AhnLab Cyber Threat Intelligence Report

TLP: GREEN

Threat Trend Report on Ransomware

May 2023 Ransomware Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Jun. 09, 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

⚠ 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 May 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 (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 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 of file detection name

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

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

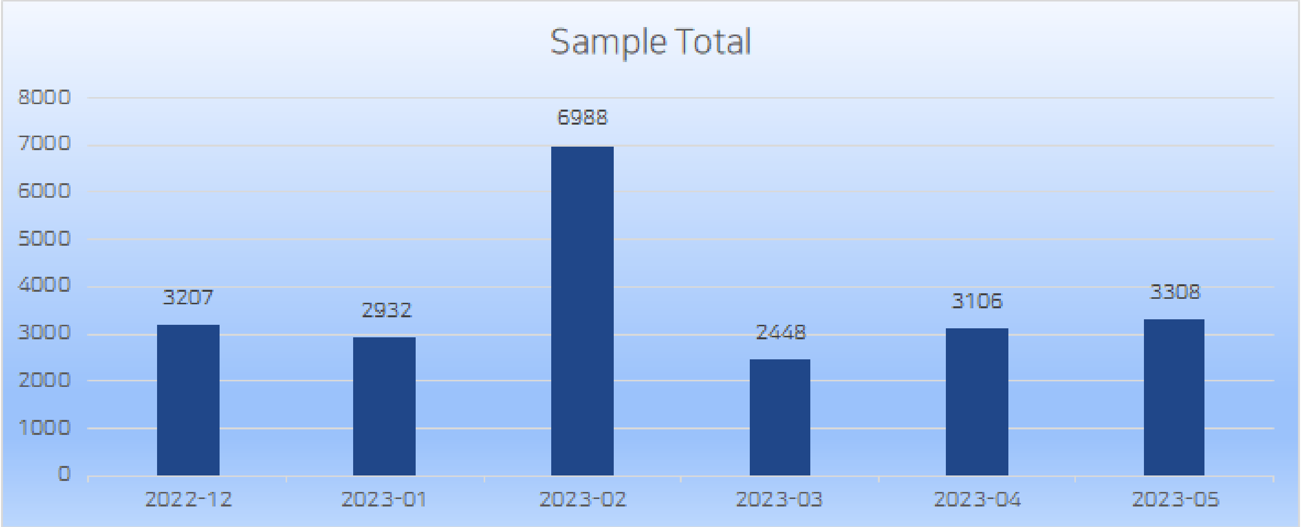


Figure 1. Number of new ransomware samples

Magniber, which displayed a rapid increase in February 2023, has continued to decrease since March. In May, there was a slight increase in the overall number of new samples compared to the previous month, but it remained at a level consistent with the recent average quantity.

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

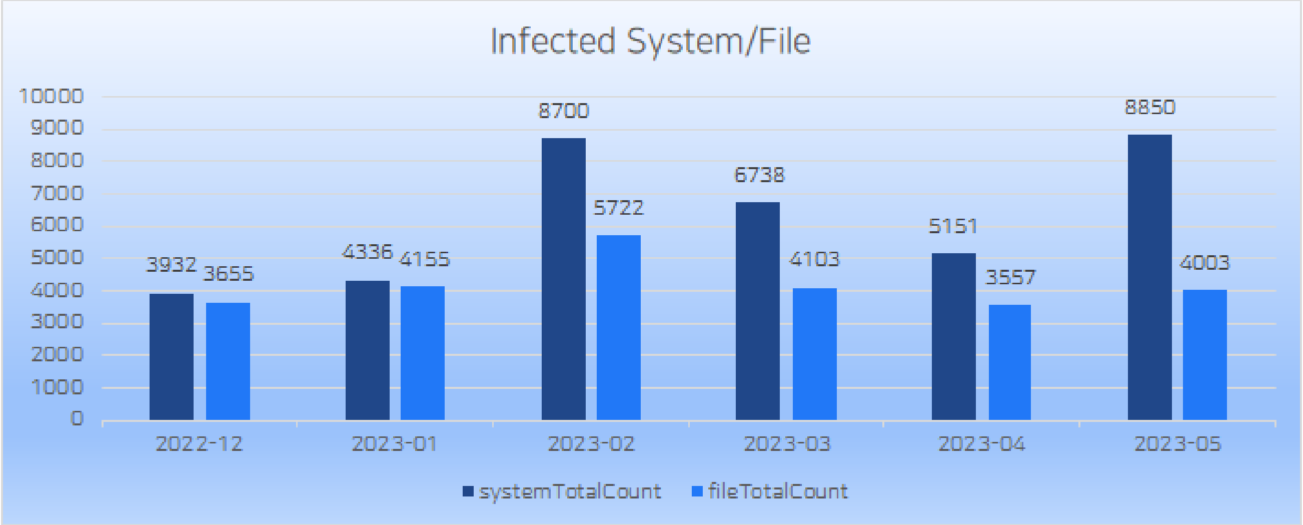


Figure 2. Systems and files affected by ransomware

Unlike the number of new samples, the statistics of targeted systems have shown a similar increase to that observed in February. It has been confirmed that Magniber infection attempts have occurred in multiple endpoint systems.

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

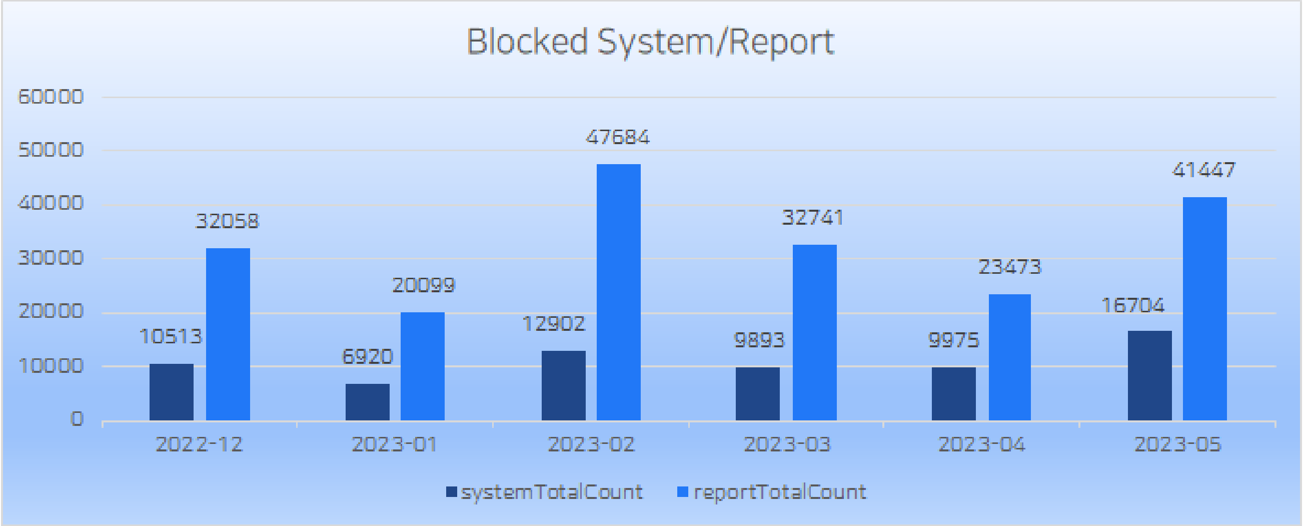


Figure 3. Ransomware behavior detection-based targeted systems and reports

Behavior detection statistics also showed a similar increase compared to the previous month, mirroring the trend observed in the targeted system statistics. The rise in the number of blocking reports indicates active ransomware infection attempts on multiple endpoint systems.

3) New Samples by Ransomware

Below is the statistics showing the 3,308 new samples that were discovered in May organized by ransomware. Only 20 ransomware with the most samples are shown.

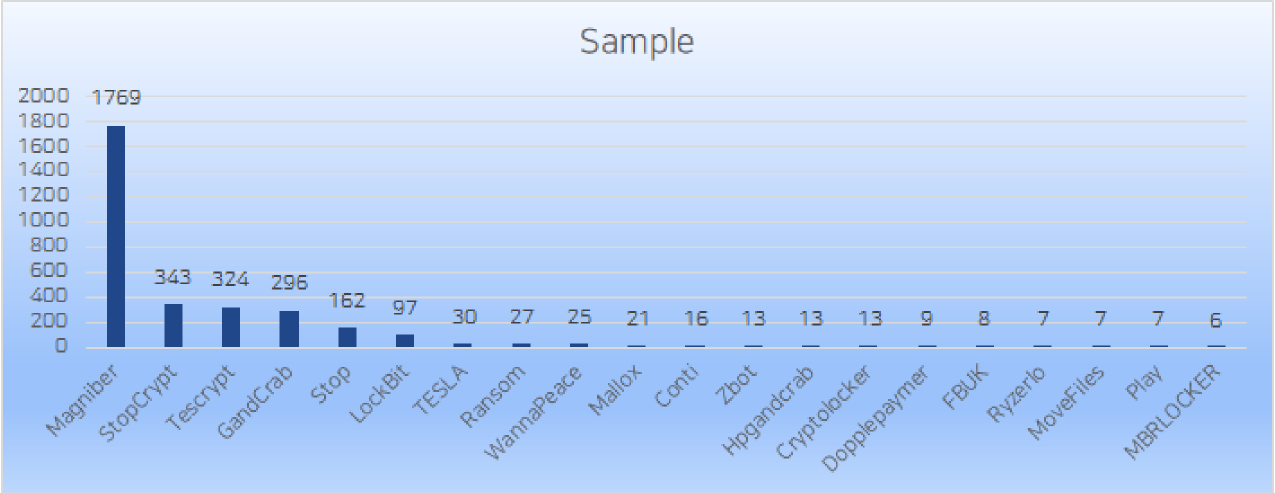


Figure 4. Number of new samples per ransomware (May 2023)

The number of new Magniber samples recorded in the new ransomware sample statistics has increased by approximately 2.5 times, rising from the 700 cases in March and April to its highest figure. The number of StopCrypt, which was over 1,300 cases the previous month, has dramatically decreased. As for other ransomware samples, there have been no significant fluctuations in their new quantity overall.

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).

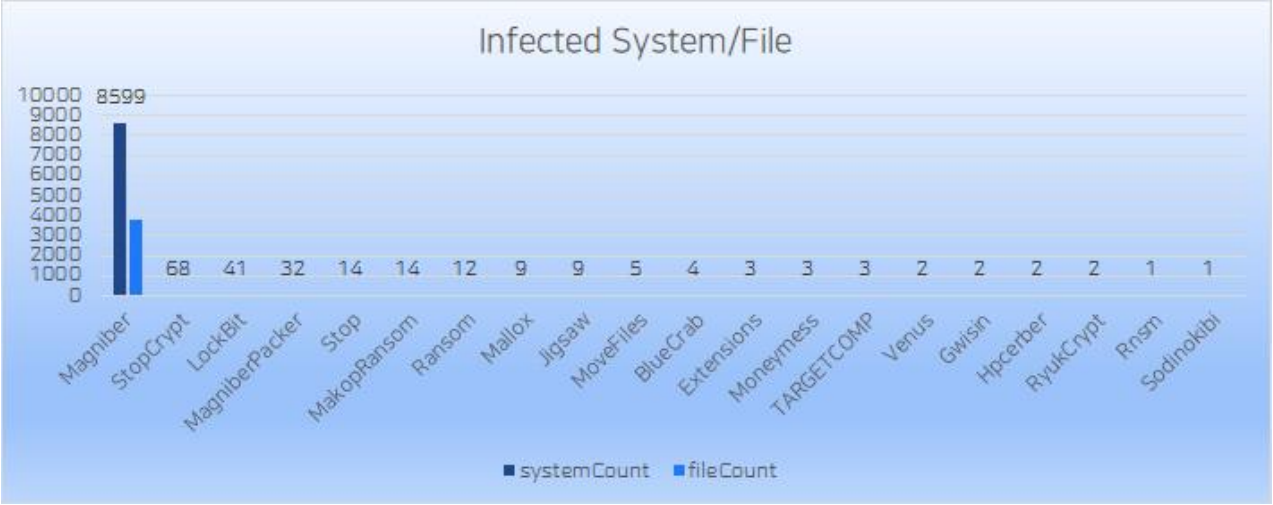


Figure 5. Number of targeted systems and files per ransomware (May 2023)

The number of systems targeted by Magniber has shown a 70% increase compared to the previous month's 5,000, recording the highest number of targeted systems in recent times.

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

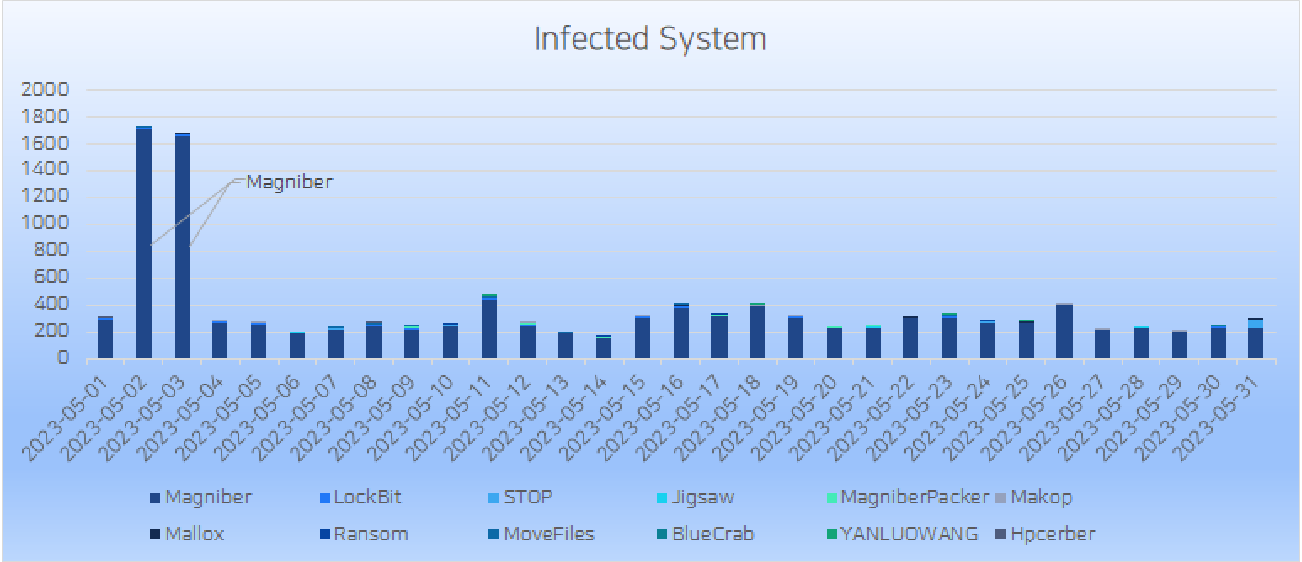


Figure 6. Daily number of targeted systems per ransomware (May 2023)

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, the daily number of systems targeted by Magniber was about 200-300 cases on average. On the other hand, there was an increase in infection through CPL and MSI files disguised with file names such as "Antivirus.System.Update", "Antivirus.Update.Hotfix", "MS.Upgrade.Database.Cloud", and "SYSTEM.Security.Update" on May 5 and 3. There were also LockBit emails involving attachments disguised as "resumes", "job applications", and "guidelines on unauthorized use of licenses", as well as multiple infection attempts by a Jigsaw file disguised as "Windows Update Assistant.exe".

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.

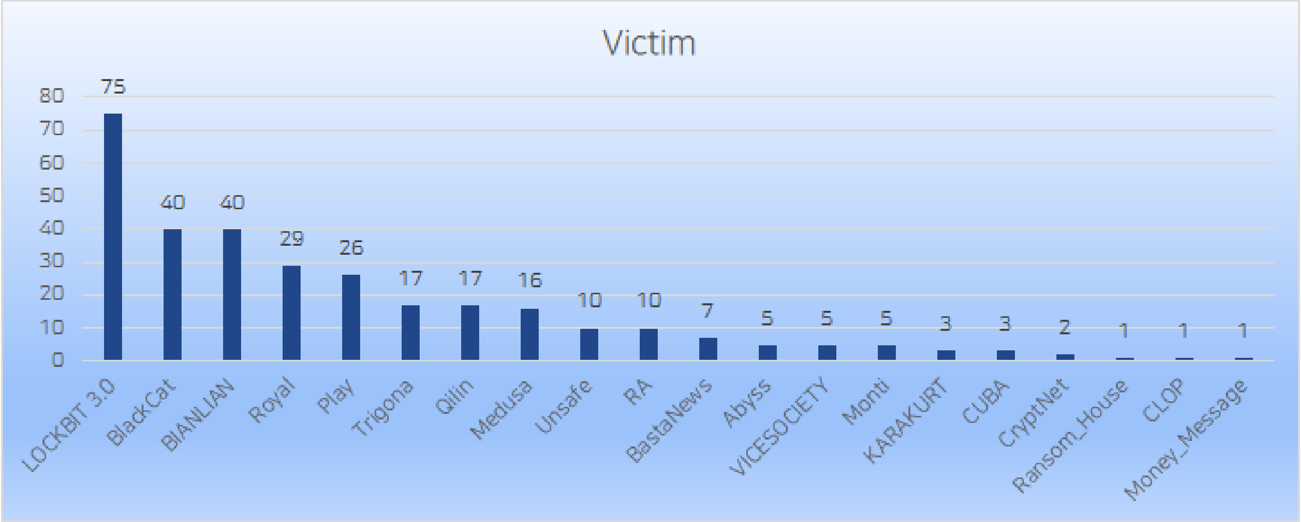
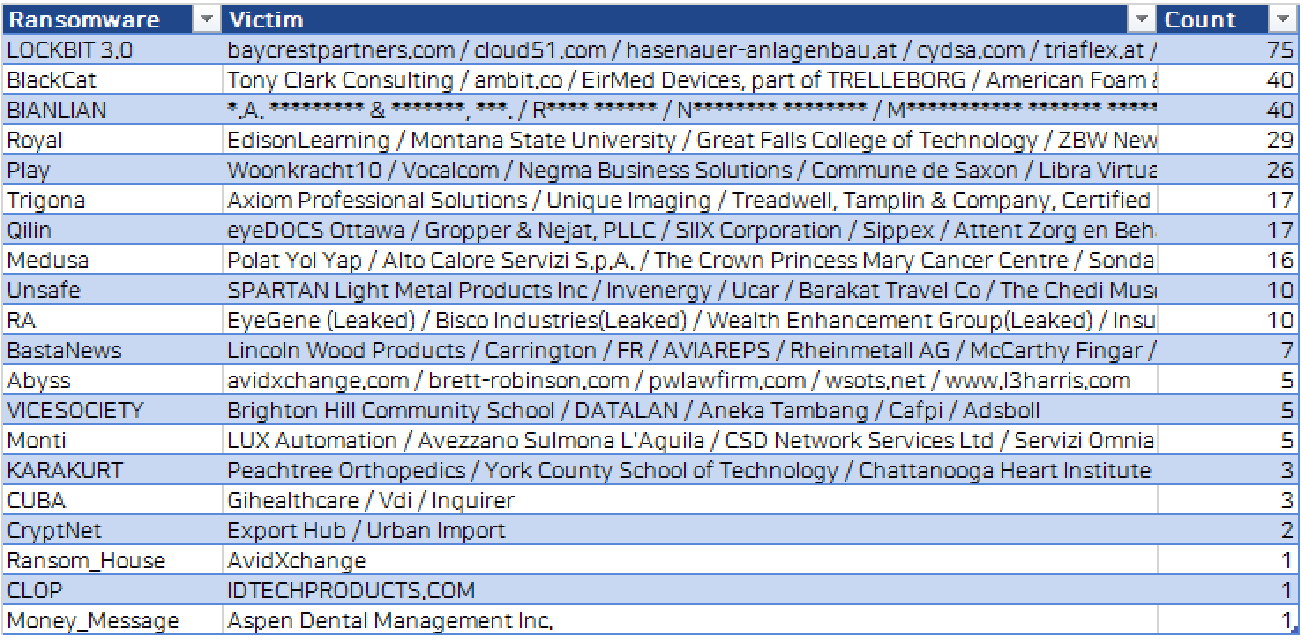


Figure 7. Number of targeted businesses per ransomware group (May 2023)

LOCKBIT 3.0, which was ranked first last month, has seen a slight decrease in the number of targeted businesses that have been disclosed. However, as shown on the DLS, it continues to hold the record for affecting the highest number of businesses. There were no significant changes in the rankings from 2nd to 5th place, and the number of targeted businesses has only slightly increased compared to the previous month.

For reference, it should be noted that the statistics do not include data on the Akira ransomware, which has been active since March 2023. However, its DLS has revealed a total of 29 targeted businesses, with 21 of them being disclosed in May, placing Akira as the 6th highest in terms of the number of targeted businesses.

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



Ransomware	Victim	Count
LOCKBIT 3.0	baycrestpartners.com / cloud51.com / hasenauer-anlagenbau.at / cydsa.com / triaflex.at /	75
BlackCat	Tony Clark Consulting / ambit.co / EirMed Devices, part of TRELLEBORG / American Foam &	40
BIANLIAN	*.A. ********** & *******, ***. / R**** ****** / N********* ********* / M************ ******* *****	40
Royal	EdisonLearning / Montana State University / Great Falls College of Technology / ZBW New	29
Play	Woonkracht10 / Vocalcom / Negma Business Solutions / Commune de Saxon / Libra Virtua	26
Trigona	Axiom Professional Solutions / Unique Imaging / Treadwell, Tamplin & Company, Certified	17
Qilin	eyeDOCS Ottawa / Gropper & Nejat, PLLC / SIIX Corporation / Sippex / Attent Zorg en Beh	17
Medusa	Polat Yol Yap / Alto Calore Servizi S.p.A. / The Crown Princess Mary Cancer Centre / Sonda	16
Unsafe	SPARTAN Light Metal Products Inc / Invenergy / Ucar / Barakat Travel Co / The Chedi Mus	10
RA	EyeGene (Leaked) / Bisco Industries(Leaked) / Wealth Enhancement Group(Leaked) / Insu	10
BastaNews	Lincoln Wood Products / Carrington / FR / AVIAREPS / Rheinmetall AG / McCarthy Fingar /	7
Abyss	avidxchange.com / brett-robinson.com / pwlawfirm.com / wsots.net / www.l3harris.com	5
VICESOCIETY	Brighton Hill Community School / DATALAN / Aneka Tambang / Cafpi / Adsboll	5
Monti	LUX Automation / Avezzano Sulmona L'Aquila / CSD Network Services Ltd / Servizi Omnia	5
KARAKURT	Peachtree Orthopedics / York County School of Technology / Chattanooga Heart Institute	3
CUBA	Gihealthcare / Vdi / Inquirer	3
CryptNet	Export Hub / Urban Import	2
Ransom_House	AvidXchange	1
CLOP	IDTECHPRODUCTS.COM	1
Money_Message	Aspen Dental Management Inc.	1

Table 1. Some of the targeted businesses per ransomware group (May 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. Additionally, the statistics information was not available from the previously used DarkFeed during the creation of this document. Therefore, the source of external statistics has been changed.

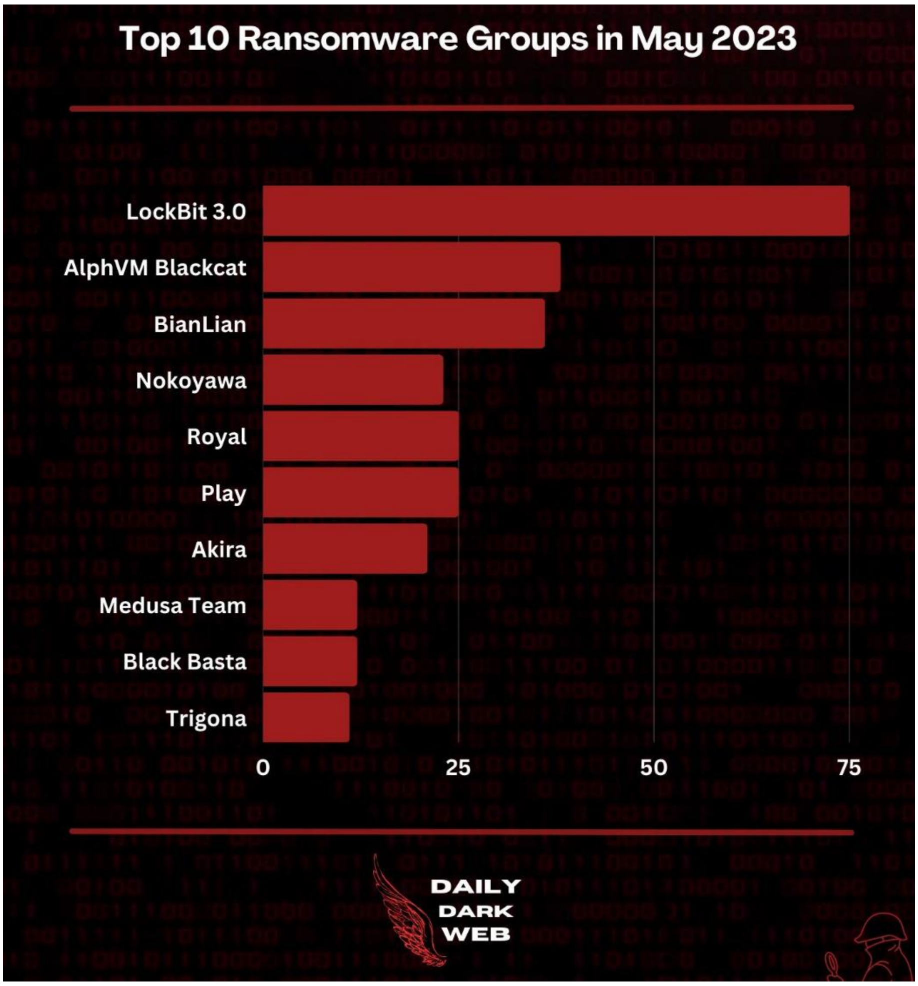


Figure 8. Targeted businesses per ransomware group <Source> dailydarkweb twitter

According to the statistics above, the number of businesses targeted by LOCKBIT 3.0, BlackCat (ALPHV), BianLian, Royal, and Play ransomware groups are generally high.

Key Trends

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

- BianLian ransomware, CISA cybersecurity advisory

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) BianLian Ransomware, CISA Cybersecurity Advisory

The Cybersecurity and Infrastructure Security Agency (CISA) has released a cybersecurity advisory regarding the BianLian ransomware group, in collaboration with the Federal Bureau of Investigation (FBI) and the Australian CyberSecurity Center (ACSC). The advisory includes the indicators of compromise (IOC) and tactics, techniques, and procedures (TTPs) used by the BianLian ransomware group.[1]

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA23-136A

May 16, 2023

ACSC Australian Cyber Security Centre

#StopRansomware: BianLian Ransomware Group

SUMMARY

Note: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and learn more about other ransomware threats and no-cost resources.

Actions to take today to mitigate cyber threats from BianLian ransomware and data extortion:
- Strictly limit the use of RDP and other remote desktop services.
- Disable command-line and scripting activities and permissions.
- Restrict usage of PowerShell and update Windows PowerShell or PowerShell Core to the latest version.

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Australian Cyber Security Centre (ACSC) are releasing this joint Cybersecurity Advisory to disseminate known BianLian ransomware and data extortion group IOCs and TTPs identified through FBI and ACSC investigations as of March 2023.

Figure 9. BianLian cybersecurity advisory <Source> www.cisa.gov

(1) BianLian Ransomware, IOC (Overview, Symptoms, Recovery)

The BianLian cybersecurity advisory, as part of the #StopRansomware program, aims to provide security managers with relevant information to strengthen their defense capabilities against the BianLian ransomware and similar threats. Please refer to the following pages for the original text of the BianLian cybersecurity advisory and related details.

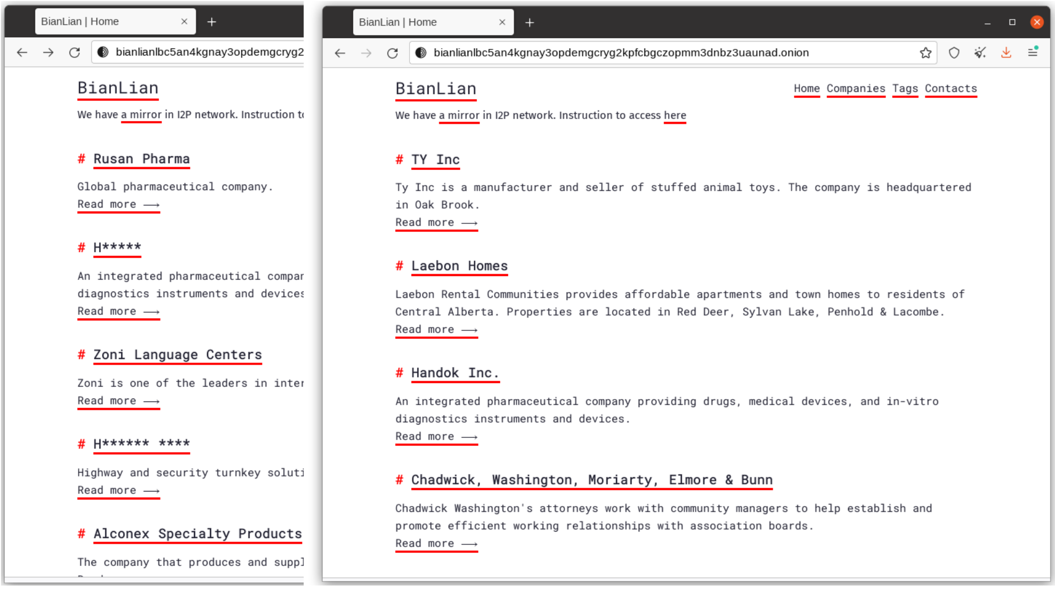
- www.cisa.gov: #StopRansomware: BianLian Ransomware Group
- www.cisa.gov: #StopRansomware: BianLian Ransomware Group (PDF)
- www.bleepingcomputer.com: FBI confirms BianLian ransomware switch to extortion only attacks

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a

- www.boannews.com: BianLian Ransomware Infection Occurring via Remote Desktop Service

The BianLian ransomware was first discovered on December 2021 and was later brought to the attention of the security community by the US cybersecurity company "Redacted." The identity of the group behind the ransomware remains unclear, and it is uncertain whether the group is the rebranding of another ransomware group. They conduct targeted attacks across various industries and publish the targeted business' information on DLS operated by the ransomware group.

The BianLian ransomware is written in the Go programming language. Starting from January 2023, the BianLian ransomware group has changed their tactics from double extortion, which involved both encryption and data exfiltration, to a tactic focused solely on data exfiltration. To hinder security researchers and companies from analyzing targeted businesses through DLS monitoring, segments of business names are masked with '*'. This can also be seen in the "Table 1. Targeted businesses per ransomware group" section of this report, and the image below shows targeted company names masked as '*' on the recent BianLian DLS. When negotiations with a targeted company fails or no response is received, the '*' are gradually removed over time to pressure the company, disclosing the full company name at the end.



BianLian | Home

bianlianlbc5an4kgnay3opdemgcryg2

BianLian

We have a mirror in I2P network. Instruction t

Rusan Pharma

Global pharmaceutical company.

Read more ⟶

H*****

An integrated pharmaceutical compar
diagnostics instruments and devices

Read more ⟶

Zoni Language Centers

Zoni is one of the leaders in inter

Read more ⟶

H****** ****

Highway and security turnkey soluti

Read more ⟶

Alconex Specialty Products

The company that produces and suppl

BianLian | Home

bianlianlbc5an4kgnay3opdemgcryg2kpfcbgczopmm3dnbz3uaunad.onion

BianLian

Home Companies Tags Contacts

We have a mirror in I2P network. Instruction to access here

TY Inc

Ty Inc is a manufacturer and seller of stuffed animal toys. The company is headquartered in Oak Brook.

Read more ⟶

Laebon Homes

Laebon Rental Communities provides affordable apartments and town homes to residents of Central Alberta. Properties are located in Red Deer, Sylvan Lake, Penhold & Lacombe.

Read more ⟶

Handok Inc.

An integrated pharmaceutical company providing drugs, medical devices, and in-vitro diagnostics instruments and devices.

Read more ⟶

Chadwick, Washington, Moriarty, Elmore & Bunn

Chadwick Washington's attorneys work with community managers to help establish and promote efficient working relationships with association boards.

Read more ⟶

Figure 10. DLS of BianLian ransomware (May 24, June 2)

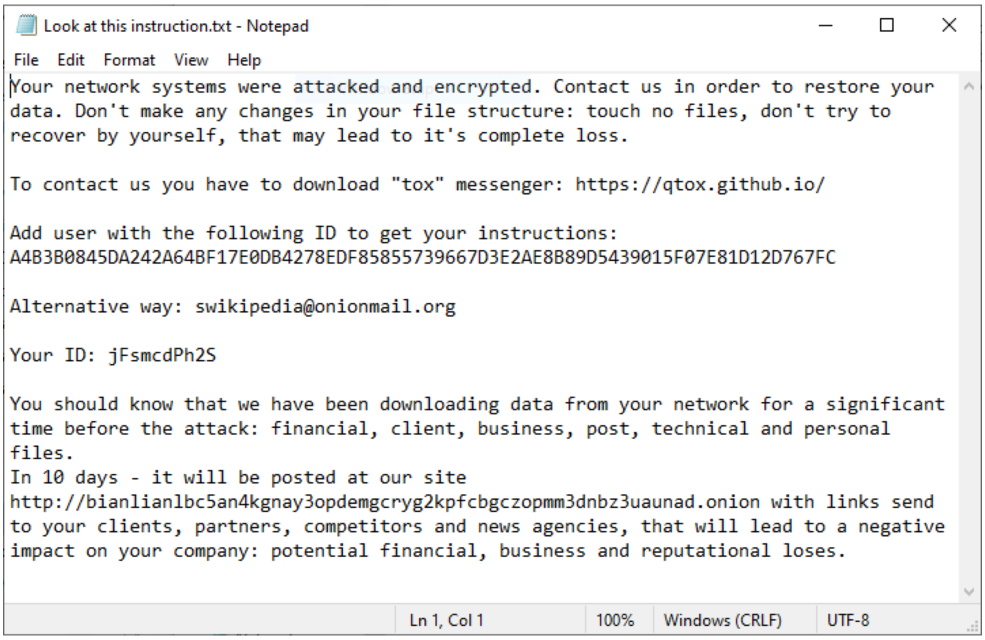
On May 24, a Korean pharmaceutical company was identified as a victim of the BianLian ransomware group through AhnLab's Deep & DarkWeb monitoring system. In response, a customer notice was posted on ATIP Notes. Through an update on June 2, it was confirmed that the BianLian ransomware group removed the '*' and publicly disclosed the full name of the targeted business. Additionally, they exposed the names, personal information, and leaked data of top-level executives. [2]

The IOCs provided in the BianLian cybersecurity advisory are as follows.

Name	SHA-256 Hash	Description
def.exe	7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893	Malware associated with BianLian intrusions, which is an example of a possible backdoor developed by BianLian group.
encryptor.exe	1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43	Example of a BianLian encryptor.
exp.exe	0c1eb11de3a533689267ba075e49d93d55308525c04d6aff0d2c54d1f52f5500	Possible NetLogon vulnerability (CVE-2020-1472) exploitation.
system.exe	40126ae71b857dd22db39611c25d3d5dd0e60316b72830e930fba9baf23973ce	Enumerates registry and files. Reads clipboard data.

Table 2. BianLian-related IOCs <Source> www.cisa.gov

In systems infected with the BianLian ransomware, the ransom note displayed to users by the encryptor.exe contains instructions to contact the threat actors via Tox messenger and includes a threatening message stating that the information will be publicly disclosed on the DLS after a certain period of time.

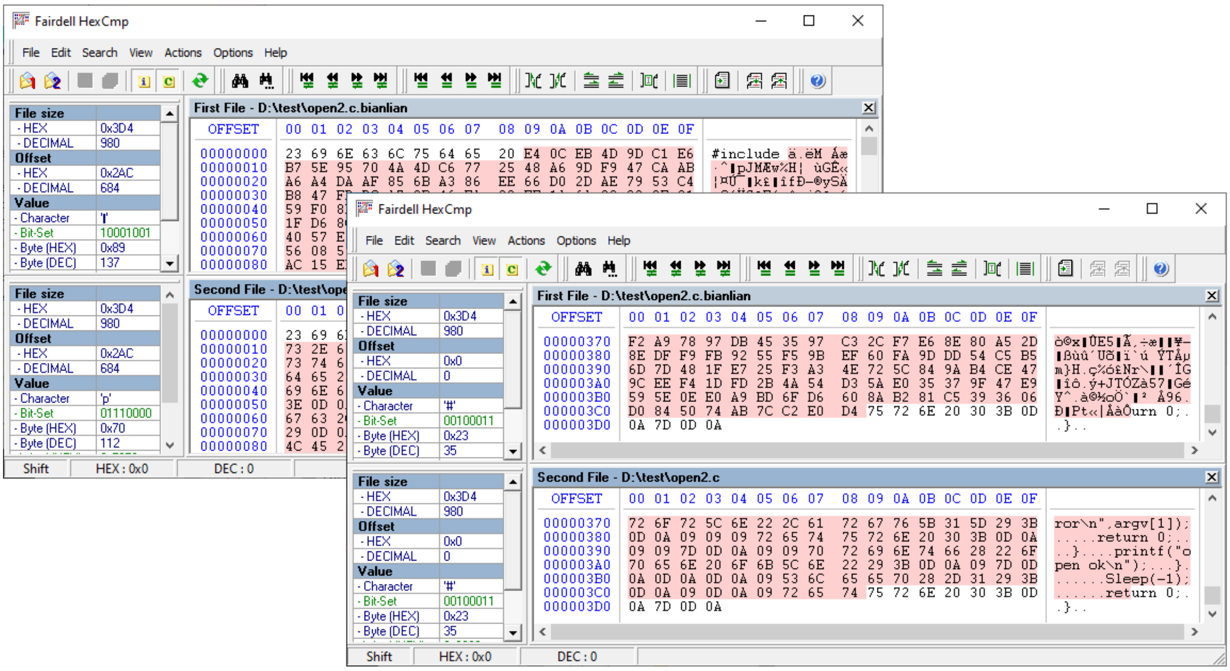

Look at this instruction.txt - Notepad
File Edit Format View Help
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8

```
Your network systems were attacked and encrypted. Contact us in order to restore your
data. Don't make any changes in your file structure: touch no files, don't try to
recover by yourself, that may lead to it's complete loss.

To contact us you have to download "tox" messenger: https://qtox.github.io/

Add user with the following ID to get your instructions:
A4B3B0845DA242A64BF17E0DB4278EDF85855739667D3E2AE8B89D5439015F07E81D12D767FC

Alternative way: swikipedia@onionmail.org

Your ID: jFsmcdPh2S

You should know that we have been downloading data from your network for a significant
time before the attack: financial, client, business, post, technical and personal
files.
In 10 days - it will be posted at our site
http://bianlianlbc5an4kgnay3opdemgcryg2kpfcbgczopmm3dnbz3uaunad.onion with links send
to your clients, partners, competitors and news agencies, that will lead to a negative
impact on your company: potential financial, business and reputational loses.
```

[2] https://atip.ahnlab.com/ti/contents/asec-notes?i=3a7e9907-b07b-4a72-8772-333de91e7836

Figure 11. Ransom note from BianLian ransomware

Within the encryptor.exe, there are reference codes for RSA and elliptic curve cryptography-related libraries, but in actual operation, they are not utilized. Instead, the targeted files are encrypted using AES-256 CBC mode. The BianLian ransomware also does not encrypt files from the beginning, nor does it encrypt files all the way to the end. The ransomware binary contains a hard-coded fixed file offset. When looking at a simple C language source code file that was encrypted in a test environment, it can be observed below that the encryption starts at the 9th byte.



```
First File - D:\test\open2.c.bianlian
OFFSET    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F
00000000  23 69 6E 63 6C 75 64 65  20 E4 0C EB 4D 9D C1 E6   #include ä.ëM Áæ
00000010  B7 5E 95 70 4A 4D C6 77  25 48 A6 9D F9 47 CA AB   ·^▮pJMÆw%H¦ ùGÊ«
00000020  A6 A4 DA AF 85 6B A3 86  EE 66 D0 2D AE 79 53 C4   ¦¤Ú¯▮k£▮îfÐ-®ySÄ
00000030  B8 47 F
00000040  59 F0 8
00000050  1F D6 8
00000060  40 57 E
00000070  56 08 5
00000080  AC 15 E

Second File - D:\test\ope
OFFSET    00 01 0
00000000  23 69 6
00000010  73 2E 6
00000020  73 74 6
00000030  64 65 2
00000040  69 6E 6
00000050  3E 0D 0
00000060  67 63 2
00000070  29 0D 0
00000080  4C 45 2
```

```
File size  - HEX 0x3D4  - DECIMAL 980
Offset     - HEX 0x2AC  - DECIMAL 684
Value      - Character 'I'  - Bit-Set 10001001  - Byte (HEX) 0x89  - Byte (DEC) 137

File size  - HEX 0x3D4  - DECIMAL 980
Offset     - HEX 0x2AC  - DECIMAL 684
Value      - Character 'p'  - Bit-Set 01110000  - Byte (HEX) 0x70  - Byte (DEC) 112

Shift    HEX : 0x0    DEC : 0
```

```
First File - D:\test\open2.c.bianlian
OFFSET    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F
00000370  F2 A9 78 97 DB 45 35 97  C3 2C F7 E6 8E 80 A5 2D   ò©x▮ÛE5▮Ã,÷æ▮▮¥-
00000380  8E DF F9 FB 92 55 F5 9B  EF 60 FA 9D DD 54 C5 B5   ▮ßùû'Uõ▮ï`ú ÝTÅµ
00000390  6D 7D 48 1F E7 25 F3 A3  4E 72 5C 84 9A B4 CE 47   m}H.ç%ó£Nr\▮▮´ÎG
000003A0  9C EE F4 1D FD 2B 4A 54  D3 5A E0 35 37 9F 47 E9   ▮îô.ý+JTÓZà57▮Gé
000003B0  59 5E 0E E0 A9 BD 6F D6  60 8A B2 81 C5 39 36 06   Y^.à©½oÖ`▮² Å96.
000003C0  D0 84 50 74 AB 7C C2 E0  D4 75 72 6E 20 30 3B 0D   Ð▮Pt«|ÂàÔurn 0;.
000003D0  0A 7D 0D 0A                                        .}..

Second File - D:\test\open2.c
OFFSET    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F
00000370  72 6F 72 5C 6E 22 2C 61  72 67 76 5B 31 5D 29 3B   ror\n",argv[1]);
00000380  0D 0A 09 09 09 72 65 74  75 72 6E 20 30 3B 0D 0A   .....return 0;..
00000390  09 09 7D 0D 0A 09 09 70  72 69 6E 74 66 28 22 6F   ..}....printf("o
000003A0  70 65 6E 20 6F 6B 5C 6E  22 29 3B 0D 0A 09 7D 0D   pen ok\n");...}.
000003B0  0A 0D 0A 0D 0A 09 53 6C  65 65 70 28 2D 31 29 3B   ......Sleep(-1);
000003C0  0D 0A 09 0D 0A 09 72 65  74 75 72 6E 20 30 3B 0D   ......return 0;.
000003D0  0A 7D 0D 0A                                        .}..
```

```
File size  - HEX 0x3D4  - DECIMAL 980
Offset     - HEX 0x0    - DECIMAL 0
Value      - Character '#'  - Bit-Set 00100011  - Byte (HEX) 0x23  - Byte (DEC) 35

File size  - HEX 0x3D4  - DECIMAL 980
Offset     - HEX 0x0    - DECIMAL 0
Value      - Character '#'  - Bit-Set 00100011  - Byte (HEX) 0x23  - Byte (DEC) 35

Shift    HEX : 0x0    DEC : 0
```

Figure 12. Comparison of file encrypted by BianLian (start and end of file)

Since the symmetric key encryption method, AES-256 CBC mode, is used, it is possible to recover the encrypted files if both the ransomware binary used for infection and the original unencrypted versions of the files are available. AVAST released a decryption tool for BianLian ransomware on January 16.[3]

It is not common for ransomware decryption tools to be provided, but searches can be performed on the following websites to check if useful information is available.

- www.nomoreransom.org: NO MORE RANSOM Decryption Tools
- seed.kisa.or.kr: Search page for KISA ransomware recovery tools

[3] https://decoded.avast.io/threatresearch/decrypted-bianlian-ransomware/

The BianLian ransomware group is known to utilize compromised Remote Desktop Protocol (RDP) credentials obtained through initial access brokers (IAB) or network access privilege acquired through phishing attacks. They are also reported to exploit the CVE-2020-1472 vulnerability for privilege escalation purposes. Please refer to the following ATIP vulnerability report for more details on the CVE-2020-1472 vulnerability, also referred to as 'Zerologon'.

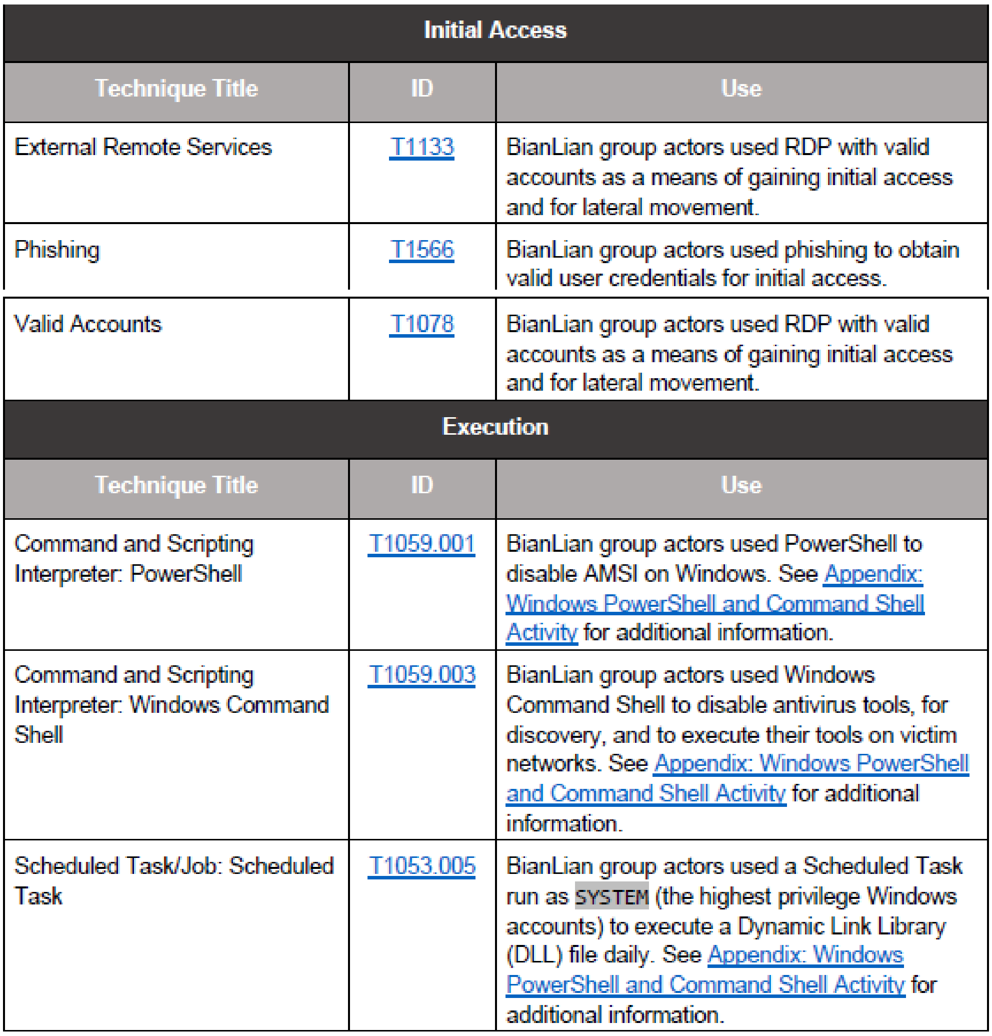
- atip.ahnlab.com: Analysis Report on CVE-2020-1472 Vulnerability (This report supports Korean only for now)

Reference IOCs

7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893
1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43
0c1eb11de3a533689267ba075e49d93d55308525c04d6aff0d2c54d1f52f5500
40126ae71b857dd22db39611c25d3d5dd0e60316b72830e930fba9baf23973ce

(2) BianLian Ransomware, TTP and IOA

The "Technical Details" and "MITRE ATT&CK Techniques" sections of the BianLian cybersecurity advisory provide the TTP based on framework version 13 of MITRE ATT&CK ® for Enterprise.



Initial Access

Technique Title	ID	Use
External Remote Services	T1133	BianLian group actors used RDP with valid accounts as a means of gaining initial access and for lateral movement.
Phishing	T1566	BianLian group actors used phishing to obtain valid user credentials for initial access.
Valid Accounts	T1078	BianLian group actors used RDP with valid accounts as a means of gaining initial access and for lateral movement.

Execution

Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001	BianLian group actors used PowerShell to disable AMSI on Windows. See Appendix: Windows PowerShell and Command Shell Activity for additional information.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	BianLian group actors used Windows Command Shell to disable antivirus tools, for discovery, and to execute their tools on victim networks. See Appendix: Windows PowerShell and Command Shell Activity for additional information.
Scheduled Task/Job: Scheduled Task	T1053.005	BianLian group actors used a Scheduled Task run as `SYSTEM` (the highest privilege Windows accounts) to execute a Dynamic Link Library (DLL) file daily. See Appendix: Windows PowerShell and Command Shell Activity for additional information.

Table 3. Some of the BianLian-related TTP <Source> www.cisa.gov

The MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) framework was initiated in 2013 by MITRE as a project to document and classify threat actors' tactics, techniques, and procedures (TTP) based on real security issues. On April 25, 2023, it was updated to ATT&CK v13. MITRE ATT&CK has been evolving to adapt to the threat landscape and has become a crucial point of reference and evaluation criteria for the security industry in understanding threat actor models, methodologies, and mitigation methods.

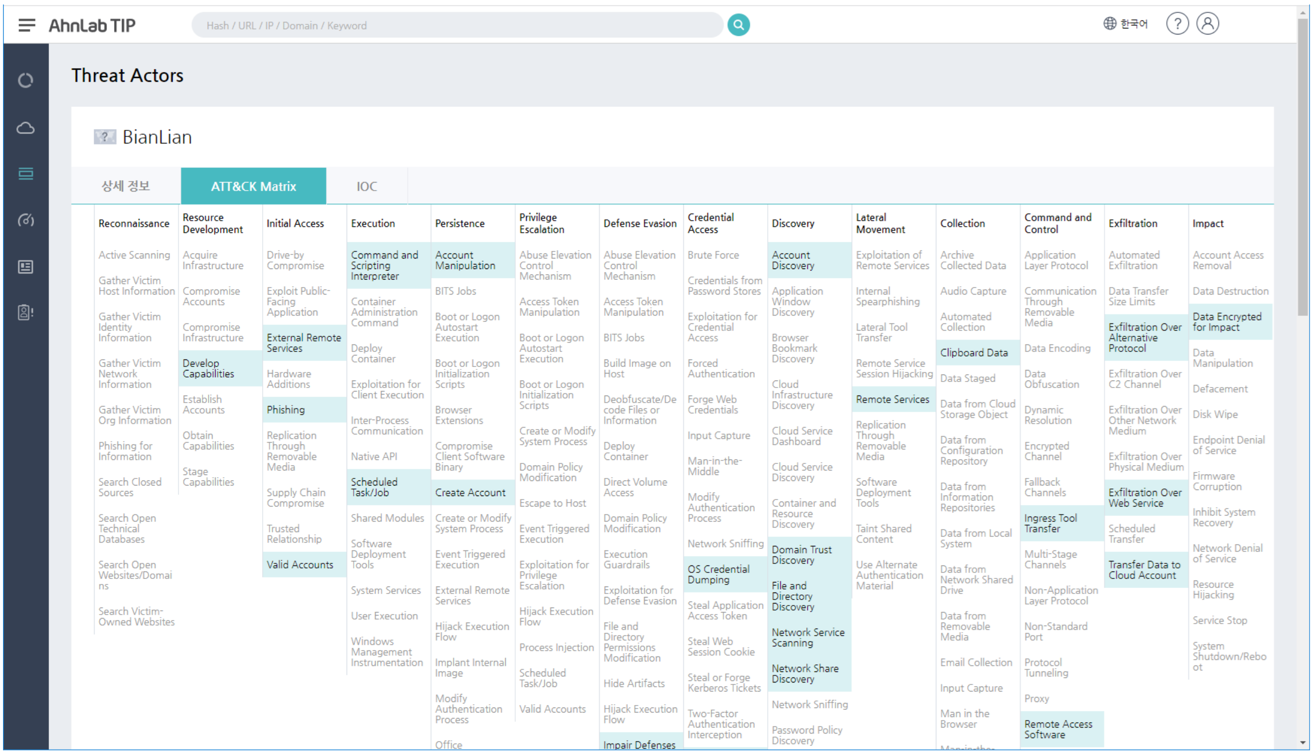
The ATT&CK framework focuses on how external threat actors infiltrate and operate within the systems or networks of organizations or individuals, with an emphasis on their objectives, behaviors, and intentions. The core elements that constitute the ATT&CK framework include the following behavior model named Tactics, Techniques, Procedures (TTP).

- Tactics - Short-term and tactical objectives of the threat actor.
- Techniques - Methods employed by the threat actor to achieve tactical objectives.

- Procedures - The threat actor's use of techniques, procedures, and other metadata.

Although ATT&CK does not provide the TTP of all attacks, it is recommended to actively refer to it when provided in security advisories and similar sources to review whether there are any points that can be utilized for defensive evaluations in one's own environment. For more details on MITRE ATT&CK, please refer to https://attack.mitre.org/.

ATIP also provides the TTP information for the BianLian ransomware group in a MITRE ATT&CK Matrix format through the "Threat Actors" menu.[4]



Threat Actors

BianLian

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Dashboard	Remote Services	Data Staged	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Deploy Container	Input Capture	Cloud Service Discovery	Replication Through Removable Media	Data from Cloud Storage Object	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Direct Volume Access	Man-in-the-Middle	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Domain Policy Modification	Modify Authentication Process	Domain Trust Discovery	Taint Shared Content	Data from Information Repositories	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Execution Guardrails	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material	Data from Local System	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services	External Remote Services	Hijack Execution Flow	Exploitation for Defense Evasion	OS Credential Dumping	Network Service Scanning		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service
			User Execution	Hijack Execution Flow	Process Injection	File and Directory Permissions Modification	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job	Hide Artifacts	Steal Web Session Cookie	Network Sniffing		Email Collection	Protocol Tunneling		Service Stop
				Modify Authentication Process	Valid Accounts	Hijack Execution Flow	Steal or Forge Kerberos Tickets	Password Policy Discovery		Input Capture	Proxy		System Shutdown/Reboot
				Office		Impair Defenses	Two-Factor Authentication Interception			Man in the Browser	Remote Access Software		
										Man-in-the-			

Figure 13. BianLian ATT&CK Matrix in the ATIP "Threat Actors" menu

The MITRE ATT&CK Matrix is used for strengthening cybersecurity intelligence, improving security response capabilities, and establishing standards for internal and external communication. Above all, it serves as a valuable reference for constructing breach and attack simulation (BAS) scenarios, which are essential for security assessments.

With a focus on the threat actors' objectives, behaviors, and intentions, the MITRE ATT&CK Matrix categorizes and enumerates the 14 tactics employed by the threat actors to achieve their objectives by Technique ID or Sub-TID. By referring to real-world cases or creating new

[4] https://atip.ahnlab.com/ti/contents/threat-actor/detail?tagSeq=25334

scenarios that incorporate context and timing information, the ATT&CK Matrix can be used to construct BAS scenarios for security assessments within an organization. The attack indicators in this context are called indicator of attack (IOA). IOAs can been seen as contrasting or supplementing concepts to IOCs which are static and discovered after an attacks.

Therefore, IOAs primarily prioritize the real-time detection of the intent threat actors seek to achieve, independent of specific indicators like malware hashes, IP addresses, or URLs. The main emphasis is on disrupting the continuity of attacks by identifying the threat actors' underlying intents. A segment or entirety of the TTP that is discovered from the whole breach or a specific malware can be formed into rules/scenarios and used in the security assessments or evaluations of individual or organization systems.

If organizations operate red teams, blue teams, or separate analysis/response teams, they may have access to commercial programs for conducting BAS. However, even in situations where such resources are not available, various open-source attack simulations can be utilized. For further review of available attack simulations, you can refer to the pentestit.com page.

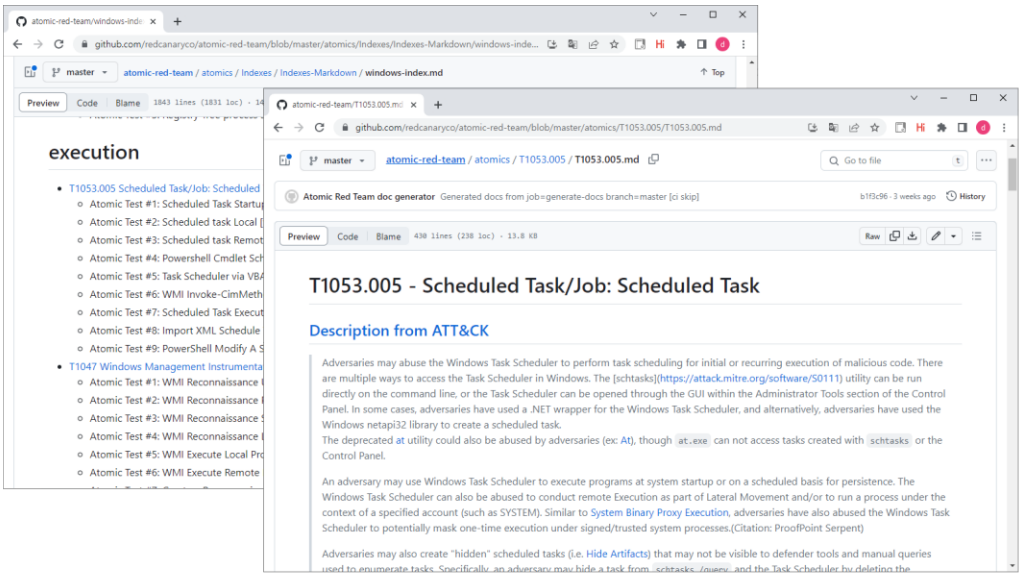
(3) BianLian Ransomware, Attack Simulation Example

"Atomic Red Team", an open-source attack simulation provided by Red Canary, was released in 2017 and provides a test scenario mapped to the MITRE ATT&CK framework which allows a singular (Atomic) TTP attack test to be performed. "Atomic Red Team" is not inherently automated, but by utilizing the accompanying PowerShell module called "Invoke-AtomicRedTeam", you can expand a single test into a sequence of scenario-based tests. Please refer to the following pages for more details.

- github.com: Atomic Red Team
- github.com: Invoke-AtomicRedTeam

A brief example will be given here on how to utilize the "Atomic Red Team" attack simulation on the "Execution" tactic, T1053.005 (Scheduled Task/Job: Scheduled Task), which is one of the BianLian ransomware group's TTPs.

The overall flow of the test starts by selecting the appropriate platform in the "Choose a test" section on the Getting started page. For BianLian, since the attack platform is Windows, you would select Tests for Windows and search for the desired TID (T1053.005) for testing. Then, you would navigate to the "Atomic Red Team" attack simulation page provided within the "atomics" subfolder.



github.com/redcanaryco/atomic-red-team/blob/master/atomics/Indexes/Indexes-Markdown/windows-inde...

atomic-red-team / atomics / Indexes / Indexes-Markdown / windows-index.md

1843 lines (1831 loc) · 14

execution

- T1053.005 Scheduled Task/Job: Scheduled
  - Atomic Test #1: Scheduled Task Startu
  - Atomic Test #2: Scheduled task Local [
  - Atomic Test #3: Scheduled task Remot
  - Atomic Test #4: Powershell Cmdlet Sch
  - Atomic Test #5: Task Scheduler via VBA
  - Atomic Test #6: WMI Invoke-CimMeth
  - Atomic Test #7: Scheduled Task Execut
  - Atomic Test #8: Import XML Schedule
  - Atomic Test #9: PowerShell Modify A S
- T1047 Windows Management Instrumenta
  - Atomic Test #1: WMI Reconnaissance
  - Atomic Test #2: WMI Reconnaissance
  - Atomic Test #3: WMI Reconnaissance
  - Atomic Test #4: WMI Reconnaissance
  - Atomic Test #5: WMI Execute Local Pr
  - Atomic Test #6: WMI Execute Remote

github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1053.005/T1053.005.md

atomic-red-team / atomics / T1053.005 / T1053.005.md

Atomic Red Team doc generator Generated docs from job=generate-docs branch=master [ci skip] b1f3c96 · 3 weeks ago History

430 lines (238 loc) · 13.8 KB

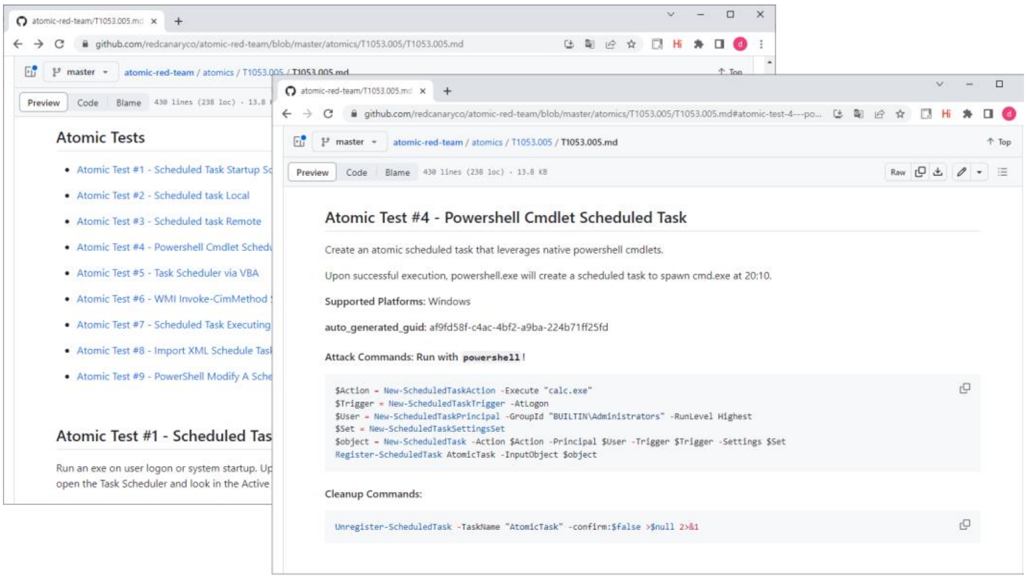
T1053.005 - Scheduled Task/Job: Scheduled Task

Description from ATT&CK

> Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The [schtasks](https://attack.mitre.org/software/S0111) utility can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel. In some cases, adversaries have used a .NET wrapper for the Windows Task Scheduler, and alternatively, adversaries have used the Windows netapi32 library to create a scheduled task.
> The deprecated at utility could also be abused by adversaries (ex: At), though `at.exe` can not access tasks created with `schtasks` or the Control Panel.
>
> An adversary may use Windows Task Scheduler to execute programs at system startup or on a scheduled basis for persistence. The Windows Task Scheduler can also be abused to conduct remote Execution as part of Lateral Movement and/or to run a process under the context of a specified account (such as SYSTEM). Similar to System Binary Proxy Execution, adversaries have also abused the Windows Task Scheduler to potentially mask one-time execution under signed/trusted system processes.(Citation: ProofPoint Serpent)
>
> Adversaries may also create "hidden" scheduled tasks (i.e. Hide Artifacts) that may not be visible to defender tools and manual queries used to enumerate tasks. Specifically, an adversary may hide a task from `schtasks /query` and the Task Scheduler by deleting the

Figure 14. Atomic Red Team - Tests for Windows

The same result can be achieved by directly searching for the TID (T1053.005) for testing from the atomics page.



github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1053.005/T1053.005.md

atomic-red-team / atomics / T1053.005 / T1053.005.md

430 lines (238 loc) · 13.8

Atomic Tests

- Atomic Test #1 - Scheduled Task Startup Sc
- Atomic Test #2 - Scheduled task Local
- Atomic Test #3 - Scheduled task Remote
- Atomic Test #4 - Powershell Cmdlet Sched
- Atomic Test #5 - Task Scheduler via VBA
- Atomic Test #6 - WMI Invoke-CimMethod
- Atomic Test #7 - Scheduled Task Executing
- Atomic Test #8 - Import XML Schedule Tas
- Atomic Test #9 - PowerShell Modify A Sche

Atomic Test #1 - Scheduled Tas

Run an exe on user logon or system startup. Up open the Task Scheduler and look in the Active

github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1053.005/T1053.005.md#atomic-test-4---po...

atomic-red-team / atomics / T1053.005 / T1053.005.md

430 lines (238 loc) · 13.8 KB

Atomic Test #4 - Powershell Cmdlet Scheduled Task

Create an atomic scheduled task that leverages native powershell cmdlets.

Upon successful execution, powershell.exe will create a scheduled task to spawn cmd.exe at 20:10.

Supported Platforms: Windows

auto_generated_guid: af9fd58f-c4ac-4bf2-a9ba-224b71ff25fd

Attack Commands: Run with `powershell`!

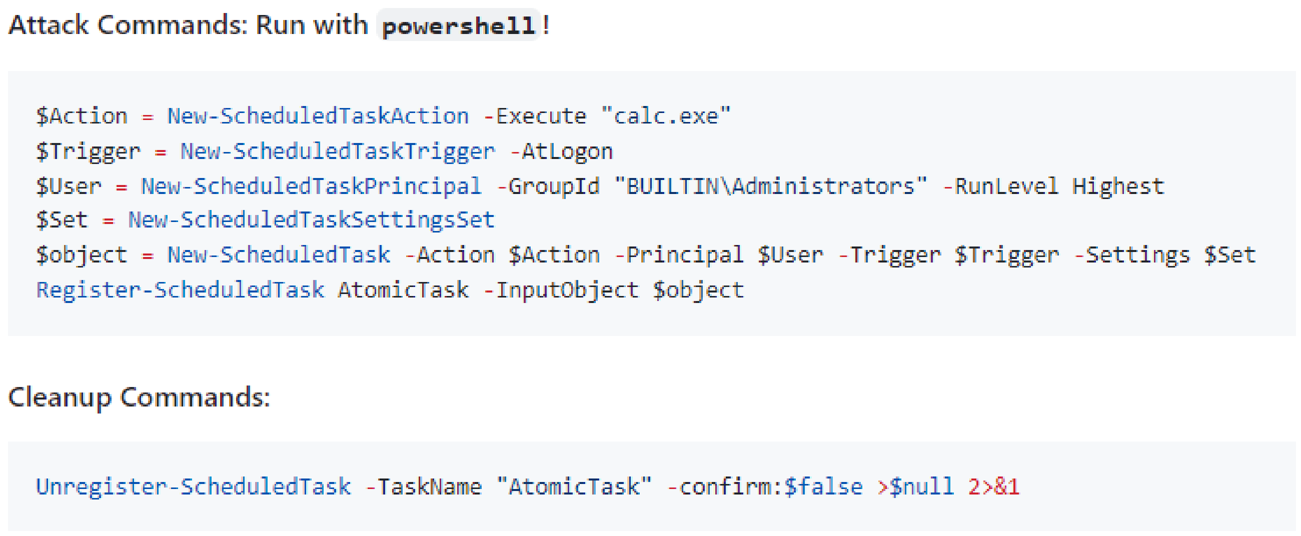
```
$Action = New-ScheduledTaskAction -Execute "calc.exe"
$Trigger = New-ScheduledTaskTrigger -AtLogon
$User = New-ScheduledTaskPrincipal -GroupId "BUILTIN\Administrators" -RunLevel Highest
$Set = New-ScheduledTaskSettingsSet
$object = New-ScheduledTask -Action $Action -Principal $User -Trigger $Trigger -Settings $Set
Register-ScheduledTask AtomicTask -InputObject $object
```

Cleanup Commands:

```
Unregister-ScheduledTask -TaskName "AtomicTask" -confirm:$false >$null 2>&1
```

Figure 15. Atomic Red Team - T1053.005

On the T1053.005.md page, there are a total of nine Atomic Test sets available for simulating T1053.005 (Scheduled Task/Job: Scheduled Task), which is one of the "Execution" tactics. Among these sets, selecting Atomic Test #4 - Powershell Cmdlet Scheduled Task provides the "test attack code" and "cleanup code" which can easily be utilized in the following way.



Attack Commands: Run with `powershell`!

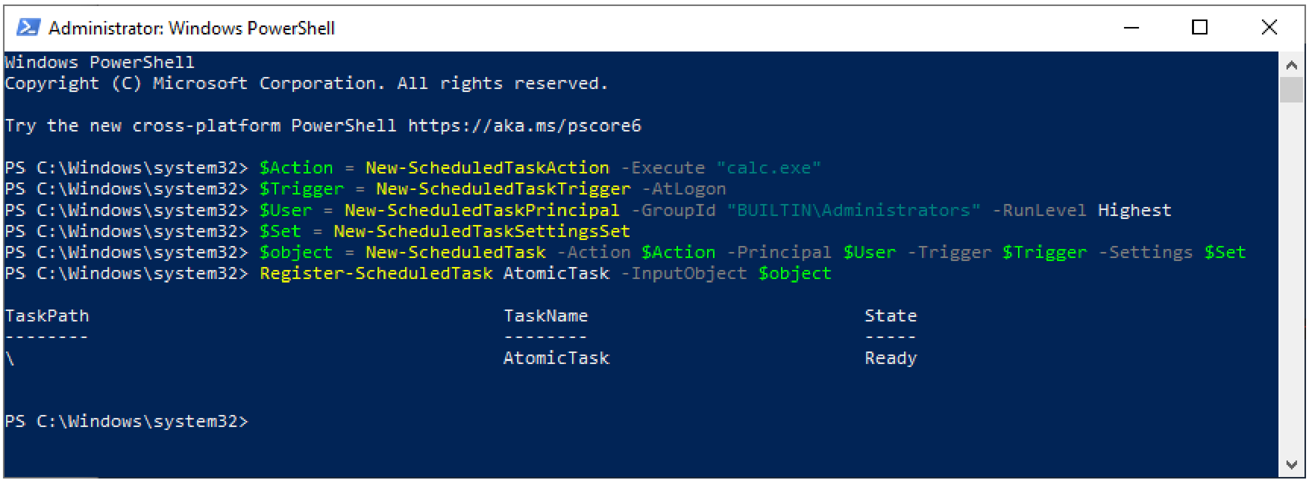
```
$Action = New-ScheduledTaskAction -Execute "calc.exe"
$Trigger = New-ScheduledTaskTrigger -AtLogon
$User = New-ScheduledTaskPrincipal -GroupId "BUILTIN\Administrators" -RunLevel Highest
$Set = New-ScheduledTaskSettingsSet
$object = New-ScheduledTask -Action $Action -Principal $User -Trigger $Trigger -Settings $Set
Register-ScheduledTask AtomicTask -InputObject $object
```

Cleanup Commands:

```
Unregister-ScheduledTask -TaskName "AtomicTask" -confirm:$false >$null 2>&1
```

Code 1. Atomic Red Team - T1053.005 test

By executing the provided test attack code in PowerShell and registering it as a scheduled task, you can observe the execution of calc.exe when you log in again.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> $Action = New-ScheduledTaskAction -Execute "calc.exe"
PS C:\Windows\system32> $Trigger = New-ScheduledTaskTrigger -AtLogon
PS C:\Windows\system32> $User = New-ScheduledTaskPrincipal -GroupId "BUILTIN\Administrators" -RunLevel Highest
PS C:\Windows\system32> $Set = New-ScheduledTaskSettingsSet
PS C:\Windows\system32> $object = New-ScheduledTask -Action $Action -Principal $User -Trigger $Trigger -Settings $Set
PS C:\Windows\system32> Register-ScheduledTask AtomicTask -InputObject $object

TaskPath                                       TaskName                          State
--------                                       --------                          -----
\                                              AtomicTask                        Ready


PS C:\Windows\system32>
```

Figure 16. Atomic Red Team - T1053.005 test

It may be difficult to verify the overall attack scenario with singular attack tests like the above example, but the attack simulation can become more detailed by utilizing the aforementioned "Invoke-AtomicRedTeam", or by adequately editing the test code. The results of such verification and evaluation should not be based on a simple detected/not detected basis or on how many were detected compared to the total. Instead, the following questions should be asked about the security products and services used by organizations or individuals:

1. Can the activities and intentions of propagating attacks within the organization be identified?
2. Are the detected activities and intentions of attacks understood in context rather than just a simple listing of information?
3. Is the detected information valuable in detecting ongoing attacks or future breaches?

Questions like the ones above should be understood and put into consideration during evaluations. This article was written with the intention of encouraging the development of expertise and a systematic approach to identify threats mapped to the MITRE ATT&CK framework provided by the cybersecurity advisory or this report. This will allow organizations to test and validate their security products and services.

2) 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.

- Warning Advised Against Play Ransomware Highly Active in the First Half of 2023 (May 4)
- New Data Theft Group RA Group Infiltrates Korean Pharmaceutical Research and Development Corporations (May 8)
- New ransomware trends in 2023 (May 11)
- IT Service Halted in US City Dallas, TX by Ransomware Attack (May 12)
- Babuk code used by 9 ransomware gangs to encrypt VMWare ESXi servers (May 12)
- MalasLocker ransomware targets Zimbra servers, demands charity donation (May 18)
- New Ransomware Akira Active in the US and Canada (May 19)
- New Buhti ransomware gang uses leaked Windows, Linux encryptors (May 25)

Conclusions

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.

N/A

2) File Hashes (MD5)

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

```
7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893
1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43
0c1eb11de3a533689267ba075e49d93d55308525c04d6aff0d2c54d1f52f5500
40126ae71b857dd22db39611c25d3d5dd0e60316b72830e930fba9baf23973ce
```

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.

```
N/A
```

References

[1] www.cisa.gov: #StopRansomware: BianLian Ransomware Group

[2] www.cisa.gov: #StopRansomware: BianLian Ransomware Group (PDF)

[3] www.bleepingcomputer.com: FBI confirms BianLian ransomware switch to extortion only attacks

[4] www.boannews.com: BianLian Ransomware Infection Occurring via Remote Desktop Service (This article is available in Korean only)

[5] www.nomoreransom.org: NO MORE RANSOM Decryption Tools

[6] seed.kisa.or.kr: Search page for KISA ransomware recovery tools (This article is available in Korean only)

[7] atip.ahnlab.com: Analysis Report on CVE-2020-1472 Vulnerability (This report supports Korean only for now)

[8] github.com: Atomic Red Team

[9] github.com: Invoke-AtomicRedTeam

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