AhnLab Cyber Threat Intelligence Report

TLP: GREEN

Threat Trend Report on Ransomware

July 2023 Ransomware Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Aug. 4, 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 the number of new ransomware samples, targeted systems, and targeted businesses in July 2023, as well as notable ransomware issues in Korea and other countries. Other major issues and statistics for ransomware that are not mentioned in the report can be found by searching for the following keywords or via the Statistics menu at AhnLab Threat Intelligence Platform (hereinafter "ATIP").

- Ransomware
- Statistics by Type

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

Major Statistics

1) Data Sources and Collection Methods

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

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

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

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

- Ransom/MDP.Magniber: Example behavior detection name

The detection names acquired at the time of detection may not allow for the identification of ransomware type (e.g. Generic, Agent, Edit, Decoy, and others), and some cases may be excluded from the ransomware statistics or be counted as a different ransomware type due to 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 data was collected belatedly, then the data may have been excluded from the statistics or have been considered to be collected at a time different from the exact date the victim was revealed.

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

2) Overall Ransomware Statistics

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

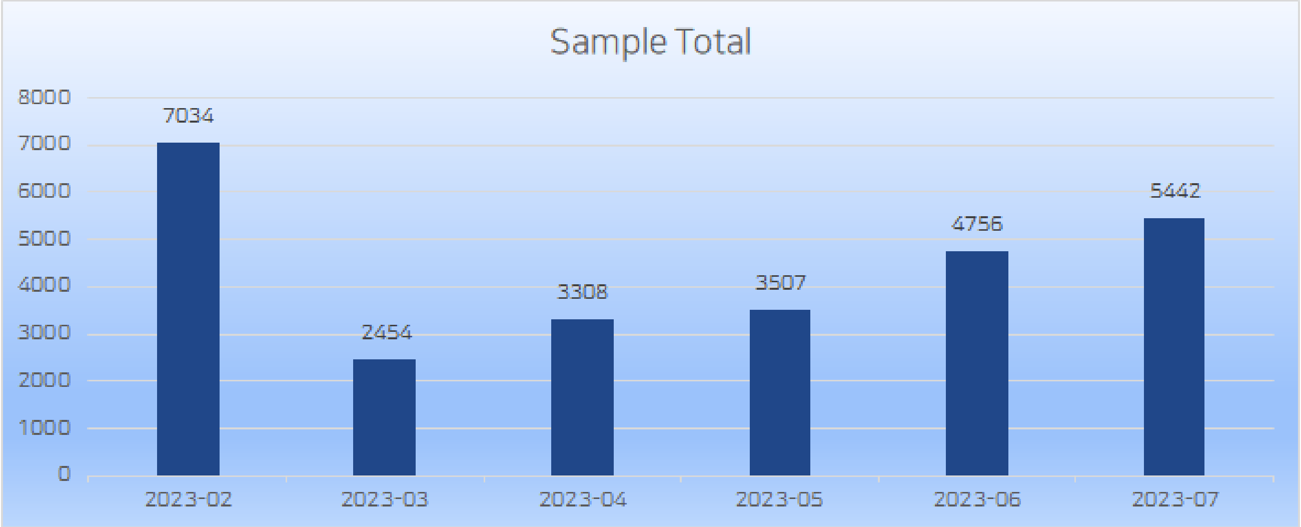


Figure 1. Number of new ransomware samples

Magniber drove a steep increase in February 2023 but the number decreased in March; however it is on the rise again. In July, the total number of new samples increased by about 14% compared to the previous month to 5442, which is attributable to the increase in the number of sample variants of Azov, LockBit, and StopCrypt ransomware.

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

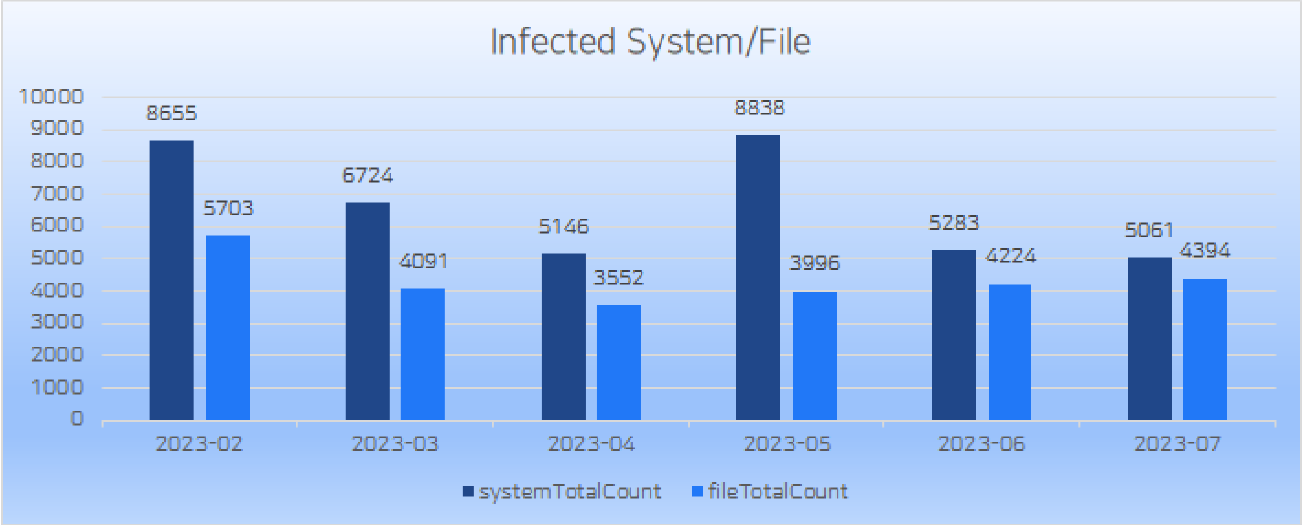


Figure 2. Systems and files infected by ransomware

The total count of targeted systems is mostly the same as those of June. Most of the damage was caused by Magniber, recording 5,061 cases in total.

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

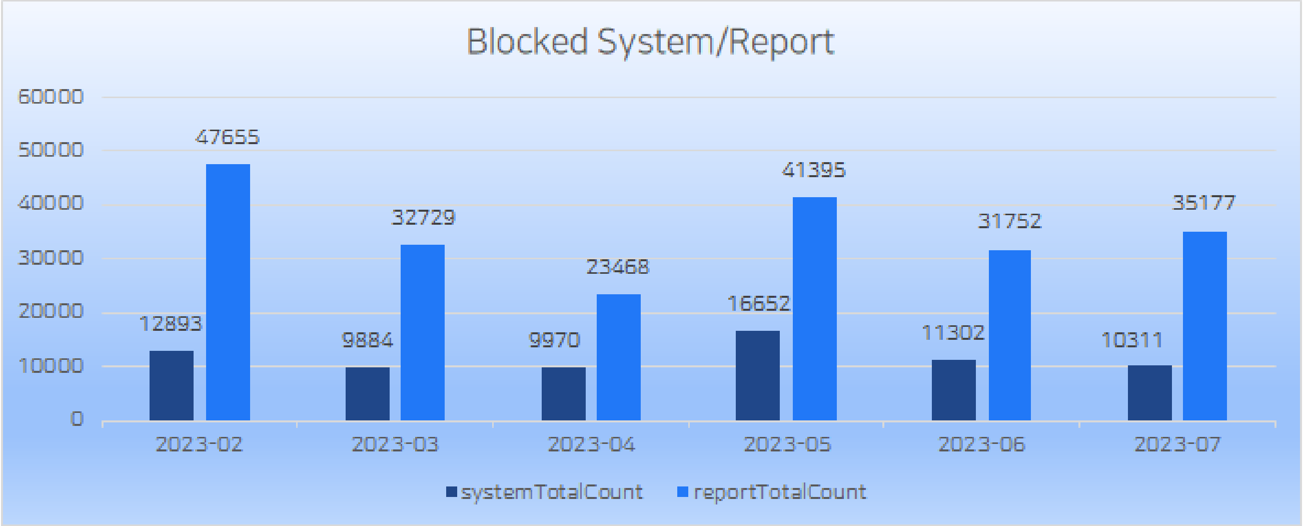


Figure 3. Ransomware behavior detection-based targeted systems and reports

Like the statistics on the above infected systems, the behavior detection system statistics remained almost the same as the previous month, only with the number of blocks being slightly higher.

3) New Samples by Ransomware

Below is the statistics showing the 5,442 new samples that were discovered in July organized by ransomware type. Only 20 ransomware with the most samples are shown.

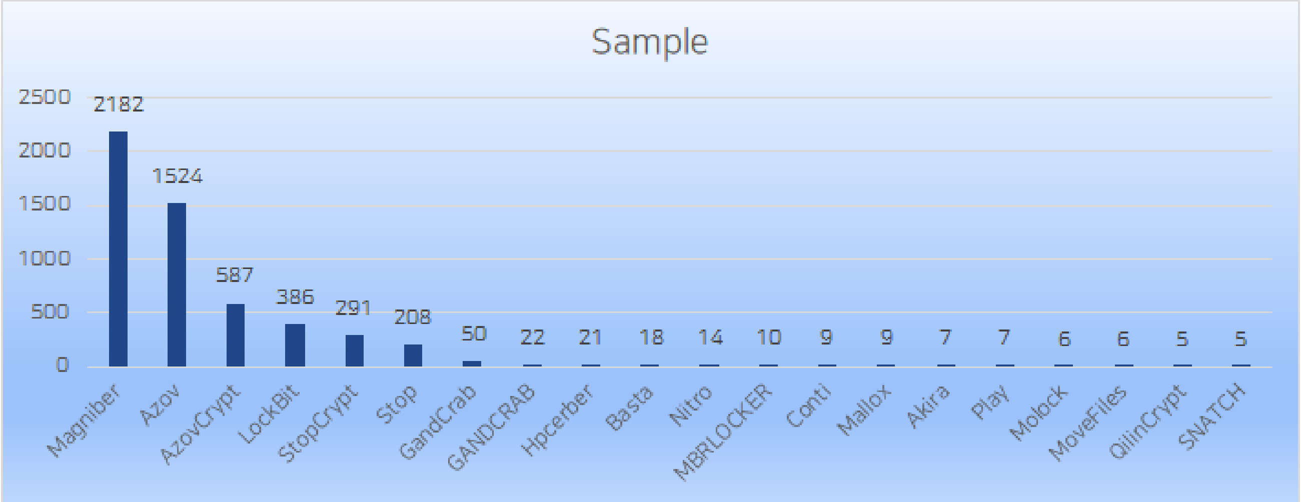


Figure 4. Number of new samples per ransomware (July 2023)

As mentioned in the total ransomware statistics, it can be seen that the number of variant samples of the Azov, LockBit, and StopCrypt ransomware increased compared to the previous month. Magniber recorded a similar figure to the previous month, but it was still the most collected among the new samples. There were no significant changes in the number 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).

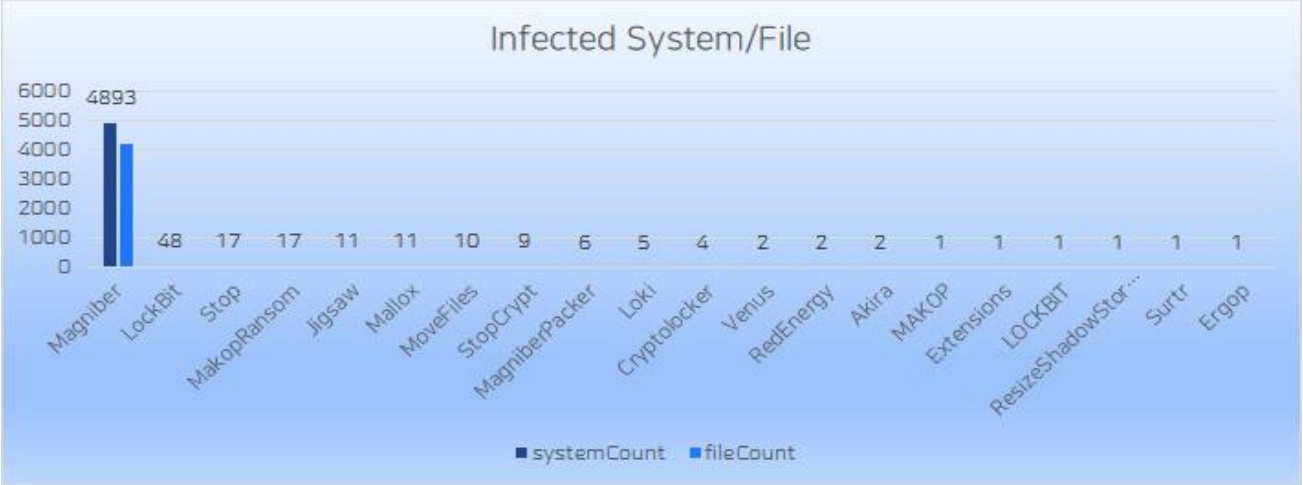


Figure 5. Number of targeted systems and files by ransomware (July 2023)

The number of systems targeted by Magniber inched down from 5,100 to 4893, which is at a similar level to those of the previous month. Other ransomware numbers remained at a similar level to those of June as well.

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

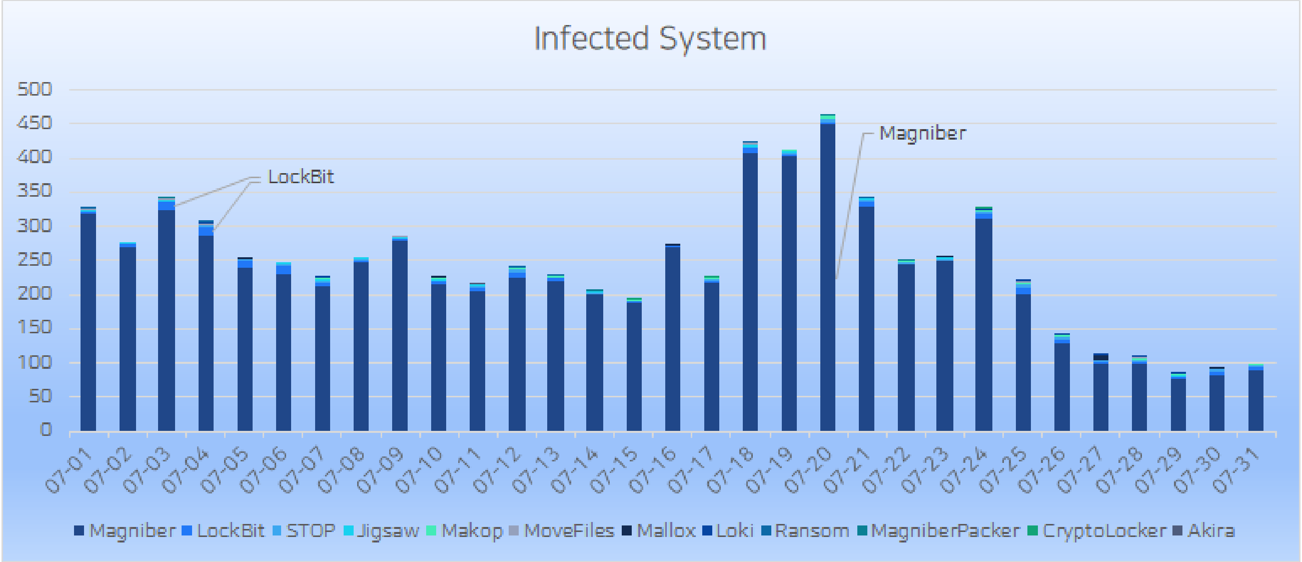


Figure 6. Daily number of targeted systems per ransomware (July 2023)

Infection cases caused by Magniber were the highest in the daily statistics as well. Aside from the typical fluctuations such as a slight decrease in attacks during weekends and subsequent pick up during weekdays, the daily number of systems affected by Magniber stayed at about an average of 230. Infection attempts had been made steadily throughout July without there being a spike on a specific day. The summer vacation season seems to have influenced the decrease in the number of affected systems after July 24. There were also LockBit and Makop ransomware's emails involving attachments disguised as "resumes", "job applications", and "guidelines on unauthorized use of licenses", as well as infection attempts by STOP ransomware disguised under the filenames "build.exe" and "setup.exe".

5) Targeted Businesses by Ransomware Group

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

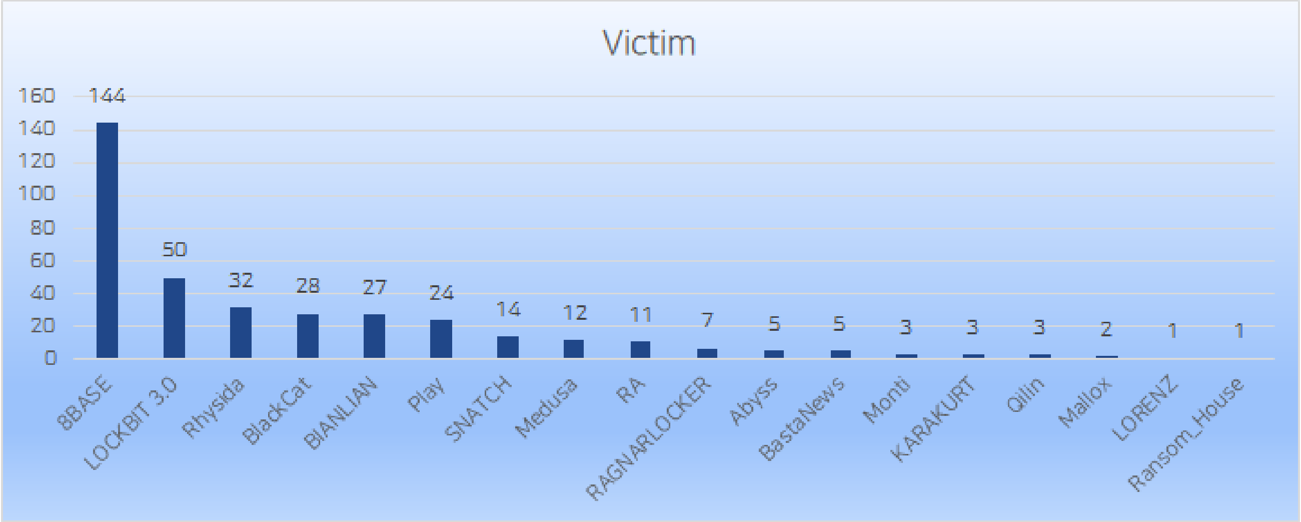
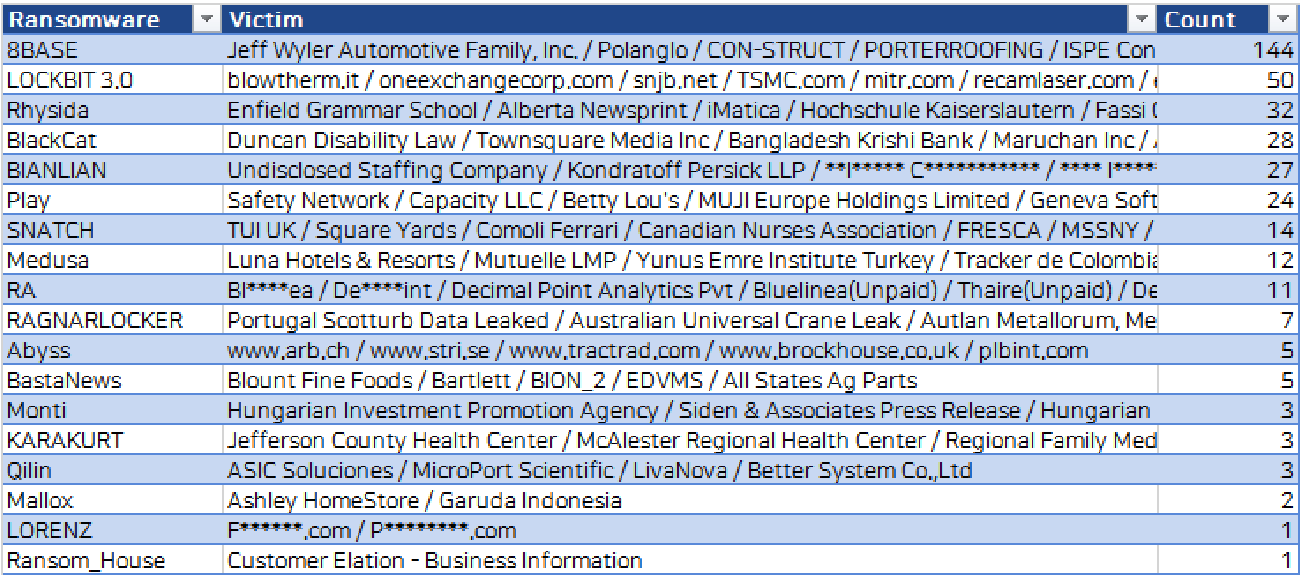


Figure 7. Number of targeted businesses per ransomware group (July 2023)

The number of businesses attacked by 8BASE, a ransomware group first observed in May 2023, topped in ATIP statistics since the number was counted cumulatively; however, the actual number of businesses affected by 8BASE announced in July is 31. The number of businesses affected by LOCKBIT 3.0 slightly decreased from the previous month, but the group continues to add many businesses to their dedicated leak sites (DLS). As for Rhysida, the group emerged at around the same time as 8Base is highly active, and the number is also a cumulative one.

Since the first report in late May on CLOP exploiting the MOVEit zero-day vulnerability to breach data from hundreds of companies, the number of victims disclosed by CLOP has increased. While the group revealed many victims in July as well, they were not reflected in the statistics because they were not collected by ATIP. For more information regarding businesses attacked by CLOP, please refer to the "Key Trends" section below.

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



Ransomware	Victim	Count
8BASE	Jeff Wyler Automotive Family, Inc. / Polanglo / CON-STRUCT / PORTERROOFING / ISPE Con	144
LOCKBIT 3.0	blowtherm.it / oneexchangecorp.com / snjb.net / TSMC.com / mitr.com / recamlaser.com /	50
Rhysida	Enfield Grammar School / Alberta Newsprint / iMatica / Hochschule Kaiserslautern / Fassi (	32
BlackCat	Duncan Disability Law / Townsquare Media Inc / Bangladesh Krishi Bank / Maruchan Inc /	28
BIANLIAN	Undisclosed Staffing Company / Kondratoff Persick LLP / **|****** C************ / ***** |****	27
Play	Safety Network / Capacity LLC / Betty Lou's / MUJI Europe Holdings Limited / Geneva Soft	24
SNATCH	TUI UK / Square Yards / Comoli Ferrari / Canadian Nurses Association / FRESCA / MSSNY /	14
Medusa	Luna Hotels & Resorts / Mutuelle LMP / Yunus Emre Institute Turkey / Tracker de Colombia	12
RA	Bl****ea / De****int / Decimal Point Analytics Pvt / Bluelinea(Unpaid) / Thaire(Unpaid) / De	11
RAGNARLOCKER	Portugal Scotturb Data Leaked / Australian Universal Crane Leak / Autlan Metallorum, Me	7
Abyss	www.arb.ch / www.stri.se / www.tractrad.com / www.brockhouse.co.uk / plbint.com	5
BastaNews	Blount Fine Foods / Bartlett / BION_2 / EDVMS / All States Ag Parts	5
Monti	Hungarian Investment Promotion Agency / Siden & Associates Press Release / Hungarian	3
KARAKURT	Jefferson County Health Center / McAlester Regional Health Center / Regional Family Med	3
Qilin	ASIC Soluciones / MicroPort Scientific / LivaNova / Better System Co.,Ltd	3
Mallox	Ashley HomeStore / Garuda Indonesia	2
LORENZ	F******.com / P*********.com	1
Ransom_House	Customer Elation - Business Information	1

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

6) Targeted Businesses by Ransomware Group (External Statistics)

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

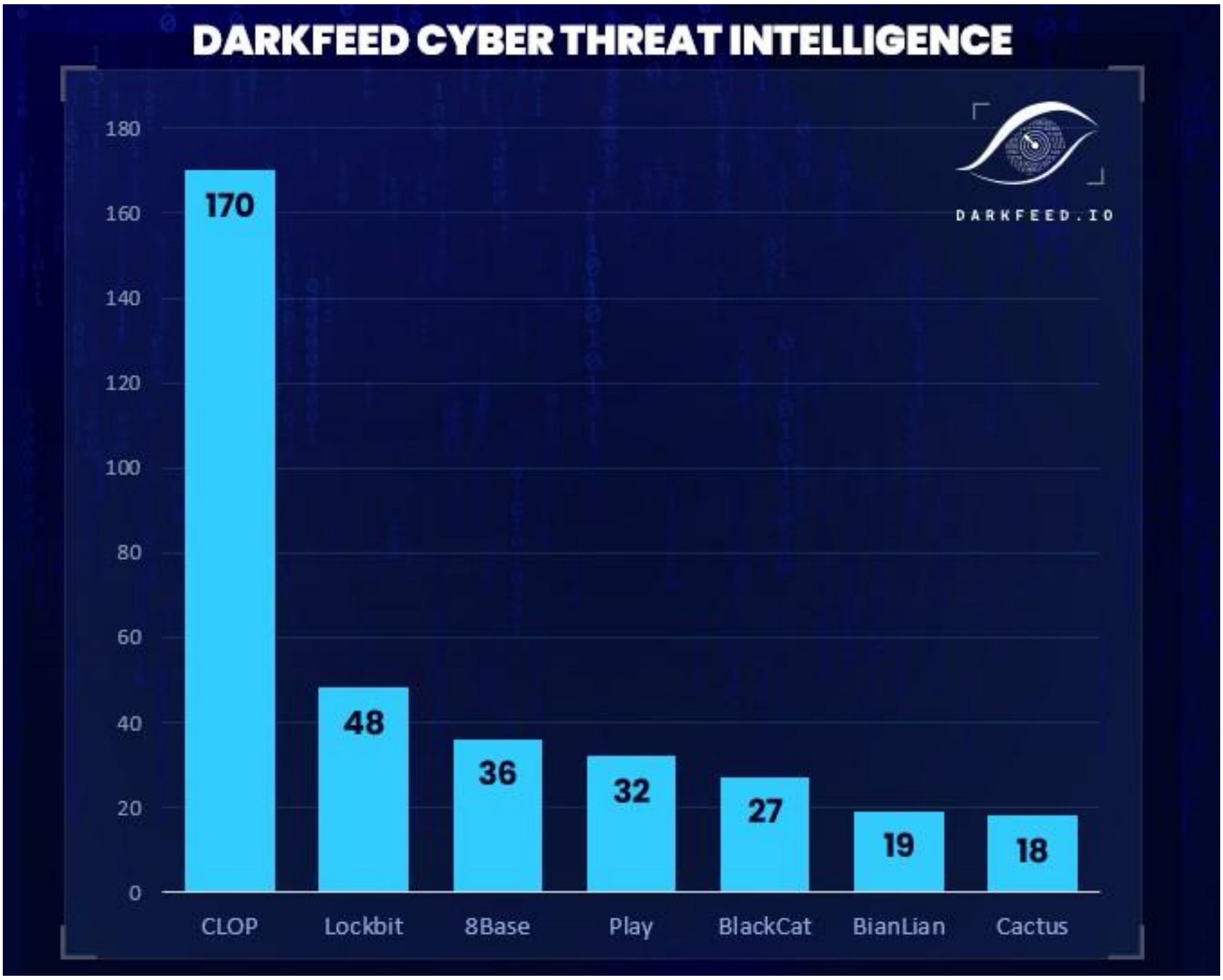


Figure 8. Targeted businesses per ransomware group <Source> DarkFeed Twitter

As mentioned above, though not counted in ATIP, the number of companies compromised by CLOP – the one who listed the most victims – as well as LOCKBIT 3.0, 8BASE, BlackCat (ALPHV), Play, and BIANLIAN ransomware groups are generally high.

Key Trends

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

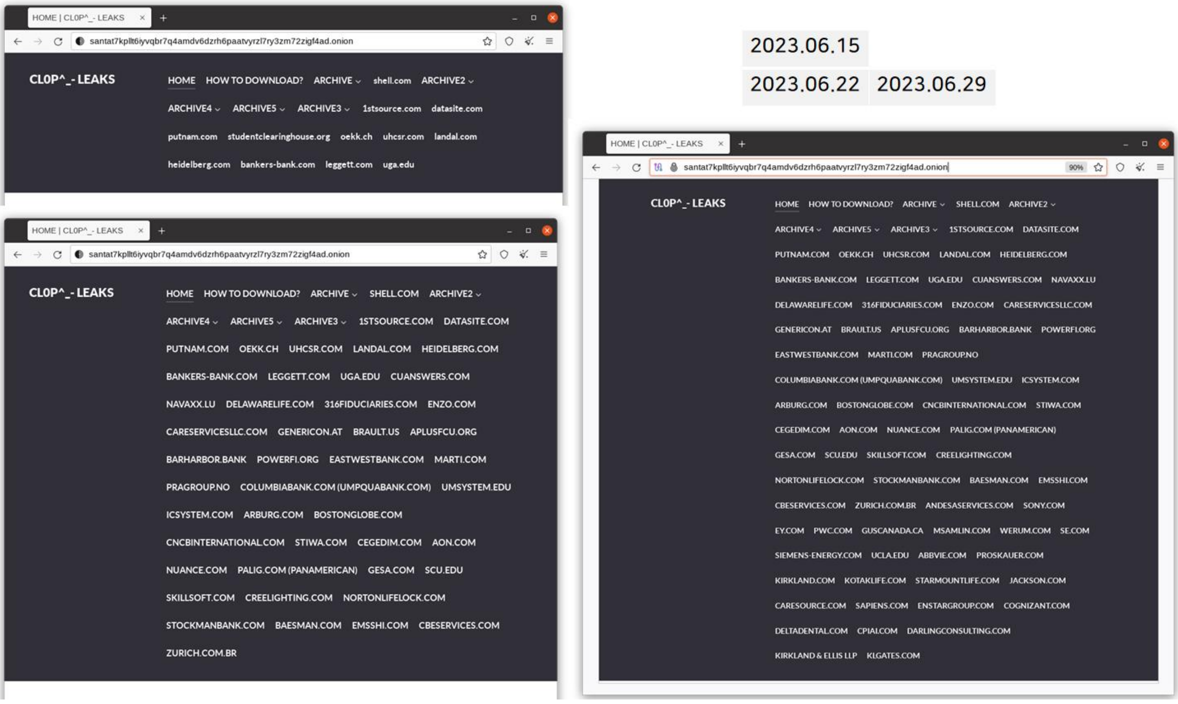
- More businesses affected by CLOP ransomware's exploitation of MOVEit zero-day vulnerability;
- Big Head ransomware disguised as an emergency Windows update; and
- Detection names for ransomware disguised as Sophos file.

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) More businesses affected by CLOP ransomware's exploitation of MOVEit zero-day vulnerability

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

[1] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=dcfc0d31-88ae-439e-ae3c-0a2746771ab7



HOME | CL0P^_- LEAKS
santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion

CL0P^_- LEAKS

HOME HOW TO DOWNLOAD? ARCHIVE shell.com ARCHIVE2
ARCHIVE4 ARCHIVE5 ARCHIVE3 1stsource.com datasite.com
putnam.com studentclearinghouse.org oekk.ch uhcsr.com landal.com
heidelberg.com bankers-bank.com leggett.com uga.edu

HOME | CL0P^_- LEAKS
santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion

CL0P^_- LEAKS

HOME HOW TO DOWNLOAD? ARCHIVE SHELL.COM ARCHIVE2
ARCHIVE4 ARCHIVE5 ARCHIVE3 1STSOURCE.COM DATASITE.COM
PUTNAM.COM OEKK.CH UHCSR.COM LANDAL.COM HEIDELBERG.COM
BANKERS-BANK.COM LEGGETT.COM UGA.EDU CUANSWERS.COM
NAVAXX.LU DELAWARELIFE.COM 316FIDUCIARIES.COM ENZO.COM
CARESERVICESLLC.COM GENERICON.AT BRAULT.US APLUSFCU.ORG
BARHARBOR.BANK POWERFI.ORG EASTWESTBANK.COM MARTI.COM
PRAGROUP.NO COLUMBIABANK.COM (UMPQUABANK.COM) UMSYSTEM.EDU
ICSYSTEM.COM ARBURG.COM BOSTONGLOBE.COM
CNCBINTERNATIONAL.COM STIWA.COM CEGEDIM.COM AON.COM
NUANCE.COM PALIG.COM (PANAMERICAN) GESA.COM SCU.EDU
SKILLSOFT.COM CREELIGHTING.COM NORTONLIFELOCK.COM
STOCKMANBANK.COM BAESMAN.COM EMSSHI.COM CBESERVICES.COM
ZURICH.COM.BR

2023.06.15

2023.06.22 2023.06.29

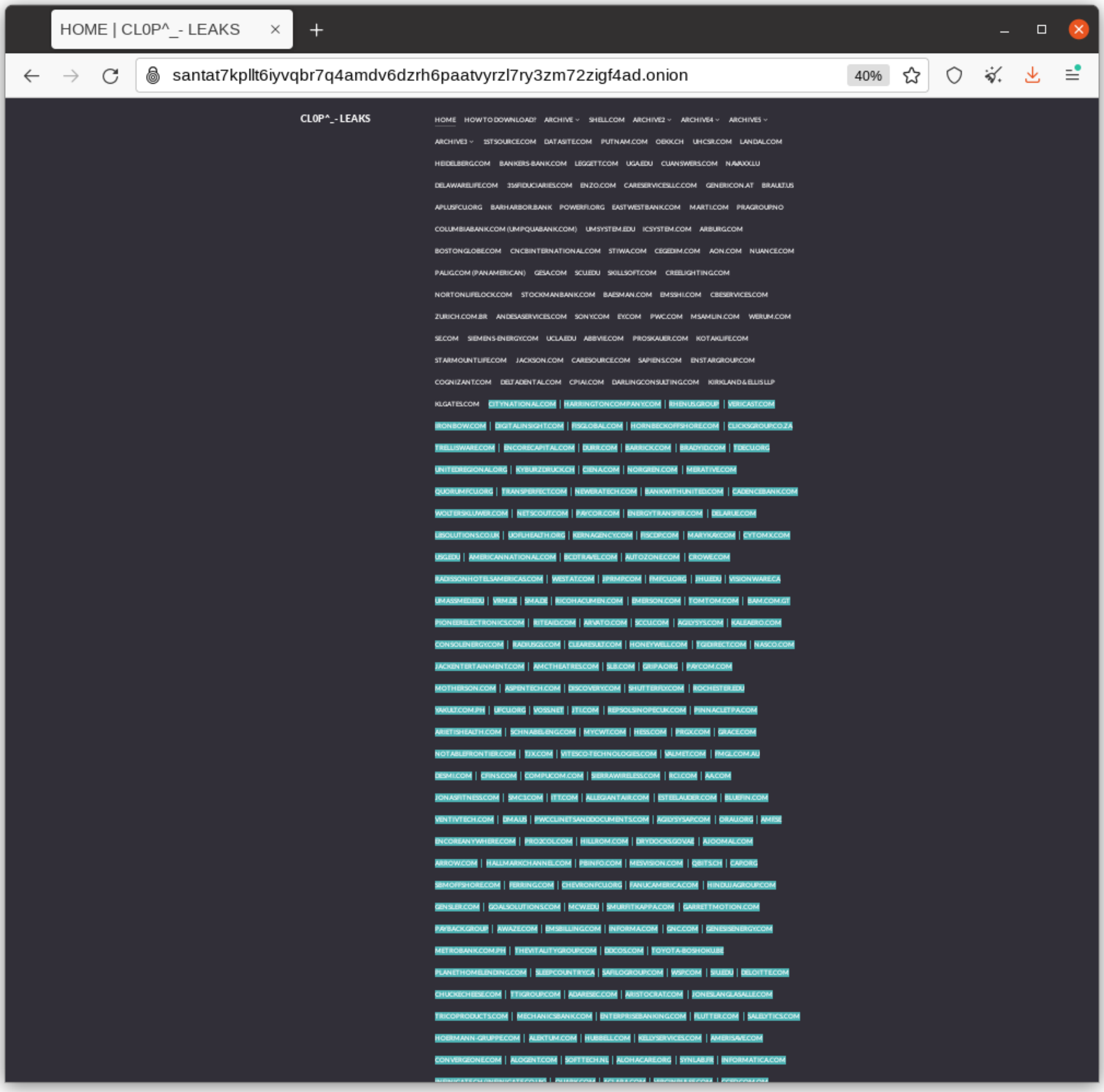
HOME | CL0P^_- LEAKS
santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion
90%

CL0P^_- LEAKS

HOME HOW TO DOWNLOAD? ARCHIVE SHELL.COM ARCHIVE2
ARCHIVE4 ARCHIVE5 ARCHIVE3 1STSOURCE.COM DATASITE.COM
PUTNAM.COM OEKK.CH UHCSR.COM LANDAL.COM HEIDELBERG.COM
BANKERS-BANK.COM LEGGETT.COM UGA.EDU CUANSWERS.COM NAVAXX.LU
DELAWARELIFE.COM 316FIDUCIARIES.COM ENZO.COM CARESERVICESLLC.COM
GENERICON.AT BRAULT.US APLUSFCU.ORG BARHARBOR.BANK POWERFI.ORG
EASTWESTBANK.COM MARTI.COM PRAGROUP.NO
COLUMBIABANK.COM (UMPQUABANK.COM) UMSYSTEM.EDU ICSYSTEM.COM
ARBURG.COM BOSTONGLOBE.COM CNCBINTERNATIONAL.COM STIWA.COM
CEGEDIM.COM AON.COM NUANCE.COM PALIG.COM (PANAMERICAN)
GESA.COM SCU.EDU SKILLSOFT.COM CREELIGHTING.COM
NORTONLIFELOCK.COM STOCKMANBANK.COM BAESMAN.COM EMSSHI.COM
CBESERVICES.COM ZURICH.COM.BR ANDESASERVICES.COM SONY.COM
EY.COM PWC.COM GUSCANADA.CA MSAMLIN.COM WERUM.COM SE.COM
SIEMENS-ENERGY.COM UCLA.EDU ABBVIE.COM PROSKAUER.COM
KIRKLAND.COM KOTAKLIFE.COM STARMOUNTLIFE.COM JACKSON.COM
CARESOURCE.COM SAPIENS.COM ENSTARGROUP.COM COGNIZANT.COM
DELTADENTAL.COM CPIAI.COM DARLINGCONSULTING.COM
KIRKLAND & ELLIS LLP KLGATES.COM

Figure 9. Posts on CLOP ransomware's DLS - Disclosure of victims (June 15, 22, 29)

The image above shows the number of victims listed over three weeks in June. As of July 31, the CLOP's DLS added approximately 180 new victims to their list. This is two to three times the number of companies disclosed in June. The group appears to be constantly updating their victims listing to explore ways to maximize their profit. Companies added between June 29 and July 31 are colored in different text background.


HOME | CLOP^_- LEAKS
santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion
40%

CL0P^_- LEAKS

HOME HOW TO DOWNLOAD? ARCHIVE SHELL.COM ARCHIVE2 ARCHIVE4 ARCHIVE5
ARCHIVE3 1STSOURCE.COM DATASITE.COM PUTNAM.COM OEKK.CH UHCSR.COM LANDAL.COM
HEIDELBERG.COM BANKERS-BANK.COM LEGGETT.COM UGA.EDU CUANSWERS.COM NAVAXX.LU
DELAWARELIFE.COM 316FIDUCIARIES.COM ENZO.COM CARESERVICESLLC.COM GENERICON.AT BRAULT.US
APLUSFCU.ORG BARHARBOR.BANK POWERFI.ORG EASTWESTBANK.COM MARTI.COM PRAGROUP.NO
COLUMBIABANK.COM (UMPQUABANK.COM) UMSYSTEM.EDU ICSYSTEM.COM ARBURG.COM
BOSTONGLOBE.COM CNCBINTERNATIONAL.COM STIWA.COM CEGEDIM.COM AON.COM NUANCE.COM
PALIG.COM (PANAMERICAN) GESA.COM SCU.EDU SKILLSOFT.COM CREELIGHTING.COM
NORTONLIFELOCK.COM STOCKMANBANK.COM BAESMAN.COM EMSSHI.COM CBESERVICES.COM
ZURICH.COM.BR ANDESASERVICES.COM SONY.COM EY.COM PWC.COM MSAMLIN.COM WERUM.COM
SE.COM SIEMENS-ENERGY.COM UCLA.EDU ABBVIE.COM PROSKAUER.COM KOTAKLIFE.COM
STARMOUNTLIFE.COM JACKSON.COM CARESOURCE.COM SAPIENS.COM ENSTARGROUP.COM
COGNIZANT.COM DELTADENTAL.COM CPIAI.COM DARLINGCONSULTING.COM KIRKLAND & ELLIS LLP
KLGATES.COM CITYNATIONAL.COM | HARRINGTONCOMPANY.COM | RHENUS.GROUP | VERICAST.COM
IRONBOW.COM | DIGITALINSIGHT.COM | FISGLOBAL.COM | HORNBECKOFFSHORE.COM | CLICKSGROUP.CO.ZA
TRELLISWARE.COM | ENCORECAPITAL.COM | DURR.COM | BARRICK.COM | BRADYID.COM | TDECU.ORG
UNITEDREGIONAL.ORG | KYBURZDRUCK.CH | CIENA.COM | NORGREN.COM | MERATIVE.COM
QUORUMFCU.ORG | TRANSPERFECT.COM | NEWERATECH.COM | BANKWITHUNITED.COM | CADENCEBANK.COM
WOLTERSKLUWER.COM | NETSCOUT.COM | PAYCOR.COM | ENERGYTRANSFER.COM | DELARUE.COM
UBSOLUTIONS.CO.UK | UOFLHEALTH.ORG | KERNAGENCY.COM | FISCDP.COM | MARYKAY.COM | CYTOMX.COM
USG.EDU | AMERICANNATIONAL.COM | BCDTRAVEL.COM | AUTOZONE.COM | CROWE.COM
RADISSONHOTELSAMERICAS.COM | WESTAT.COM | JPRMP.COM | FMFCU.ORG | JHU.EDU | VISIONWARE.CA
UMASSMED.EDU | VRM.DE | SMA.DE | RICOHACUMEN.COM | EMERSON.COM | TOMTOM.COM | BAM.COM.GT
PIONEERELECTRONICS.COM | RITEAID.COM | ARVATO.COM | SCCU.COM | AGILYSYS.COM | KALEAERO.COM
CONSOLENERGY.COM | RADIUSGS.COM | CLEARESULT.COM | HONEYWELL.COM | TGIDIRECT.COM | NASCO.COM
JACKENTERTAINMENT.COM | AMCTHEATRES.COM | SLB.COM | GRIPA.ORG | PAYCOM.COM
MOTHERSON.COM | ASPENTECH.COM | DISCOVERY.COM | SHUTTERFLY.COM | ROCHESTER.EDU
YAKULT.COM.PH | UFCU.ORG | VOSS.NET | JTI.COM | REPSOLSINOPECUK.COM | PINNACLETPA.COM
ARIETISHEALTH.COM | SCHNABEL-ENG.COM | MYCWT.COM | HESS.COM | PRGX.COM | GRACE.COM
NOTABLEFRONTIER.COM | TJX.COM | VITESCO-TECHNOLOGIES.COM | VALMET.COM | FMGL.COM.AU
DESMI.COM | CFINS.COM | COMPUCOM.COM | SIERRAWIRELESS.COM | RCI.COM | AA.COM
JONASFITNESS.COM | SMC3.COM | ITT.COM | ALLEGIANTAIR.COM | ESTEELAUDER.COM | BLUEFIN.COM
VENTIVTECH.COM | DMA.US | PWCCLINETSANDDOCUMENTS.COM | AGILYSYSAP.COM | ORAU.ORG | AM.SE
ENCOREANYWHERE.COM | PRO2COL.COM | HILLROM.COM | DRYDOCKS.GOV.AE | AJOOMAL.COM
ARROW.COM | HALLMARKCHANNEL.COM | PBINFO.COM | MESVISION.COM | QBITS.CH | CAP.ORG
SBMOFFSHORE.COM | FERRING.COM | CHEVRONFCU.ORG | FANUCAMERICA.COM | HINDUJAGROUP.COM
GENSLER.COM | GOALSOLUTIONS.COM | MCW.EDU | SMURFITKAPPA.COM | GARRETTMOTION.COM
PAYBACK.GROUP | AWAZE.COM | EMSBILLING.COM | INFORMA.COM | GNC.COM | GENESISENERGY.COM
METROBANK.COM.PH | THEVITALITYGROUP.COM | DDCOS.COM | TOYOTA-BOSHOKU.BE
PLANETHOMELENDING.COM | SLEEPCOUNTRY.CA | SAFILOGROUP.COM | WSP.COM | SIU.EDU | DELOITTE.COM
CHUCKECHEESE.COM | TTIGROUP.COM | ADARESEC.COM | ARISTOCRAT.COM | JONESLANGLASALLE.COM
TRICOPRODUCTS.COM | MECHANICSBANK.COM | ENTERPRISEBANKING.COM | FLUTTER.COM | SALELYTICS.COM
HOERMANN-GRUPPE.COM | ALEKTUM.COM | HUBBELL.COM | KELLYSERVICES.COM | AMERISAVE.COM
CONVERGEONE.COM | ALOGENT.COM | SOFTTECH.NL | ALOHACARE.ORG | SYNLAB.FR | INFORMATICA.COM

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

In mid-July, when the CLOP ransomware group was actively listing and threatening their victims, bleepingcomputer published an article titled "Clop gang to earn over $75 million from MOVEit extortion attacks"[2] based on Coveware's blog post.[3] According to this article, the CLOP ransomware group is expected to raise between $75-100 million from extorting victims of their large-scale MOVEit data leakage campaign.

[2] https://www.bleepingcomputer.com/news/security/clop-gang-to-earn-over-75-million-from-moveit-extortion-attacks/

[3] https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments

The ransomware groups who launched massive data exfiltration attacks like CLOP and 8BASE seem to change their tactics to demanding far more significant ransom to a small handful of victims who succumb to "name-and-shame" pressure, because these payments outweighs the sum coming from large pool of victims with moderate ransom payment.
According to Coveware's report, the number of victims paying ransom has dropped to an all-time low of 34%, luring ransomware groups to adopt a tactic that makes their attacks more profitable.

Below are some articles that describes the profit generation and negotiation tactics of some ransomware groups including CLOP.

- www.bleepingcomputer.com: Ransomware payments on record-breaking trajectory for 2023
- www.bleepingcomputer.com: Clop gang to earn over $75 million from MOVEit extortion attacks
- www.coveware.com: Ransom Monetization Rates Fall to Record Low Despite Jump In Average Ransom Payments

CLOP continues to add tens of new victims their DLS in July. It is predicted that the issue of "CLOP ransomware's activities involving the exploitation of the MOVEit zero-day vulnerability and the group's disclosure of their victims" will continue for a while.

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

2) Big Head ransomware disguised as an emergency Windows update

Analysis information on the Big Head ransomware first introduced in the Fortinet blog post titled "Ransomware Roundup - Big Head".[4] Afterward, bleepingcomputer published an article titled "New 'Big Head' ransomware displays fake Windows update alert",[5] based on Trend Micro's blog post "Tailing Big Head Ransomware's Variants, Tactics, and Impact"[6] uploaded on

[4] https://www.fortinet.com/blog/threat-research/fortiguard-labs-ransomware-roundup-big-head

[5] https://www.bleepingcomputer.com/news/security/new-big-head-ransomware-displays-fake-windows-update-alert/

[6] https://www.trendmicro.com/en_us/research/23/g/tailing-big-head-ransomware-variants-tactics-and-impact.html

July 7.

The Big Head ransomware is a new kind of ransomware that can spread through malicious advertisements for fake Windows updates and Microsoft Word installers. While Big Head neither has any technical advantages that set it apart from other ransomware nor inflicted any serious harm, it is included in this report because its tactic to block users' attempts to intervene or stop the encryption was interesting; during the file encryption process, a pop-up window with the message "Configuring critical Windows Updates..." was used to cover the whole screen, disguising the ransomware as a normal Windows update process.

There are many variants of the Big Head ransomware, but this report will summarize the details of the tests run with the first sample type provided by Trend Micro's analysis post.

- www.trendmicro.com: Tailing Big Head Ransomware's Variants, Tactics, and Impact

The first sample of Big Head ransomware '1.exe' file contains three encrypted files in its resources, as shown in the figure below. This section will take a look at BXIuSsB.exe, which is dropped by the third file, Xarch.exe. The BXIuSsB.exe code contains the file encryption and the "Fake Windows updates" features.

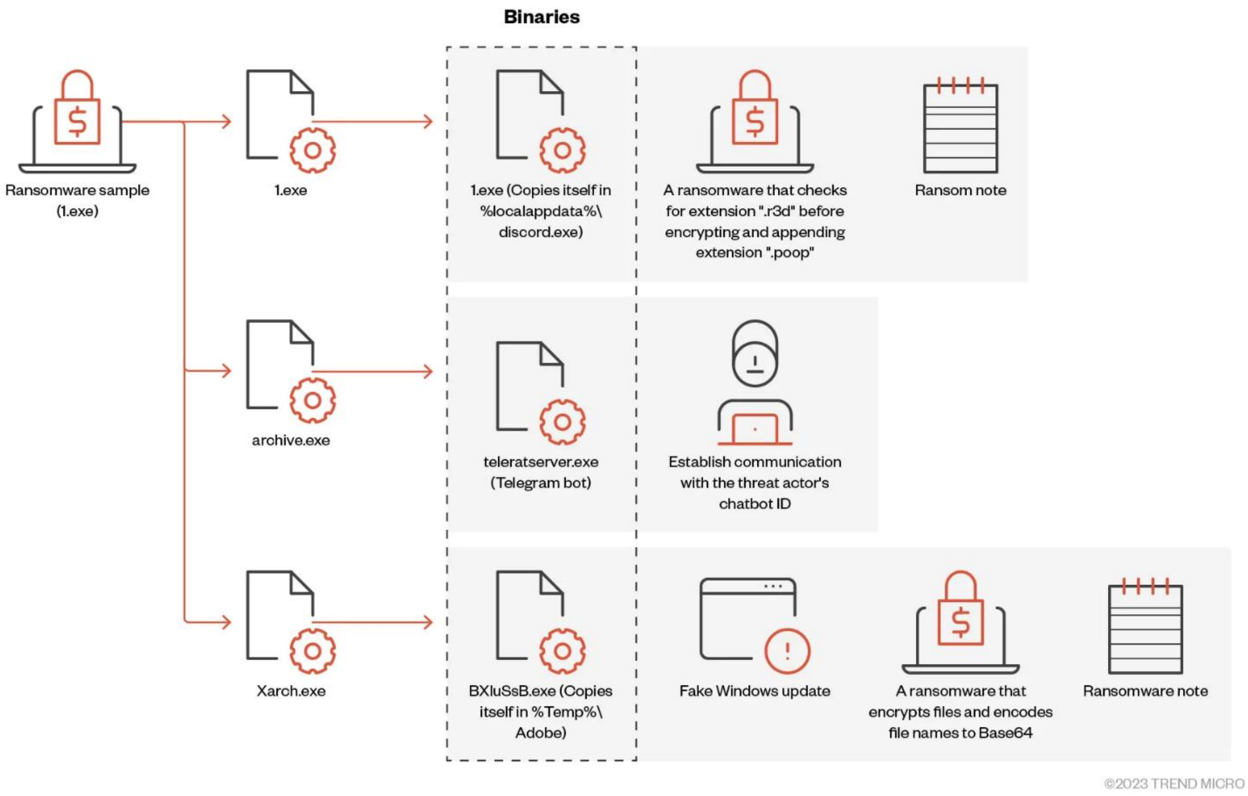
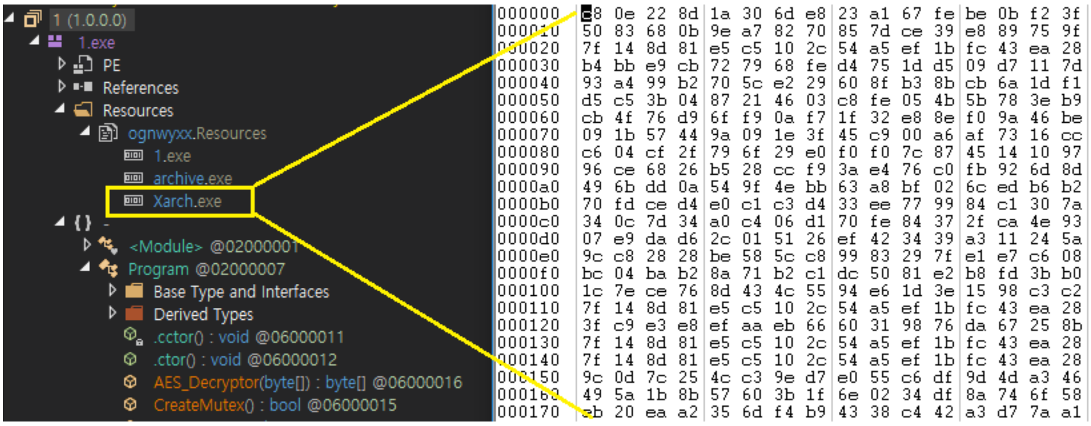

Binaries
Ransomware sample (1.exe)
1.exe
1.exe (Copies itself in %localappdata%\discord.exe)
A ransomware that checks for extension ".r3d" before encrypting and appending extension ".poop"
Ransom note
archive.exe
teleratserver.exe (Telegram bot)
Establish communication with the threat actor's chatbot ID
Xarch.exe
BXIuSsB.exe (Copies itself in %Temp%\Adobe)
Fake Windows update
A ransomware that encrypts files and encodes file names to Base64
Ransomware note
©2023 TREND MICRO

Figure 11. First sample of Big Head Ransomware <Source>www.trendmicro.com

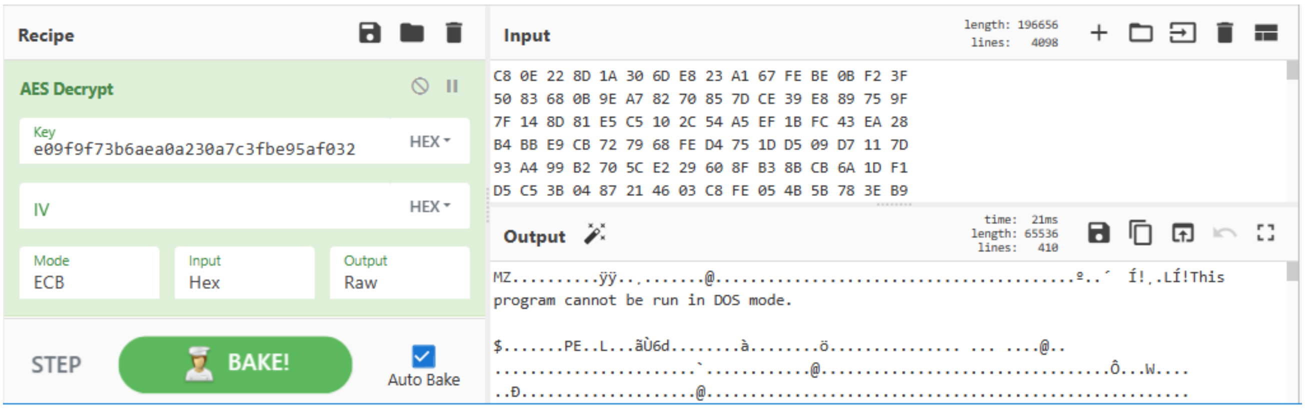
Xarch.exe, which is included in the resources of 1.exe, is encrypted as shown below. Using a hard-coded key value within the code, this is decrypted with an AES algorithm before being executed.



```
1 (1.0.0.0)
  1.exe
    PE
    References
    Resources
      ognwyxx.Resources
        1.exe
        archive.exe
        Xarch.exe
    { } -
      <Module> @02000001
      Program @02000007
        Base Type and Interfaces
        Derived Types
        .cctor() : void @06000011
        .ctor() : void @06000012
        AES_Decryptor(byte[]) : byte[] @06000016
        CreateMutex() : bool @06000015
```

```
000000 c8 0e 22 8d 1a 30 6d e8 23 a1 67 fe be 0b f2 3f
000010 50 83 68 0b 9e a7 82 70 85 7d ce 39 e8 89 75 9f
000020 7f 14 8d 81 e5 c5 10 2c 54 a5 ef 1b fc 43 ea 28
000030 b4 bb e9 cb 72 79 68 fe d4 75 1d d5 09 d7 11 7d
000040 93 a4 99 b2 70 5c e2 29 60 8f b3 8b cb 6a 1d f1
000050 d5 c5 3b 04 87 21 46 03 c8 fe 05 4b 5b 78 3e b9
000060 cb 4f 76 d9 6f f9 0a f7 1f 32 e8 8e f0 9a 46 be
000070 09 1b 57 44 9a 09 1e 3f 45 c9 00 a6 af 73 16 cc
000080 c6 04 cf 2f 79 6f 29 e0 f0 f0 7c 87 45 14 10 97
000090 96 ce 68 26 b5 28 cc f9 3a e4 76 c0 fb 92 6d 8d
0000a0 49 6b dd 0a 54 9f 4e bb 63 a8 bf 02 6c ed b6 b2
0000b0 70 fd ce d4 e0 c1 c3 d4 33 ee 77 99 84 c1 30 7a
0000c0 34 0c 7d 34 a0 c4 06 d1 70 fe 84 37 2f ca 4e 93
0000d0 07 e9 da d6 2c 01 51 26 ef 42 34 39 a3 11 24 5a
0000e0 9c c8 28 28 be 58 5c c8 99 83 29 7f e1 e7 c6 08
0000f0 bc 04 ba b2 8a 71 b2 c1 dc 50 81 e2 b8 fd 3b b0
000100 1c 7e ce 76 8d 43 4c 55 94 e6 1d 3e 15 98 c3 c2
000110 7f 14 8d 81 e5 c5 10 2c 54 a5 ef 1b fc 43 ea 28
000120 3f c9 e3 e8 ef aa eb 66 60 31 98 76 da 67 25 8b
000130 7f 14 8d 81 e5 c5 10 2c 54 a5 ef 1b fc 43 ea 28
000140 7f 14 8d 81 e5 c5 10 2c 54 a5 ef 1b fc 43 ea 28
000150 9c 0d 7c 25 4c c3 9e d7 e0 55 c6 df 9d 4d a3 46
000160 49 5a 1b 8b 57 60 3b 1f 6e 02 34 df 8a 74 6f 58
000170 eb 20 ea a2 35 6d f4 b9 43 38 c4 42 a3 d7 7a a1
```

Figure 12. Resource configuration of Big Head ransomware's 1.exe



Recipe

AES Decrypt

Key: e09f9f73b6aea0a230a7c3fbe95af032 (HEX)

IV: (HEX)

Mode: ECB

Input: Hex

Output: Raw

Input — length: 196656, lines: 4098

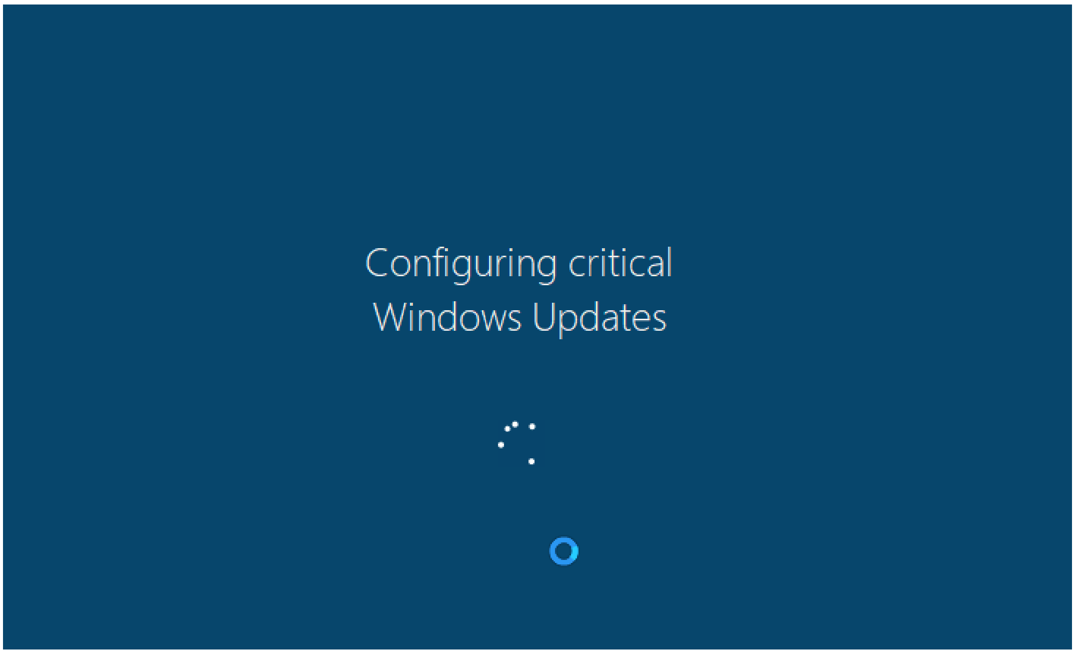
```
C8 0E 22 8D 1A 30 6D E8 23 A1 67 FE BE 0B F2 3F
50 83 68 0B 9E A7 82 70 85 7D CE 39 E8 89 75 9F
7F 14 8D 81 E5 C5 10 2C 54 A5 EF 1B FC 43 EA 28
B4 BB E9 CB 72 79 68 FE D4 75 1D D5 09 D7 11 7D
93 A4 99 B2 70 5C E2 29 60 8F B3 8B CB 6A 1D F1
D5 C5 3B 04 87 21 46 03 C8 FE 05 4B 5B 78 3E B9
```

Output — time: 21ms, length: 65536, lines: 410

```
MZ.........ÿÿ..,.......@....................................º..´ Í!,.LÍ!This
program cannot be run in DOS mode.

$.......PE..L...ãÙ6d........à........ö............... ... ....@..
......................`...........@..............................Ô...W....
..Ð..................@...............................................
```

Figure 13. Decrypting Xarch.exe

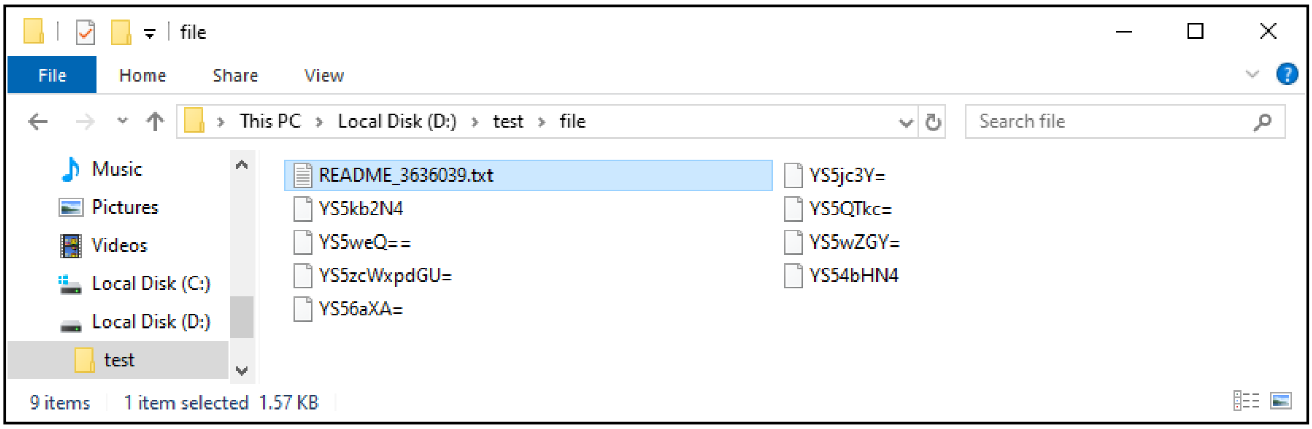
Afterward, Xarch.exe is put through an AES decryption code using a key value different from 1.exe and executes BXluSsB.exe which displays the fake Windows update screen and has ransomware features. At the user file encryption stage, it employs the strategy of covering the whole screen with the fake Windows update screen shown below. Additionally, the code was to display the message "x% complete Do not turn off your computer." at the bottom of the screen, but this was not displayed in the test system.



Configuring critical
Windows Updates

Figure 14. Big Head ransomware's fake Windows update window

While the fake Windows update screen is being displayed, files are encrypted. The encrypted files are changed to have the previous file name encoded in Base64 shown below, and finally, a ransom note is created with a file name containing an ID in the format "README_3636039.txt".



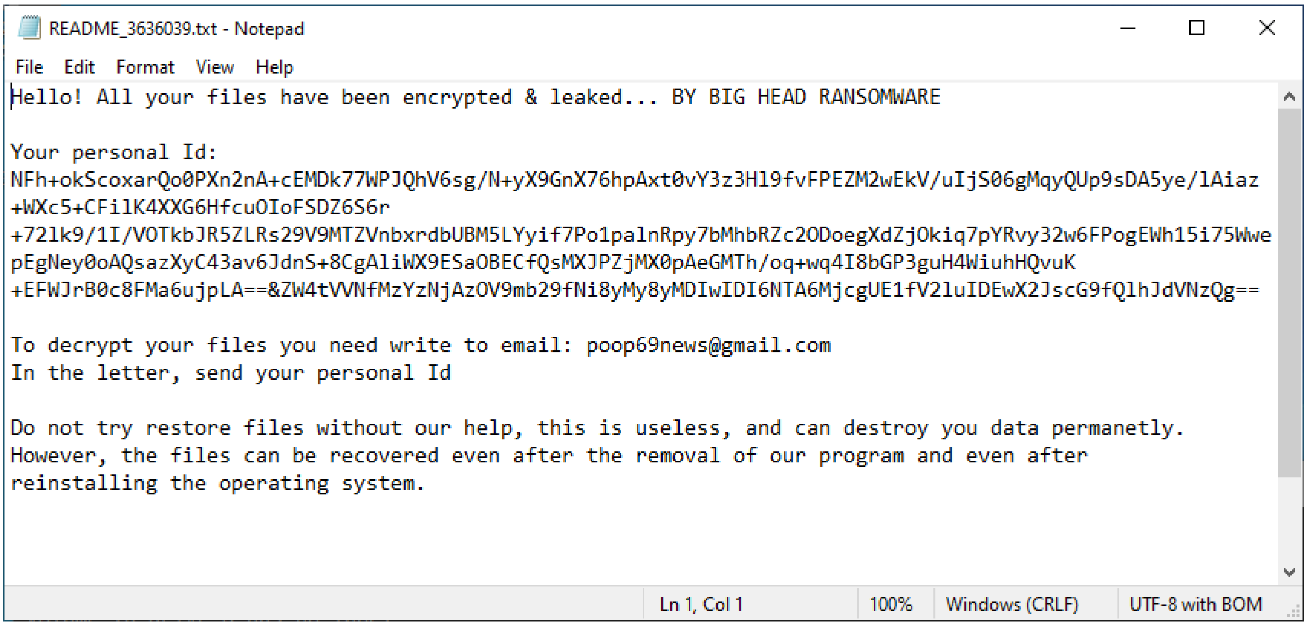
README_3636039.txt
YS5kb2N4
YS5weQ==
YS5zcWxpdGU=
YS56aXA=
YS5jc3Y=
YS5QTkc=
YS5wZGY=
YS54bHN4

9 items 1 item selected 1.57 KB

Figure 15. Big Head ransomware's encryption

For your information, the file names on the left of the above explorer screen are as follows.

YS54bHN4	// a.xlsx
YS5weQ==	// a.py
YS5zcWxpdGU=	// a.sqlite
YS56aXA=	// a.zip

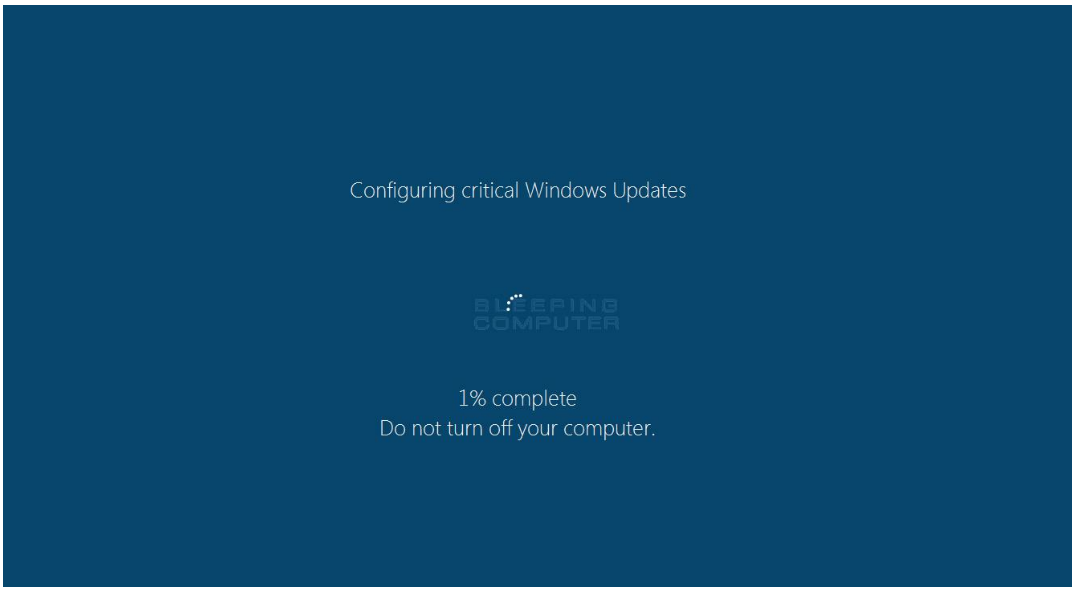


```
Hello! All your files have been encrypted & leaked... BY BIG HEAD RANSOMWARE

Your personal Id:
NFh+okScoxarQo0PXn2nA+cEMDk77WPJQhV6sg/N+yX9GnX76hpAxt0vY3z3Hl9fvFPEZM2wEkV/uIjS06gMqyQUp9sDA5ye/lAiaz
+WXc5+CFilK4XXG6HfcuOIoFSDZ6S6r
+72lk9/1I/VOTkbJR5ZLRs29V9MTZVnbxrdbUBM5LYyif7Po1palnRpy7bMhbRZc2ODoegXdZjOkiq7pYRvy32w6FPogEWh15i75Wwe
pEgNey0oAQsazXyC43av6JdnS+8CgAliWX9ESaOBECfQsMXJPZjMX0pAeGMTh/oq+wq4I8bGP3guH4WiuhHQvuK
+EFWJrB0c8FMa6ujpLA==&ZW4tVVNfMzYzNjAzOV9mb29fNi8yMy8yMDIwIDI6NTA6MjcgUE1fV2luIDEwX2JscG9fQlhJdVNzQg==

To decrypt your files you need write to email: poop69news@gmail.com
In the letter, send your personal Id

Do not try restore files without our help, this is useless, and can destroy you data permanetly.
However, the files can be recovered even after the removal of our program and even after
reinstalling the operating system.
```

Figure 16. Big Head ransomware's ransom note - README_xxxxxxx.txt

Before concluding this section, we searched for past cases where a fake but legitimate-looking "Configuring critical Windows Updates…" screen was used. It was confirmed that a fake Windows update screen with the same message and style was used by the Fantom ransomware in August 2016. The URL of the article and the screen image are included here as a reference, as the screen was not fully shown during our test.

- www.bleepingcomputer.com: Fantom Ransomware Encrypts your Files while pretending to be Windows Update


Configuring critical Windows Updates

1% complete
Do not turn off your computer.

Figure 17. Fantom's fake Windows update screen <Source> www.bleepingcomputer.com

The Big Head ransomware is known to disguise itself as fake Windows updates and

Microsoft Word installers, so users must download operating systems, work productivity software, and games from their official websites. Users should also follow the general guidelines of doing periodic backups, as well as installing, using, and updating security software.

IOCs for Reference
6d27c1b457a34ce9edfb4060d9e04eb44d021a7b03223ee72ca569c8c4215438 1.exe
bcf8464d042171d7ecaada848b5403b6a810a91f7fd8f298b611e94fa7250463 Xarch.exe
64246b9455d76a094376b04a2584d16771cd6164db72287492078719a0c749ab BXIuSsB.exe

3) Detection names for ransomware disguised as Sophos file

New ransomware disguised as a file created by cyber security vendor Sophos was introduced with the name SophosEncrypt. At first, it was thought to be a part of the activities of the Sophos Red Team, but the Sophos X-Ops team uploaded a tweet stating that they are in no part connected to such activities and that the ransomware was being detected by their product. [7]

The bleepingcomputer wrote an article about this titled "Cybersecurity firm Sophos impersonated by new SophosEncrypt ransomware"[8] on July 18. A few days later, on July 23, Sophos released detailed analysis results titled "Sophos Discovers Ransomware Abusing “Sophos” Name" along with a decryption tool for encrypted files.[9]

Additionally, the ransomware name "SophosEncrypt" had been already added to ID Ransomware (a ransomware type identification service provided by MalwareHunterTeam) at the time of discovery, but currently, most cyber security companies use a different detection name. This will be covered in more detail further on.

Based on the ransomware hash shared in the MalwareHunterTeam tweet, we will briefly examine the execution results of this file (3da31ee0a6c6410b3c66aad41623d05aac61a4dbb85045eb89f5810ffdc93066).This ransomware is run

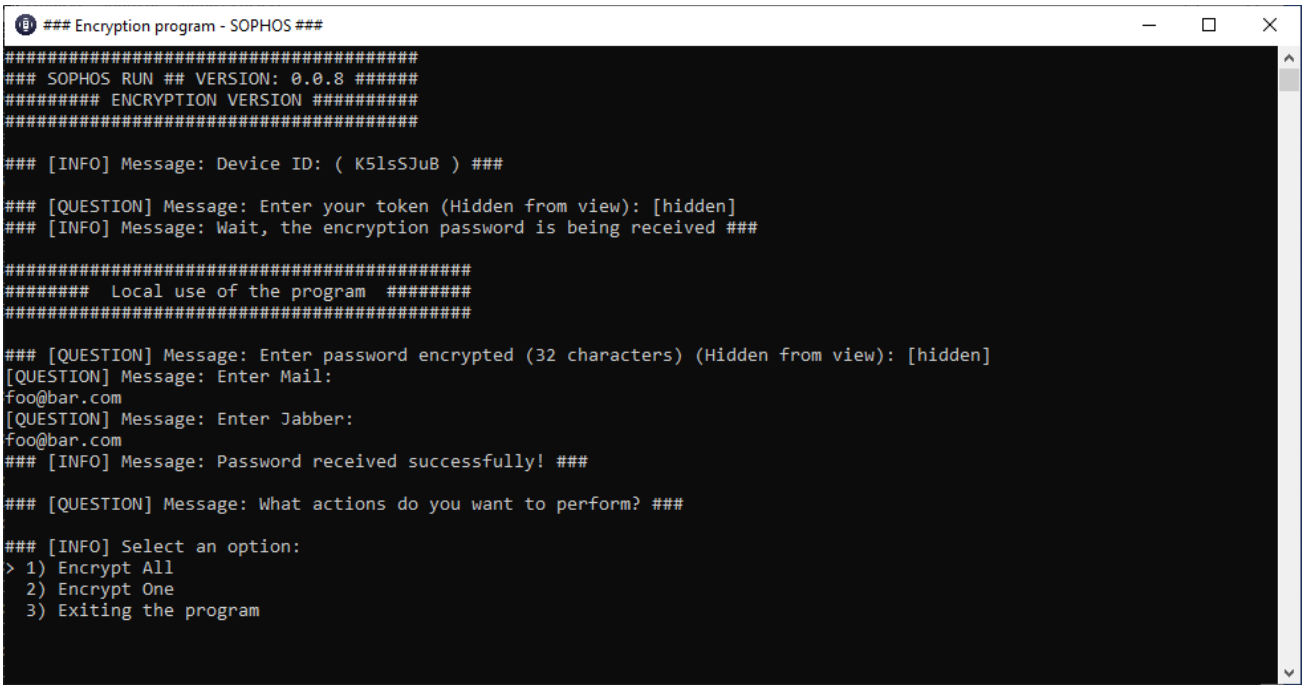
[7] https://twitter.com/SophosXOps/status/1681048700209045505

[8] https://www.bleepingcomputer.com/news/security/cybersecurity-firm-sophos-impersonated-by-new-sophosencrypt-ransomware/

[9] https://news.sophos.com/en-us/2023/07/18/sophos-discovers-ransomware-abusing-sophos-name/

through the command line interface (CLI) and requires the threat actor to input a few things. The arguments given during testing are as follows. If the password is not 32 characters in length, it is terminated.

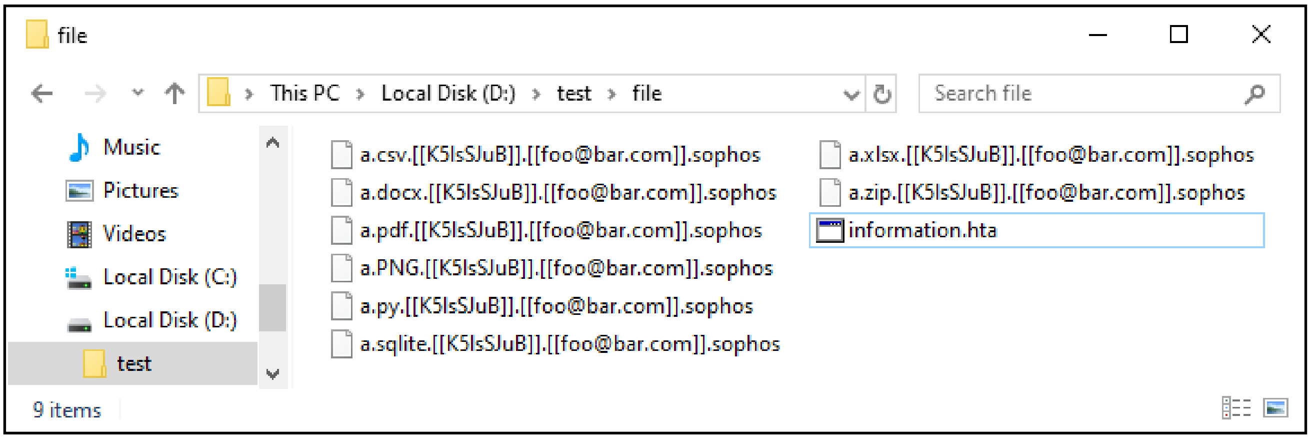
- token: aaa
- password: 111…111 (32 characters)
- Mail/Jabber: foo@bar.com
- option: 1) Encrypt All



```
#######################################
### SOPHOS RUN ## VERSION: 0.0.8 ######
######### ENCRYPTION VERSION ##########
#######################################

### [INFO] Message: Device ID: ( K5lsSJuB ) ###

### [QUESTION] Message: Enter your token (Hidden from view): [hidden]
### [INFO] Message: Wait, the encryption password is being received ###

############################################
########  Local use of the program  ########
############################################

### [QUESTION] Message: Enter password encrypted (32 characters) (Hidden from view): [hidden]
[QUESTION] Message: Enter Mail:
foo@bar.com
[QUESTION] Message: Enter Jabber:
foo@bar.com
### [INFO] Message: Password received successfully! ###

### [QUESTION] Message: What actions do you want to perform? ###

### [INFO] Select an option:
> 1) Encrypt All
  2) Encrypt One
  3) Exiting the program
```

Figure 18. Executing the ransomware

The file encryption process scrolls on the command window. File extensions with the format ".[[-ID-]].[[-Mail-]].sophos" are added to the file names and the ransom note "information.hta" is created in each directory.



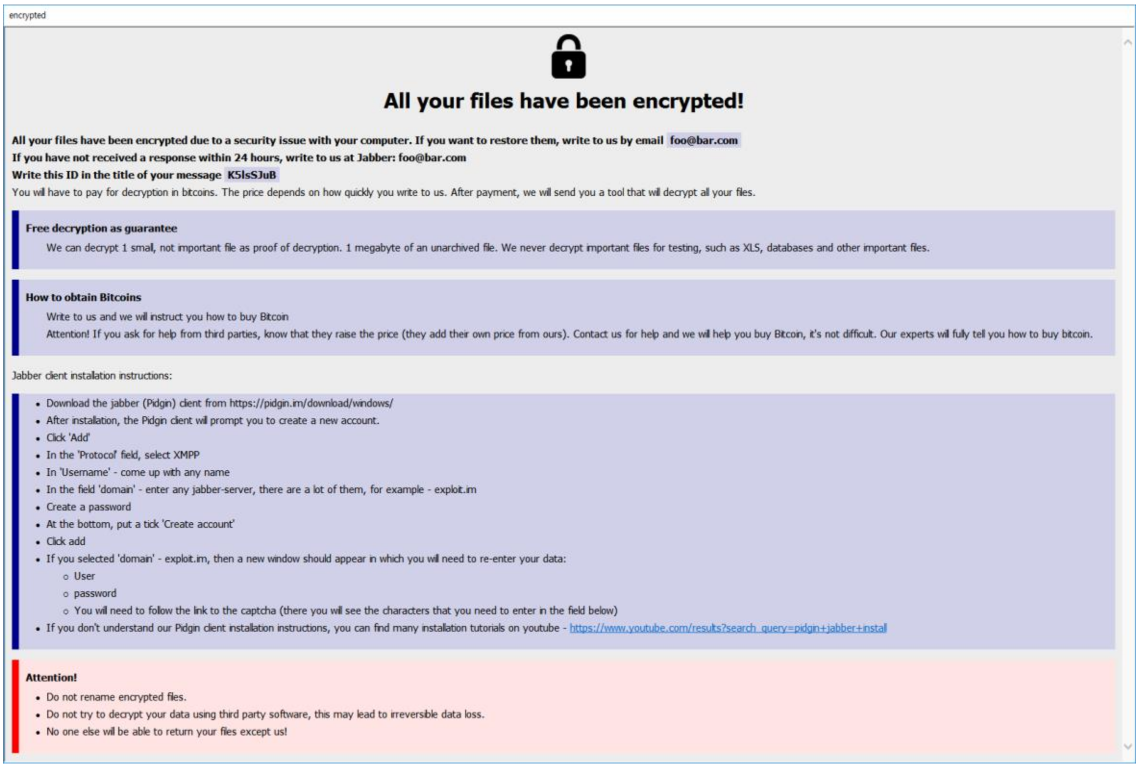
a.csv.[[K5lsSJuB]].[[foo@bar.com]].sophos
a.docx.[[K5lsSJuB]].[[foo@bar.com]].sophos
a.pdf.[[K5lsSJuB]].[[foo@bar.com]].sophos
a.PNG.[[K5lsSJuB]].[[foo@bar.com]].sophos
a.py.[[K5lsSJuB]].[[foo@bar.com]].sophos
a.sqlite.[[K5lsSJuB]].[[foo@bar.com]].sophos
a.xlsx.[[K5lsSJuB]].[[foo@bar.com]].sophos
a.zip.[[K5lsSJuB]].[[foo@bar.com]].sophos
information.hta

Figure 19. Files encrypted with the ransomware and the ransom note

Additionally, Sophos released the POC Python code for the ransomware decryption tool which receives the password used in the encryption process as an input.[10] It is not often that a decryption tool is released for ransomware, but if necessary following websites may be useful for reference materials.

- www.nomoreransom.org: NO MORE RANSOM decryption tools
- Seed.kisa.or.kr:: Search page for KISA's ransomware decryption tools (This page is available in Korean only)

The ransom note "information.hta" consists of a unique device ID value assigned to each infected system upon ransomware execution and the threat actor's email address given as an input argument, as shown below.



All your files have been encrypted!

All your files have been encrypted due to a security issue with your computer. If you want to restore them, write to us by email foo@bar.com
If you have not received a response within 24 hours, write to us at Jabber: foo@bar.com
Write this ID in the title of your message K5lsSJuB
You will have to pay for decryption in bitcoins. The price depends on how quickly you write to us. After payment, we will send you a tool that will decrypt all your files.

Free decryption as guarantee
We can decrypt 1 small, not important file as proof of decryption. 1 megabyte of an unarchived file. We never decrypt important files for testing, such as XLS, databases and other important files.

How to obtain Bitcoins
Write to us and we will instruct you how to buy Bitcoin
Attention! If you ask for help from third parties, know that they raise the price (they add their own price from ours). Contact us for help and we will help you buy Bitcoin, it's not difficult. Our experts will fully tell you how to buy bitcoin.

Jabber client installation instructions:

- Download the jabber (Pidgin) client from https://pidgin.im/download/windows/
- After installation, the Pidgin client will prompt you to create a new account.
- Click 'Add'
- In the 'Protocol' field, select XMPP
- In 'Username' - come up with any name
- In the field 'domain' - enter any jabber-server, there are a lot of them, for example - exploit.im
- Create a password
- At the bottom, put a tick 'Create account'
- Click add
- If you selected 'domain' - exploit.im, then a new window should appear in which you will need to re-enter your data:
  - User
  - password
  - You will need to follow the link to the captcha (there you will see the characters that you need to enter in the field below)
- If you don't understand our Pidgin client installation instructions, you can find many installation tutorials on youtube - https://www.youtube.com/results?search_query=pidgin+jabber+install

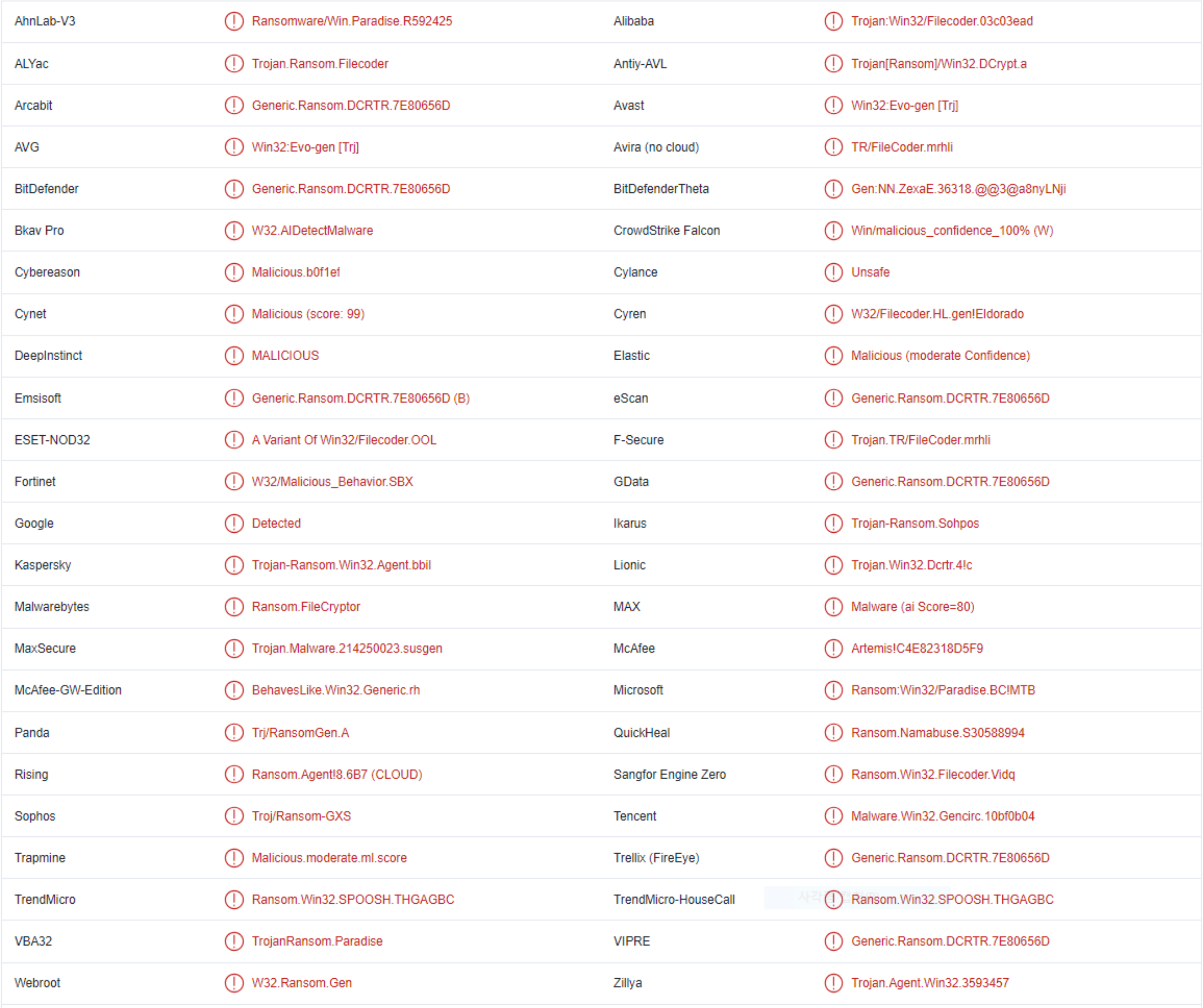
Attention!
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, this may lead to irreversible data loss.
- No one else will be able to return your files except us!

Figure 20. Ransom note "information.hta"

This is as far as this post will cover on this ransomware. For more technical details, please refer to Sophos's analysis details. We investigated to see what detection names are used by other security companies for the SophosEncrypt ransomware mentioned at the beginning of this

[10] https://news.sophos.com/en-us/2023/07/18/sophos-discovers-ransomware-abusing-sophos-name/

section. The following figure is a screenshot of search result of hash value used in the above example on VirusTotal.



AhnLab-V3	ⓘ Ransomware/Win.Paradise.R592425	Alibaba	ⓘ Trojan:Win32/Filecoder.03c03ead
ALYac	ⓘ Trojan.Ransom.Filecoder	Antiy-AVL	ⓘ Trojan[Ransom]/Win32.DCrypt.a
Arcabit	ⓘ Generic.Ransom.DCRTR.7E80656D	Avast	ⓘ Win32:Evo-gen [Trj]
AVG	ⓘ Win32:Evo-gen [Trj]	Avira (no cloud)	ⓘ TR/FileCoder.mrhli
BitDefender	ⓘ Generic.Ransom.DCRTR.7E80656D	BitDefenderTheta	ⓘ Gen:NN.ZexaE.36318.@@3@a8nyLNji
Bkav Pro	ⓘ W32.AIDetectMalware	CrowdStrike Falcon	ⓘ Win/malicious_confidence_100% (W)
Cybereason	ⓘ Malicious.b0f1ef	Cylance	ⓘ Unsafe
Cynet	ⓘ Malicious (score: 99)	Cyren	ⓘ W32/Filecoder.HL.gen!Eldorado
DeepInstinct	ⓘ MALICIOUS	Elastic	ⓘ Malicious (moderate Confidence)
Emsisoft	ⓘ Generic.Ransom.DCRTR.7E80656D (B)	eScan	ⓘ Generic.Ransom.DCRTR.7E80656D
ESET-NOD32	ⓘ A Variant Of Win32/Filecoder.OOL	F-Secure	ⓘ Trojan.TR/FileCoder.mrhli
Fortinet	ⓘ W32/Malicious_Behavior.SBX	GData	ⓘ Generic.Ransom.DCRTR.7E80656D
Google	ⓘ Detected	Ikarus	ⓘ Trojan-Ransom.Sohpos
Kaspersky	ⓘ Trojan-Ransom.Win32.Agent.bbil	Lionic	ⓘ Trojan.Win32.Dcrtr.4!c
Malwarebytes	ⓘ Ransom.FileCryptor	MAX	ⓘ Malware (ai Score=80)
MaxSecure	ⓘ Trojan.Malware.214250023.susgen	McAfee	ⓘ Artemis!C4E82318D5F9
McAfee-GW-Edition	ⓘ BehavesLike.Win32.Generic.rh	Microsoft	ⓘ Ransom:Win32/Paradise.BC!MTB
Panda	ⓘ Trj/RansomGen.A	QuickHeal	ⓘ Ransom.Namabuse.S30588994
Rising	ⓘ Ransom.Agent!8.6B7 (CLOUD)	Sangfor Engine Zero	ⓘ Ransom.Win32.Filecoder.Vidq
Sophos	ⓘ Troj/Ransom-GXS	Tencent	ⓘ Malware.Win32.Gencirc.10bf0b04
Trapmine	ⓘ Malicious.moderate.ml.score	Trellix (FireEye)	ⓘ Generic.Ransom.DCRTR.7E80656D
TrendMicro	ⓘ Ransom.Win32.SPOOSH.THGAGBC	TrendMicro-HouseCall	ⓘ Ransom.Win32.SPOOSH.THGAGBC
VBA32	ⓘ TrojanRansom.Paradise	VIPRE	ⓘ Generic.Ransom.DCRTR.7E80656D
Webroot	ⓘ W32.Ransom.Gen	Zillya	ⓘ Trojan.Agent.Win32.3593457

Figure 21.Some of the VirusTotal detection results <Source> www.virustotal.com

Most companies (44 products) used common names such as Generic, Agent, and FileCoder instead of identifiable names, and some companies (2 products) used the detection name Paradise, which is the previous version of the ransomware.

- Ransomware/Win.Paradise.R592425
- Ransom:Win32/Paradise.BC!MTB

Other companies (3 products) use detection names with adequately rearranged versions of the string "Sophos".

- Trojan-Ransom.Sohpos
- Ransom.Win32.SPOOSH.THGAGBC

Each security company has its own way of assigning detection names to malware. The variety of detection names as shown above are not problematic but rather natural outcomes. Ordinarily, security companies select detection names by grouping the malware by common characteristics (e.g., same malware developer, type of code, or feature properties). However, some security companies may give different names for the same malware type. Despite of that, there is an implicit rule among security companies to use detection names with no discernible connection to certain companies, individuals, countries, or areas, as shown above.

We, at Ahnlab, assigned the detection name Paradise to the ransomware considering the similarity in the naming pattern for the encrypted files used in recently observed Paradise ransomware and in the layouts of the html ransom notes.

The encrypted file names and ransom notes used by the Paradise ransomware are as follows.

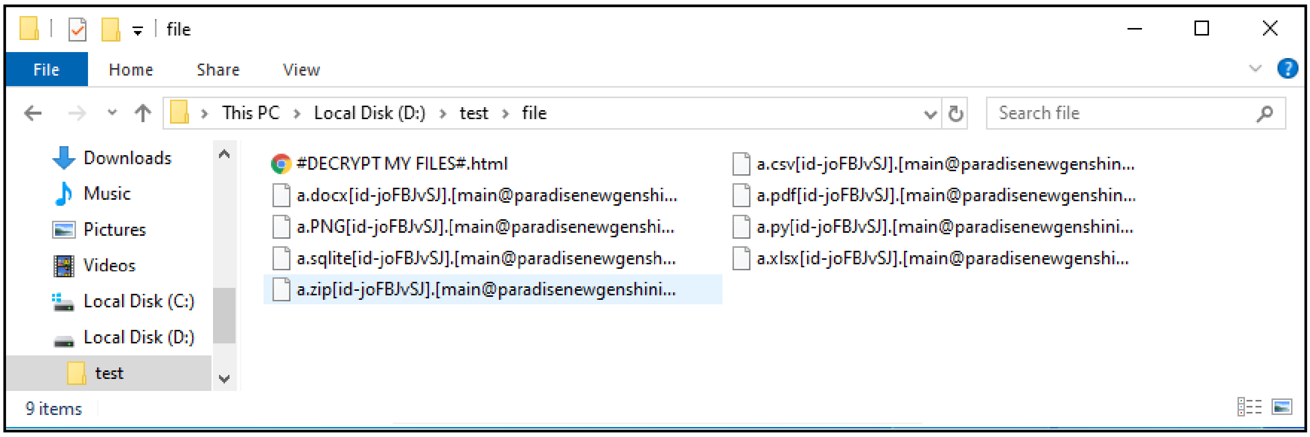
- [-ID-][-Mail-].honkai
- #DECRYPT MY FILES#.html

For additional analysis details on the Paradise ransomware, please refer to the post below.

- asec.ahnlab.com: Paradise Ransomware Distributed Through AweSun Vulnerability Exploitation

IOC for Reference (Paradise Ransomware)

5cbbc1adfd22f852a37a791a2415c92c

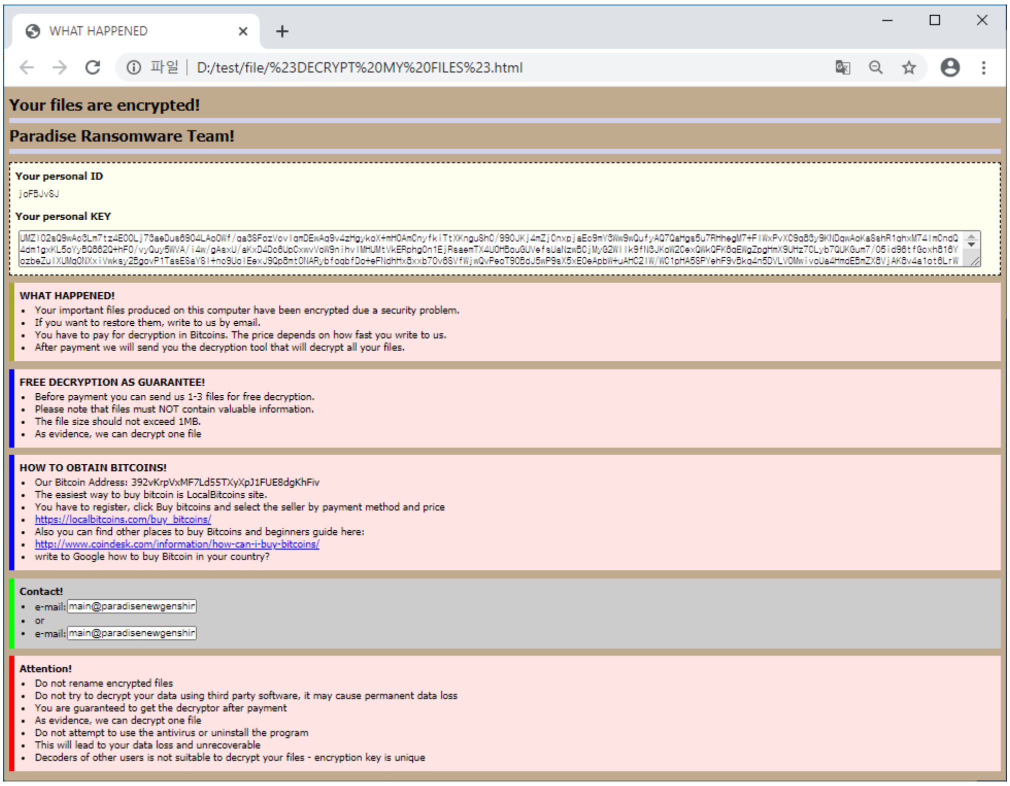


#DECRYPT MY FILES#.html
a.docx[id-joFBJvSJ].[main@paradisenewgenshi...
a.PNG[id-joFBJvSJ].[main@paradisenewgenshi...
a.sqlite[id-joFBJvSJ].[main@paradisenewgensh...
a.zip[id-joFBJvSJ].[main@paradisenewgenshini...
a.csv[id-joFBJvSJ].[main@paradisenewgenshin...
a.pdf[id-joFBJvSJ].[main@paradisenewgenshin...
a.py[id-joFBJvSJ].[main@paradisenewgenshini...
a.xlsx[id-joFBJvSJ].[main@paradisenewgenshi...

Figure 22. Encrypted files and ransom note of the Paradise ransomware

The encrypted file name of a.zip in the image above is as follows.

- a.zip[id-joFBJvSJ].[main@paradisenewgenshinimpact.top].honkai



Your files are encrypted!

Paradise Ransomware Team!

Your personal ID

joFBJvSJ

Your personal KEY

```
UMZI02sQ9wAo3Lm7tz4E00Lj73aeDus6904LAo0Wf/qa3SFozVovIqmDEwAq9v4zHgykoX+mH0AmCnyfkiTtXKnguShC/990JKj4mZjCnxpjaEo9mY3Ww9wQufyAQ7QaHgs5u7RHhegM7+FIWxPvXC9q83y9KNDqwAoKaSshR1qhxM74ImCndQ
4dm1gxKL5oYyBQ862Q+hF0/vyQuy5WVA/i4w/gAsxU/aKxD4Do6UpCxwvVoW9nihvIMHUMtVkERphg0n1EjRsaemTX4U0HBouGUVefsUaNzwBCjMyG2WIIk9fN3JKoW2CexQWkQFK6qEWgZpgHmX9UHz7CLyb7QUKGum7/05id96tfGoxh816Y
ozbeZuIXUMq0NXxiVwksy2BgovP1TasESaYSI+no9UoIEexJ9Qp8mt0NARybfoqbfDo+eFNdhHx8xxb70v6SVfWjwQvPeoT905dJ5wP9aX5xE0eApbW+uAHC2IW/WC1pHA5SPYehF9vBkq4n5DVLV0MwivoUa4HmdEBmZX8VjAK8v4a1ot6LrW
```

WHAT HAPPENED!

- Your important files produced on this computer have been encrypted due a security problem.
- If you want to restore them, write to us by email.
- You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
- After payment we will send you the decryption tool that will decrypt all your files.

FREE DECRYPTION AS GUARANTEE!

- Before payment you can send us 1-3 files for free decryption.
- Please note that files must NOT contain valuable information.
- The file size should not exceed 1MB.
- As evidence, we can decrypt one file

HOW TO OBTAIN BITCOINS!

- Our Bitcoin Address: 392vKrpVxMF7Ld55TXyXpJ1FUE8dgKhFiv
- The easiest way to buy bitcoin is LocalBitcoins site.
- You have to register, click Buy bitcoins and select the seller by payment method and price
- https://localbitcoins.com/buy_bitcoins/
- Also you can find other places to buy Bitcoins and beginners guide here:
- http://www.coindesk.com/information/how-can-i-buy-bitcoins/
- write to Google how to buy Bitcoin in your country?

Contact!

- e-mail: main@paradisenewgenshir
- or
- e-mail: main@paradisenewgenshir

Attention!

- Do not rename encrypted files
- Do not try to decrypt your data using third party software, it may cause permanent data loss
- You are guaranteed to get the decryptor after payment
- As evidence, we can decrypt one file
- Do not attempt to use the antivirus or uninstall the program
- This will lead to your data loss and unrecoverable
- Decoders of other users is not suitable to decrypt your files - encryption key is unique

Figure 23. Paradise ransomware's ransom note "#DECRYPT MY FILES#.html"

The ransomware that disguised itself as a Sophos file cannot inflict substantive damage in its current state. However, ransomware groups make various attempts to avoid suspicion from users and maximize profit through tactics such as impersonating legitimate programs of security companies or using social issues and news grabbing users' attention. To minimize harm from such attack methods, organizations and individual users must comply with security guidelines, such as applying the latest security updates, removing unnecessary software, practicing periodic backups as well as installing, using, and updating security software.

IOCs for Reference

3da31ee0a6c6410b3c66aad41623d05aac61a4dbb85045eb89f5810ffdc93066

f15a0f660ef0bd9e116ff19b433451d403ffedea9469a095c2f429227500e87a

4) Others

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

- BlackCat ransomware pushes Cobalt Strike via WinSCP search ads (July 2)
- Underground, New Ransomware (July 11)
- FIN8 deploys ALPHV ransomware using Sardonic malware variant (July 18)
- Ransomware Variants of the Vice Society Gang Focusing Attacks on the US and European Education and Medical Fields (July 19)
- Global US Cosmetics Company Listed as a Victim of ALPHV (BlackCat) (July 20)
- Understanding the rising threat of Money Message ransomware (July 20)
- Mallox Ransomware Operators Infiltrate Networks Through MS-SQL Servers (July 21)
- Monti Ransomware Group Posts Hungarian Investment Promotion Agency (HIPA) as a Victim (July 25)
- New Nitrogen malware pushed via Google Ads for ransomware attacks (July 27)
- Global Consulting Company Listed as a Victim of the Akira Ransomware Group (July 31)

Conclusion

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

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

- Apply the latest security updates for operating systems and software. Enable auto-update.
- Install and use security software. Maintain the latest updates.
- Back up data regularly and store said data in an offline or separate network.

- Be cautious of websites from unreliable sources and viewing/executing email links and attachments.
- Use strong passwords and two-factor authentication (2FA).

Indicators Of Compromise (IOC)

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

1) File Paths and Names

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

2) File Hashes

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

```
6d27c1b457a34ce9edfb4060d9e04eb44d021a7b03223ee72ca569c8c4215438 // Big Head
226bec8acd653ea9f4b7ea4eaa75703696863841853f488b0b7d892a6be3832a
ff900b9224fde97889d37b81855a976cddf64be50af280e04ce53c587d978840
cf9410565f8a06af92d65e118bd2dbaeb146d7e51de2c35ba84b47cfa8e4f53b
1c8bc3890f3f202e459fb87acec4602955697eef3b08c93c15ebb0facb019845
64246b9455d76a094376b04a2584d16771cd6164db72287492078719a0c749ab
0dbfd3479cfaf0856eb8a75f0ad4fccb5fd6bd17164bcfa6a5a386ed7378958d
6698f8ffb7ba04c2496634ff69b0a3de9537716cfc8f76d1cfea419dbd880c94
b8e456861a5fb452bcf08d7b37277972a4a06b0a928d57c5ec30afa101d77ead
6b3bf710cf4a0806b2c5eaa26d2d91ca57575248ff0298f6dee7180456f37d2e
6b771983142c7fa72ce209df8423460189c14ec635d6235bf60386317357428a
627b920845683bd7303d33946ff52fb2ea595208452285457aa5ccd9c01c3b0a
40d11a20bd5ca039a15a0de0b1cb83814fa9b1d102585db114bba4c5895a8a44
```

```
159fbb0d04c1a77d434ce3810d1e2c659fda0a5703c9d06f89ee8dc556783614
9aa38796e0ce4866cff8763b026272eb568fa79d8a147f7d61824752ad6d8f09
39caec2f2e9fda6e6a7ce8f22e29e1c77c8f1b4bde80c91f6f78cc819f031756
1ada91cb860cd3318adbb4b6fd097d31ad39c2718b16c136c16407762251c5db
be6416218e2b1a879e33e0517bcacaefccab6ad2f511de07eebd88821027f92d
9a7889147fa53311ba7ec8166c785f7a935c35eba4a877c1313a8d2e80e3230d
f6a2ec226c84762458d53f5536f0a19e34b2a9b03d574ae78e89098af20bcaa3
1942aac761bc2e21cf303e987ef2a7740a33c388af28ba57787f10b1804ea38e
f354148b5f0eab5af22e8152438468ae8976db84c65415d3f4a469b35e31710f
037f9434e83919506544aa04fecd7f56446a7cc65ee03ac0a11570cf4f607853
980bac6c9afe8efc9c6fe459a5f77213b0d8524eb00de82437288eb96138b9a2
603fcc53fd7848cd300dad85bef9a6b80acaa7984aa9cb9217cdd012ff1ce5f0
bcf8464d042171d7ecaada848b5403b6a810a91f7fd8f298b611e94fa7250463
64aac04ffb290a23ab9f537b1143a4556e6893d9ff7685a11c2c0931d978a931
f59c45b71eb62326d74e83a87f821603bf277465863bfc9c1dcb38a97b0b359d
2a36d1be9330a77f0bc0f7fdc0e903ddd99fcee0b9c93cb69d2f0773f0afd254
66bb57338bec9110839dc9a83f85b05362ab53686ff7b864d302a217cafb7531
806f64fda529d92c16fac02e9ddaf468a8cc6cbc710dc0f3be55aec01ed65235
9c1c527a826d16419009a1b7797ed20990b9a04344da9c32deea00378a6eeee2
40e5050b894cb70c93260645bf9804f50580050eb131e24f30cb91eec9ad1a6e
25294727f7fa59c49ef0181c2c8929474ae38a47b350f7417513f1bacf8939ff
dcfa0fca8c1dd710b4f40784d286c39e5d07b87700bdc87a48659c0426ec6cb6
3da31ee0a6c6410b3c66aad41623d05aac61a4dbb85045eb89f5810ffdc93066 // Sophos impersonation
f15a0f660ef0bd9e116ff19b433451d403ffedea9469a095c2f429227500e87a
```

3) Relevant Domains, URLs, and IP Addresses

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

References

[1] atip.ahnlab.com: June 2023 Threat Trend Report on Ransomware

[2] www.coveware.com: Ransom Monetization Rates Fall to Record Low Despite Jump In Average Ransom Payments

[3] www.bleepingcomputer.com: Clop gang to earn over $75 million from MOVEit extortion attacks

[4] www.bleepingcomputer.com: Ransomware payments on record-breaking trajectory for 2023

[5] www.fortinet.com: Ransomware Roundup - Big Head

[6] www.trendmicro.com: Tailing Big Head Ransomware's Variants, Tactics, and Impact

[7] www.bleepingcomputer.com: New 'Big Head' ransomware displays fake Windows update alert
[8] www.bleepingcomputer.com: Cybersecurity firm Sophos impersonated by new SophosEncrypt ransomware
[9] news.sophos.com: Sophos Discovers Ransomware Abusing "Sophos" Name

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.