TLP: GREEN

Threat Trend Report on Ransomware

April 2023 Ransomware Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

May 04, 2023

AhnLab

Classification

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

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

Remarks

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

Contents

CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Objectives and Scope

This report provides statistics on new ransomware samples, attacked systems, and targeted businesses in April 2023, as well as notable ransomware issues in Korea and overseas. 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 (ATIP).

- Ransomware
- Statistics by Type

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 diagnosed 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 malicious files and behaviors were diagnosed under the category of Ransomware/ or Ransom/.

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

- Ransom/MDP.Magniber : Example of behavior detection name

In addition, the diagnosis at the time of detection may not allow for the identification of ransomware type (e.g. Generic, Agent, Edit, Decoy), and some cases may be excluded from the ransomware statistics or be counted as a different ransomware type due to a change in diagnosis after detection or a failure of detection.

The statistics on targeted businesses are the statistical 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.

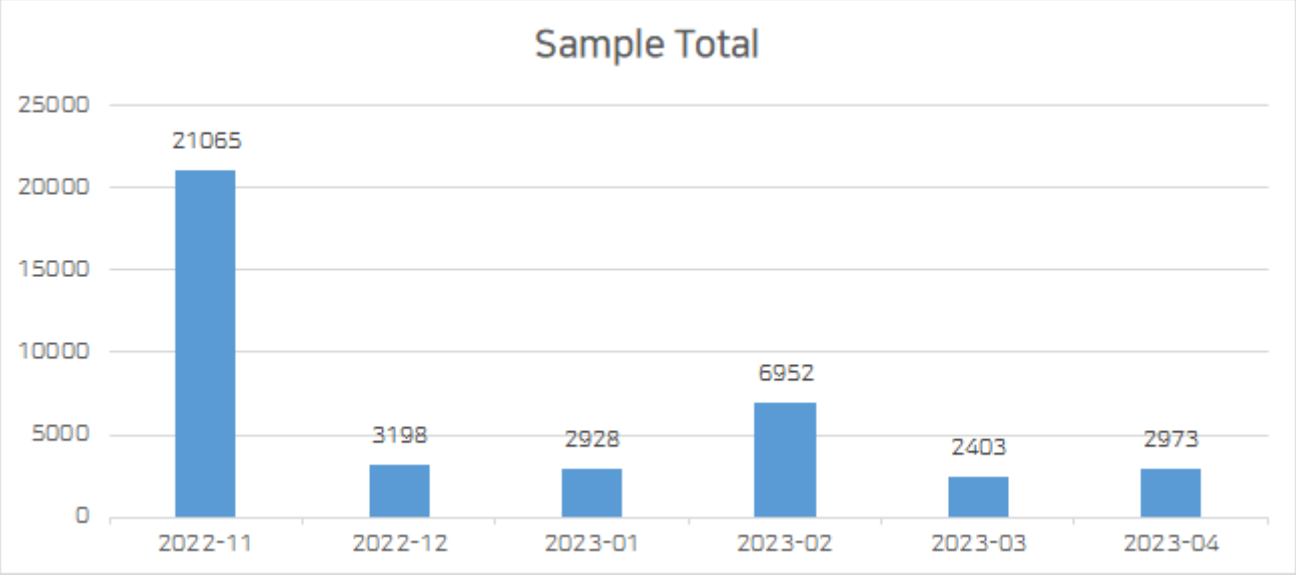

Figure 1. Number of new ransomware samples

The ransomware sample total that saw a steep decline in December 2022 was brought back up by Magniber which showed an increase in February; however, along with its decline, the sample total maintained the average in April, where it showed a slight increase from the previous month.

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

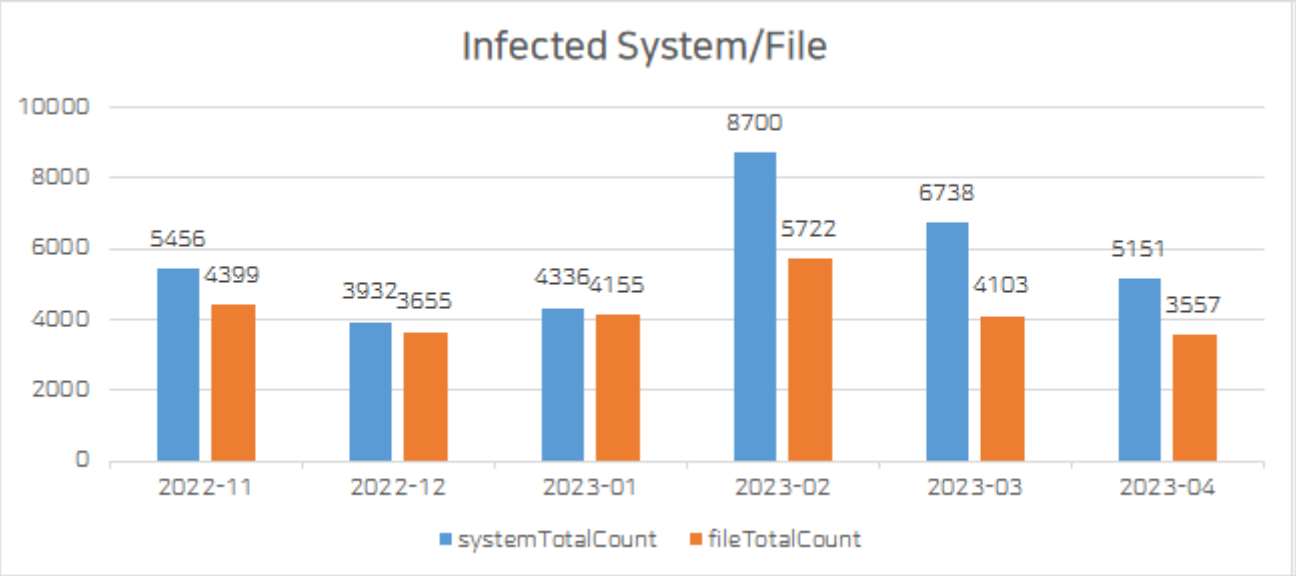

Figure 2. Systems and files affected by ransomware

The targeted system statistics showed a slight decrease following the increase in February.

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

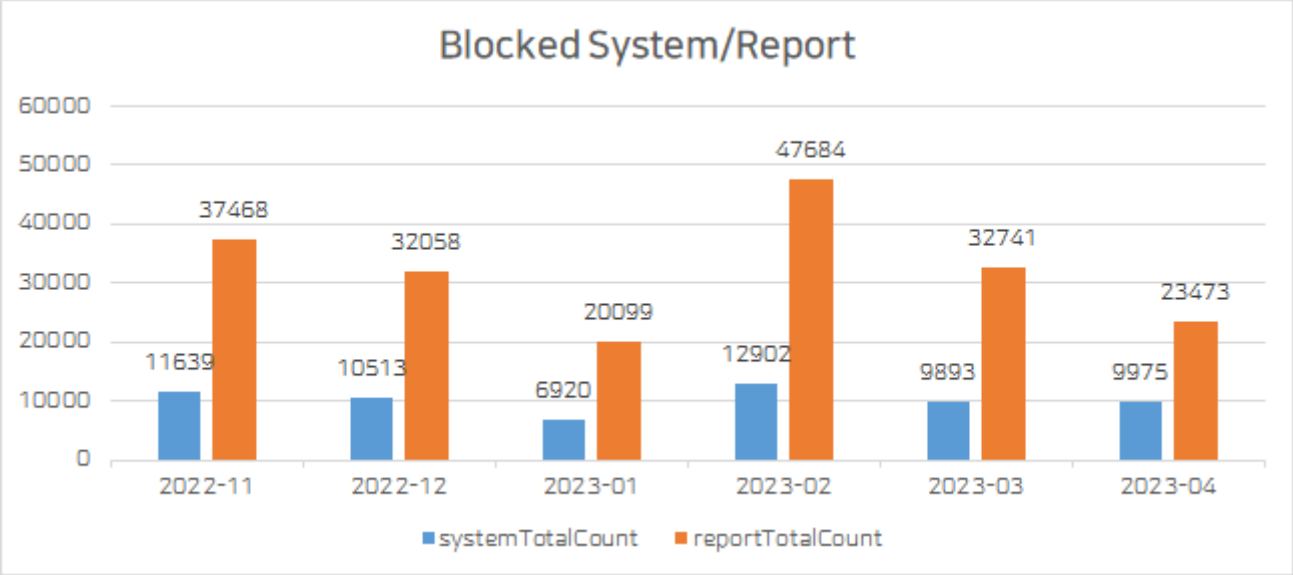

Figure 3. Ransomware behavior detection-based targeted systems and reports

Behavior detection statistics also showed a similar figure to the sample total statistics.

3) New Samples by Ransomware

Below is the statistics showing the 2,973 new samples that were discovered in April organized by ransomware. Only 20 ransomware with the most samples are shown.

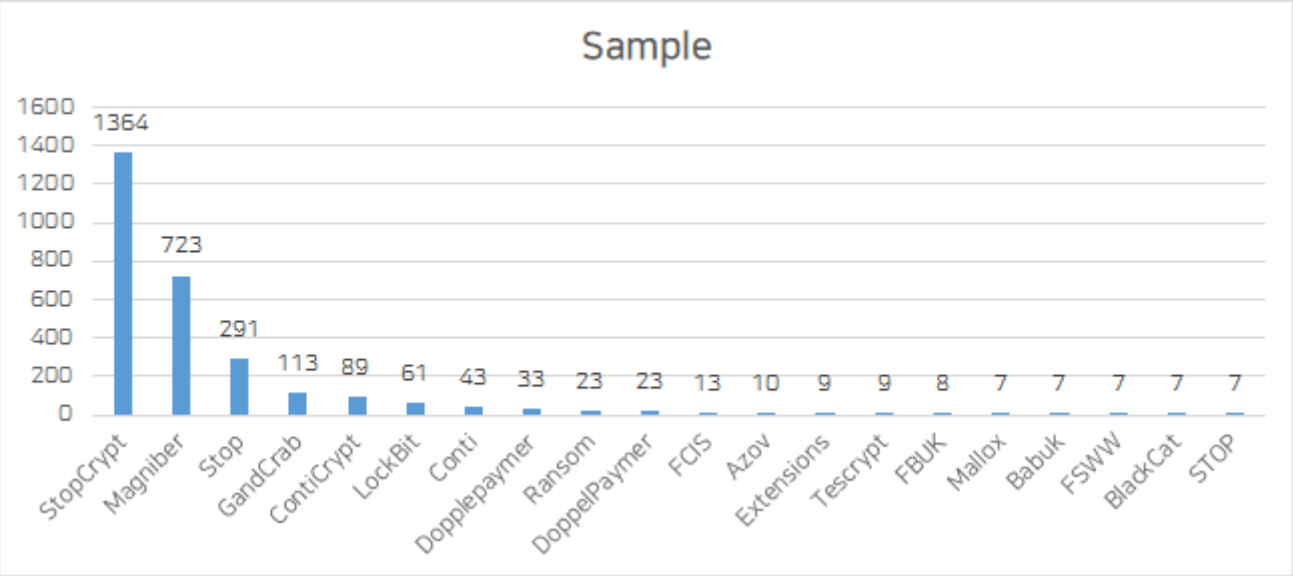

Figure 4. Number of new samples per ransomware (Apr. 2023)

The StopCrypt sample count almost doubled from 700 in the previous month, overtaking Magniber in the new ransomware samples category. StopCrypt, with few reported cases in

Korea, was the most collected; In comparison, an overall decrease was observed for new samples of other ransomware.

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).

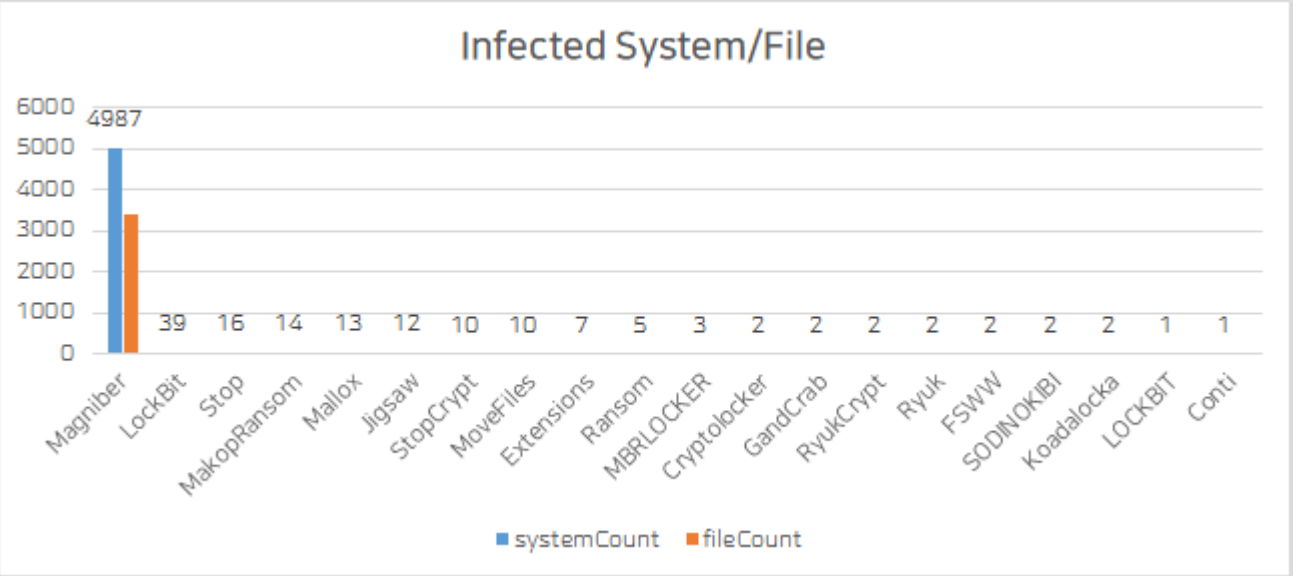

Figure 5. Number of targeted systems and files per ransomware (Apr. 2023)

The number of systems targeted by Magniber has shown a 20% decrease compared to the previous month's 6,300 cases, yet is still the highest in the number of targeted systems.

The following shows the statistics on the number of systems targeted daily extracted from the top 12 ransomware.

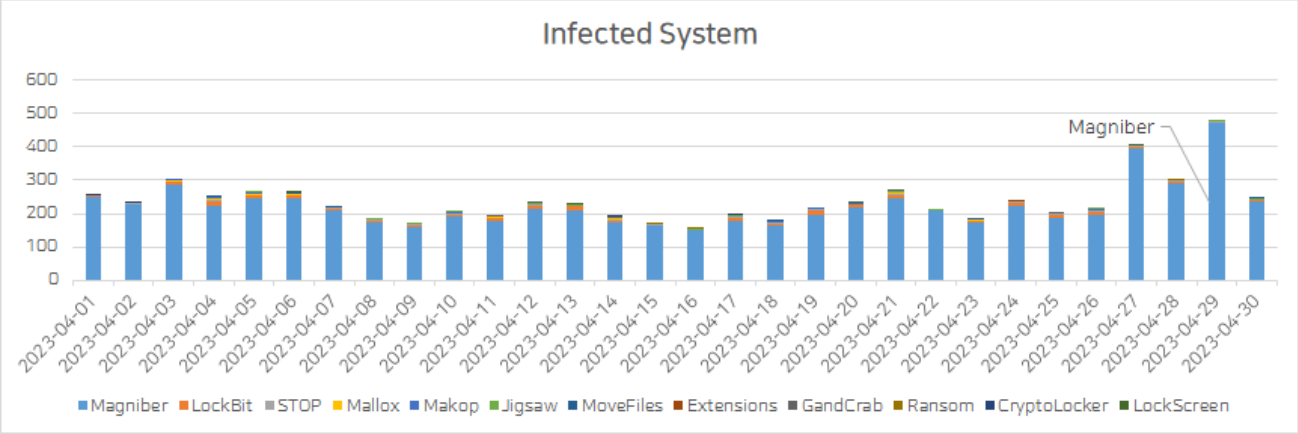

Figure 6. Daily number of targeted systems per ransomware (Apr. 2023)

Cases of Magniber infection were the highest in the daily statistics as well. Aside from the typical fluctuations such as a slight decrease in attacks during weekends, there was an increase in Magniber infection through MSI files disguised with file names such as “System.Hotfix.Win10.0”, “Update.System.Win10.0 “, “Security.Upgrade.Win10.0 “, and “Antivirus.Upgrade.Database.Cloud” on April 27 and 29. There were also email attacks of LockBit and Makop involving attachments disguised as “resumes” and “job applications”.

5) Targeted Businesses by Ransomware Group

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

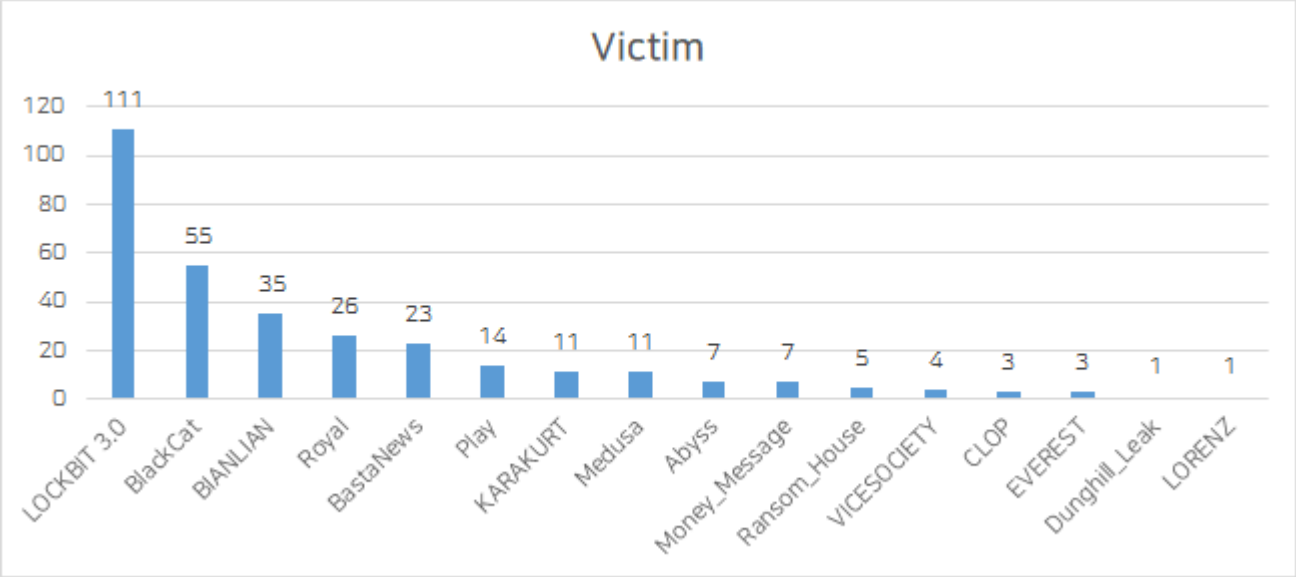

Figure 7. Number of targeted businesses per ransomware group (Apr. 2023)

CLOP, which was ranked first place through its exploitation of the GoAnywhere MFT zero-day vulnerability (CVE-2023-0669), fell behind in April. LOCKBIT 3.0 had the most identified victims at 111.

Some of the targeted businesses revealed per ransomware group can be seen below.

Ransomware	Victim	Count
LOCKBIT 3.0	ativy.com / p-and-r.com / revvaviation.com / errebielle.it / vernegroup.com / the	111
BlackCat	TRUSSWAY / Ruekert & Mielke / Mutual de Seguros de Chile / Electronic SYSTEI	55
BIANLIAN	E*** ****** / *j****** ***** / Quad-County Ready Mix / Meriton / Harvard Energy	35
Royal	Benning Construction / Vending Group / Steve Silver furniture / Toho Tenax Am	26
BastaNews	The Shively Bros / Precision Fabrics Group / Corporate Technologies / HUSKY / R	23
Play	Schirm / Vleeswarenfabriek Jac Michiels / Legion Aero / PKF Antares / Palo Alto	14
KARAKURT	Officeworks Inc / Medicalodges, Inc / Petaluma Health Center / Pharm-Pacc Corp	11
Medusa	Arandell Corp / Sonda / Open University of Cyprus / Atlantic International Unive	11
Abyss	siebold.com / stonehillcontracting.com / jones-hamilton.com / igadiltd.com / hos	7
Money_Message	Pharmerica.com & BrightSpring Health Services / Micro Star International / mida	7
Ransom_House	Aero Engine Solution INC / OMT Officine Meccaniche Torino S.p.A. / Tranztec Sol	5
VICESOCIETY	CommScope / Lakeland Community College / Neptune Lines / CMC Group	4
CLOP	LASOTEL.FR / AUT-TECH-GROUP.COM / GC-EMPLOYMENT.COM	3
EVEREST	US District Court / On sale / US District Court IL / On sale / US District Court / Lav	3
Dunghill_Leak	Incredible Technologies	1
LORENZ	Intrasect Technologies / Joy Cone Co, Joy Baking group, BoDeans Baking, Altesa	1

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

6) Targeted Businesses by Ransomware Group (External Statistics)

The statistics on targeted businesses during the same period were provided by DarkFeed twitter, run by an external TI business or security expert, and this can be seen below.

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

It can be seen that the number of businesses targeted by LOCKBIT 3.0, BlackCat, Royal, BastaNews, and Play ransomware groups are generally high.

Key Trends

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

- BabLock (Rorschach) ransomware
- Nokoyawa ransomware exploits the CLFS zero-day vulnerability
- Kadavro ransomware, an interactive ransom note

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) BabLock (Rorschach) Ransomware

Based on the analysis details in Check Point Research (CPR)'s blog post "RORSCHACH – A NEW SOPHISTICATED AND FAST RANSOMWARE"[1], bleepingcomputer uploaded an article titled "New Rorschach ransomware is the fastest encryptor seen so far"[2] on April 4.

The highly efficient and fast encryption emphasized in both titles is explained as using a hybrid encryption system created by combining curve25519 and eSTREAM encryption hc-128 algorithm, encrypting only a portion of the files.

CPR stated that the ransomware shown to users following a Rorschach ransomware infection is similar to that of Yanluowang, but as some variants show similarities to DarkSide's ransom note, some security companies misjudge this ransomware as DarkSide. Due to the differing judgment from each company or researcher that analyzed this ransomware, it was given the name Rorschach ransomware after a famous psychological test.

The definition of Rorschach quoted from the en.wikipedia.org (Rorschach Test) page is given below. (The quote has been translated from the Korean Wikipedia page and may differ from the English Wikipedia page.)

> *The Rorschach Inkblot test is a projective psychological test developed by Swiss psychologist Hermann Rorschach in 1921. It examines a person's personality and is composed of ten cards with bilaterally symmetrical inkblots. After presenting the test subject with an inkblot with no discernible form, the subject is encouraged to freely comment on what the figure looks like to them and what thoughts it elicits. These responses are interpreted to expose the test subject's personality. It is called the Rorschach test for short.*

[1] https://research.checkpoint.com/2023/rorschach-a-new-sophisticated-and-fast-ransomware/

[2] https://www.bleepingcomputer.com/news/security/new-rorschach-ransomware-is-the-fastest-encryptor-seen-so-far/

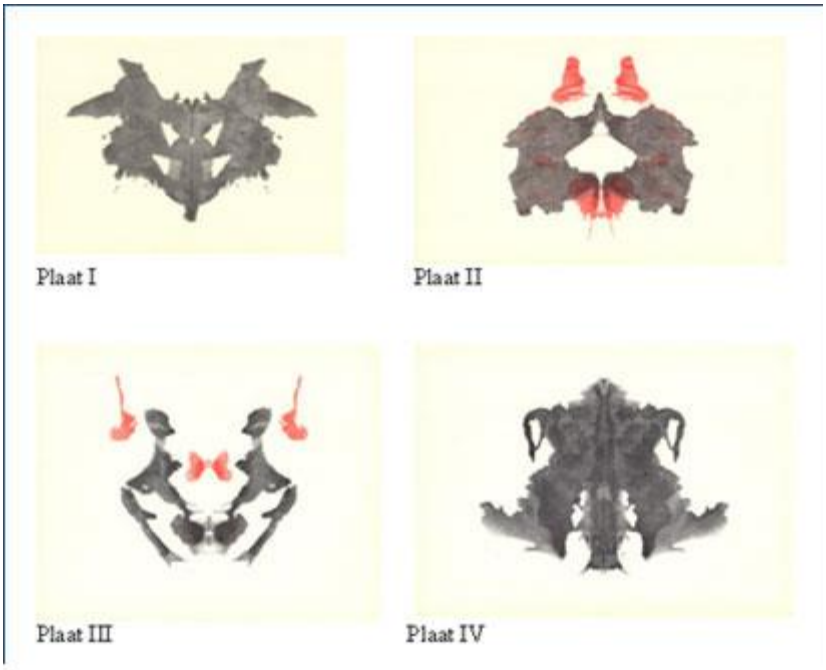

Figure 9. Examples of Rorschach cards <Source> ko.wikipedia.org

The operator of the Rorschach ransomware has not yet been identified, and no DLS for the ransomware has been discovered either. CPR disclosed the following relevant IOC, but files have not been procured.

Name	Hash	Comments
cy.exe	2237ec542cdcd3eb656e86e43b461cd1	PA Cortex Dump Service Tool (benign file)
winutils.dll	4a03423c77fe2c8d979caca58a64ad6c	Loader and injector into notepad.exe
config.ini	6bd96d06cd7c4b084fe9346e55a81cf9	Encrypted ransomware payload

Table 2. Rorschach-related IOC <Source> research.checkpoint.com

- cy.exe – Cortex XDR Dump Service Tool version 7.3.0.16740, abused to side-load winutils.dll
- winutils.dll – Packed Rorschach loader and injector, used to decrypt and inject the ransomware.
- config.ini – Encrypted Rorschach ransomware which contains all the logic and configuration.

On the same day the above details were released, the Group-IB team uploaded a blog post[3] stating that the new ransomware group discovered in mid-January of 2023 has been named BabLock. It was revealed that the BabLock ransomware's encryption routine is similar to the source code of the leaked Babuk ransomware and also shared similar characteristics to the Windows version of the LockBit ransomware in light of the complexity and its use of group

[3] https://www.group-ib.com/blog/bablock-ransomware/

policies. It seems that the name BabLock stemmed from such features. // Babuk + LockBit

A test was conducted on similar files which could be procured based on the IOC presented by Group-IB; the process tree is given below. The "DLL side-loading" technique is used, where a normal program is launched first, followed by a malicious file. The "config.ini" file, containing the ransomware features, is then run through being injected into the Notepad process.

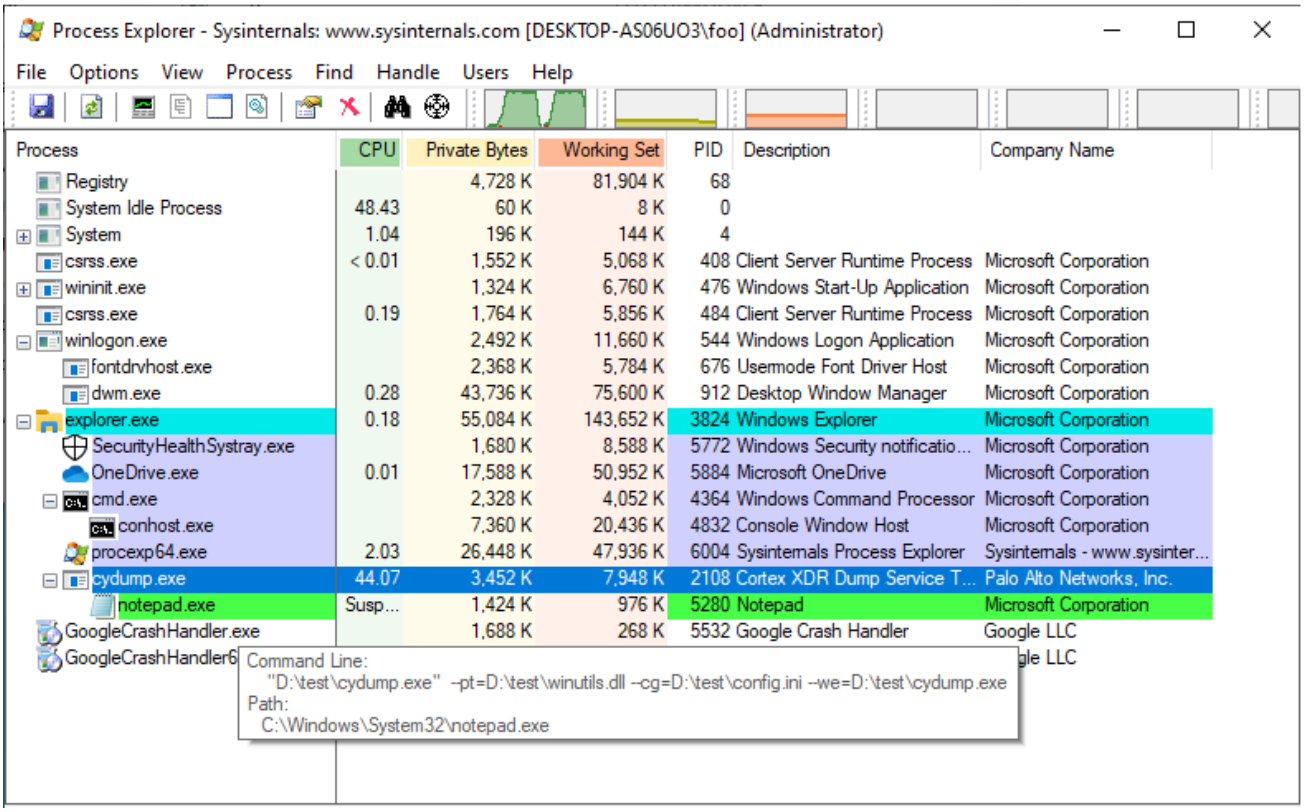

Figure 10. BabLock process tree

Please refer to the following web pages for additional details on the BabLock (Rorschach) ransomware.

- www.boannews.com : Mysterious Ransomware Rorschach Shows Unmatched Encryption Speed
- Www.trendmicro.com : An Analysis of the BabLock (aka Rorschach) Ransomware
- www.group-ib.com : BabLock, new ransomware quietly cruising around Europe, Middle East, and Asia

For precise classification of malware, security companies develop, run, and make improvements on their internal classification and detection infrastructure, but some ransomware such as BabLock (Rorschach) evoke confusion with different judgments given by different parties. As can be seen from the word "Mysterious" used in the title of a certain security news article, it is not easy to precisely determine and classify the overall changes to

various malware including ransomware, such as the history of each version, changes to source codes in feature actualization, changes to performance or codes for detection evasion, simple changes to appearance such as changing the compiler, etc. This is a task the cyber security industry is presented with.

Reference IOC

cy.exe 2237ec542cdcd3eb656e86e43b461cd1 (normal) PA Cortex Dump Service Tool (benign file)
winutils.dll 4a03423c77fe2c8d979caca58a64ad6c (undisclosed) Loader and injector into notepad.exe
config.ini 6bd96d06cd7c4b084fe9346e55a81cf9 (undisclosed) Encrypted ransomware payload

winutils.dll

8280E83A4405420632CCA6FAB9F9584E
f02ff25c2169c6575bdf3cd6f120c324
4b4fd546be8d9f32fb852c000fcc24f7

config.ini

3e3d20f82c4ce395b4a1d1ab60363fc6

2) Nokoyawa Ransomware Exploiting the CLFS Zero-day Vulnerability

Through a blog post[4], Kaspersky revealed that attempts of privilege escalation through the Common Log File System (CLFS) in Microsoft Windows servers of multiple small and medium companies in the Middle East and North America were identified in February. The post stated that this vulnerability was identified to be a different zero-day vulnerability from the previously known CLFS elevation of privilege vulnerability (CVE-2022-24521), and it has been reported to Microsoft.

The CLFS elevation of privilege vulnerability with the code CVE-2023-28252 was discovered by Kaspersky during an attack process that involved a cyber criminal attempting to distribute a new version of the Nokoyawa ransomware as the final payload. The Nokoyawa ransomware group has been exploiting vulnerabilities that target CLFS drivers since June 2022. Seeing the fact that these vulnerabilities all have similar characteristics, we assumed that the same creator is behind the exploits. CVE-2023-28252 was patched through the regular MS security update on April 11, 2023.

[4] https://securelist.com/nokoyawa-ransomware-attacks-with-windows-zero-day/109483/

- www.bleepingcomputer.com : Windows zero-day vulnerability exploited in ransomware attacks
- securelist.com : Nokoyawa ransomware attacks with Windows zero-day

CLFS is a Windows log file subsystem actualized in the clfs.sys driver. This file system can be used in all applications, and Microsoft provides an API for this system. Logs are created through the CreateLogFile function. The system is composed of the basic log file (.blf extension) which is the master file that includes the metadata and multiple containers where actual data is stored. CVE-2023-28252 is an out-of-bounds write vulnerability that can be exploited when the system attempts to expand the metadata block. [5]

Like the explanation above, CLFS is a default feature of Windows for logging for applications; exploiting the aforementioned vulnerability enables privilege escalation to the SYSTEM level. Please refer to the ATIP reports below for more details on the CLFS elevation of privilege vulnerability (CVE-2023-28252) and the Nokoyawa ransomware.

- atip.ahnlab.com : Nokoyawa Ransomware
- atip.ahnlab.com : Caution Advised for Elevation of Privilege Vulnerability Using CLFS (CVE-2023-28252)
- atip.ahnlab.com : April 2023 Regular Security Update Advisory for MS Products (This report supports Korean only for now)
- atip.ahnlab.com : Analysis Report on the CVE-2022-24521 Vulnerability (This report supports Korean only for now)

Seeing from the fact that the Nokoyawa ransomware (8800e6f1501f69a0a04ce709e9fa251c) revealed as the final payload is run with separate command arguments (--config, --dir, --file, --safe-mode ···), it seems to be version 2.0 or earlier, and not the Nevada ransomware which has the encryption arguments within the file. [6]

[5] https://www.wiz.io/blog/microsoft-april-2023-patch-tuesday-highlights

[6] https://www.zscaler.com/blogs/security-research/nevada-ransomware-yet-another-nokoyawa-variant

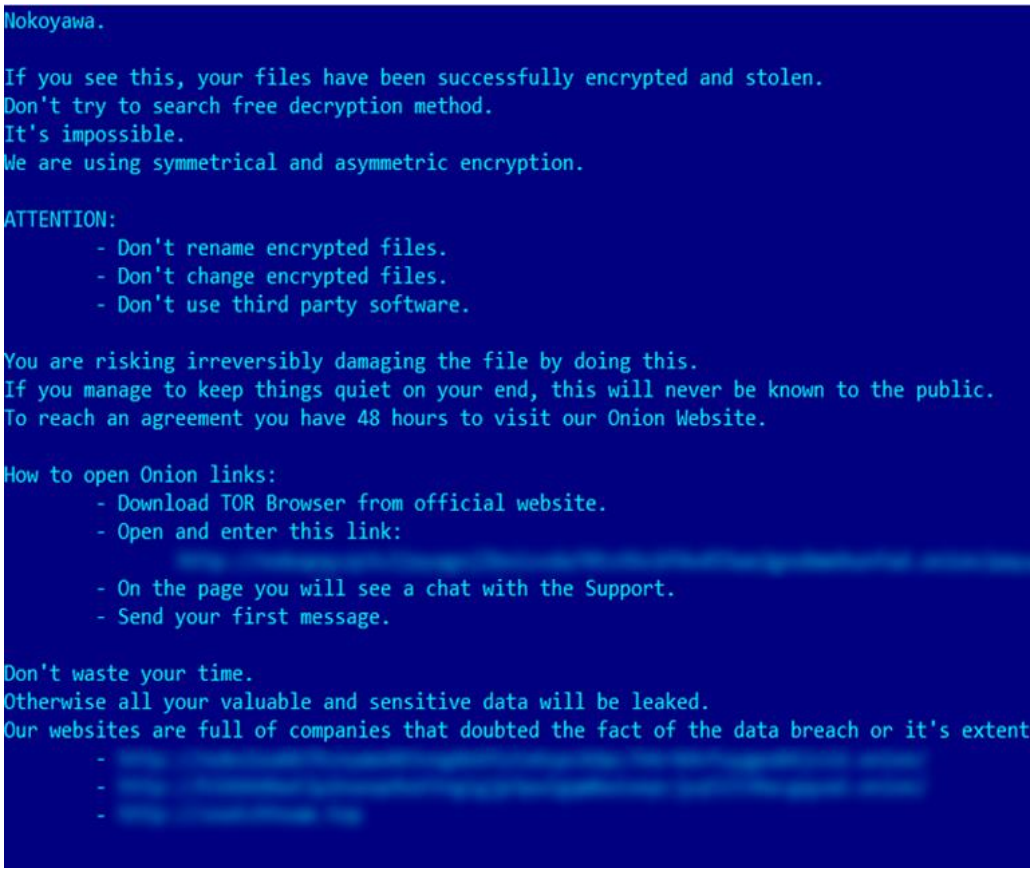

Figure 11. Nokoyawa ransom note <Source> securelist.com

To prevent ransomware infection through vulnerabilities in the OS, users and organizations must apply the latest security patch for their operating system, and they are advised to remove unnecessary software. Other than that, the standard procedure of regular backups and security software installation and update should be performed.

Reference IOC

8800e6f1501f69a0a04ce709e9fa251c : Nokoyawa Ransomware

3) Kadavro Ransomware, an Interactive Ransom Note

FortiGuard Labs disclosed analysis details on the Kadavro ransomware, which is a variant of the NoCry ransomware that encrypts user files and demands payment with Monero (XMR) cryptocurrency for file recovery. [7]

The latest Kadavro variant is a Tor browser installation program, and it evades suspicion from

[7] https://www.fortinet.com/blog/threat-research/ransomware-roundup-kadavro-vector-ransomware

users with disguised file name and icon. The file name used is "torbrowser-install-win64-12.0.4_ALL2.exe", and following infection, it encrypts files and adds the file extension ".vector_".

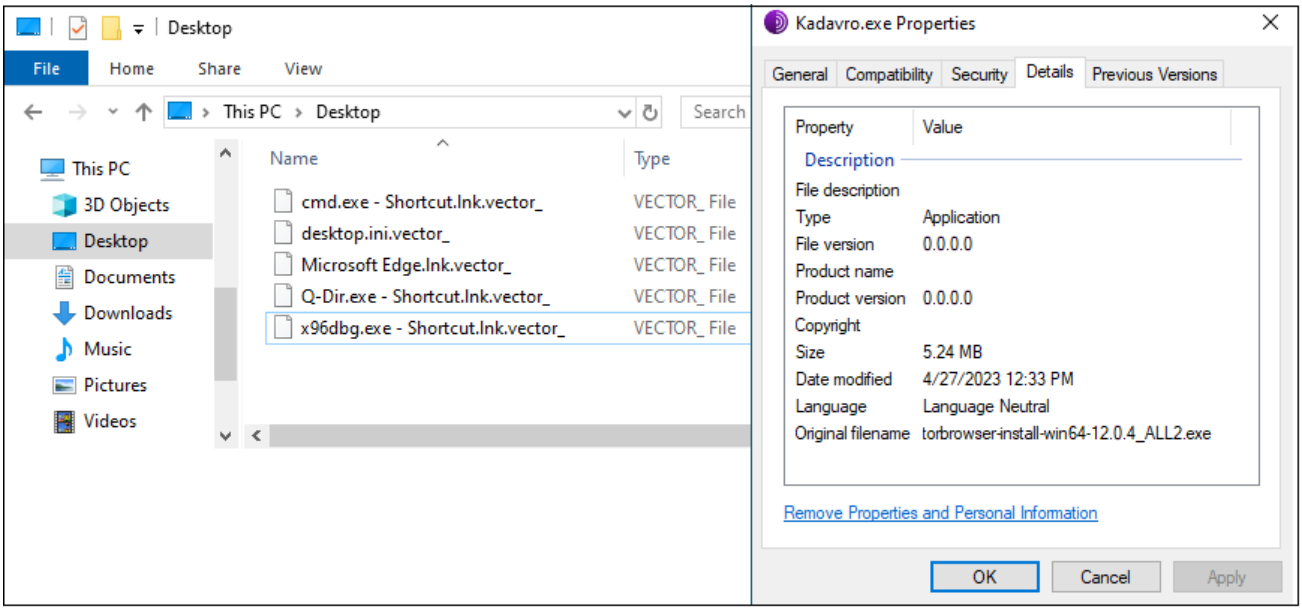

Figure 12. Example file name following Kadavro encryption, and disguised file name

When the encryption process is complete, it displays an interactive ransom note on the desktop, demanding $250 in Monero cryptocurrency to be sent to a certain address.

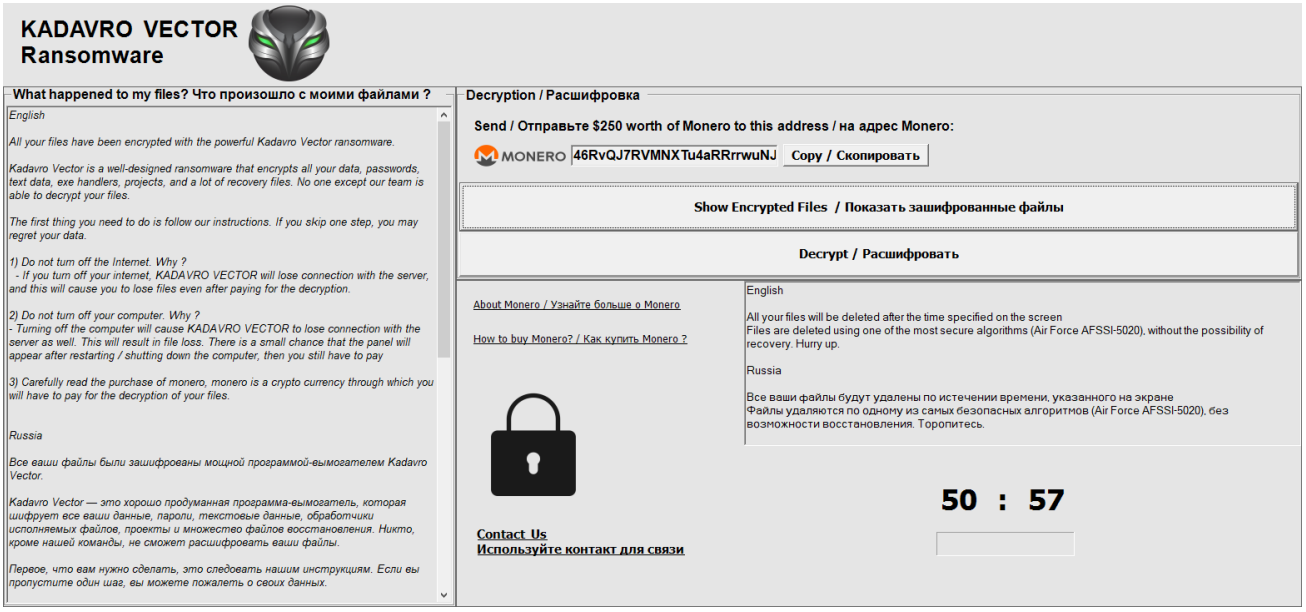

Figure 13. Kadavro ransom note

The ransom note of Kadavro is presented in an interactive format, unlike previous TEXT, HTML,

and HTA formats. The buttons and links on the right-hand panel in the above image are used to provide the list of encrypted files, the file recovery feature, and contact details.

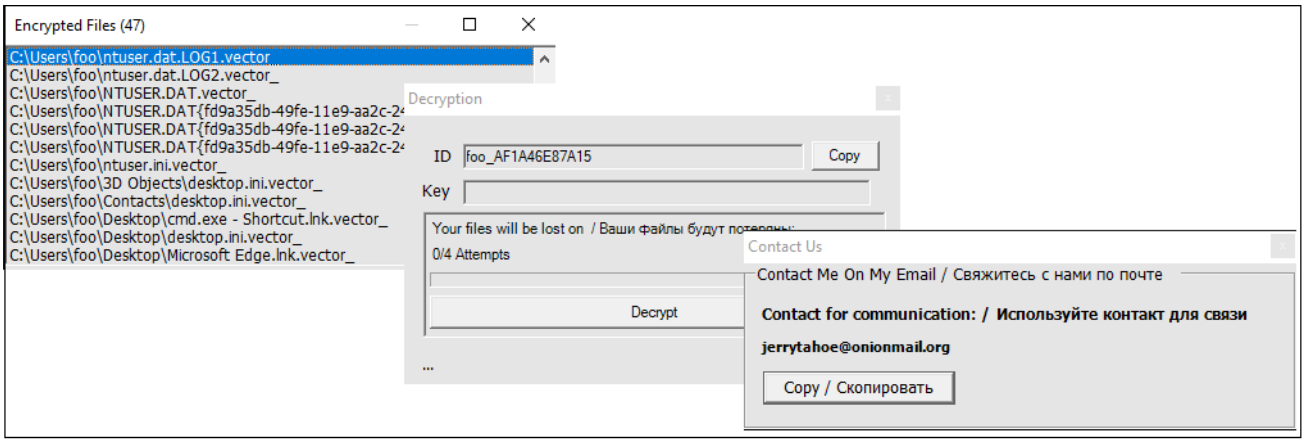

Figure 14. Kadavro ransomware's show enc file, decrypt, and contact menus

A total of four recovery attempts may be made, and when all attempts fail, encrypted files are deleted and the del.vbs script is generated in the %TEMP% folder and executed, deleting itself.

```
On Error Resume Next
WScript.Sleep 2900
CreateObject("Scripting.FileSystemObject").DeleteFile("C:\Users\...\AppData\Local\torbrowser-install-win64-12.0.4_ALL.exe")
CreateObject("Scripting.FileSystemObject").DeleteFile("C:\Users\...\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\g3lvBNlCChHm1YYK.exe")
```

Figure 15. Auto-delete feature of del.vbs

Using file names carefully disguised as those of normal software is a technique not only employed by ransomware but by most malware types such as downloaders, Infostealers, and backdoors. When downloading work or game software in particular, users must check that they are downloading them from the official websites. Other than that, the standard procedure of regular backups and security software installation and update should be performed.

Reference IOC

8dc6ff90357e8e2d598beb83240cefabe22054036ec2e2e91377c7125f8f8b89
39308dee3ad1f5ce7ccc3d52b3783db204d12694d6c00ec7ec301ecb73e7c8b6
b7ca2dde7789da13d1b8729cc26f3d5dc596cbd710306c17ff6eb4ef2d9d1182
b30ef4dbcc89cd4bf0da3e7787f43e42023ddc2b5f0bb4f24937538e10817533

Additional Payloads

124c17b099d8c09db4bd82b5ef3d41cea61727a480abfd56a943208d858ea8cf
e6e62b3fd2be817c41537b9e3244a40b052e78e826b87c77d1bfdfa1644be199
af19fd4147c2253070e345cfcef86b1236c759911ff6b1ef90955d2e86cb8aa4
8ea5398c46a9a53f15d94a6c627ac591aa13bd2f2ac2cd35c9022c8e4dfa43fe

7694bfd321345364659539de8b4664e5d0cba8bc137b007089c63ec12e32f4d9
a076adcf9a2c8298549c22e5059cc5cd90ddc65abadaec417c3dcc74d9ce484b
2ed272aaa05d80a8504772192d5fc99035e5634e8fc306d0a3e09593c466e969

4) Others

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

- New Money Message ransomware demands million dollar ransoms (Apr. 3)
- ALPHV ransomware exploits Veritas Backup Exec bugs for initial access (Apr. 5)
- Medusa ransomware claims attack on Open University of Cyprus (Apr. 7)
- KFC, Pizza Hut owner discloses data breach after ransomware attack (Apr. 11)
- Vice Society ransomware uses new PowerShell data theft tool in attacks (Apr. 15)
- Hackers start abusing Action1 RMM in ransomware attacks (Apr. 16)
- BlackBit Ransomware Being Distributed In Korea (Apr. 20)
- LockBit Ransomware Operators Launch an Attack Targeting Mac Devices (Apr. 17)
- Microsoft SQL servers hacked to deploy Trigona ransomware (Apr. 20)
- Clop, LockBit ransomware gangs behind PaperCut server attacks (Apr. 27)
- Linux version of RTM Locker ransomware targets VMware ESXi servers (Apr. 28)

Conclusion

There are periodic changes in ransomware sample and targeted system numbers according to the success rates of attack campaigns and early infection attempts. As can be seen in the statistics above, these numbers vary between thousands to tens of thousands. After having been attacked by ransomware groups, hundreds of businesses were also posted on DLS.

As can be seen in the trends above, ransomware attack groups actively exploit the vulnerabilities of operating systems used by corporations. In the case of private users, the threat groups take advantage of users' negligence, use malware carefully disguised as normal software, or exploit vulnerabilities that bypass security software. According to the characteristics used in initial infection attempts, corporate and private users are advised to adhere to 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 wary 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.

cy.exe cydump.exe winutils.dll config.ini torbrowser-install-win64-12.0.4_ALL2.exe

2) File Hashes (MD5)

The MD5 of the related files are as follows. However, sensitive samples may have been excluded.

2237ec542cdcd3eb656e86e43b461cd1 - cy.exe (normal) 4a03423c77fe2c8d979caca58a64ad6c - winutils.dll (undisclosed) 6bd96d06cd7c4b084fe9346e55a81cf9 - config.ini (undisclosed) 8280E83A4405420632CCA6FAB9F9584E - winutils.dll

f02ff25c2169c6575bdf3cd6f120c324 - winutils.dll 4b4fd546be8d9f32fb852c000fcc24f7 - winutils.dll 3e3d20f82c4ce395b4a1d1ab60363fc6 - config.ini 8800e6f1501f69a0a04ce709e9fa251c - Nokoyawa ef61b4fcf27afb47000a7e5739f45712 - Kadavro

3) Related 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] research.checkpoint.com: RORSCHACH – A NEW SOPHISTICATED AND FAST RANSOMWARE
[2] www.bleepingcomputer.com: New Rorschach ransomware is the fastest encryptor seen so far
[3] en.wikipedia.org: Rorschach Inkblot Test
[4] www.trendmicro.com: An Analysis of the BabLock (aka Rorschach) Ransomware
[5] www.group-ib.com: BabLock, new ransomware quietly cruising around Europe, Middle East, and Asia
[6] www.bleepingcomputer.com: Windows zero-day vulnerability exploited in ransomware attacks
[7] securelist.com: Nokoyawa ransomware attacks with Windows zero-day
[8] www.wiz.io: Microsoft April 2023 Patch Tuesday Highlights: everything you need to know
[9] www.zscaler.com: Nevada Ransomware: Yet Another Nokoyawa Variant
[10] www.fortinet.com: Ransomware Roundup – Kadavro Vector Ransomware

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
https://www.ahnlab.com
https://asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency response (ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks

AhnLab