TLP: GREEN

Threat Trend Report on Ransomware

August 2023 Ransomware Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Sep. 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.

This report is a work of authorship protected by the Copyright Act.
Unauthorized copying or reproduction for profit is strictly prohibited under any circumstances.

Seek permission from AhnLab in advance
if you wish to use a part or all of the report.

If you reprint or reproduce the material without the permission of the organization mentioned above, you may be held accountable for criminal or civil liability.

Contents

Objectives and Scope 5
Major Statistics 5
1) Data Sources and Collection Methods 5
2) Overall Ransomware Statistics 6
3) New Samples by Ransomware 8
4) Targeted Systems by Ransomware 9
5) Targeted Businesses by Ransomware Group 10
6) Targeted Businesses by Ransomware Group (External Statistics) 12
Key Trends 13
1) CLOP ransomware expanded pressure tactics on targeted businesses 14
2) Rhysida ransomware connection with Vice Society 20
3) Monti ransomware introduced new Linux encryption technique 25
4) Others 32
Conclusion 32
Indicators Of Compromise (IOC) 33
1) File Paths and Names 33
2) File Hashes 33
3) Relevant Domains, URLs, and IP Addresses 34
References 35

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.

Objectives and Scope

This report provides statistics on the number of new ransomware samples, targeted systems, and targeted businesses in August 2023, as well as notable ransomware issues in Korea and other countries. Other major issues and statistics for ransomware that are not mentioned in the report can be found by searching for the following keywords or via the Statistics menu at AhnLab Threat Intelligence Platform (hereinafter "ATIP").

- Ransomware
- Statistics by Type

Disclaimer: The number of ransomware samples and targeted systems are based on the detection names designated by AhnLab, and the statistics on targeted businesses are based on the time the information on the ransomware group's dedicated leak sites (DLS, identical to ransomware PR sites or PR pages) was collected by the ATIP infrastructure.

Major Statistics

1) Data Sources and Collection Methods

ATIP uses its internal infrastructure to monitor and analyze the following ransomware information.

- List of malicious files and behaviors detected and collected by AhnLab Smart Defense (ASD)
- List of targeted businesses posted on ransomware groups' DLS

The number of new ransomware samples and statistics on targeted systems were calculated based on the detection names designated by AhnLab. They were also limited to cases where the detected files and behaviors were diagnosed under the category of "Ransomware/" or "Ransom/".

- **Ransomware/**Win.Magniber: Example file detection name

- Ransom/MDP.Magniber: Example behavior detection name

The detection names acquired at the time of detection may not allow for the identification of ransomware type (e.g. Generic, Agent, Edit, Decoy, and others), and some cases may be excluded from the ransomware statistics or be counted as a different ransomware type due to changed detection names after detection or a failed detection.

The statistics on targeted businesses are the values that have been organized based on the data accumulated through regular monitoring of ransomware groups' DLS, where the groups reveal the targeted businesses. If the DLS page was inaccessible or the data was collected belatedly, then the data may have been excluded from the statistics or have been considered to be collected at a time different from the exact date the victim was revealed.

Therefore, this report should be used as a reference to check the general trends of ransomware samples and targeted systems and to see which ransomware groups are actively engaged in attacks through the statistics on targeted businesses to gain a general understanding of trends.

2) Overall Ransomware Statistics

The total number of new ransomware samples collected during the past six months is as follows.

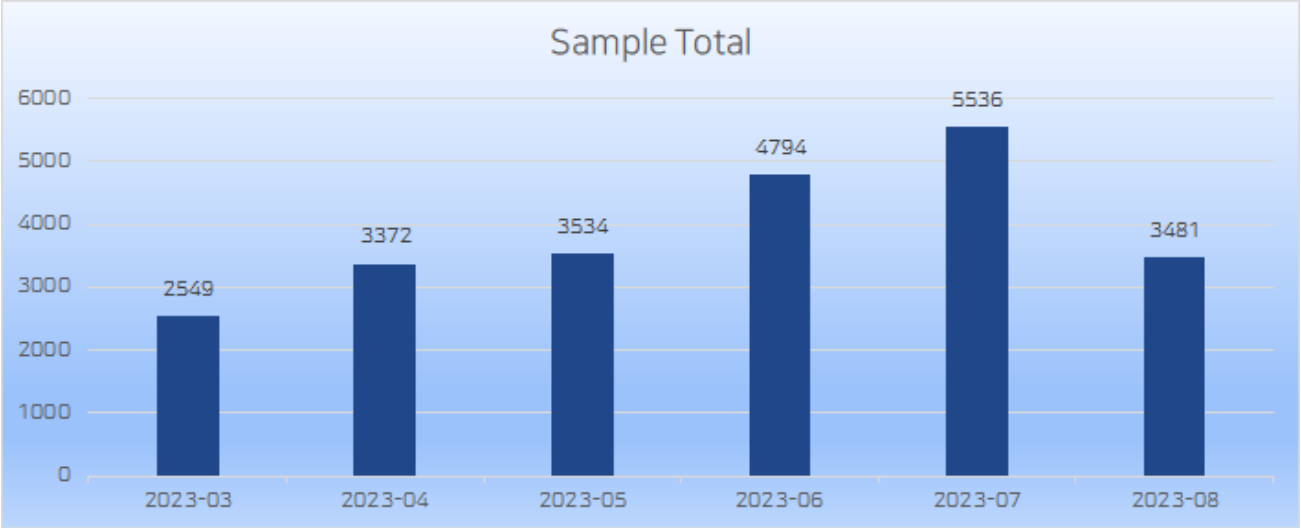


Figure 1. Number of new ransomware samples

Magniber drove a steep increase in February 2023, but the number decreased in March. It was on the rise again since then but faced another drastic decrease in August. In August, the total number of new samples decreased by about 37% compared to the previous month, reaching 3,481, and this reduction can be attributed to the fact that the number of Magniber samples decreased by more than 90% from around 2,000 in the previous month to 169.

The table below shows the total numbers after removing redundant data of ransomware files used in targeted systems and infection. (The term "targeted systems" is used for your convenience, yet it should be understood as systems where ransomware files and behaviors were detected or systems that were exposed to infections.)

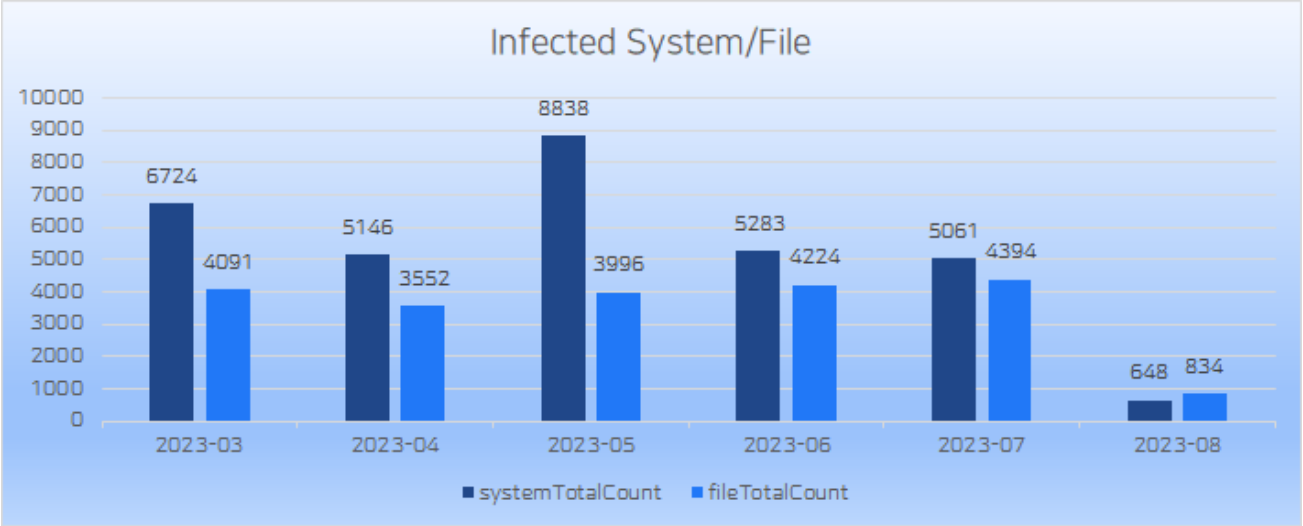


Figure 2. Systems and files affected by ransomware

The statistics for affected systems have decreased by 87% compared to the previous month, resulting in the lowest number of affected systems since statistics started being compiled, with a total of 648 cases. This decrease is attributed to a significant reduction in the distribution of Magniber samples, which previously accounted for the majority of affected systems.

The total number of ransomware behavior detection (MDP)-based targeted systems and blocked report cases are as follows.

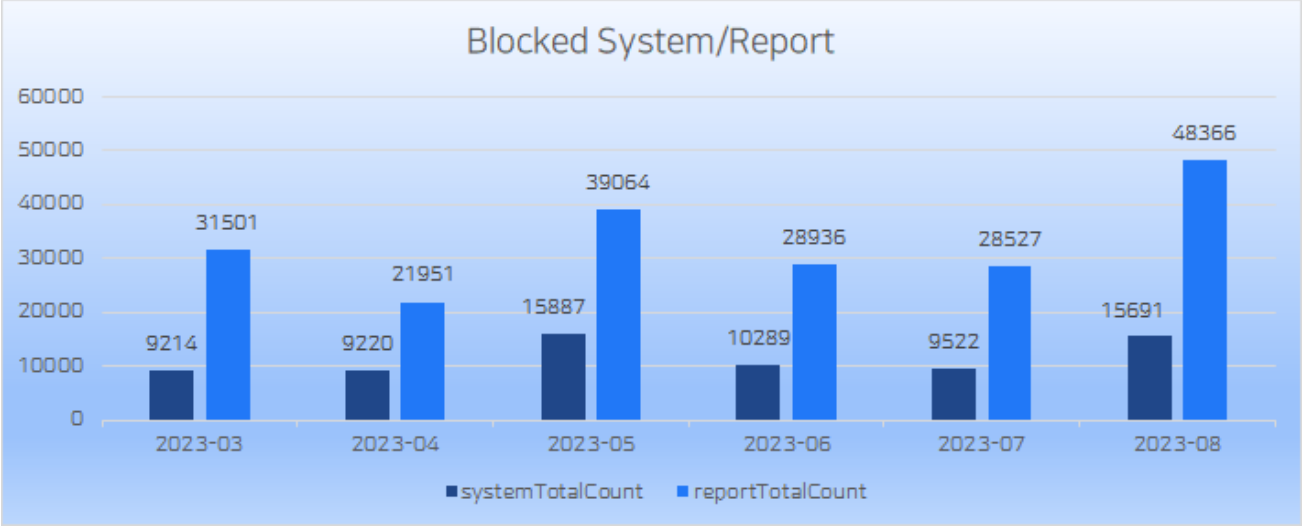


Figure 3. Ransomware behavior detection-based targeted systems and reports

In contrast to the aforementioned file detection-based statistics, the statistics for behavior detection systems have increased by more than 65% compared to the previous month. This increase has been attributed to the rise in the number of block reports for Direct Syscall, document modification, and task scheduler registration behaviors, which Magniber abused to bypass detection.

3) New Samples by Ransomware

Below is the statistics showing the 3,481 new samples that were discovered in August organized by ransomware type. Only 20 ransomware with the most samples are shown.

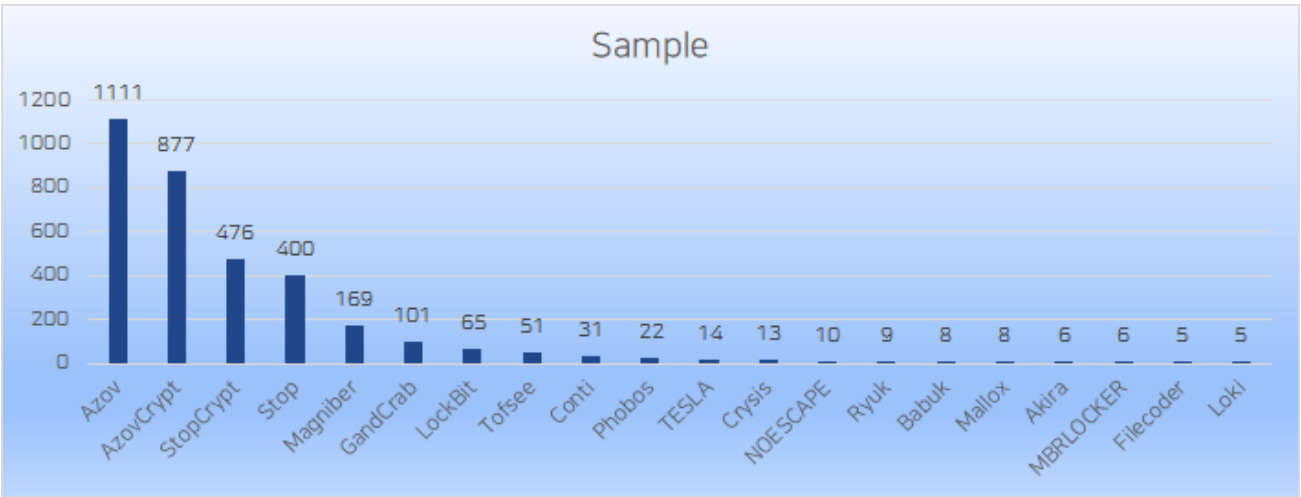


Figure 4. Number of new samples per ransomware (August 2023)

As mentioned in the total ransomware statistics, the number of Magniber samples decreased by over 90% from over 2,000 in the previous month to a total of 169. The number of remaining

ransomware samples, such as Azov, AzovCrypt, StopCrypt, and Stop, remains similar to the previous month, with no significant fluctuations.

4) Targeted Systems by Ransomware

The top 20 cases with the highest number of files used in targeted systems and infection are as follows (duplicates have been excluded).

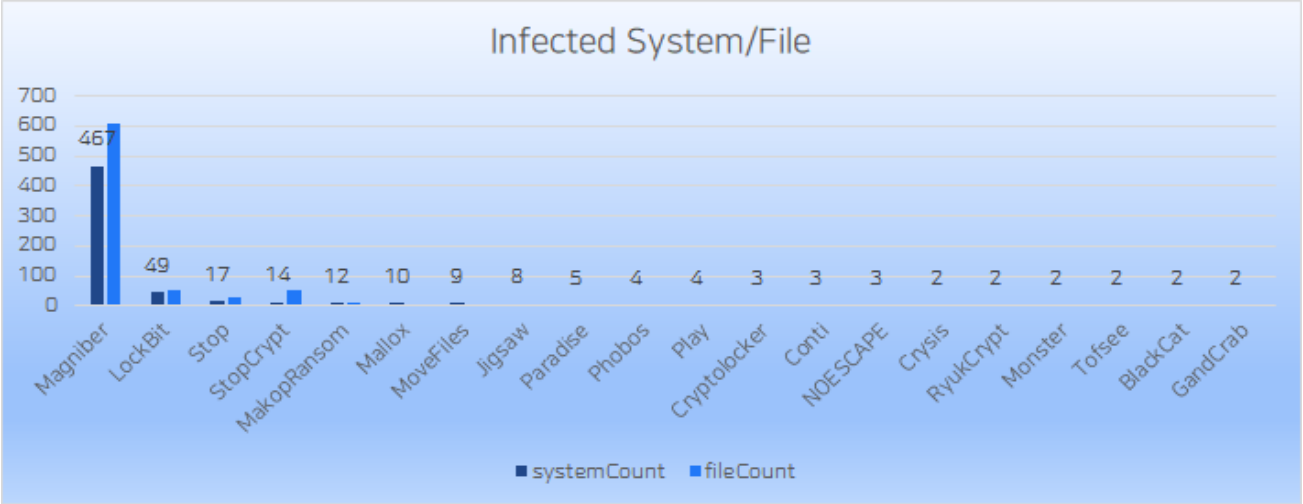


Figure 5. Number of targeted systems and files by ransomware (August 2023)

The number of systems targeted by Magniber decreased drastically from 4,800 to 467 since the previous month. The number of affected systems by other ransomware remained at a similar level to that of the previous month.

The following statistics show the daily number of affected systems from the top 12 ransomware out of total affected systems.

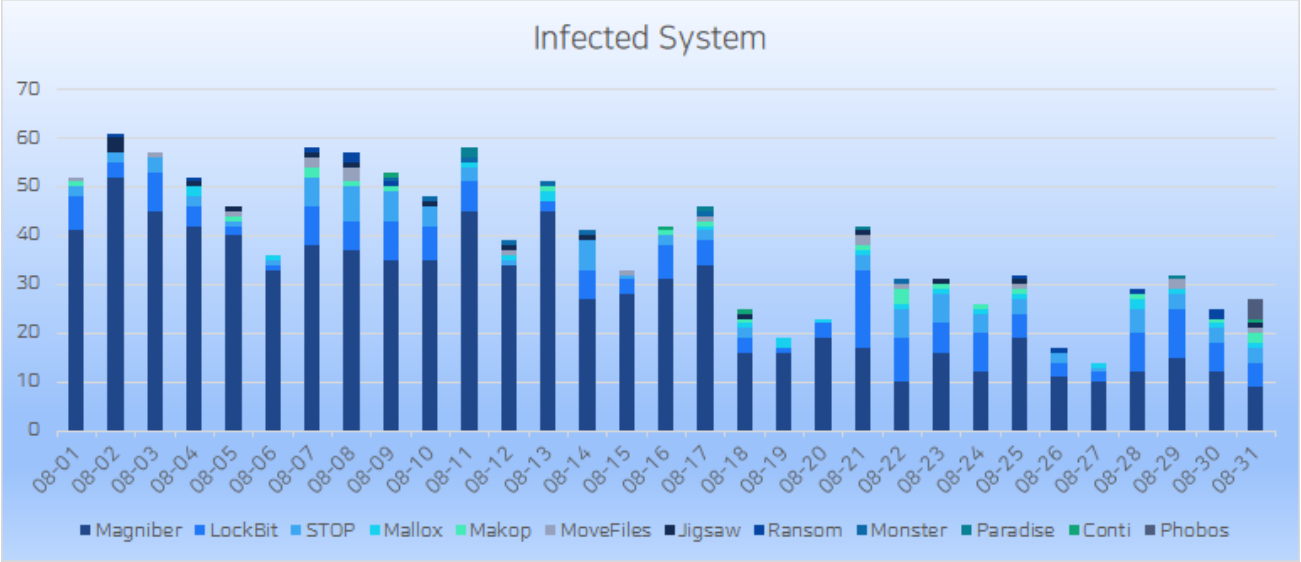


Figure 6. Daily numbers of targeted systems by ransomware (August 2023)

The decrease in Magniber was also reflected in the daily statistics. The graph now clearly displays the other ransomware samples that were difficult to identify since most of the previously affected systems were attributed to Magniber infections. The daily average of systems affected by Magniber decreased significantly to about 27 cases per day. Typical fluctuations such as the slight decrease in attacks during weekends and subsequent pick up during weekdays remained the same. The reduction in the number of affected systems since the end of July, previously attributed to the impact of summer vacation, has been identified as having been caused by the sharp decrease in the distribution of Magniber samples in August. There were also LockBit and Makop ransomware's emails involving attachments disguised as "resumes", "job applications", and "guidelines on unauthorized use of licenses", as well as continuous infection attempts by STOP ransomware disguised under the filenames "build.exe" and "setup.exe".

5) Targeted Businesses by Ransomware Group

Below are the statistics on targeted businesses posted on the ransomware groups' dedicated leak sites (DLS) collected by ATIP. As data on some ransomware groups were collected late or could not be collected, the report refers to the table "Targeted Businesses by Ransomware Group (External Statistics)" that follows as well.

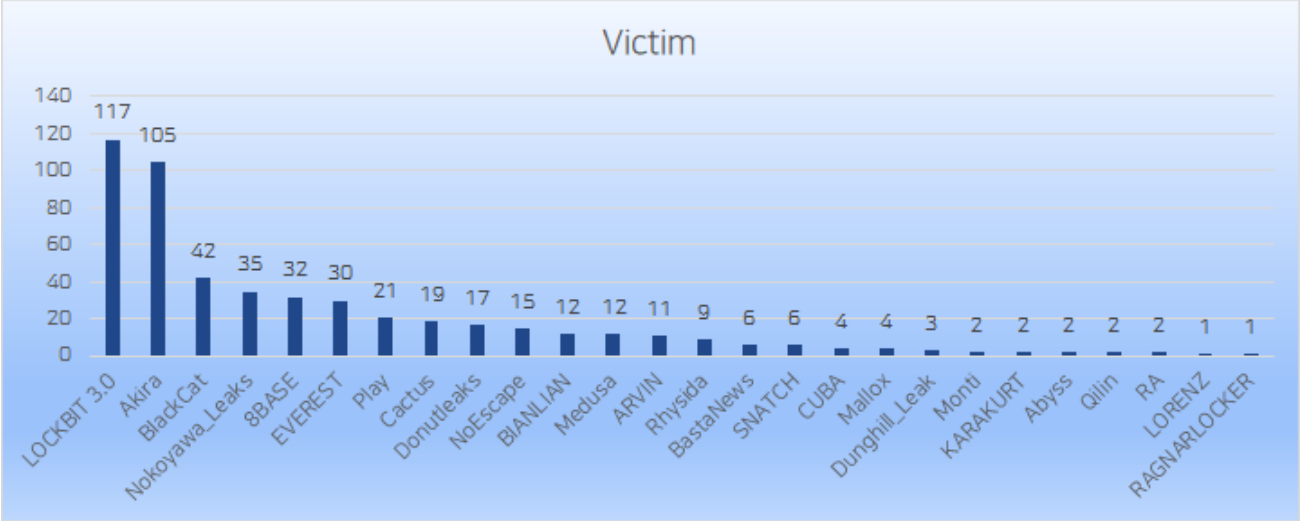


Figure 7-1. Number of targeted businesses per ransomware group (August 2023)

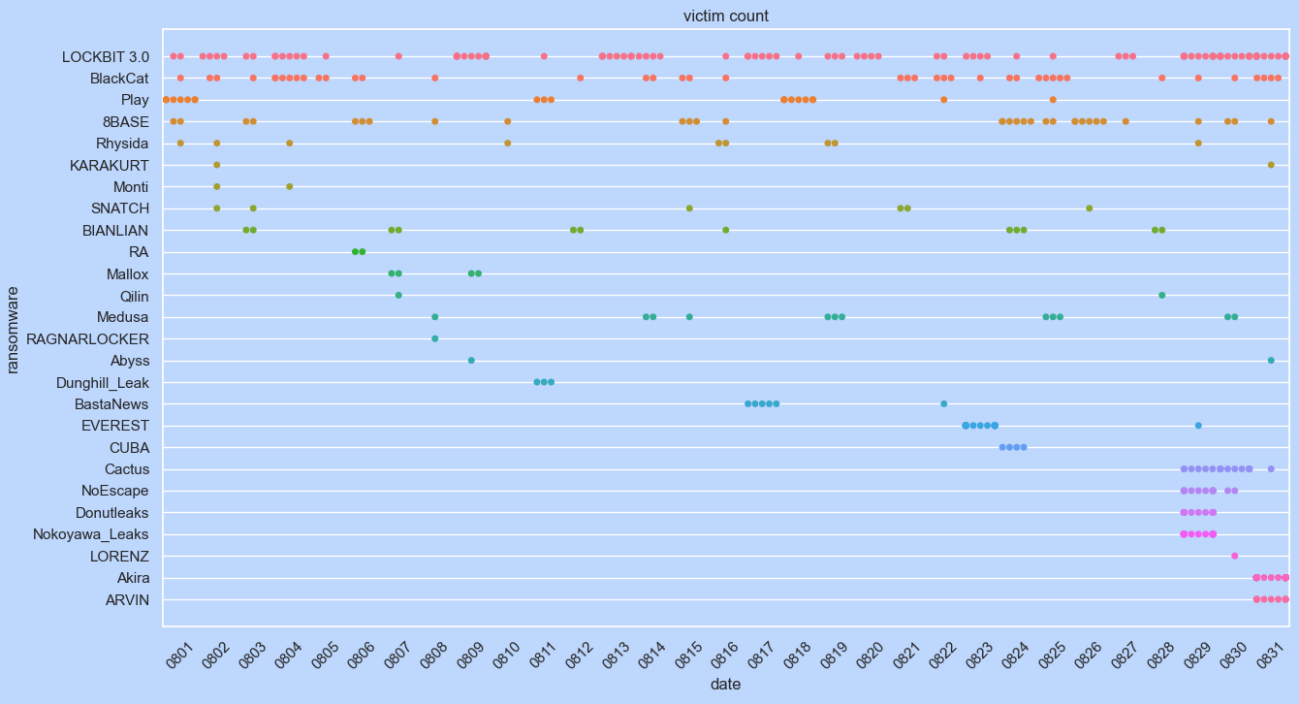


Figure 7-2. Number of targeted businesses per ransomware group - daily (August 2023)

The number of companies affected by LOCKBIT 3.0 increased by more than two-fold compared to the previous month, making it top the ATIP statistics. They have consistently exposed a significant number of affected companies on their dedicated leak sites (DLS). Since the report in late May on CLOP exploiting the MOVEit zero-day vulnerability to breach data from hundreds of companies, the number of victims disclosed by CLOP had increased. However, only 4 affected companies were disclosed in August. For more information regarding businesses attacked by CLOP and details related to the expansion of pressure tactics, please refer to the "Key Trends" section below.

Additionally, out of the ransomware groups displayed on the bottom of the daily targeted businesses graph, the figures for Cactus, NoEscape, Donutleaks, Nokoyawa_Leaks, and Akira are the cumulative data collected from targeted companies disclosed prior to August. As a result, these groups may rank higher in the ATIP statistics than their actual ranks. Newly monitored ransomware groups that are added to the list will have their accurate number of targeted companies reflected in the statistics from the following month.

Some of the targeted businesses revealed per ransomware group are as follows.

Ransomware	Victim	Count
LOCKBIT 3.0	persingerlaw.com / gerb.bg / unicorpusa.com / ohiohistory.org / bestmotel.de / constructioncr	117
Akira	Schottenstein Property Group / Green Diamond Resource / Knights of Old Group / WTI - Weste	105
BlackCat	KIMCO Staffing Service / Helen F. Dalton Lawyers / Tempur Sealy International / riggsabney / Of	42
Nokoyawa_Leaks	Studio Domaine LLC / Roman Catholic Diocese of Albany / Pea River Electric Cooperative / One I	35
8BASE	Jacklett Construction LLC / MBS Equipment TTI / Rossman Realty Group, inc. / RevZero, Inc / Sa	32
EVEREST	Agriloja.pt demo-leak / Agriloja.pt / ZESA Holdings / Kovair Software Data Leak / Great Opportur	30
Play	Aquatlantis / ACTIVA Group / Professionnel France / Coral Resort / DAL-TECH Engineering / Bir	21
Cactus	Americold / Wasserstrom / Phoenix Taxis / Rotomail Italia SpA / Reyes Automotive Group / Arte	19
Donutleaks	Jackson Township Police Department and Administration. / Peroni Pompe / Jacklyn Dawson Soli	17
NoEscape	www.qigroup.com / www.iinaba.com / www.contact121.com.au / www.verdeil.ch / gipcl.com / w	15
BIANLIAN	Spokane Spinal Sports Care Clinic / H********** ********* *** / T******** / G***** ******* / **;	12
Medusa	Emerson School District / Borets (Levare.com) / CB Energy Australlia / Postel SpA / Sartrouville	12
ARVIN	hamyari Shahrdari golestan / AFTA Isfahan / Parsian Bitumen / seaside-kish co / Haraz dairy / 15	11
Rhysida	University of the West of Scotland / University of Salerno / ESKA Erich Schweizer / United Tract	9
BastaNews	TWINTOWER / SYNQUESTLABS / VDVEN / DEUTSCHELEASING / ALLIANCE / GROUPHC	6
SNATCH	Fittingbox / Premium Transportation Group / Einatec / Department of Defence South African / I	6
CUBA	goldmedalbakery / txmplant.co.uk / hydrex.co.uk / gis4.addison-il	4
Mallox	Kogetsu / Franklins european bathrooms / Contec Systems / West Cargo	4
Dunghill_Leak	Sysco Corporation / Gentex Corporation / ANDRADE GUTIERREZ & ZAGOPE	3
Monti	Bickel & Brewer - Press Release / Abatti Companies - Press Release	2
KARAKURT	COSI / Valley Mountain Regional Center	2
Abyss	www.finitia.net / www.lasaterandmartin.com	2
Qilin	Thonburi Energy Storage Systems (TESM) / GYP New Tree SA	2
RA	Z****ta / P****X	2
LORENZ	Felling Trailers, Inc. / De*****.com / B***.com	1
RAGNARLOCKER	Batesville didn't react on appeal and allows Full Leak	1

Table 1. Some of the targeted businesses per ransomware group (August 2023)

6) Targeted Businesses by Ransomware Group (External Statistics)

The following statistics on targeted businesses during the same period were provided by DarkFeed Twitter – a platform run by an external threat intelligence (TI) business or security expert. Note that this report used the statistical information from DarkFeed or Dailydarkweb Twitter available at the time of writing.

Figure 8. Targeted businesses per ransomware group <Source> DarkFeed Twitter

As mentioned above, excluding the ransomware groups with cumulative statistics in ATIP for August, the number of businesses targeted by LOCKBIT 3.0, BlackCat (ALPHV), 8BASE, PLAY, and other ransomware groups that disclose many targeted businesses, is generally high. Additionally, the Cloak ransomware group appeared in August and disclosed 24 targeted businesses.

Key Trends

Multiple issues regarding various ransomware occurred in August 2023. This report presents brief introductions to the following key topics and details for reference.

- CLOP ransomware expanded pressure tactics on targeted businesses;
- Rhysida ransomware connection with Vice Society; and
- Monti ransomware introduced new Linux encryption technique.

Readers are recommended to check and refer to issues that are not covered in this report through ATIP if the current security management system or situation requires so.

1) CLOP ransomware expanded pressure tactics on targeted businesses

The 2023 June and July ATIP Threat Trend Reports on Ransomware[1,2] have covered the issue of "CLOP ransomware's activities involving the exploitation of the MOVEit zero-day vulnerability and the group's disclosure of their victims." This report follows suit by looking at the companies that have been additionally disclosed in August.

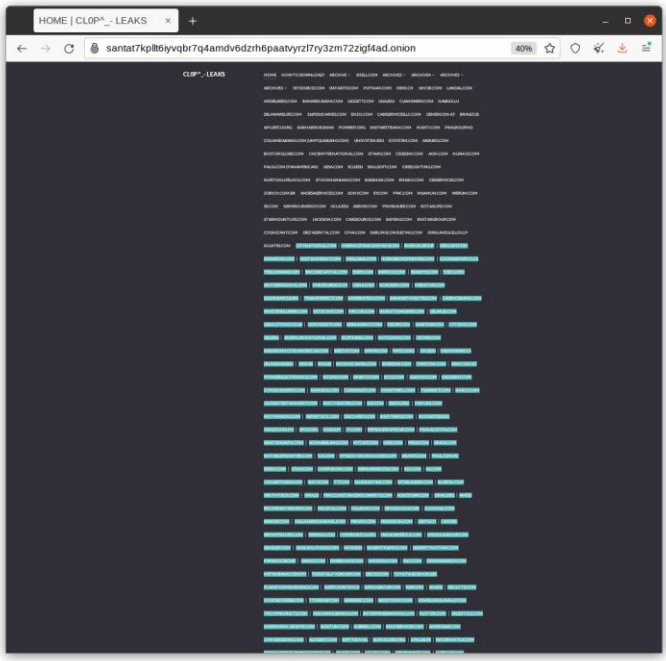


Figure 9. Posts on CLOP ransomware's DLS - Disclosure of victims (July 31)

The image above shows the victims that were listed on CLOP's DLS as of July 31, with approximately 180 new victims having been added in July. This is two to three times the number of affected companies disclosed in June and was introduced as the group's "name-and-shame" strategy. This strategy involves earning substantial profits by applying pressure on a minority of companies via the consistent disclosure of many other companies.

[1] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=dcfc0d31-88ae-439e-ae3c-0a2746771ab7
[2] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=ba4ce03f-68dc-466e-bf69-19efcbda2e21

In contrast to this strategy of disclosing affected companies and increasing profits, the CLOP ransomware DLS observed on August 31 displayed only four newly listed companies for the entire month of August.

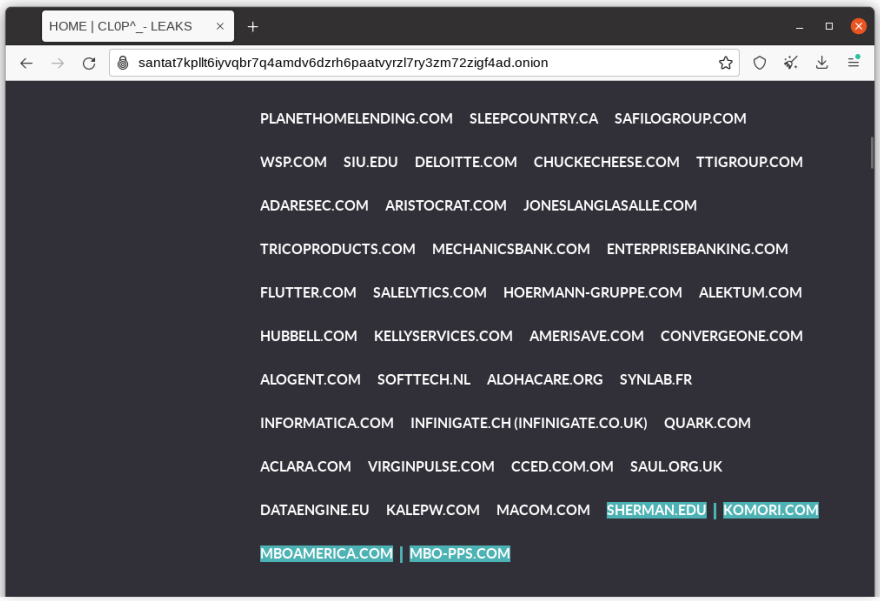


Figure 10. Posts on CLOP ransomware's DLS - Disclosure of victims (August 31)

In their proactive strategy of publicly disclosing affected companies through their DLS, the CLOP ransomware group has recently introduced a new disclosure strategy of leaking data via the clear web and torrents to exert stronger pressure on affected companies.

In late July, CLOP announced through their DLS that they had disclosed the PwC company's leaked data, which was initially disclosed in June, on the clear web site https://pwcclinetsanddocuments.com.

Figure 11. CLOP announcing that they had posted the PwC company's leaked data to the clear web

BleepingComputer reported the change in CLOP ransomware group's data disclosure strategy

through an article titled "Clop now leaks data stolen in MOVEit attacks on clearweb sites".[3] The article highlighted that the CLOP ransomware group has altered their data disclosure approach by creating Internet-accessible websites dedicated to specific victims. This change makes the leaked data more easily accessible and puts pressure on victims to pay the ransom.

It was noted that the CLOP ransomware group had created websites for disclosing leaked data from Aon, EY (Ernst & Young), Kirkland, and TD Ameritrade. CLOP's clear web sites are less sophisticated than those created by ALPHV last year as they only list the download links for the leaked data.

Figure 12. CLOP disclosing PwC's leaked data on the clear web <Source> BleepingComputer

Clear web sites like the one above have their drawbacks, including the potential for being blocked by law enforcement agencies or vulnerability to DDoS attacks from rival groups. To address these issues, CLOP has adopted a new solution by using torrents to distribute the data stolen through their MOVEit attacks.

[3] https://www.bleepingcomputer.com/news/security/clop-now-leaks-data-stolen-in-moveit-attacks-on-clearweb-sites/

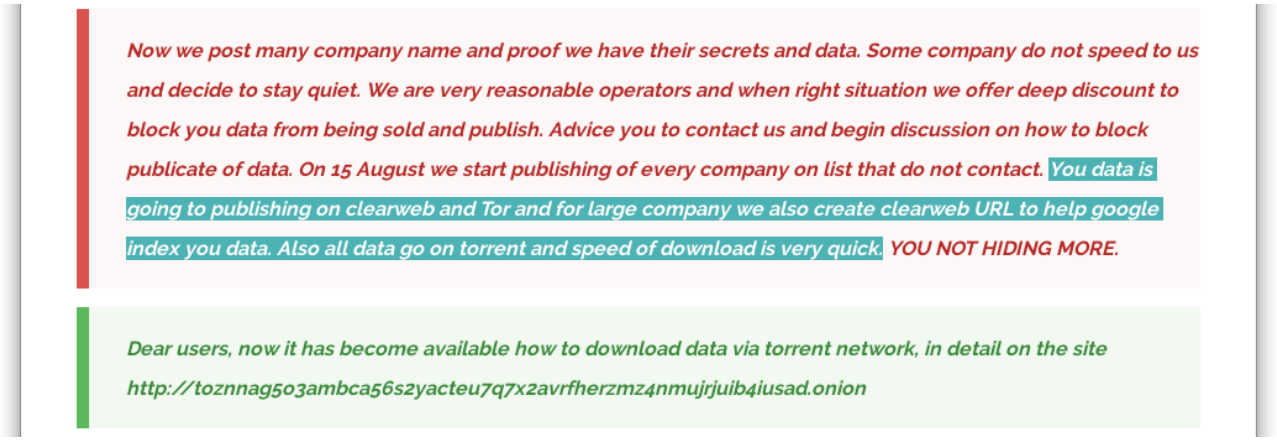


Figure 13. CLOP ransomware announcing that they will disclose data through the clear web and torrents

The reason for the CLOP ransomware group's choice of torrents as a means of data disclosure appears to be due to the following advantages of torrents:

- Torrents utilize peer-to-peer (P2P) transfers among different users, resulting in faster transfer speeds
- Their decentralized distribution method makes it challenging for law enforcement agencies to block them

Afterward, the CLOP ransomware group publicly announced that the affected companies listed on their DLS had until August 15 to contact them. For those companies that did not respond by the specified time, the group announced that they would upload the leaked data on the clear web, Tor, and as torrents. For further information regarding the disclosure of leaked data by the CLOP ransomware group using torrents, please refer to the following article.

- www.bleepingcomputer.com: Clop ransomware now uses torrents to leak data and evade takedowns

As of August 31, a total of 184 affected companies had been registered on the CLOP ransomware's torrent site.

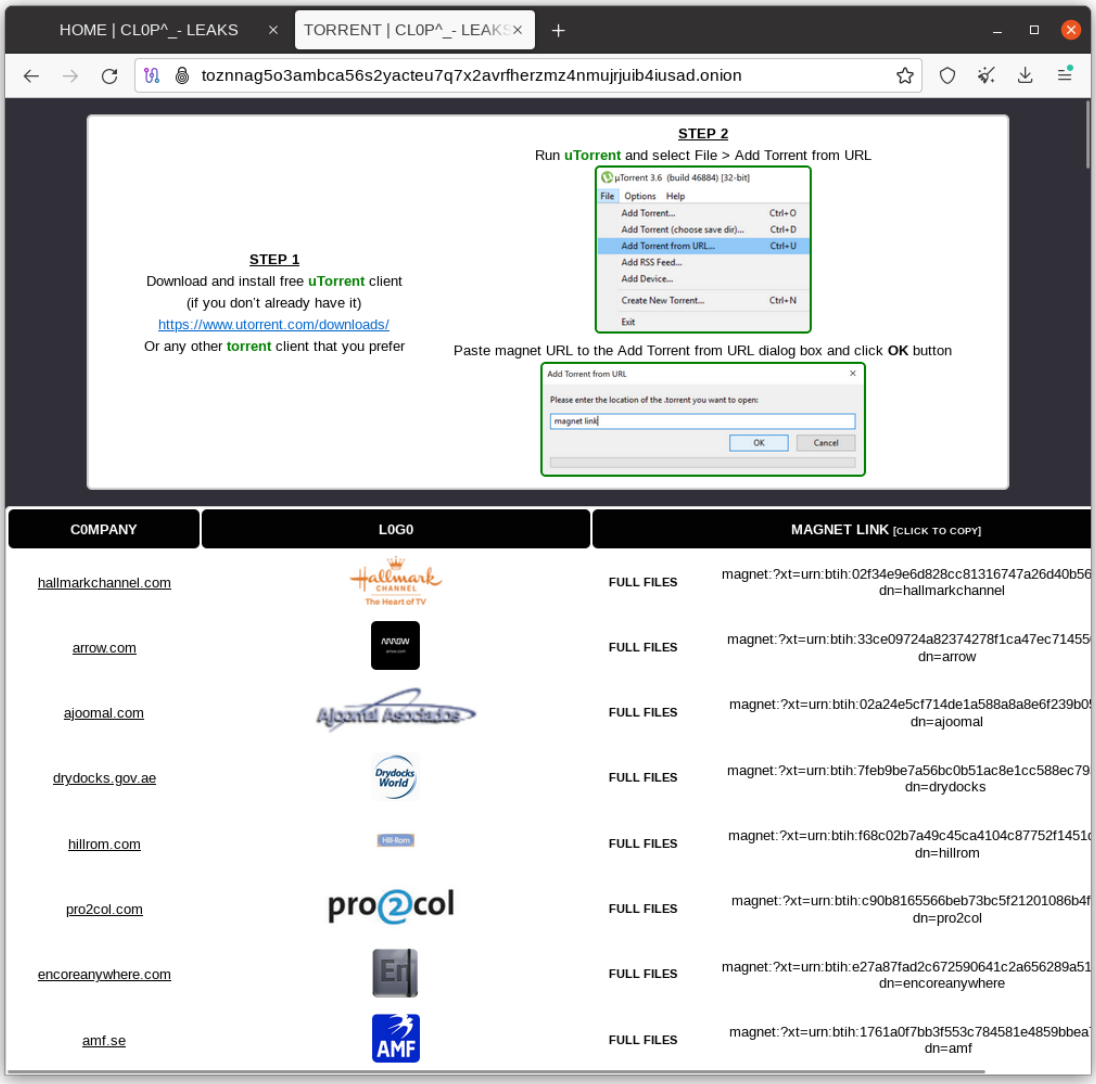
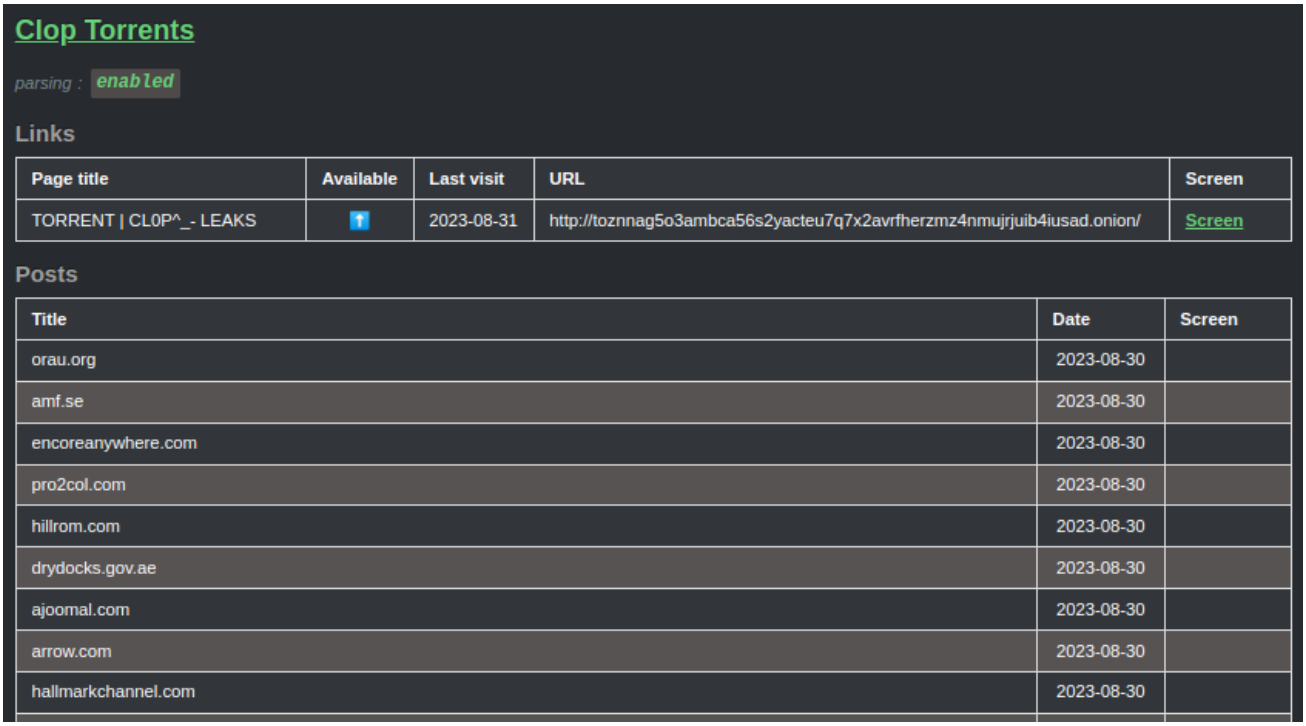


Figure 14. Post on CLOP ransomware's torrents - Disclosure of victims (August 31)

Additionally, websites like https://www.ransomlook.io occasionally add the CLOP torrents as a separate list in their ransomware group statistics. Given that the companies listed on "Clop Torrents" are those that have already had their leaked data exposed due to unsuccessful negotiations after being listed on CLOP's DLS, it is highly improbable that they would be excluded from the statistics of companies affected by the CLOP ransomware.



Clop Torrents

parsing : enabled

Links

Page title	Available	Last visit	URL	Screen
TORRENT | CL0P^_- LEAKS		2023-08-31	http://toznnag5o3ambca56s2yacteu7q7x2avrfherzmz4nmujrjuib4iusad.onion/	Screen

Posts

Title	Date	Screen
orau.org	2023-08-30	
amf.se	2023-08-30	
encoreanywhere.com	2023-08-30	
pro2col.com	2023-08-30	
hillrom.com	2023-08-30	
drydocks.gov.ae	2023-08-30	
ajoomal.com	2023-08-30	
arrow.com	2023-08-30	
hallmarkchannel.com	2023-08-30	

Figure 15. List of companies affected by CLOP ransomware torrents <Source> www.ransomlook.io

As such, the CLOP ransomware group is exerting pressure on affected companies through the diversification of its leaked data disclosure strategy, likely making profits exceeding hundreds of millions of dollars. Since August, there has been a decrease in the frequency of new disclosures of affected companies, and the method for disclosing exfiltrated data has shifted towards using torrents. With the disclosure of torrents concluding the month of August, the issue of "CLOP ransomware's activities involving the exploitation of the MOVEit zero-day vulnerability and the group's disclosure of their victims" that has persisted for about three months, must be observed to see if it will come to an end. Or if it will continue with new changes. Continued monitoring is required.

To prevent ransomware attacks, it is essential for organizations and users who use software that can be directly used in malware infection such as file transfer tools to apply the latest security updates and remove unnecessary software. Users should also follow the general guidelines of practicing periodic backups, as well as installing, using, and updating security software.

2) Rhysida ransomware connection with Vice Society

The Rhysida ransomware group, first identified in May 2023, gained prominence by attacking the Chilean Army at the end of May and publicly disclosing the exfiltrated documents on their DLS. They have been actively operating since then, and as of the end of August, they have listed approximately 40 affected companies on their DLS.

On August 4, the Health Sector Cybersecurity Coordination Center (HC3) of the US Department of Health and Human Services released a security advisory titled "Rhysida Ransomware Sector Alert"[4] about the Rhysida ransomware. Afterward, several cybersecurity firms and media outlets published numerous reports related to the Rhysida ransomware, highlighting an increase in attacks primarily targeting healthcare and public health organizations, as well as analysis of the group's connection with Vice Society and their attack techniques.

Please refer to the following for the recent activities of the Rhysida ransomware group and related reports.

- atip.ahnlab.com: Refer to the Threat Actors – Rhysida page
- www.boannews.com: Rhysida ransomware exfiltrates documents containing confidential information from the Chilean army
- www.bleepingcomputer.com: Rhysida ransomware leaks documents stolen from Chilean Army
- www.trendmicro.com: An Overview of the New Rhysida Ransomware Targeting the Healthcare Sector
- blog.talosintelligence.com: What Cisco Talos knows about the Rhysida ransomware
- research.checkpoint.com: RHYSIDA RANSOMWARE: ACTIVITY ANALYSIS AND TIES TO VICE SOCIETY
- socradar.io: Threat Profile: Rhysida Ransomware

Among these, we will focus on the reports published by Check Point Research (CPR) and SOCRADAR, which delve into the and attack techniques analysis and the connection between the Rhysida ransomware and Vice Society.

Recently, security researchers have claimed an association between the Rhysida ransomware group and Vice Society. When looking at similarities, both groups primarily target the education sector, with 38.4% of Vice Society's attacks targeting this sector and Rhysida at 30%. More recently, it was discovered that both groups have shifted their focus not only to the education sector but also to healthcare and medical sectors. Additionally, Vice Society only disclosed two affected companies after the emergence of Rhysida, and since the end of June,

[4] https://www.hhs.gov/sites/default/files/rhysida-ransomware-sector-alert-tlpclear.pdf

all postings on their DLS have ceased. These observations support the analysis of a clear correlation between the two ransomware groups.

When examining the volume of affected companies collected and the timing of disclosures for Vice Society and Rhysida ransomware over the past year, as gathered from the ATIP DDW infrastructure, the connection between these two ransomware groups becomes evident, as explained above.

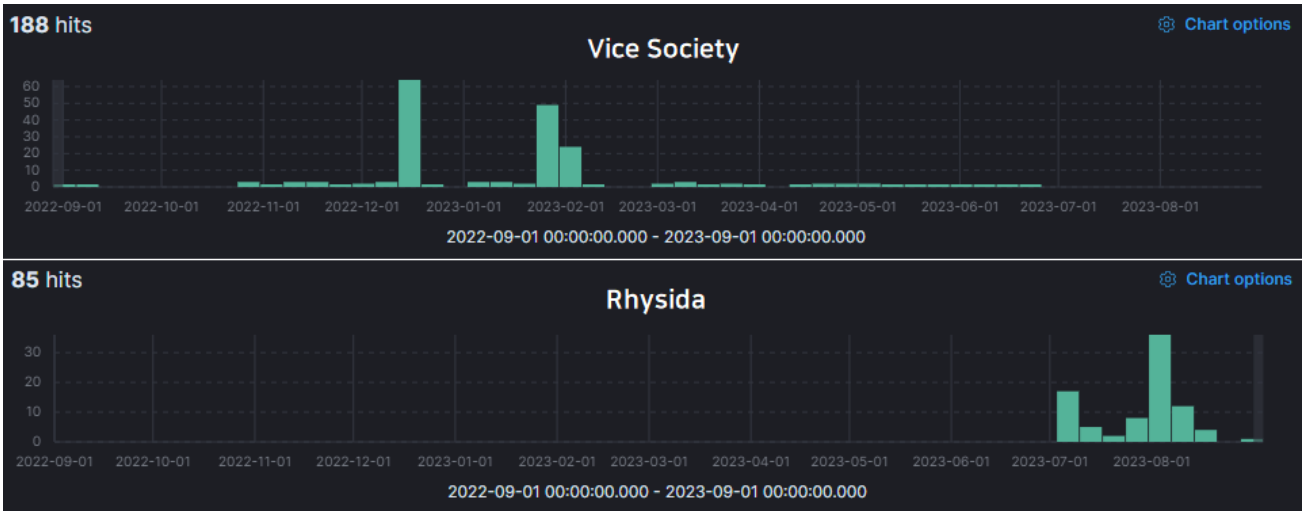


Figure 16. Distribution of victim companies collected by Vice Society and Rhysida over the past year

Besides the analysis of the volume and timing of target entities or affected companies, the association between the two groups is further enhanced by the following technical similarities.

- Lateral Movement: Uses Remote Desktop Protocol (RDP), remote PowerShell sessions, and PsExec
- Credential Access: Both groups gain access to the domain administrator accounts
- Command and Control: Uses backdoors and implants to maintain persistence
- Defense Evasion: Uses defense evasion techniques that delete logs and forensic artifacts

As such, there is a technical similarity in the tactics, techniques, and procedures (TTP) between Rhysida and Vice Society, and a connection has been confirmed between Rhysida's emergence and the decrease in Vice Society's activities.

Among the publicly disclosed Rhysida ransomware IOC, we will now briefly examine the behaviors and characteristics of the sample that corresponds to the SHA1 below, which is a

PE32+ (64-bit) file.

- 7abc07e7f56fc27130f84d1c7935a0961bd58cb9

The Rhysida ransomware used for testing was selected as a standalone executable, requiring no additional command line arguments or environmental configurations. In some variants, they exhibited abnormal termination or failed to manifest encryption symptoms. Upon performing the file encryption process in the test environment, it appended the ".rhysida" extension to file names, and a ransom note in the form of a PDF file named "CriticalBreachDetected.pdf" was generated in the infected directory.

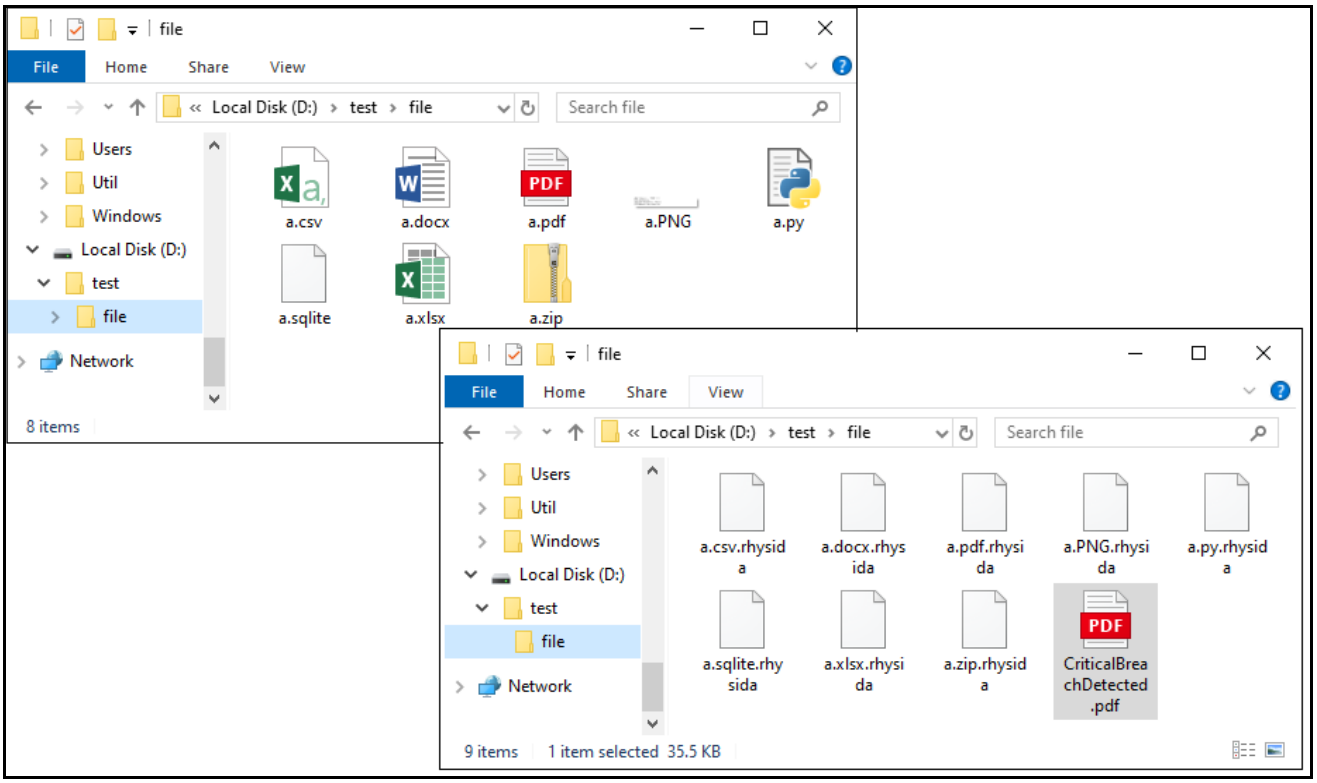


Figure 17. Files encrypted with the Rhysida ransomware

Unlike typical ransomware notes, Rhysida's ransom note disguises itself as an automatic alert from the "Cyber Security Team Rhysida" rather than simply conveying a message about ransom payment and informing the victim that their system was compromised. In order to receive payment for the decryption of files, the "unique key (private key)" issued to targets is utilized to guide them into visiting a security portal site.

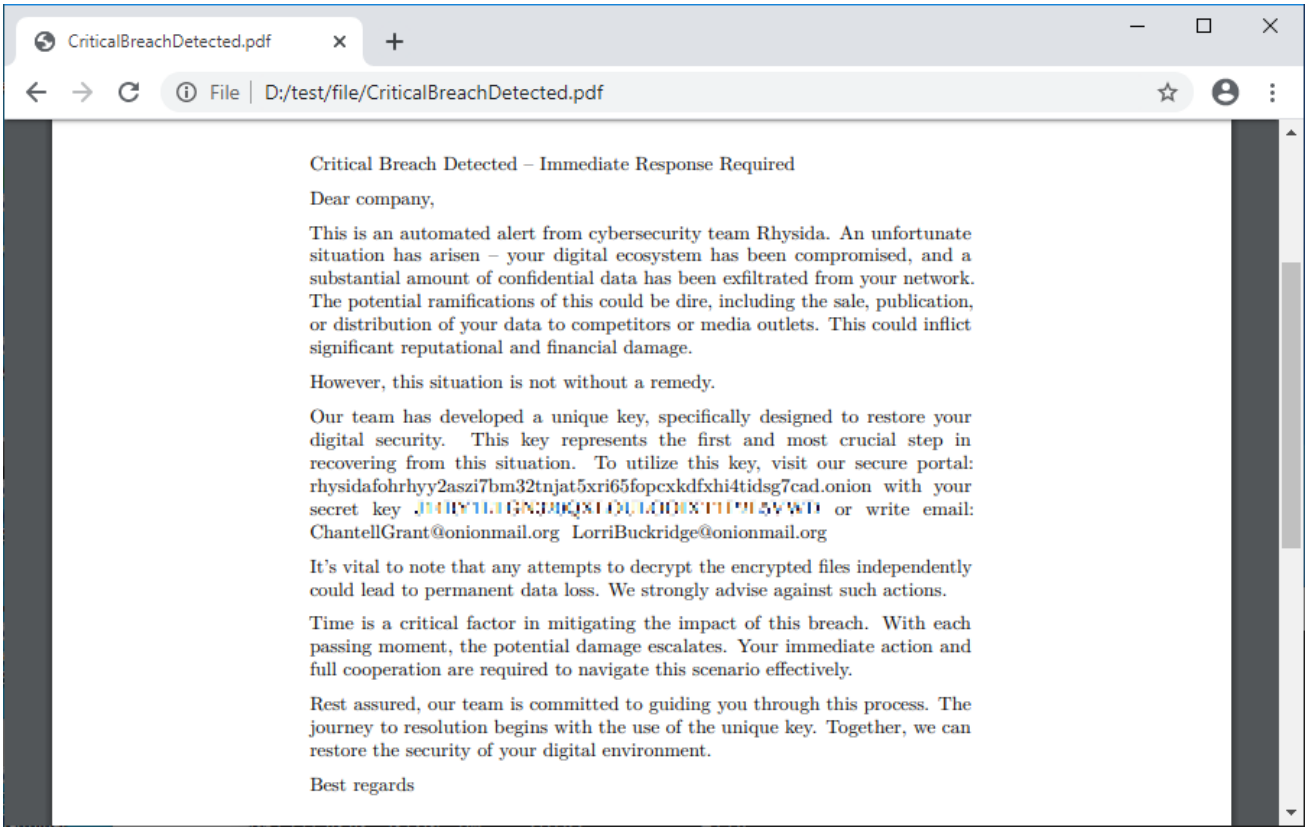


Figure 18. Rhysida ransom note, "CriticalBreachDetected.pdf"

The name Rhysida refers to the Rhysida genus of centipedes in biological classification, and it is also displayed on the first page of their DLS. When the victim enters the "unique key (private key)" mentioned in the ransom note into the "Token" input field, an input page form is provided, allowing the victim to provide additional information such as authentication and contact details to the threat actor.

The unique key used in this process is a combination of 32 characters, consisting of letters and numbers, and it is not possible to access the additional information page with a random combination. Only a validly generated unique key allows access to the following page.

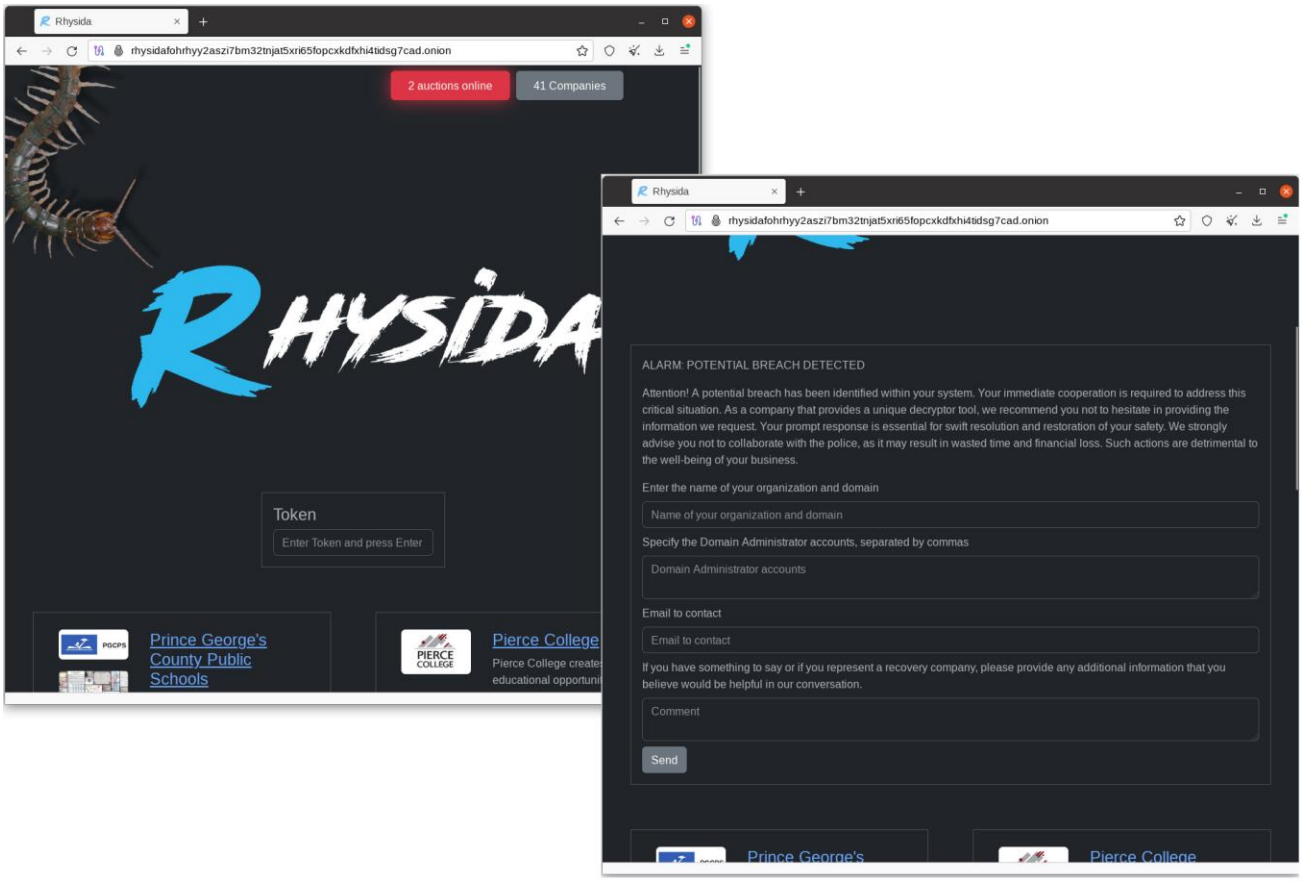


Figure 19. Rhysida ransomware group's DLS and the page displayed after entering the token

Threat actors are employing various methods such as email attachments, malicious website redirection, and phishing emails to infect systems with ransomware. In particular, the Rhysida group frequently uses phishing campaigns for ransomware infections. Therefore, if running an organization, it is crucial to provide regular security lectures on phishing awareness for all members in order to detect and prevent phishing attempts. Also, both organizations and individuals must follow the guidelines including applying the latest security updates, removing unnecessary software, practicing regular backups, and installing, using, and updating security software to protect their files and data from ransomware attacks.

IOCs for Reference

69b3d913a3967153d1e91ba1a31ebed839b297ed
338d4f4ec714359d589918cee1adad12ef231907
b07f6a5f61834a57304ad4d885bd37d8e1badba8
7abc07e7f56fc27130f84d1c7935a0961bd58cb9
2543857b275ea5c6d332ab279498a5b772bd2bd4
eda3a5b8ec86dd5741786ed791d43698bb92a262

3) Monti ransomware introduced new Linux encryption technique

Based on the content of the blog "Monti Ransomware Unleashes a New Encryptor for Linux" by Trend Micro,[5] BleepingComputer published an article titled "Monti ransomware targets VMware ESXi servers with new Linux locker" on August 14.[6]

The Monti ransomware group first became known sometime between May and June 2022. They are known to be a derivative or subsidiary group of the Conti ransomware group which disbanded in May of the same year. The Monti ransomware is assumed to have been created based on the source code of the Conti ransomware that was leaked in March 2022. The tactics, techniques, and procedures (TTP) of this ransomware group, along with many tools and encryption methods used, are similar to Conti ransomware.

- atip.ahnlab.com: Refer to the Threat Actors – Monti page

The Monti ransomware group recently targeted government and legal institutions through its renewed activities. A new variant of the Linux platform-based Monti ransomware emerged, showing differences from the previous Linux versions.

While it still utilizes a significant portion of the source code from the previous Conti ransomware, there have been substantial changes to the encryption algorithm in the new variant. The previous version of Monti ransomware for Linux was nearly identical (99%) to the Conti ransomware, based on the leaked code. However, the new Linux variant exhibits a 29% similarity when measured using BinDiff,[7] with significant changes observed in encryption techniques and file sizes. This variant uses the 'soft' parameter in the command syntax that detects and terminates virtual machines on Linux systems and applies various encryption methods based on file size. Encrypted files have a ".monti" extension, and traces of a decryption code have been found.

Examining the activities of the Monti ransomware group collected from the ATIP DDW infrastructure, shows that the group, which halted its activities since the end of May 2023, resumed its activities in late July and publicly disclosed two victim companies on their DLS in July and August, respectively. (The figure does not include duplicate company names.)

[5] https://www.trendmicro.com/en_us/research/23/h/monti-ransomware-unleashes-a-new-encryptor-for-linux.html
[6] https://www.bleepingcomputer.com/news/security/monti-ransomware-targets-vmware-esxi-servers-with-new-linux-locker/
[7] https://www.zynamics.com/bindiff.html

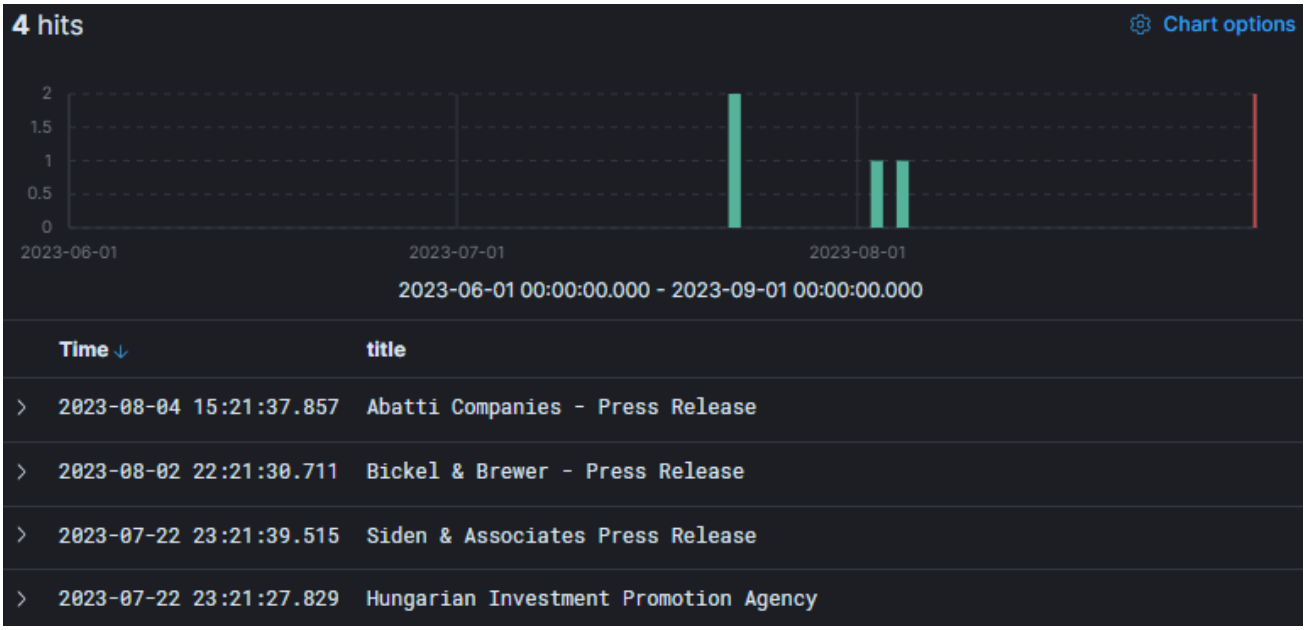


Figure 20. Number of targeted businesses disclosed by the Monti ransomware group in July and August

Please refer to the following for details regarding recent information on the Monti ransomware.

- atip.ahnlab.com: Monti Ransomware Group Posts Hungarian Investment Promotion Agency (HIPA) as a Victim
- atip.ahnlab.com: July 2023 Deep Web & Dark Web Threat Trend Report

Among the publicly disclosed Monti ransomware IOC shared by Trend Micro, we will now briefly examine the behaviors and characteristics of the file that corresponds to the SHA1 below, which is an ELF 64-bit file.

- f1c0054bc76e8753d4331a881cdf9156dd8b812a

The usage of the ransomware is guided as follows when executed with the "--help" argument. The exclusion or new addition to the arguments of previous Conti ransomware can be observed. The minimum required command argument for the ransomware to run is "--path", and this information must be given to the path of the files to be encrypted.

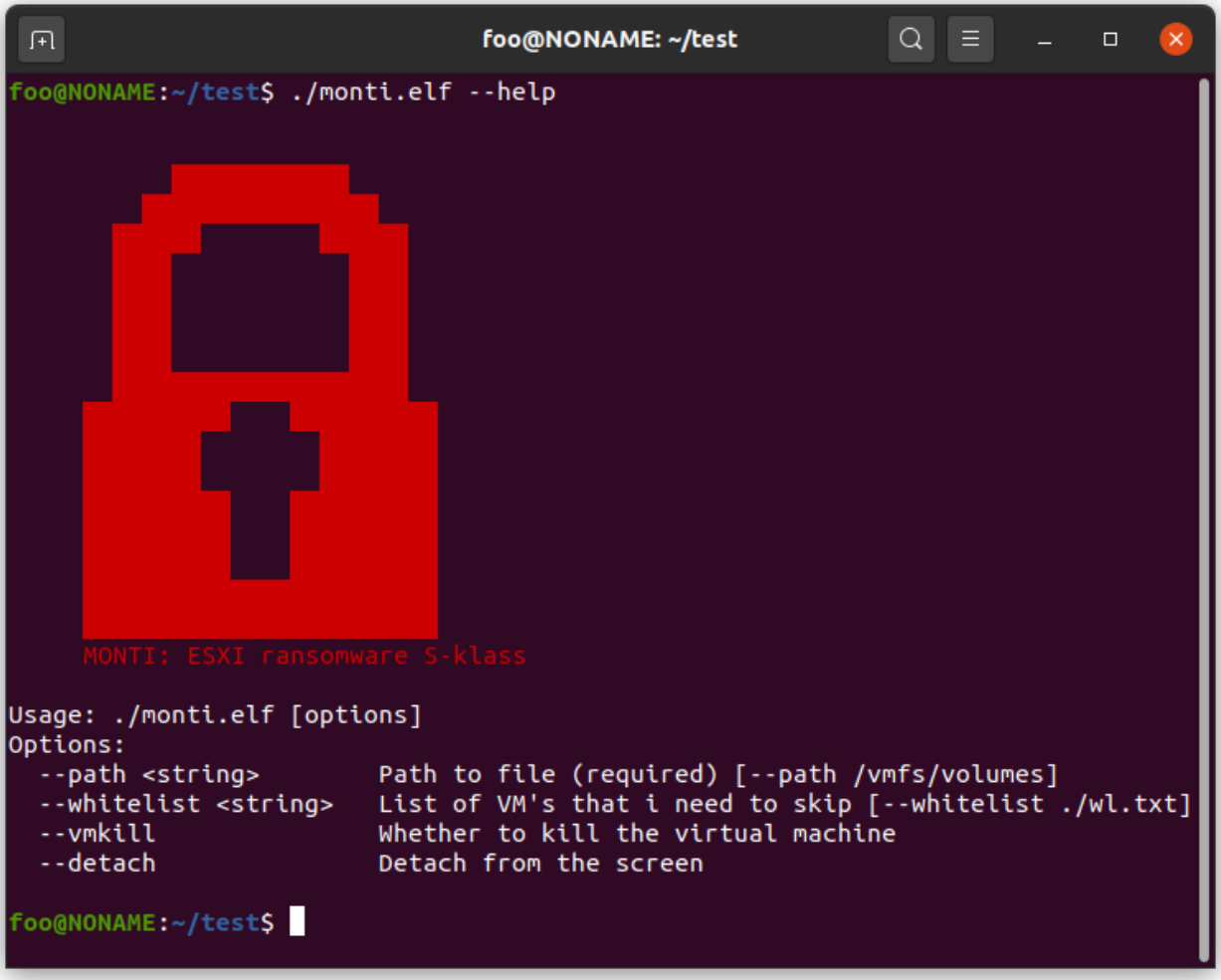


Figure 21. Execution of --help in Monti ransomware

After specifying the appropriate location in the command argument "--path" used as the path for encrypted files and executing the command, the encryption process is initiated (the current directory path "." was used for the test). Consequently, the encryption process was outputted, resulting in files being encrypted and given the ".monti" extension, as shown below. Additionally, a ransom note with the filename "readme.txt" was generated within the encrypted directory.

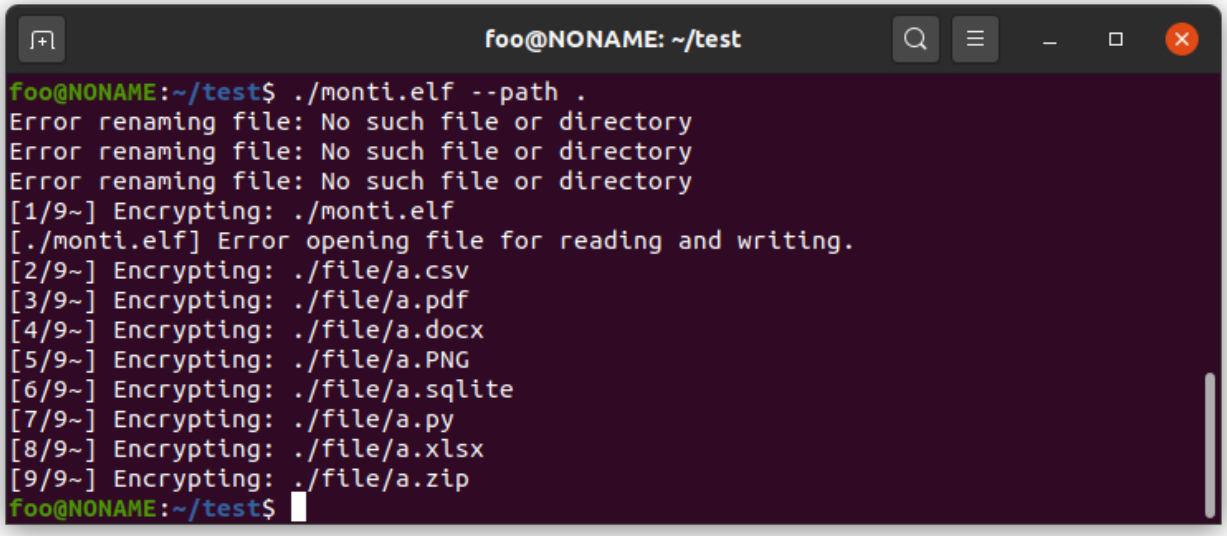


Figure 22. Execution of Monti ransomware

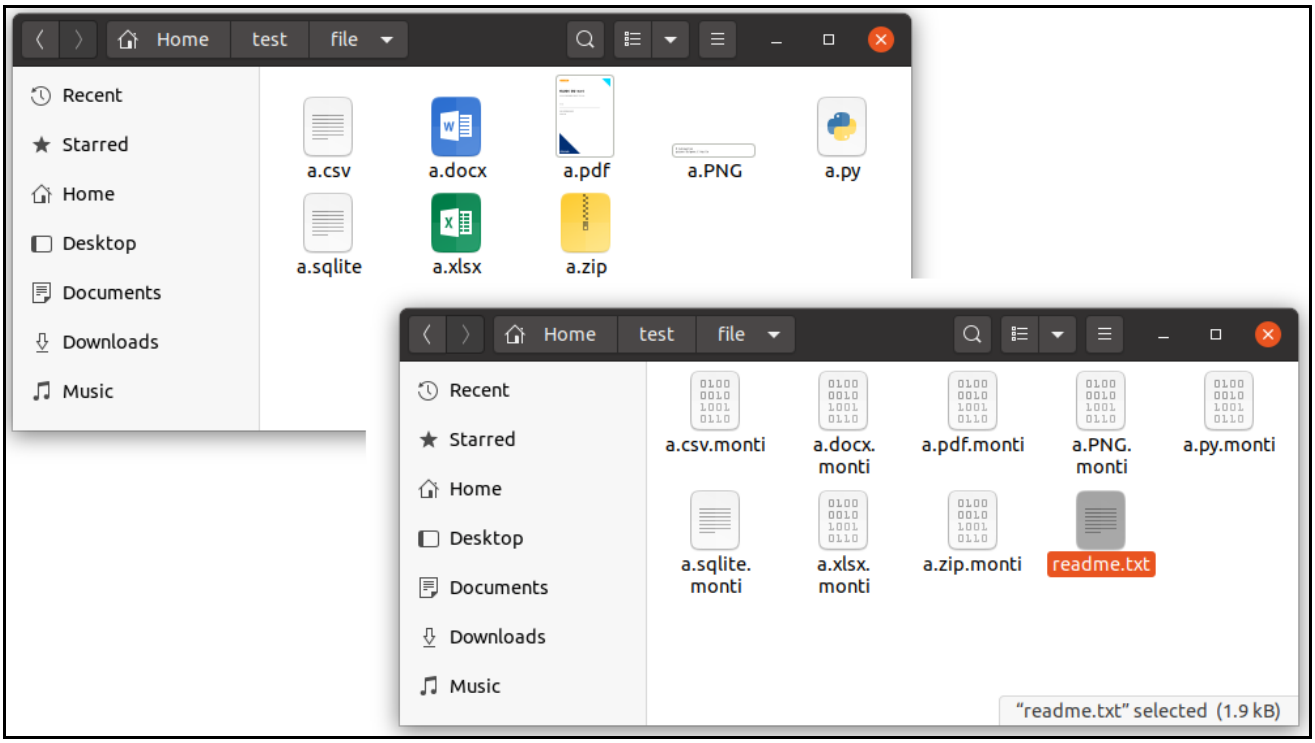


Figure 23. Files before and after .monti encryption via Monti ransomware

In the new variant of Monti ransomware, /etc/motd and index.html files are replaced with ransom notes saying that the system has been successfully infected. No changes were observed when tested with a regular user account. However, when granted root permissions using the sudo command, a change in the motd file could be observed, and its content matched the ransom note in readme.txt.

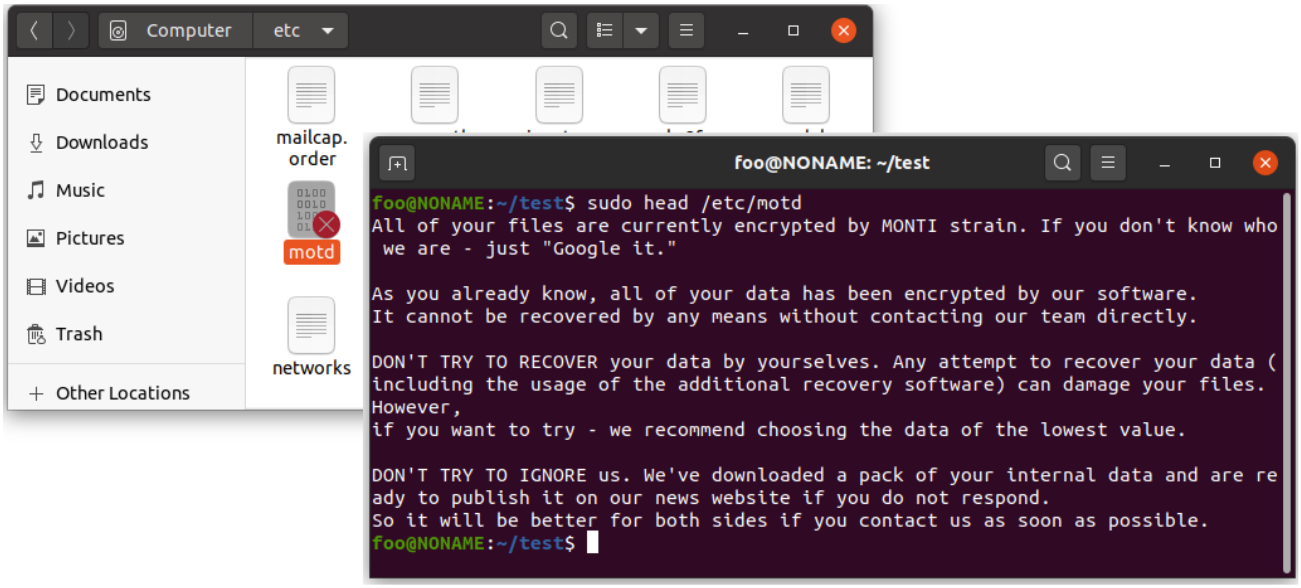


Figure 24. Monti ransomware ransom note - /etc/motd

Also, an "infection marker" with the string “MONTI” and a 256-byte encryption key were added to the ends of the encrypted files. The ransomware confirms whether a file has been previously infected or not by checking the file size and the presence of the "MONTI" marker. This influences their encryption strategy.

Below is a comparison screen for a.docx, which has a size of approximately 2.5MB, before and after encryption. A certain portion from the beginning of the file (1 MB) is encrypted, while the rest remains unchanged. Additionally, you can see that the "infection marker" and encryption key, as described earlier, have been added to the end of the file.

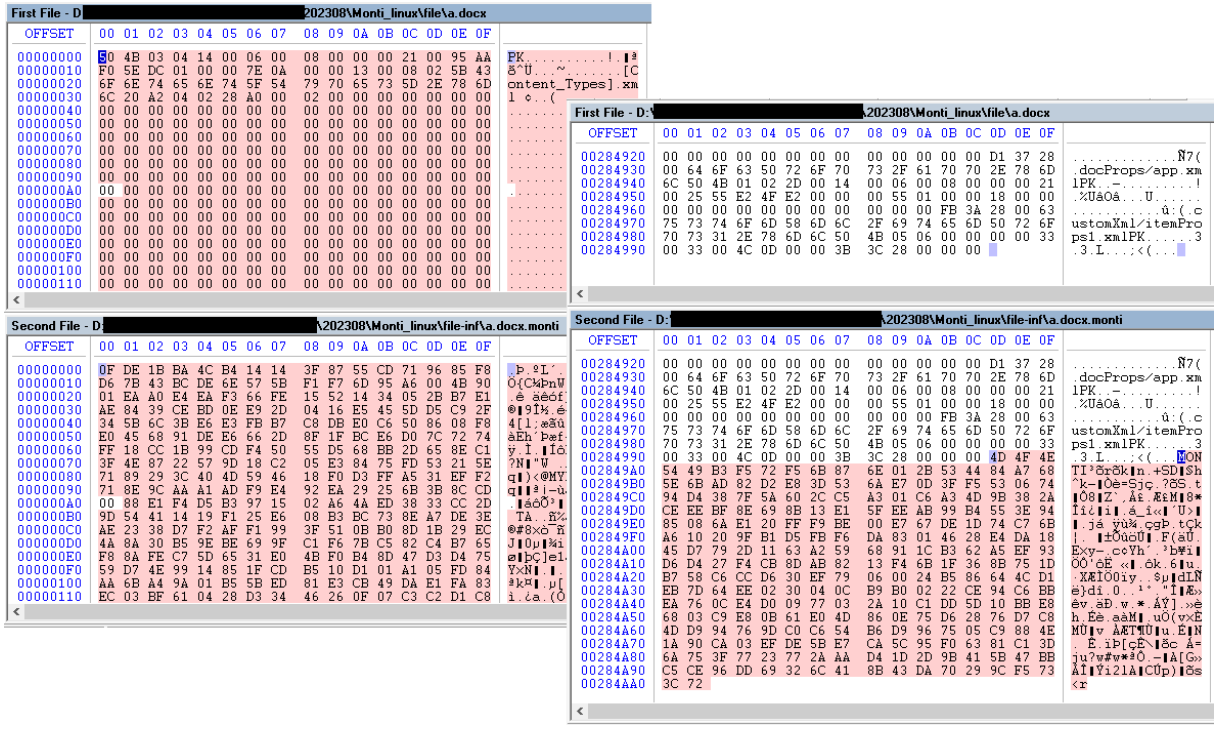


Figure 25. Example of a.docx.monti before and after encryption via Monti ransomware

The ransom note, "readme.txt," is composed of typical content, with one notable feature being the inclusion of an individual chat page's .onion address, guided by the phrase "You can contact our team directly for further instructions through our website :".

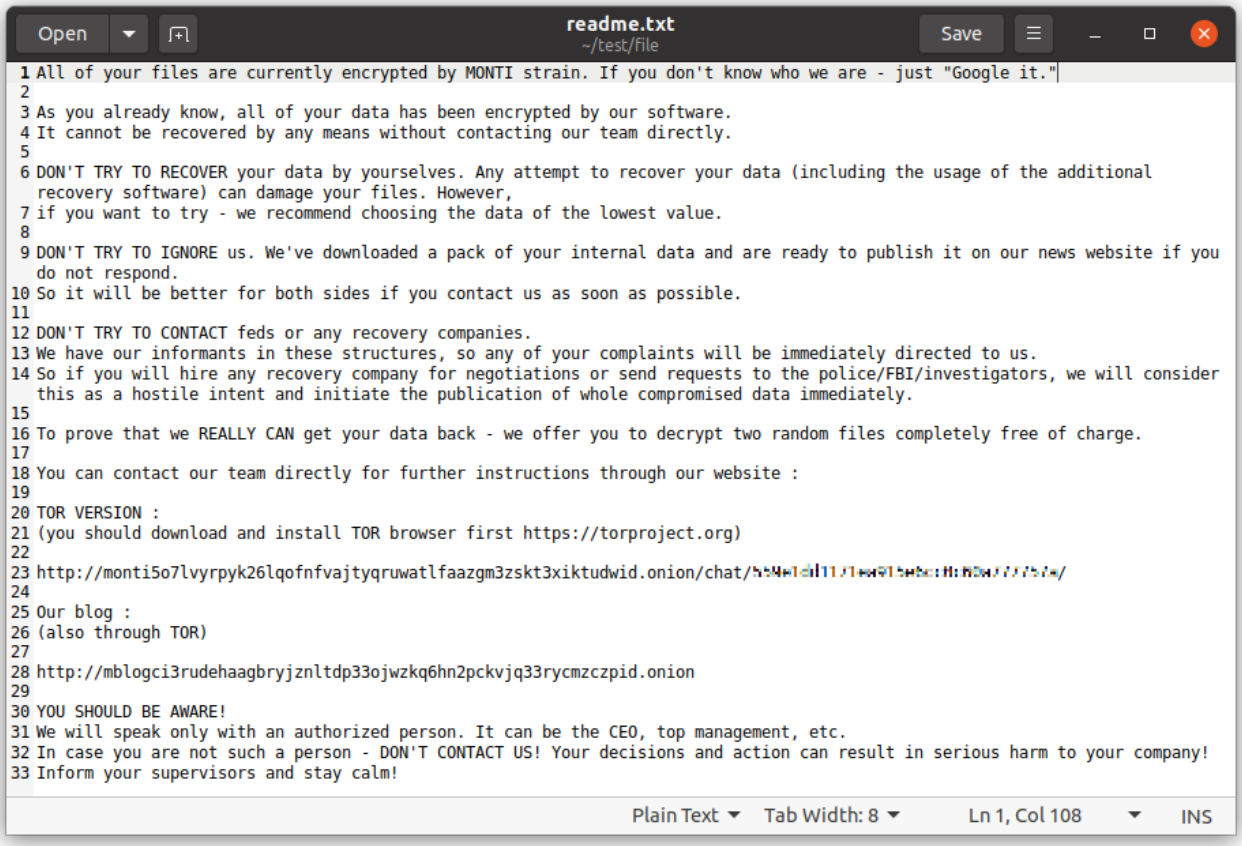


Figure 26. Monti ransomware ransom note - readme.txt

When attempting to access the separate chat page guided by the ransom note, a 500 server error occurred. As a result, we could not verify the content being provided. However, it is assumed that the page functions similarly to the Akira ransomware, with chatting capabilities, or like the aforementioned Rhysida ransomware, where the information of targeted companies is submitted to the threat actor.

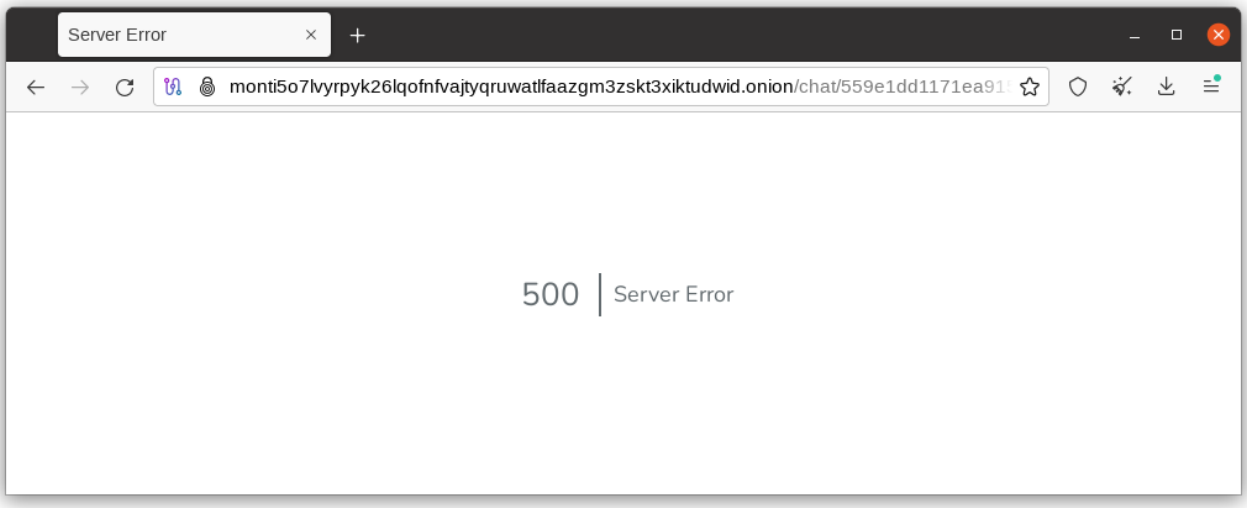


Figure 27. Monti ransomware chat page error

The emergence of the Monti ransomware has pertinence to the Conti ransomware, and this is concrete proof that ransomware operators are editing existing codes to develop unique ransomware to find more effective attack tools for extorting financial gains from their victims. To minimize harm from such attack methods, organizations and individual users must comply with security guidelines, such as applying the latest security updates, removing unnecessary software, practicing periodic backups as well as installing, using, and updating security software.

IOCs for Reference

f1c0054bc76e8753d4331a881cdf9156dd8b812a

a0c9dd3f3e3d0e2cd5d1da06b3aac019cdbc74ef

4) Others

Refer to the following posts to see issues other than the abovementioned ones. All ransomware-related major news, issues, and reports can be found by searching with the keyword Ransomware on ATIP.

- V3 Detects and Blocks Magniber Ransomware Injection (Direct Syscall Detection) (Aug 10)
- Hakuna Matata Ransomware Targeting Korean Companies (Aug 16)
- Cuba ransomware uses Veeam exploit against critical U.S. organizations (Aug 20)
- Cuba Ransomware Exploits New Vulnerabilities and Targets the US and South America (Aug 21, this link is only available in Korean)
- ALPHV (BlackCat) Ransomware Gang Infiltrates Watch Manufacturer of Japan (Aug 22)
- Akira Ransomware Targets Corporations Using Cisco VPN (Aug 24, this link is only available in Korean)
- LockBit 3.0 Builder Contributed Toward the Creation of Hundreds of Variants (Aug 28 this link is only available in Korean)

Conclusion

Although the number of ransomware samples and affected systems may change periodically depending on the success rate of attack campaigns or initial infection attempts, each month records at least hundreds or thousands of such cases as can be seen in the statistics herein. Also, hundreds of victimized companies are listed on ransomware groups' leak sites.

As described in this trend report, ransomware attack groups actively exploit the vulnerabilities of operating systems and software used by corporations. As for individual users, the threat groups take advantage of users' negligence, use malware carefully disguised as legitimate software, or exploit vulnerabilities that evade security software. According to the characteristics used in such initial infection attempts, corporate and individual users are advised to observe the following guidelines to protect and manage their major assets.

- Apply the latest security updates for operating systems and software. Enable auto-update.
- Install and use security software. Maintain the latest updates.
- Back up data regularly and store said data in an offline or separate network.
- Be cautious of websites from unreliable sources and viewing/executing email links and attachments.
- Use strong passwords and two-factor authentication (2FA).

Indicators Of Compromise (IOC)

A portion of the following IOC quotes other analysis reports, and there are some cases that could not be verified because samples could not be obtained. Updates may occur without prior notice when new information is found.

1) File Paths and Names

The file paths and names used by the threat group are as follows. File names of some malware or tools may be the same as those of normal files.

2) File Hashes

The hashes of the related files are as follows. However, sensitive samples may have been excluded.

69b3d913a3967153d1e91ba1a31ebed839b297ed // Rhysida 338d4f4ec714359d589918cee1adad12ef231907 b07f6a5f61834a57304ad4d885bd37d8e1badba8 7abc07e7f56fc27130f84d1c7935a0961bd58cb9 2543857b275ea5c6d332ab279498a5b772bd2bd4 eda3a5b8ec86dd5741786ed791d43698bb92a262 D5C2F87033A5BAEEB1B5B681F2C4A156FF1C05CCD1BFDAF6EAE019FC4D5320EE 1A9C27E5BE8C58DA1C02FC4245A07831D5D431CDD1A91CD35D2DD0AD62DA71CD 258DDD78655AC0587F64D7146E52549115B67465302C0CBD15A0CBA746F05595 0BB0E1FCFF8CCF54C6F9ECFD4BBB6757F6A25CB0E7A173D12CF0F402A3AE706F F6F74E05E24DD2E4E60E5FB50F73FC720EE826A43F2F0056E5B88724FA06FBAB 250E81EEB4DF4649CCB13E271AE3F80D44995B2F8FFCA7A2C5E1C738546C2AB1 A864282FEA5A536510AE86C77CE46F7827687783628E4F2CEB5BF2C41B8CD3C6 6903B00A15EFF9B494947896F222BD5B093A63AA1F340815823645FD57BD61DE 3BC0340007F3A9831CB35766F2EB42DE81D13AEB99B3A8C07DEE0BB8B000CB96 2A3942D213548573AF8CB07C13547C0D52D1C3D72365276D6623B3951BD6D1B2 f1c0054bc76e8753d4331a881cdf9156dd8b812a // Monti a0c9dd3f3e3d0e2cd5d1da06b3aac019cdbc74ef

3) Relevant Domains, URLs, and IP Addresses

The download or C2 addresses used are as follows. http was changed to hxxp, and sensitive information may have been excluded.

References

[1] atip.ahnlab.com: June 2023 Threat Trend Report on Ransomware
[2] atip.ahnlab.com: July 2023 Threat Trend Report on Ransomware
[3] www.bleepingcomputer.com : Clop now leaks data stolen in MOVEit attacks on clearweb sites
[4] www.bleepingcomputer.com : Clop ransomware now uses torrents to leak data and evade takedowns
[5] www.ransomlook.io : Clop Torrents
[6] research.checkpoint.com : RHYSIDA RANSOMWARE: ACTIVITY ANALYSIS AND TIES TO VICE SOCIETY
[7] socradar.io : Threat Profile: Rhysida Ransomware
[8] www.hhs.gov : Rhysida Ransomware Sector Alert
[9] www.trendmicro.com : Monti Ransomware Unleashes a New Encryptor for Linux
[10] www.bleepingcomputer.com : Monti ransomware targets VMware ESXi servers with new Linux locker

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