Breached Forums, many similar forums of varying scales appeared, including "dataforums", "pwnedforums", and "d4rkforums". These forums all disappeared due to a variety of reasons including management security failure.


Hello. Dear **PwnedForums** users!

I have to shut down the site until we find hosting that will serve our needs!

If any of you are willing to **help with a hosting idea** or are willing to **become the owner** and host the site, I will provide them with the necessary things!

Contact me at email:

Figure 10. PwnedForums' service termination message

After the closing of Breached Forums, it is said that more users are joining a cyber crime forum run by the threat group ARES.[6] This group first appeared on Telegram in late 2021, and has been linked to the RansomHouse ransomware, data leakage platform KelvinSecurity, and network access group Adrastea.[7]

[6] https://www.bleepingcomputer.com/news/security/breached-shutdown-sparks-migration-to-ares-data-leak-forums/

[7] https://www.cyfirma.com/outofband/ares-leaks-emerging-cyber-crime-cartel/

Figure 11. ARES Leaks' data sales page

ARES manages ARES Leaks, its own website, and provides access to data stolen from companies from a variety of countries, including the US, France, Spain, Australia, and Italy. This website hosts various types of stolen data from phone numbers, email addresses, client information, business-to-business (B2B) transactions, Social Security numbers (SSN), and company databases, to foreign currency data, government information, and passports. The group uses cryptocurrency as their method of payment. They not only host leaked information but also provide a variety of malicious services such as vulnerability exploitation, pen-tests, malware development, and Distributed Denial of Service (DDoS) attacks. ARES also runs personal and VIP channels, and it is likely that these clients would be sold data leaked from high-value targets.

3) Threat Actor

(1) Bassterlord's Retirement

Bassterlord, a 27-year-old hacker from Ukraine, had been active on various cyber crime forums. He was known to have run a team named National Hazard Agency, known to have been affiliated with at least four ransomware gangs, including REvil, RansomEXX, Avadon, and

LockBit. [8] He was famous for being an initial access broker (IAB), selling access permissions to other cyber criminals.

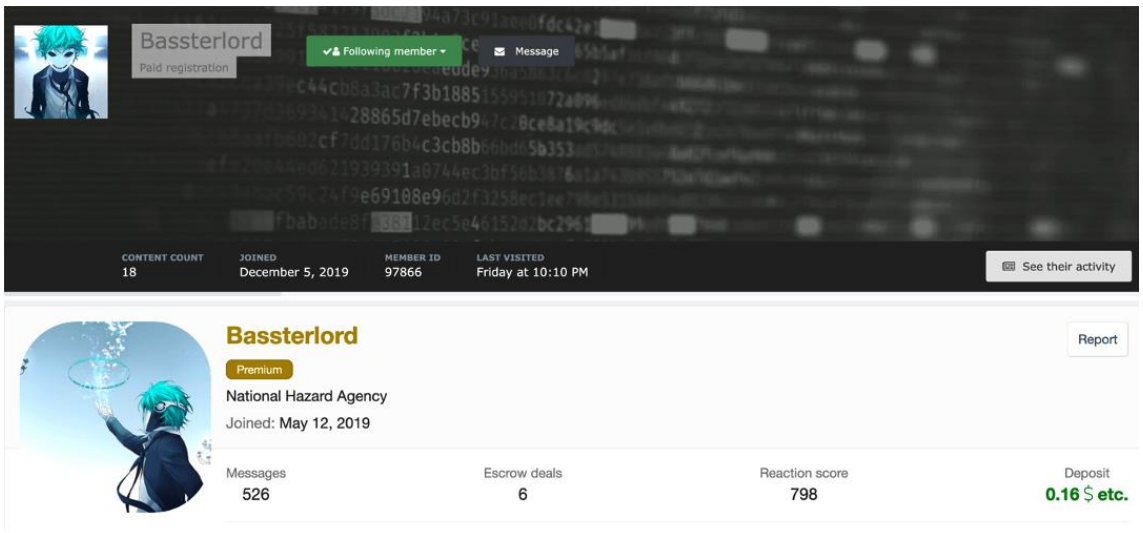


Figure 12. Bassterlord's profile information uploaded on a cyber crime forum
<Source> https://analyst1.com/ransomware-diaries-volume-2/

He was active in Russian cyber crime forums and was known to have learned ransomware attack techniques from a hacker named Lalartu (a.k.a. Sheriff). He volunteered to become a mentor for other hackers, and the ransomware manual he wrote was also popular among cyber criminals. This hacker suddenly announced his retirement in March. Bassterlord revealed through an interview with a security company that he had made sufficient money through collecting ransom, and he feels no remorse. [9] He explained that he officially announced his retirement from the forum after erasing his traces to avoid interrogation and interest from Russian law enforcement. However, in the interview, he revealed that he was continuing initial breach-related services with eight others, except he is no longer a direct participant and instead receives 20% of the profits. Bassterlord is behind ransomware infiltration incidents that have caused large-scale damage. When an investigation order for REvil ransomware affiliates was given in the conference between the presidents of the US and Russia in 2020, Bassterlord was summoned to the Federal Security Service of Russia (FSB) and interrogated.

[8] https://analyst1.com/ransomware-diaries-volume-2/

[9] https://therecord.media/bassterlord-interview-hacker-initial-access-broker

(2) Hacktivist Group's Activity

- Anonymous Sudan

Anonymous Sudan's attacks are large in scale, persistent, and include a variety of targets. Following their attack on an Australian target last month, this group has been attacking government organizations, schools, universities, hospitals, and communication and utility services in other countries including Israel, India, and Denmark. Anonymous Sudan often promotes hacktivism and has been selecting targets that hurt the threat group's religious sentiments. This group also competes against other hacker groups and set new attack targets due to the emergence of a new hacktivist group (GoneTeam). Through these attacks, the websites of many corporations and government organizations suffered damage of varying degrees. This group continues to search for other attack targets; recently, they attacked the US, including the website of an international airport and the website of a multinational shipping and logistics service company.

Figure 13. Affiliation between KillNet and UserSec

Meanwhile, KillNet announced its affiliation with another pro-Russian hacktivist group, UserSec. Regarding this, some security researchers claimed that Anonymous Sudan is the same group as one of these parties.

- NoName057(16)

Pro-Russian hacktivist NoName057(16) is running the DDosia project to improve the efficiency of DDoS attacks.[10] This is an attempt to make a new parallel botnet to facilitate DDoS attacks. This group publicly announced their DDosia project, through which their previously concealed Bobik botnet distribution also became exposed. NoName057(16) is known for maintaining their member pool by rewarding its members who had launched the most successful DDoS attacks with cryptocurrency. This project is run on a private Telegram channel, and the channel is estimated to have about 1,000 participants.

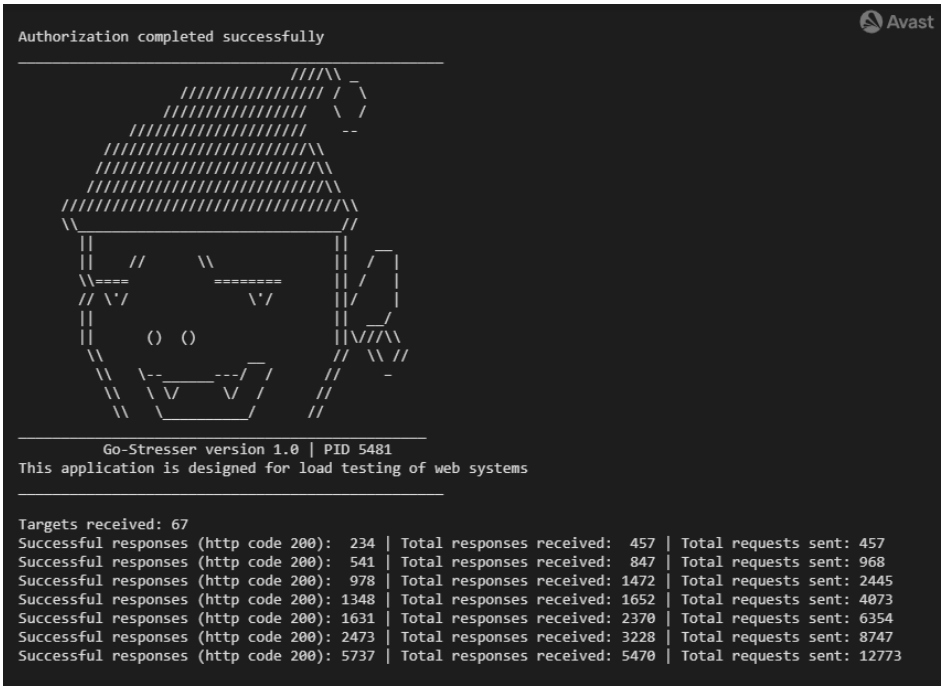


Figure 14. Stresser used in DDosia, developed in the Go language
<Source> - https://decoded.avast.io/

Security company Avast mentioned in a post analyzing the DDosia project that they wished to bring awareness to people who have installed NoName057(16)'s DDoS tools on their PC that they are not only contributing to cyber crime, but they are also partaking in the activities of a group that supports war activities.[11]

[10] https://decoded.avast.io/martinchlumecky/ddosia-project-how-noname05716-is-trying-to-improve-the-efficiency-of-ddos-attacks/

[11] https://decoded.avast.io/martinchlumecky/ddosia-project-how-noname05716-is-trying-to-improve-the-efficiency-of-ddos-attacks/

Conclusion

The cyber crime market Genesis Market had its website closed as a result of the efforts of the FBI and law enforcement from multiple countries, and many of their active members were apprehended. Along with the shutdown of Breached, a cyber crime forum, and the apprehension and persecution of its operator, this was a grave warning to cyber criminals. Genesis Market in particular was a mainstream cyber crime market and an autoshop providing 'ImpaaS'. Accounts sold through Genesis Market are mainly from non-financial services, but using cookies stolen by Infostealers, users who purchase the information can impersonate the identities of the actual account owners. The popularity of such ImpaaS autoshops is continuing, and there exist multiple other autoshops besides Genesis Market.

The DLS of a ransomware group discovered this month includes the aforementioned Akira, as well as CrossLock and Trigona. Trigona first became known in October 2022, and usually targeted poorly managed MS-SQL servers for ransomware infection. The Trigona DLS where companies affected by the ransomware are listed was discovered six months after their ransomware became known, and six victims were listed on the DLS. The CrossLock DLS had two victims. These trends show that ransomware still continues to be a severe security issue.

IAB Bassterlord who had announced his retirement from his forum revealed through an interview with a security company that he had not ceased his activities completely. He announced that he would be in a managerial position, not directly partaking in the work but instead collecting 20% of the profits. This statement contradicts his announcement to retire, depicting a typical criminal who finds it hard to walk away from the huge financial gains from illegal activities. [12]

NoName057(16) is still launching DDoS attacks through its DDosia project and has recently expanded its targets from European countries that support Ukraine to Canada as well. This group publicly announced over their Telegram channel that they are taking action to support Russia. It is certain that their activities will continue amidst the Russo-Ukrainian War. Everyone must be aware that participating in this project is not only contributing to cyber crime but also

[12] https://analyst1.com/ransomware-diaries-volume-2/

supporting the war.

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.

AhnLab