AhnLab Cyber Threat Intelligence Report

TLP: GREEN

Threat Trend Report on Ransomware

March 2023 Ransomware Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Apr. 06, 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 March 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 aliases 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-related 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 aliases 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 alias

- Ransom/MDP.Magniber - Example behavior alias

The alias 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 alias 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.

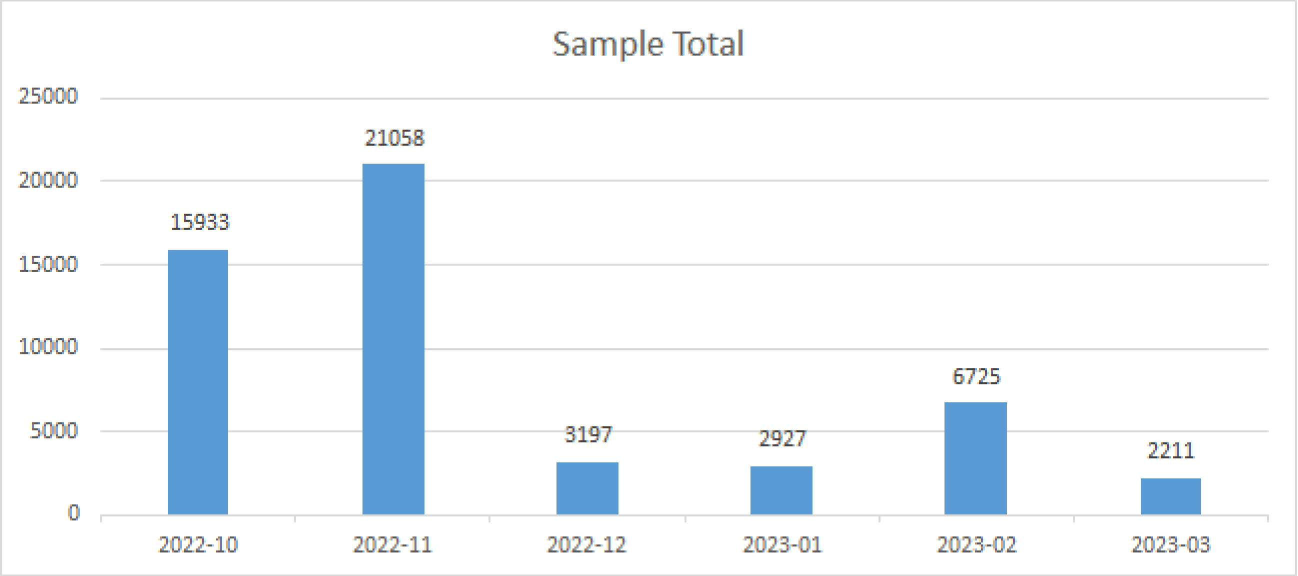


Figure 1. Number of new ransomware samples

The ransomware sample total that saw a steep decline in December 2022 was brought back up by Magniber which showed an increase last February, but along with its decline, the sample total was also reduced to the average in March.

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).

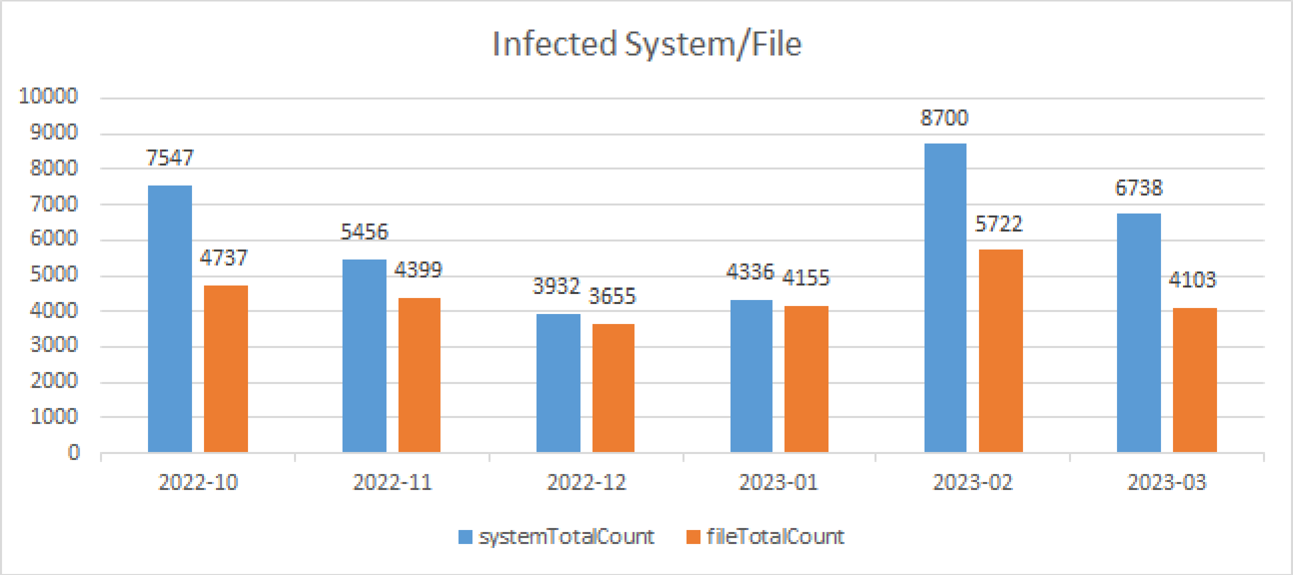


Figure 2. Systems and files affected by ransomware

Similar to the sample total statistics, the targeted systems also show a decrease compared to last month.

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

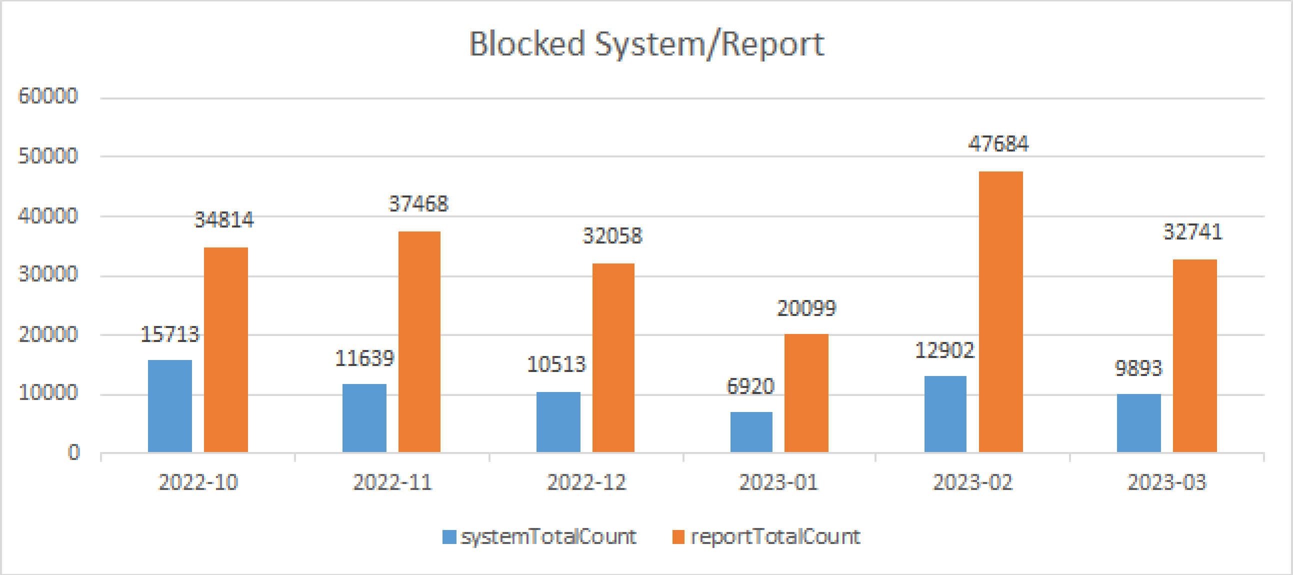


Figure 3. Ransomware behavior detection-based targeted systems and reports

Behavior detection statistics also showed a decline in numbers compared to the previous month, similar to the sample total statistics.

3) New Samples by Ransomware

Below is the statistics showing the 2,211 new samples that were discovered in March organized by ransomware. Only 20 ransomware with the most samples are shown.

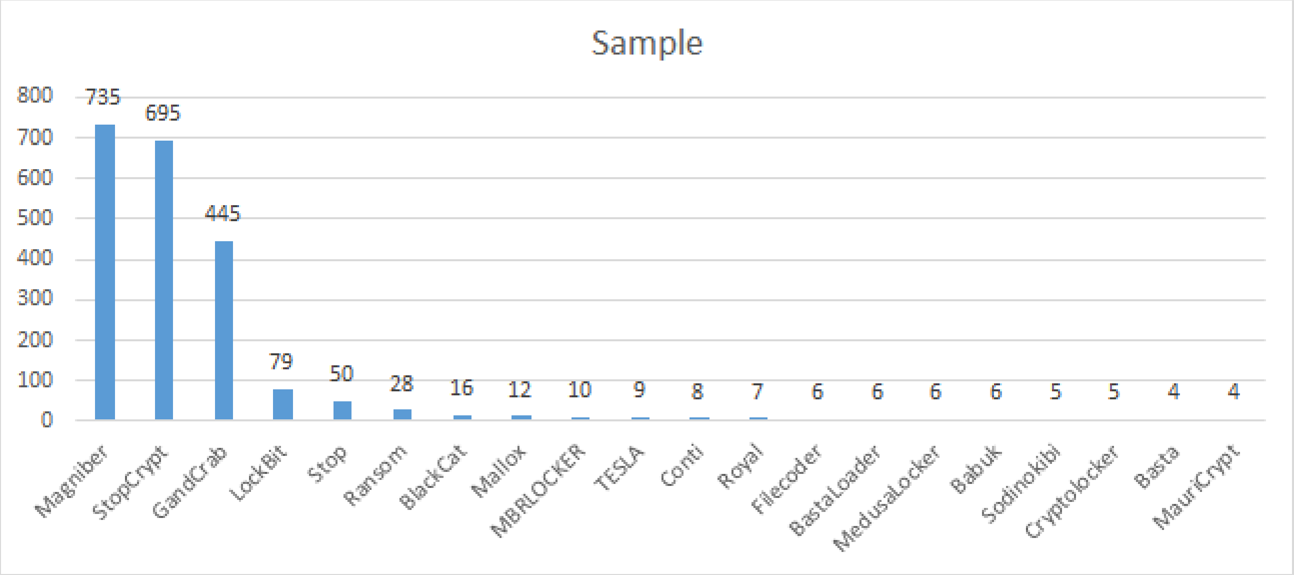


Figure 4. Number of new samples per ransomware (Mar. 2023)

Just like the total ransomware sample statistics mentioned above, new Magniber samples showed a sharp decline and fell to one-eighth of the previous month's 5,500 cases. StopCrypt increased to approximately double the previous month's 360 cases. GandCrab also showed a threefold increase compared to the 150 cases in the previous month.

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).

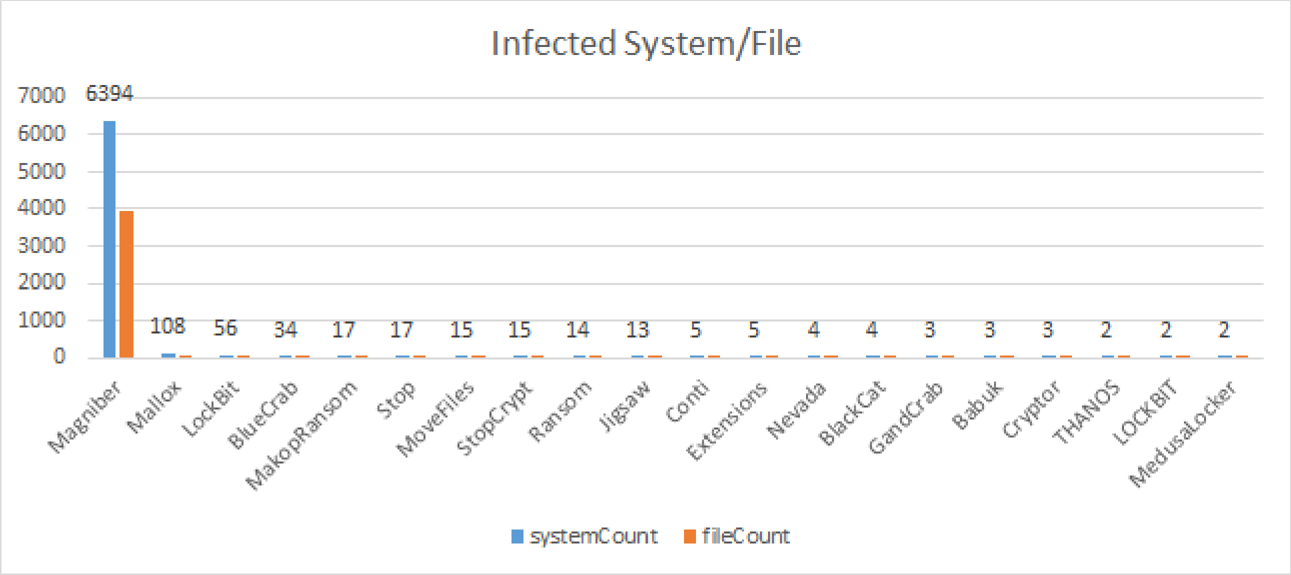


Figure 5. Number of targeted systems and files per ransomware (Mar. 2023)

The number of systems targeted by Magniber has shown a slight decrease compared to the previous month's 8,000 cases, yet is still the highest in the number of targeted systems. Although there is a vast difference in numbers compared to Magniber, Mallox has recently shown an increase in targeted systems, whereas LockBit is showing a decrease in both the number of samples and targeted systems.

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

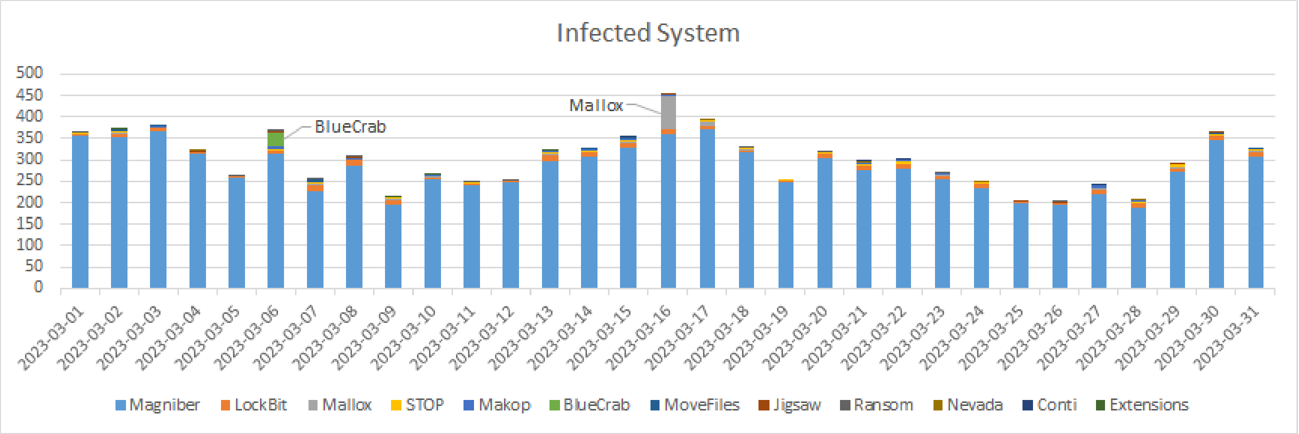


Figure 6. Daily number of targeted systems per ransomware (Mar. 2023)

Cases of Magniber infection were the highest in the daily statistics as well. Apart from the typical changes such as a reduction in case numbers during weekends, another noteworthy difference was the increase of BlueCrab infections through emails attached with compressed files, whose names were disguised as cover letters, application forms, and portfolios on March 6. Other than BlueCrab, attack methods using emails with disguised attached files were found in the cases of LockBit and Makop. On March 16, there was an increase in infection cases of Mallox (Fargo) targeting vulnerable MS-SQL server systems.

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.

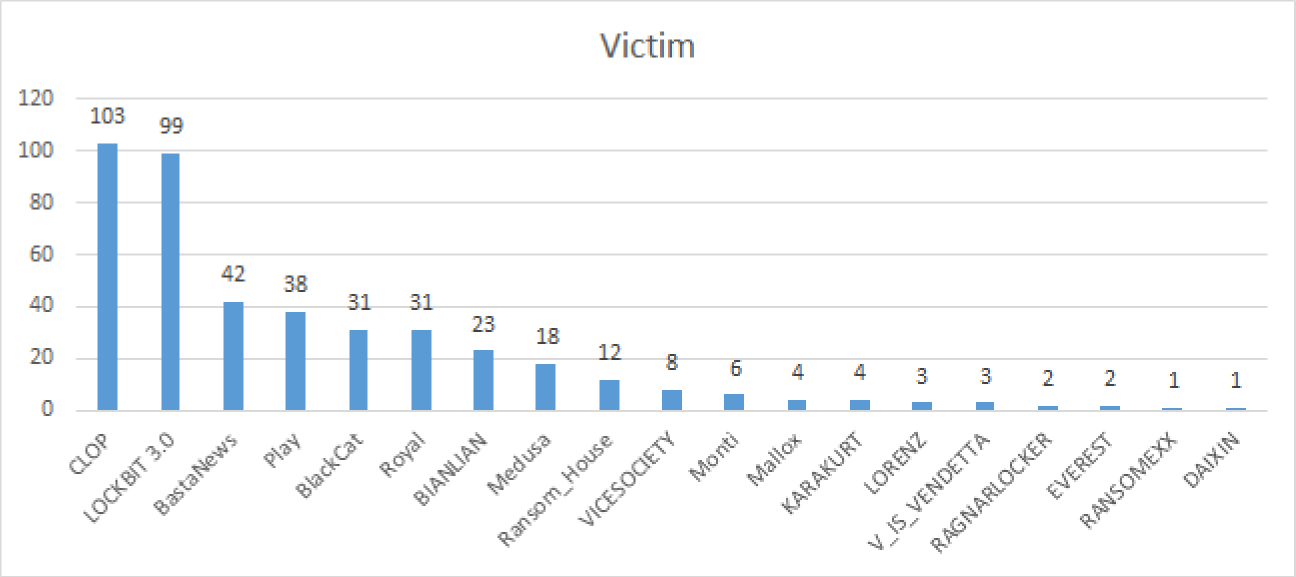
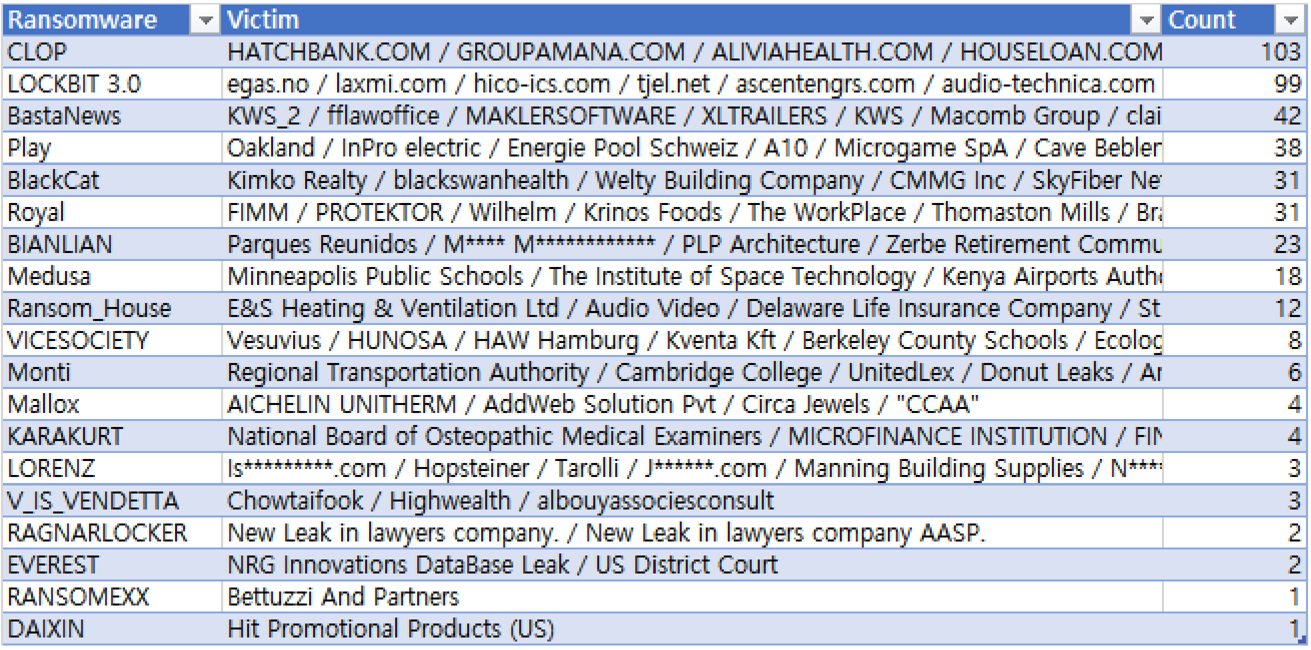


Figure 7. Number of targeted businesses per ransomware group (Mar. 2023)

CLOP, whose numbers were lower than that of LOCKBIT 3.0 and Royal, has seen an increase in targeted businesses ever since it exploited the GoAnywhere MFT zero-day vulnerability (CVE-2023-0669) last February to attack 130 companies.[1] This increase followed on into March where it revealed the highest number of targeted businesses with 103 cases.

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



Ransomware	Victim	Count
CLOP	HATCHBANK.COM / GROUPAMANA.COM / ALIVIAHEALTH.COM / HOUSELOAN.COM	103
LOCKBIT 3.0	egas.no / laxmi.com / hico-ics.com / tjel.net / ascentengrs.com / audio-technica.com	99
BastaNews	KWS_2 / fflawoffice / MAKLERSOFTWARE / XLTRAILERS / KWS / Macomb Group / clai	42
Play	Oakland / InPro electric / Energie Pool Schweiz / A10 / Microgame SpA / Cave Bebler	38
BlackCat	Kimko Realty / blackswanhealth / Welty Building Company / CMMG Inc / SkyFiber Ne	31
Royal	FIMM / PROTEKTOR / Wilhelm / Krinos Foods / The WorkPlace / Thomaston Mills / Bra	31
BIANLIAN	Parques Reunidos / M**** M************ / PLP Architecture / Zerbe Retirement Commu	23
Medusa	Minneapolis Public Schools / The Institute of Space Technology / Kenya Airports Auth	18
Ransom_House	E&S Heating & Ventilation Ltd / Audio Video / Delaware Life Insurance Company / St	12
VICESOCIETY	Vesuvius / HUNOSA / HAW Hamburg / Kventa Kft / Berkeley County Schools / Ecolog	8
Monti	Regional Transportation Authority / Cambridge College / UnitedLex / Donut Leaks / Ar	6
Mallox	AICHELIN UNITHERM / AddWeb Solution Pvt / Circa Jewels / "CCAA"	4
KARAKURT	National Board of Osteopathic Medical Examiners / MICROFINANCE INSTITUTION / FIN	4
LORENZ	Is*********.com / Hopsteiner / Tarolli / J******.com / Manning Building Supplies / N***	3
V_IS_VENDETTA	Chowtaifook / Highwealth / albouyassociesconsult	3
RAGNARLOCKER	New Leak in lawyers company. / New Leak in lawyers company AASP.	2
EVEREST	NRG Innovations DataBase Leak / US District Court	2
RANSOMEXX	Bettuzzi And Partners	1
DAIXIN	Hit Promotional Products (US)	1

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

[1] https://atip.ahnlab.com/ti/contents/asec-notes?i=eb62d9b4-2320-4d2b-ae6e-d751cd97e268

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.

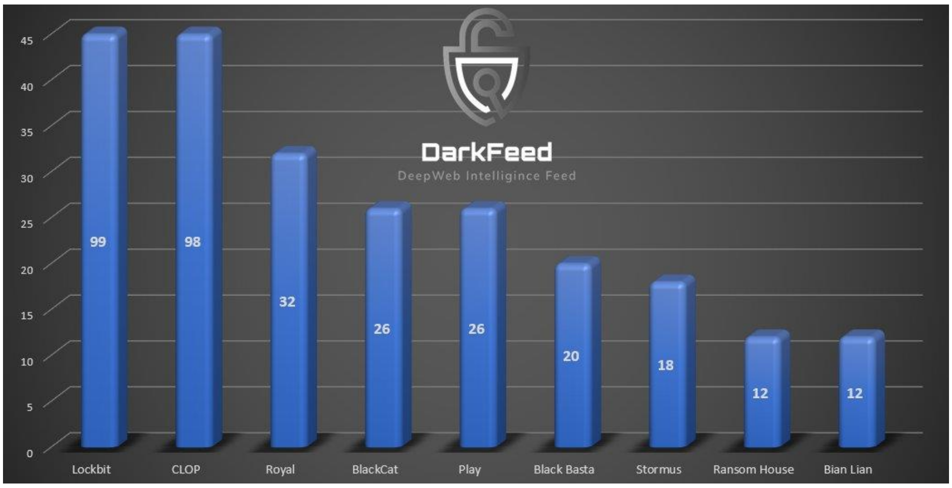


Figure 8. Targeted businesses per ransomware group <Source> DarkFeed twitter[2]

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

Key Trends

Many issues regarding various ransomware occurred in March 2023. This report presents brief introductions to the following key topics and response measures.

- IceFire ransomware exploits IBM Aspera Faspex vulnerability to infect Linux systems
- Magniber ransomware bypasses SmartScreen for distribution
- Number of businesses targeted by CLOP Ransomware sharply increase after the exploitation of the GoAnywhere vulnerability

[2] https://twitter.com/ido_cohen2 https://twitter.com/ido_cohen2/status/1642218169765883907/photo/1

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

1) IceFire Ransomware Infects Linux

SentinelLabs analyzed[3] the IceFire ransomware, which exploits the IBM Aspera Faspex file-sharing software's YAML deserialization vulnerability (CVE-2022-47986)[4] to infect Linux systems, and bleepingcomputer also published an article based on this information.[5]

More details on the CVE-2022-47986 vulnerability are available in the ATIP security advisory below.

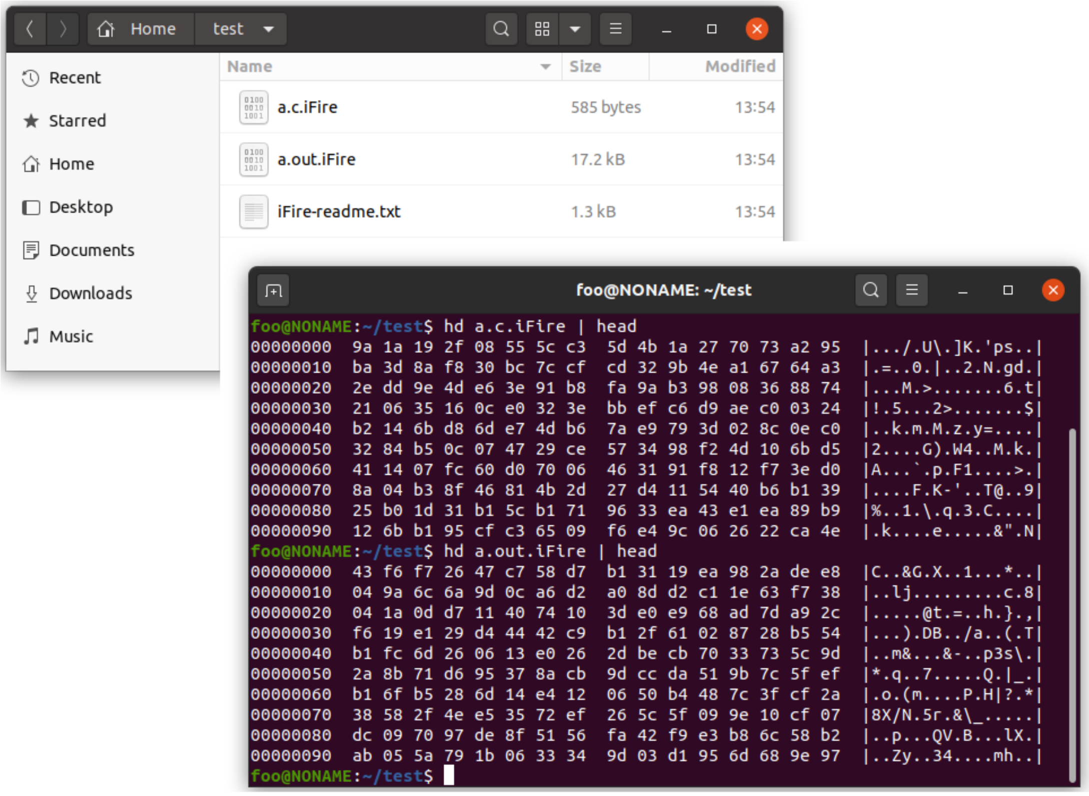
- atip.ahnlab.com: Security Update Advisory for IBM Aspera Faspex Vulnerability (CVE-2022-47986) (This report supports Korean only for now.)

The IceFire ransomware adds ".iFire" to the file extension upon encrypting them and creates a ransom note named "iFire-readme.xtx" in each directory. When the infection is complete, it deletes itself and any additional "iFire.pid" files. The IceFire ransomware runs a directory whitelist for infection in order to run the system stably, so it does not encrypt all Linux system files.

[3] https://www.sentinelone.com/labs/icefire-ransomware-returns-now-targeting-linux-enterprise-networks/

[4] https://atip.ahnlab.com/ti/contents/security-advisory?i=5db8e58e-983c-4a86-9bdb-3a75661c1632

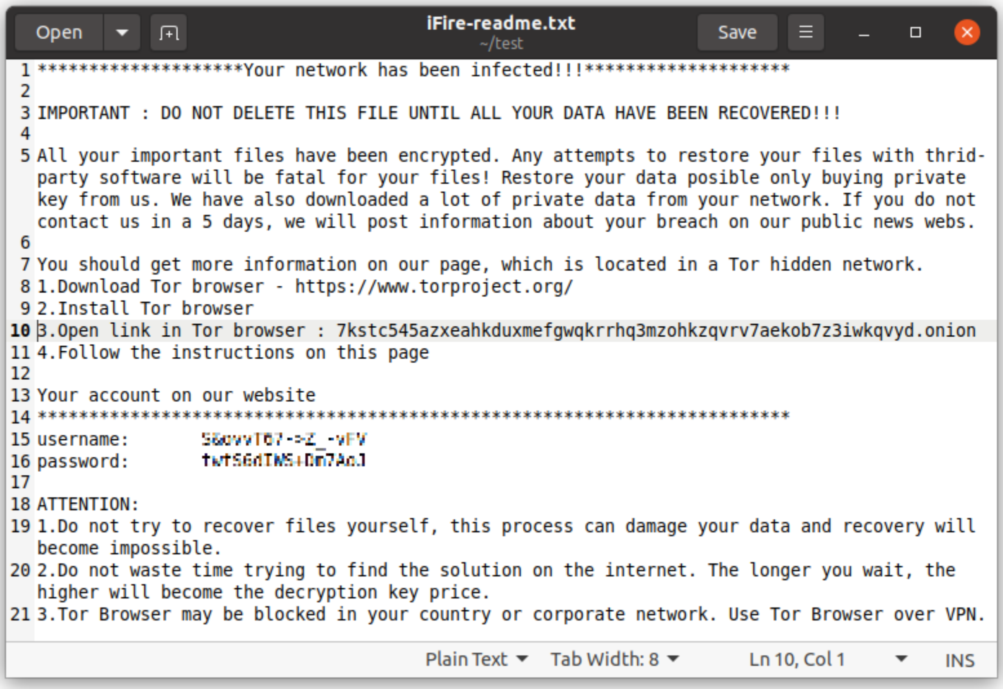
[5] https://www.bleepingcomputer.com/news/security/icefire-ransomware-now-encrypts-both-linux-and-windows-systems/



Name	Size	Modified
a.c.iFire	585 bytes	13:54
a.out.iFire	17.2 kB	13:54
iFire-readme.txt	1.3 kB	13:54

```
foo@NONAME:~/test$ hd a.c.iFire | head
00000000  9a 1a 19 2f 08 55 5c c3  5d 4b 1a 27 70 73 a2 95  |.../.U\.]K.'ps..|
00000010  ba 3d 8a f8 30 bc 7c cf  cd 32 9b 4e a1 67 64 a3  |.=..0.|..2.N.gd.|
00000020  2e dd 9e 4d e6 3e 91 b8  fa 9a b3 98 08 36 88 74  |...M.>.......6.t|
00000030  21 06 35 16 0c e0 32 3e  bb ef c6 d9 ae c0 03 24  |!.5...2>.......$|
00000040  b2 14 6b d8 6d e7 4d b6  7a e9 79 3d 02 8c 0e c0  |..k.m.M.z.y=....|
00000050  32 84 b5 0c 07 47 29 ce  57 34 98 f2 4d 10 6b d5  |2....G).W4..M.k.|
00000060  41 14 07 fc 60 d0 70 06  46 31 91 f8 12 f7 3e d0  |A...`.p.F1....>.|
00000070  8a 04 b3 8f 46 81 4b 2d  27 d4 11 54 40 b6 b1 39  |....F.K-'..T@..9|
00000080  25 b0 1d 31 b1 5c b1 71  96 33 ea 43 e1 ea 89 b9  |%..1.\.q.3.C....|
00000090  12 6b b1 95 cf c3 65 09  f6 e4 9c 06 26 22 ca 4e  |.k....e.....&".N|
foo@NONAME:~/test$ hd a.out.iFire | head
00000000  43 f6 f7 26 47 c7 58 d7  b1 31 19 ea 98 2a de e8  |C..&G.X..1...*..|
00000010  04 9a 6c 6a 9d 0c a6 d2  a0 8d d2 c1 1e 63 f7 38  |..lj.........c.8|
00000020  04 1a 0d d7 11 40 74 10  3d e0 e9 68 ad 7d a9 2c  |.....@t.=..h.}.,|
00000030  f6 19 e1 29 d4 44 42 c9  b1 2f 61 02 87 28 b5 54  |...).DB../a..(.T|
00000040  b1 fc 6d 26 06 13 e0 26  2d be cb 70 33 73 5c 9d  |..m&...&-..p3s\.|
00000050  2a 8b 71 d6 95 37 8a cb  9d cc da 51 9b 7c 5f ef  |*.q..7.....Q.|_.|
00000060  b1 6f b5 28 6d 14 e4 12  06 50 b4 48 7c 3f cf 2a  |.o.(m....P.H|?.*|
00000070  38 58 2f 4e e5 35 72 ef  26 5c 5f 09 9e 10 cf 07  |8X/N.5r.&\_.....|
00000080  dc 09 70 97 de 8f 51 56  fa 42 f9 e3 b8 6c 58 b2  |..p...QV.B...lX.|
00000090  ab 05 5a 79 1b 06 33 34  9d 03 d1 95 6d 68 9e 97  |..Zy..34....mh..|
foo@NONAME:~/test$
```

Figure 9. Files encrypted by IceFire



```
********************Your network has been infected!!!********************

IMPORTANT : DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED!!!

All your important files have been encrypted. Any attempts to restore your files with thrid-
party software will be fatal for your files! Restore your data posible only buying private
key from us. We have also downloaded a lot of private data from your network. If you do not
contact us in a 5 days, we will post information about your breach on our public news webs.

You should get more information on our page, which is located in a Tor hidden network.
1.Download Tor browser - https://www.torproject.org/
2.Install Tor browser
3.Open link in Tor browser : 7kstc545azxeahkduxmefgwqkrrhq3mzohkzqvrv7aekob7z3iwkqvyd.onion
4.Follow the instructions on this page

Your account on our website
*************************************************************************
username:       [redacted]
password:       [redacted]

ATTENTION:
1.Do not try to recover files yourself, this process can damage your data and recovery will
become impossible.
2.Do not waste time trying to find the solution on the internet. The longer you wait, the
higher will become the decryption key price.
3.Tor Browser may be blocked in your country or corporate network. Use Tor Browser over VPN.
```

Figure 10. IceFire's ransom note "iFire-readme.txt"

Previously, the IceFire ransomware only targeted Windows systems, but it has been recently confirmed that they have expanded their range to Linux systems. This seems to be a strategic change to widen their attack platforms, just like other ransomware groups that have begun attacking Linux systems for the past few years.

In order to spread ransomware to Windows systems, various methods such as attaching files to emails, guiding users to malicious websites, and phishing emails are used. Since Linux systems are mostly run as servers, these attack methods are ineffective as infection strategies. IceFire has overcome these limits by using file sharing software Aspera Faspex's vulnerability.

When using software that can be used directly for malware infection such as those with file sending and receiving features, users must apply the latest security updates and remove unnecessary software. Other than that, the standard procedure of regular backups and security software installation and update should be performed.

Reference IOCs
01DE715B0F9E3725EF453D31ACAAF598
hxxp[://]159.65.217.216:8080/demo

2) Magniber Ransomware Bypasses SmartScreen for Distribution

Google's Threat Analysis Group (TAG) has recently posted an analysis on the Magniber ransomware that used an unpatched security bypassing technique to get past Microsoft's SmartScreen security feature.[6] The threat actor sent an MSI file signed with a uniquely fabricated, invalid Authenticode to prevent the user from viewing the Mark of the Web (MOTW) security warning from SmartScreen that pops up when an unreliable file is downloaded. This vulnerability has been named CVE-2023-24880 and has been patched through the regular security update for MS products on March 14.[7]

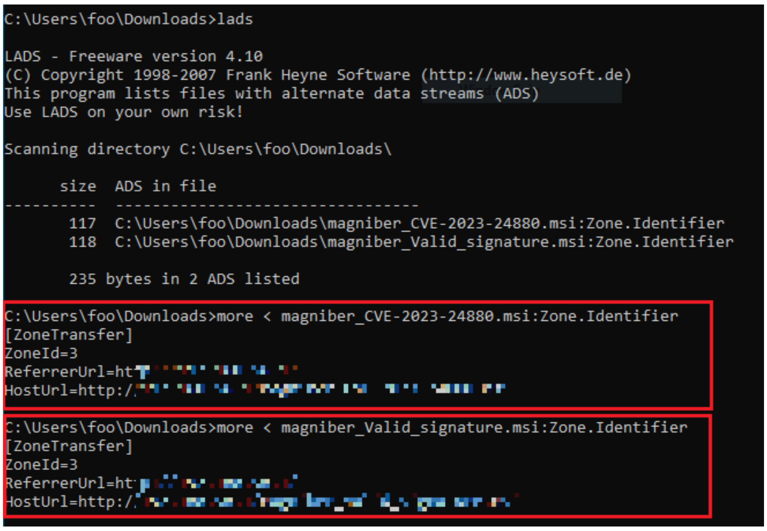
It has been reported that the Windows SmartScreen bypassing vulnerability CVE-2023-24880 bypassed the CVE-2022-44698 vulnerability patched in December 2022. Refer to the ATIP report below for more details.

[6] https://blog.google/threat-analysis-group/magniber-ransomware-actors-used-a-variant-of-microsoft-smartscreen-bypass/
[7] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880

- Atip.ahnlab.com : December 2022 Regular Security Update Advisory for MS Products (This report supports Korean only for now.)
- Atip.ahnlab.com : Zero-day Vulnerability Bypassing Windows SmartScreen Security Feature (CVE-2022-44698)
- Atip.ahnlab.com :March 2023 Regular Security Update Advisory for MS Products (This report supports Korean only for now.)

Upon executing Magniber with a valid signature downloaded from a test internet environment for MOTW settings, the SmartScreen security warnings were displayed. However, Magniber samples of the CVE-2023-24880 vulnerability bypassed the warnings and were executed without the user's confirmation. The two types of samples used in the test are as follows.

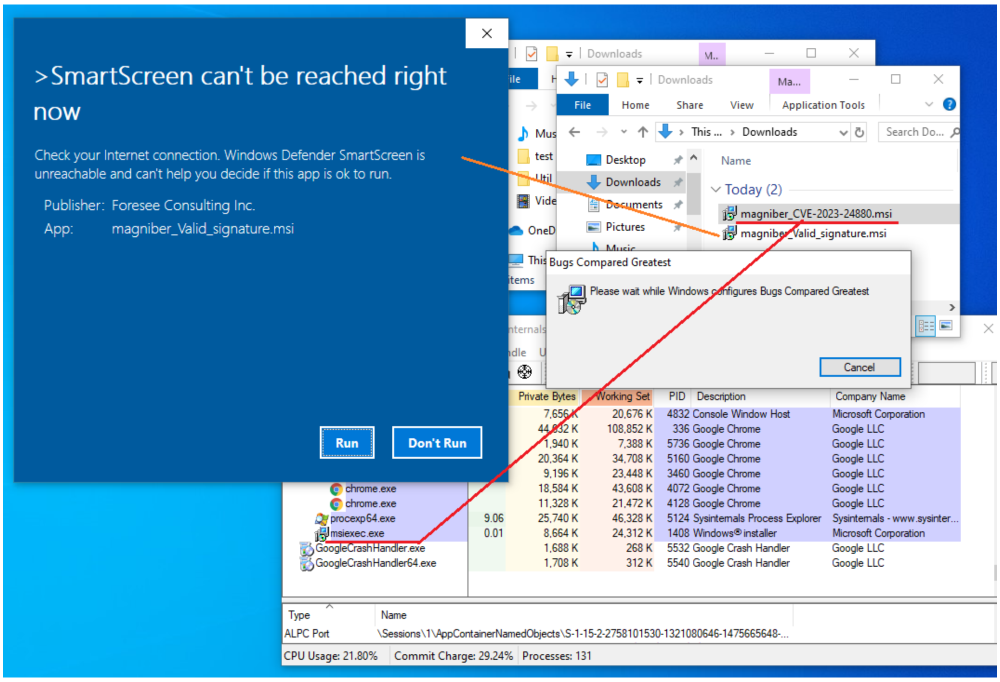
1. magniber_Valid_signature.msi (B3ECE680F2D56D0CE3D95F97DD36487B)
2. magniber_CVE-2023-24880.msi (779A5C56DA80C053E03CEA35FBB363FB)



```
C:\Users\foo\Downloads>lads

LADS - Freeware version 4.10
(C) Copyright 1998-2007 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory C:\Users\foo\Downloads\

      size  ADS in file
----------  ---------------------------------
       117  C:\Users\foo\Downloads\magniber_CVE-2023-24880.msi:Zone.Identifier
       118  C:\Users\foo\Downloads\magniber_Valid_signature.msi:Zone.Identifier

       235 bytes in 2 ADS listed

C:\Users\foo\Downloads>more < magniber_CVE-2023-24880.msi:Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=ht[redacted]
HostUrl=http:/[redacted]

C:\Users\foo\Downloads>more < magniber_Valid_signature.msi:Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=ht[redacted]
HostUrl=http:/[redacted]
```

Figure 11. ADS information of the downloaded magniber msi file.

When the two samples were executed without a network connection, the first sample showed the SmartScreen security warning (left), but the second sample was executed without any security warnings due to the CVE-2023-24880 vulnerability (right).



>SmartScreen can't be reached right now

Check your Internet connection. Windows Defender SmartScreen is unreachable and can't help you decide if this app is ok to run.

Publisher: Foresee Consulting Inc.
App: magniber_Valid_signature.msi

Run | Don't Run

Bugs Compared Greatest

Please wait while Windows configures Bugs Compared Greatest

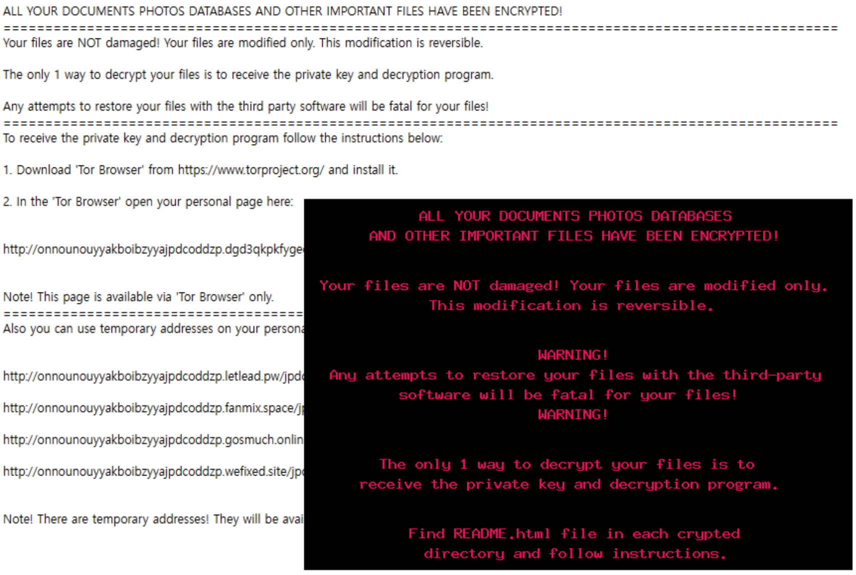
Cancel

		Private Bytes	Working Set	PID	Description	Company Name
		7,656 K	20,676 K	4832	Console Window Host	Microsoft Corporation
		44,632 K	108,852 K	336	Google Chrome	Google LLC
		1,940 K	7,388 K	5736	Google Chrome	Google LLC
		20,364 K	34,708 K	5160	Google Chrome	Google LLC
		9,196 K	23,448 K	3460	Google Chrome	Google LLC
chrome.exe		18,584 K	43,608 K	4072	Google Chrome	Google LLC
chrome.exe		11,328 K	21,472 K	4128	Google Chrome	Google LLC
procexp64.exe	9.06	25,740 K	46,328 K	5124	Sysinternals Process Explorer	Sysinternals - www.sysinter...
msiexec.exe	0.01	8,664 K	24,312 K	1408	Windows® installer	Microsoft Corporation
GoogleCrashHandler.exe		1,688 K	268 K	5532	Google Crash Handler	Google LLC
GoogleCrashHandler64.exe		1,708 K	312 K	5540	Google Crash Handler	Google LLC

Type	Name
ALPC Port	\Sessions\1\AppContainerNamedObjects\S-1-15-2-2758101530-1321080646-1475665648-...

CPU Usage: 21.80% | Commit Charge: 29.24% | Processes: 131

Figure 12. Upon executing magniber_CVE-2023-24880.msi (right)



ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!
==
Your files are NOT damaged! Your files are modified only. This modification is reversible.

The only 1 way to decrypt your files is to receive the private key and decryption program.

Any attempts to restore your files with the third party software will be fatal for your files!
==
To receive the private key and decryption program follow the instructions below:

1. Download 'Tor Browser' from https://www.torproject.org/ and install it.

2. In the 'Tor Browser' open your personal page here:

http://onnounouyyakboibzyyajpdcoddzp.dgd3qkpkfyge

Note! This page is available via 'Tor Browser' only.
================================
Also you can use temporary addresses on your persona

http://onnounouyyakboibzyyajpdcoddzp.letlead.pw/jpd

http://onnounouyyakboibzyyajpdcoddzp.fanmix.space/j

http://onnounouyyakboibzyyajpdcoddzp.gosmuch.onlin

http://onnounouyyakboibzyyajpdcoddzp.wefixed.site/jp

Note! There are temporary addresses! They will be avai

ALL YOUR DOCUMENTS PHOTOS DATABASES
AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!

Your files are NOT damaged! Your files are modified only.
This modification is reversible.

WARNING!
Any attempts to restore your files with the third-party
software will be fatal for your files!
WARNING!

The only 1 way to decrypt your files is to
receive the private key and decryption program.

Find README.html file in each crypted
directory and follow instructions.

Figure 13. The ransom note and the background screen when infected with Magniber

Suppliers of vulnerable software often release patches with narrow coverage, allowing threat actors to discover new vulnerability variants. Patching security flaws requires the correction of the fundamental flaws, but this seems difficult to achieve due to the trade-off between providing quick patches and the impact those patches will have on the whole software. Because the fundamental cause of the SmartScreen bypassing issue has not been solved, threat actors were able to find the existing bug's variant, CVE-2023-24880.

As seen in the "Statistics on Targeted Systems by Ransomware", Magniber has the highest number of ransomware attacks in Korea. Their activities are mostly focused on the typosquatting method which exploits typos in domain address input or distribution through clicks on top advertisement banners that are displayed when searching for major software. TAG has confirmed over 100,000 cases of malicious MSI file downloads through the CVE-2023-24880 vulnerability since January 2023. Over 80% of these cases were by European users, which is different from Magniber's typical attack pattern that focuses on Korea and Taiwan. There were attempts to check system damage through the revealed IOC, yet these attempts were unsuccessful.

Although it is crucial that both corporate and private users adhere to security protocols, more emphasis should be put on identifying the fundamental cause and applying defensive codes to prevent similar vulnerabilities when software vendors apply security updates with appropriate changes.

Reference IOCs
779A5C56DA80C053E03CEA35FBB363FB
8F0F46A64ADE3501A2DBE249B9B9F61C

3) Significantly More Businesses Targeted by CLOP Ransomware

In February, the CLOP ransomware exploited the GoAnywhere MFT zero-day vulnerability (CVE-2023-0669)[8] to leak information from about 130 businesses.[9] No further activity had been detected from them prior to mid-March, which is when they began to post targeted businesses on their DLS. These are speculated to be businesses targeted by ransomware attacks that have been exploiting the CVE-2023-0669 vulnerability since February.

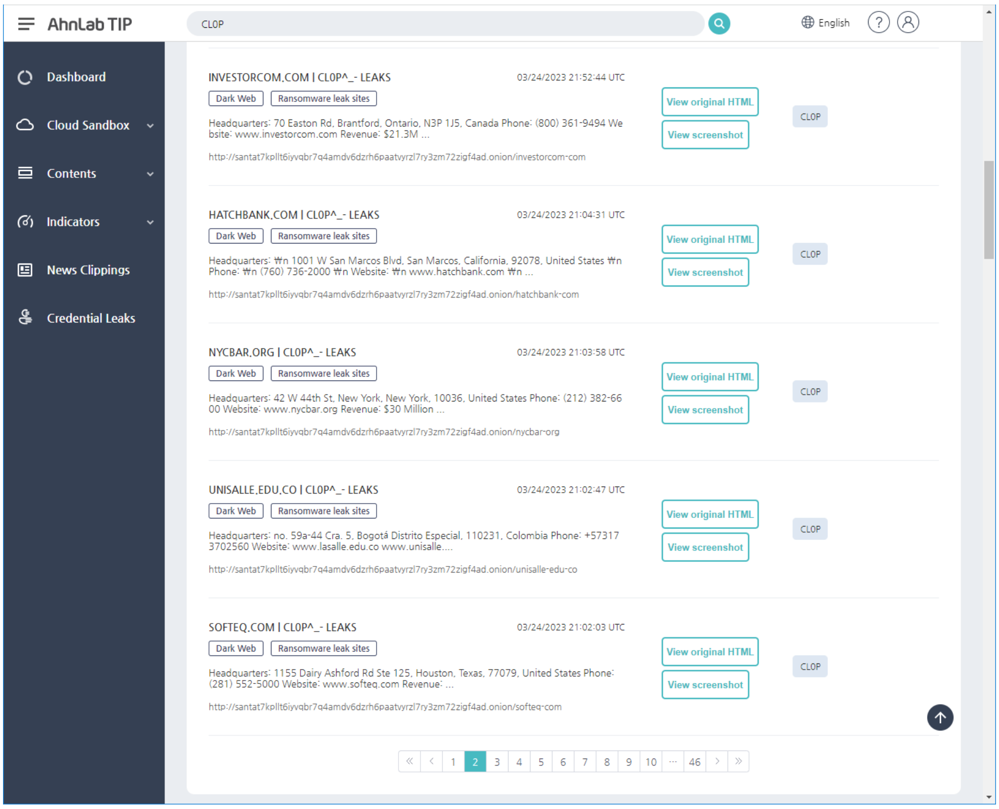
More details on the CVE-2023-0669 vulnerability are available in the ATIP security advisory below.

- Atip.ahnlab.com : Caution Advised for GoAnywhere MFT Zero-Day Vulnerability (CVE-2023-0669) (This report supports Korean only for now.)

[8] https://atip.ahnlab.com/ti/contents/security-advisory?i=840d61f6-858e-4ed1-9d62-4601cacc59a2

[9] https://atip.ahnlab.com/ti/contents/asec-notes?i=eb62d9b4-2320-4d2b-ae6e-d751cd97e268

Detailed numbers of the targeted businesses and the names of some of the businesses can be seen in "Targeted Businesses by Ransomware Group". Searching "CLOP" on ATIP yields the following "Deep&Dark Web" results. There has been a sharp increase in the number of businesses targeted by the CLOP ransomware since early March.



INVESTORCOM.COM | CL0P^_- LEAKS 03/24/2023 21:52:44 UTC
Dark Web | Ransomware leak sites
Headquarters: 70 Easton Rd, Brantford, Ontario, N3P 1J5, Canada Phone: (800) 361-9494 Website: www.investorcom.com Revenue: $21.3M ...
http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion/investorcom-com

HATCHBANK.COM | CL0P^_- LEAKS 03/24/2023 21:04:31 UTC
Dark Web | Ransomware leak sites
Headquarters: ₩n 1001 W San Marcos Blvd, San Marcos, California, 92078, United States ₩n Phone: ₩n (760) 736-2000 ₩n Website: ₩n www.hatchbank.com ₩n ...
http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion/hatchbank-com

NYCBAR.ORG | CL0P^_- LEAKS 03/24/2023 21:03:58 UTC
Dark Web | Ransomware leak sites
Headquarters: 42 W 44th St, New York, New York, 10036, United States Phone: (212) 382-6600 Website: www.nycbar.org Revenue: $30 Million ...
http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion/nycbar-org

UNISALLE.EDU.CO | CL0P^_- LEAKS 03/24/2023 21:02:47 UTC
Dark Web | Ransomware leak sites
Headquarters: no. 59a-44 Cra. 5, Bogotá Distrito Especial, 110231, Colombia Phone: +57317 3702560 Website: www.lasalle.edu.co www.unisalle....
http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion/unisalle-edu-co

SOFTEQ.COM | CL0P^_- LEAKS 03/24/2023 21:02:03 UTC
Dark Web | Ransomware leak sites
Headquarters: 1155 Dairy Ashford Rd Ste 125, Houston, Texas, 77079, United States Phone: (281) 552-5000 Website: www.softeq.com Revenue: ...
http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion/softeq-com

Figure 14. Search results of businesses targeted by "CLOP"

Fortra provided a patch for the CVE-2023-0669 vulnerability on February 14. Users of the vulnerable version of GoAnywhere MFT are advised to update the software to GoAnywhere MFT 7.1.2 through Product Downloads.

Just like the IceFire ransomware's Linux system infection strategies, when using software equipped with features that can be used directly for malware infection, such as file transfer, users must apply the latest security updates and remove unnecessary software. Other than that, the standard procedure of regular backups and security software installation and update should be performed.

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.

- Mallox Ransomware Being Distributed In Korea (Mar. 14)
- Ransomware Distributed Through Zero-Day Found in MS SmartScreen Feature (Mar. 15)
- Nevada Ransomware Being Distributed In Korea (Mar. 23)
- CLOP Ransomware Group Posts a List of Over 20 Victims (Mar. 16)
- New Dark Power ransomware claims 10 victims in its first month (Mar. 25)
- LockBit Ransomware Group Designates the National Tax Service as a Victim (Mar. 29)

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 major software used by corporations. In the case of private users, they take advantage of users' negligence, use malware carefully disguised as normal software, or 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.
- Take caution to not access websites from unreliable sources and viewing/executing email links and attachments.
- Use hard-go-guess 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.

```
iFire
MS.Update.Center.Security.KB99435793.msi
MS_Update_Center_Security.KB89598422.msi
```

2) File Hashes (MD5)

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

```
01DE715B0F9E3725EF453D31ACAAF598
779A5C56DA80C053E03CEA35FBB363FB
8F0F46A64ADE3501A2DBE249B9B9F61C
```

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.

```
hxxp://159.65.217.216:8080/demo
```

References

[1] atip.ahnlab.com : CLOP Ransomware Group Posts a List of Over 20 Victims
[2] https://twitter.com/ido_cohen2 : DarkFeed twitter
[3] www.sentinelone.com : IceFire Ransomware Returns | Now Targeting Linux Enterprise Networks
[4] www.bleepingcomputer.com : IceFire ransomware now encrypts both Linux and Windows systems
[5] blog.google : Magniber ransomware actors used a variant of Microsoft SmartScreen bypass
[6] www.bleepingcomputer.com : Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day

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