KARA
Korea Anti Ransomware Alliance

2023.04.

# KARA ransomware trend report

# KARA ransomware trend report

## ■ Ransomware trends

### ✓ Analysis of ransomware trends

Recently, ransomware groups are carrying out attacks strategically, using various means from initial infiltration to securing victims and bypassing detection. Last February, ESXiArgs ransomware attackers, who carried out a massive attack worldwide and infected 3,800 ESXi servers, exploited a vulnerability discovered two years ago for initial infiltration, and the Play and Cuba Group exploited the Zero Day vulnerability of MS Exchange servers. They are carrying out initial infiltration by seeking various paths.

Meanwhile, while the movement of the groups looking for an IAB (Initial Access Broker), which specializes in initial infiltration, is confirmed, the Medusa Group posts a video of how to access the data stolen from victims, and the BlackCat Group creates a domain similar to the victim's site, and posts the stolen data. It can be seen that methods of threatening victims and leaking data are also becoming more advanced. Attempts to create ransomware with the Go and Rust language to interfere with analysis and bypass detection are also continuously confirmed.

**New ransomware and group activities**

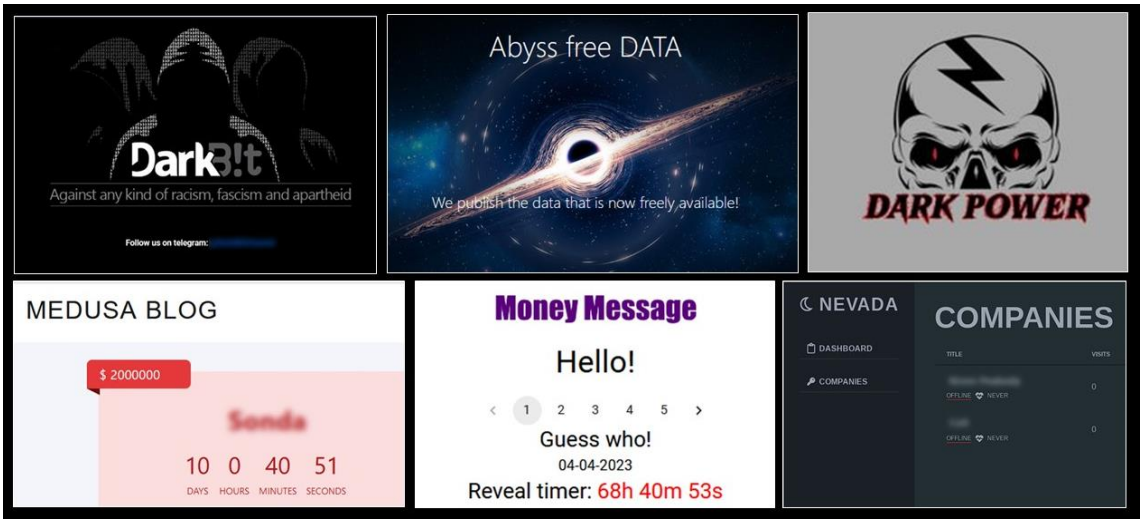



**Figure 1. New ransomware and group activities**

The Nevada, Medusa, DarkBit, Abyss, DarkPower, and MoneyMessage ransomware groups found in the first quarter all operate on the dark web and use a double extortion strategy. The Nevada group is a group discovered in February and is attacking Windows and VMware ESXi systems. Traces of borrowing Nokoyawa ransomware's code and encryption algorithm were found, suggesting that it is a variant of the Nokoyawa ransomware. Although there are many guesses as its name is similar to that of the MedusaLocker group, the Medusa group, which started activities in 2021, is separate from MedusaLocker, which has been carrying out activities since 2019. The Medusa group started activities in June 2021, has been sluggish in activities, and had few victims, but from February of this year, it has continued its activities in earnest, e.g., operating the dark web and leaking a lot of corporate data.

The DarkBit group, discovered around the same time, shows the nature of Hacktivism[1], e.g., expressing anti-government messages against Israel and antipathy against racism through SNS such as dark web, Twitter, and Telegram. It was speculated that it was a personal retaliation due to layoffs as it pointed out this issue several times and also mentioned it through a ransom note, but it turned out to be the work of MuddyWater, the hacking organization backed by Iran.

Among the groups discovered in March, the DarkPower group posted a number of damaged companies on the dark web as soon as it started its activities, but since then, no additional victims have occurred, and the Abyss and MoneyMessage groups continue to attack companies.

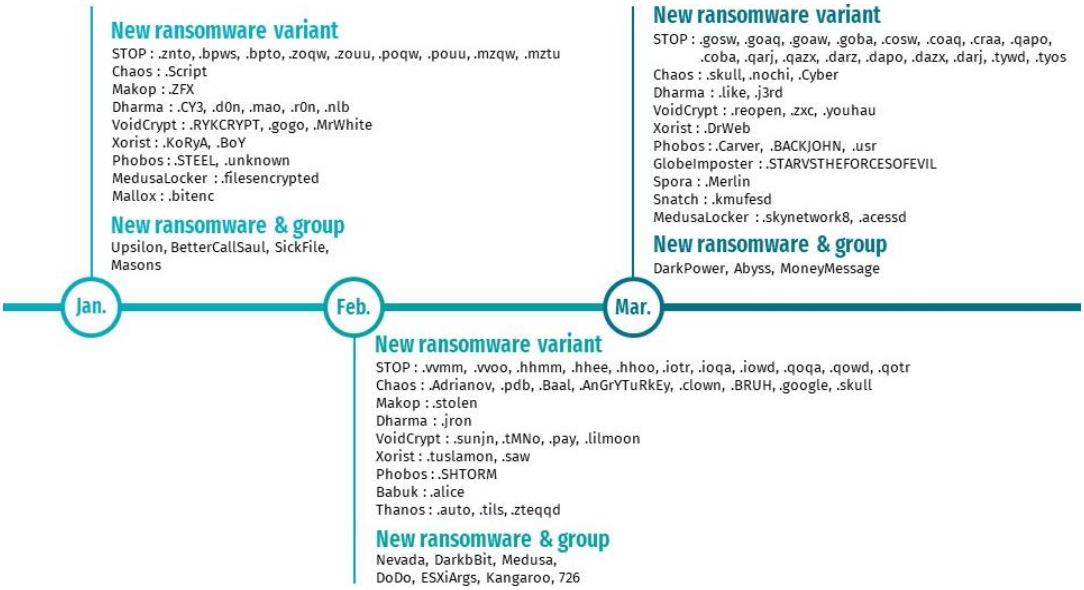



**Figure 2. Activities of new ransomware/variants**

[1] Hacktivism: Hacking and incapacitating the system to achieve political/social goals

New ransomware and variants are also continuously discovered. Among them, a variant of the Royal ransomware targeting Linux and ESXi servers and a variant of the Clop ransomware targeting Linux were found. In early February, BlackCat v3 (version 3) and v3 morph with polymorphism were discovered, and at the end of the same month, v3 morph2 was also discovered. Meanwhile, following LockBit Red and LockBit Black (used the source codes of the and BlackMatter) ransomware discovered in June 2022, LockBit Green was found in the first quarter. It was confirmed that LockBit Green borrowed the source code of the Conti ransomware leaked in March last year, and we can guess that the LockBit Group is continuously recruiting affiliates and showing off their activities.

**Ransomware attack group trends**

The movements of some ransomware groups preparing for division of labor are being confirmed. In March, the Bl00dy Group posted an article to recruit IABs through Telegram, which is not only for the purpose of making the initial infiltration smoother, but also for the purpose of dividing each person's role and labor within the group. We can guess that some groups are preparing for division of labor to scale up.

Meanwhile, as some operators of the hacker community Breached Forum (the major place of activity for some ransomware such as Radar and Endurance), were arrested by the FBI and the site was closed, we guess that there will be changes in the activity areas of some ransomware groups.

Groups that use non-mainstream languages to develop ransomware are also continuously discovered. Following ransomware such as Hive, BlackCat, and BianLian discovered last year, attempts to develop ransomware in the Go and Rust languages are continuously confirmed, e.g., DarkBit made in the Go language and the Nevada ransomware made in the Rust language discovered in the first quarter. Attackers develop ransomware with the Go and Rust languages that guarantee stability and high speed. A large number of dummy codes and complex structures generated by language characteristics, which guarantee static compile[2] and memory stability delay analysis and avoid detection compared to ransomware developed in the existing mainstream languages (C/C++/C#), and cross compile[3]. Through the cross compile function, ransomware is developed targeting various operating systems, and attacks are carried out.

[2] Static Compile: The process of converting all parts of the source code into a machine language to create an exec file.

[3] Cross Compile: The process of generating executable programs on other CPUs or operating systems

**South Korea trends**

Several ransomware attacks targeting South Korea companies and unspecified individuals have been found, and among them, Nevada, LockBit 2.0, and Magniber ransomware are being distributed to unspecified individuals. Magniber ransomware, which began to be distributed in Korea in 2017, was distributed under the disguise of a filename related to COVID-19 in the last quarter, and then under the disguise of a Windows installer (MSI) in the first quarter, and the LockBit 2.0 ransomware was circulated through e-mails disguised as a resume or copyright infringement, and continues to be found in the first quarter as well.

Some groups, such as GlobeImposter, Mallox, Play, and LockBit, carried out attacks against South Korea companies. In February, the GlobeImposter (tzw) campaign targeting South Korea companies was confirmed, and cases where South Korea manufacturers were infected with the Monster ransomware were confirmed. In February and March, the Mallox Group and the Play Group leaked data stolen from semiconductor companies and law firms, respectively. Damage to South Korea companies is steadily occurring. At the end of March, the LockBit Group posted an article claiming to have stolen data from the National Tax Service and the expected date of leakage on the dark web, but the leaked data has not been posted until past the scheduled date, and there is a possibility that it is an eventful post given that the expected date of the leak was April Fool's Day. But as there is a possibility that data was actually stolen and negotiations are in progress, it is necessary to keep an eye on it.

Meanwhile, after unspecified attackers infiltrated the systems of some South Korea companies, they exploited BitLocker[4], which is installed by default in Windows operating systems, to encrypt drives and demand money. Damage caused by ransomware without ransomware was also found on many occasions in the first quarter.

[4] BitLocker: Function to protect data by encrypting storage devices such as hard disks and USBs

## 1. Ransomware group activities and statistics

The number of victims per month has increased for the last 3 months, and you can see that the number has increased rapidly especially between February and March. This is because the Clop ransomware group exploited the Zero Day vulnerability (CVE-2023-0669)[5] of GoAnyWhere MFT, a file transfer software, to damage a number of companies. Until now, damage has been confirmed in about 100 companies, but it is predicted that additional victims will be found over time. Additional activities and victims of the Hive Group, which started activities in 2021 and has been steadily securing victims, has not been found since the dark web was shut down by the FBI in January, and the Stormous Group, which has been quiet since the first quarter of last year, secured a number of victims and resumed activities. Changes in the activities of some groups are confirmed. Subsequently, the LockBit, BlackCat, Royal, and BianLian Groups continue to inflict damage on companies, and the victimized countries are the US, the UK, and Canada in that order, and the manufacturing industry, the service industry, and the distribution industry in that order.

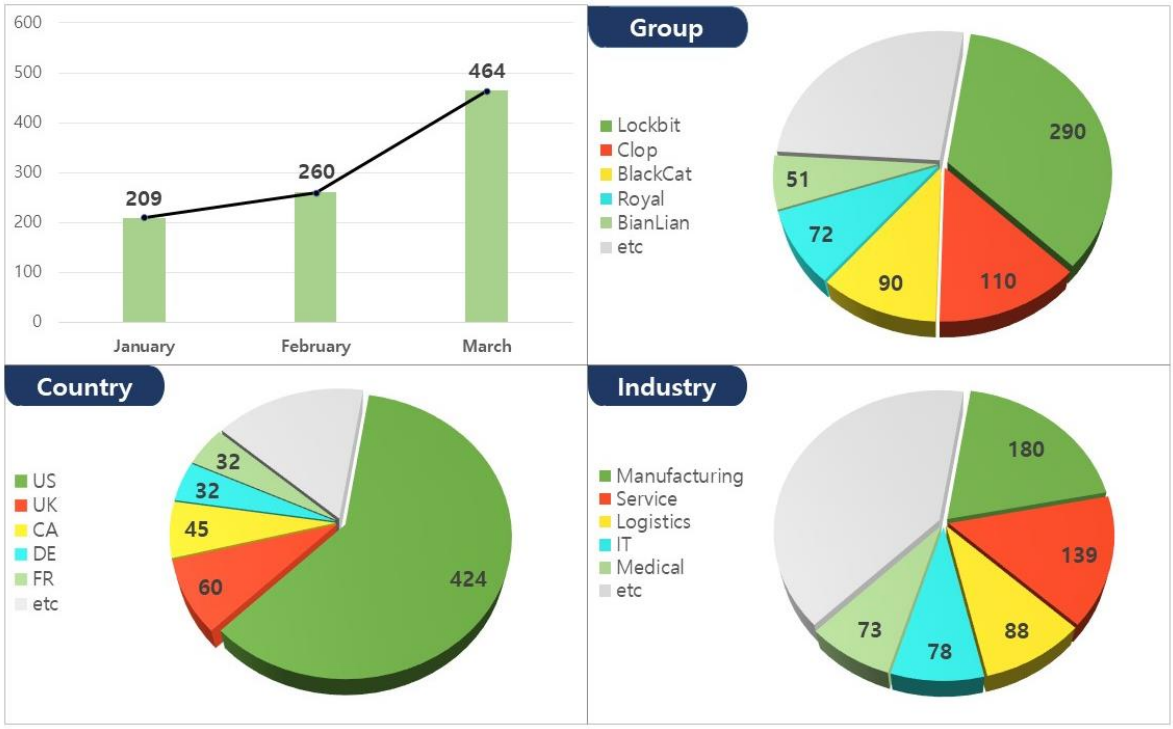



**Figure 3. Activities of ransomware groups**

[5] CVE-2023-0669: Remote code execution vulnerability in the GoAnyWhere software

## 2. GlobeImposter ransomware targeting RDP

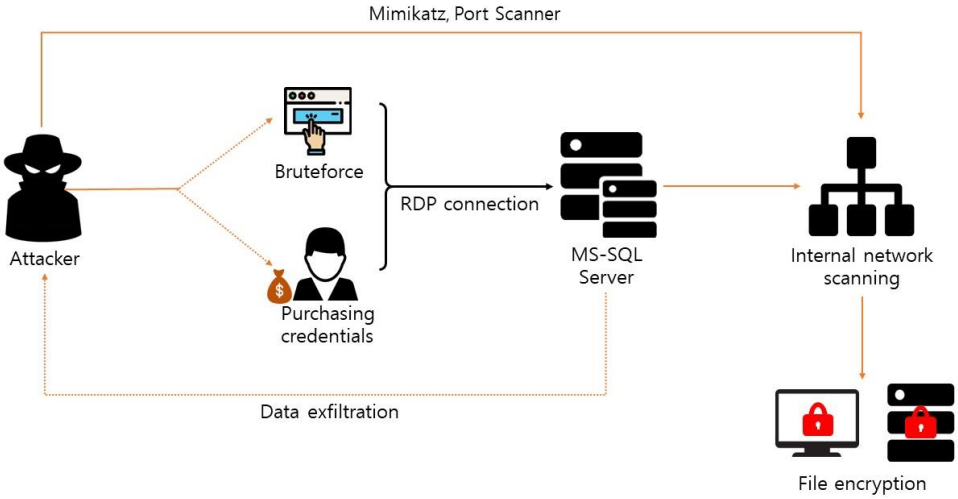



**Figure 4. RDP infiltration scenario**

In the last quarter, the GlobeImposter ransomware has been actively targeting vulnerable MS-SQL servers through brute force attacks and default accounts. On the other hand, it is confirmed that it is distributed through the RDP in the first quarter, and used in South Korea attacks, such as the GlobeImposter (tzw) campaign targeting South Korea companies.

The GlobeImposter ransomware has been confirmed to be associated with several groups. In the last quarter, as the extension (.Globeimposter-Alpha865qqz) was excluded from encryption for the Mallox ransomware in the case of GlobeImposter ransomware infection, some association with the Mallox Group was confirmed. Meanwhile, in the first quarter, a connection with the MedusaLocker Group is raised. In particular, the fact that the initial infiltration method of the two groups is the same, i.e. RDP, and the recently discovered e-mail included in the ransom note used by the MedusaLocker Group in the past is included in the recently discovered ransom note of GlobeImposter confirms the association.

Ransomware groups, which use the RDP as an initial infiltration path, attempt initial infiltration by purchasing an RDP account through the dark web or IAB or performing a brute force attack. If the infiltration succeeds, it can cause damage by not only encrypting the files of the server, but also downloading tools such as Mimikatz[6] and a port scanner and accessing the internal network system to encrypt files. So appropriate protective measures are required

[6] Mimikatz: A tool for stealing Windows OS accounts and passwords

## GlobeImposter ransomware

### 1) Background


- GlobeImposter is ransomware discovered in early 2017 that has been dubbed the FakeGlobe ransomware because how Globe ransomware works and ransom notes are similar. It mainly uses phishing mail and the RDP as an initial infiltration method, and has been trying to attack the US, Europe, and Asia.
- In September 2017, a variant that includes both the function of the Locky ransomware and the function of the GlobeImposter ransomware was discovered, and when the ransomware is executed, the victim is first infected with the Locky ransomware and additionally infected with the GlobeImposter ransomware, paying two times and performing the decryption process to recover files.
- GlobeImposter ransomware infection extension (.Globeimposter-Alpha865qqz) was included in the encryption exclusion targets of the Mallox ransomware discovered in the last quarter, and some association between the two groups was confirmed. But the connection with the MedusaLocker Group is confirmed in that it has the same initial infiltration method as the RDP and that the e-mail included in the ransom note used by the MedusaLocker Group is included in the recently discovered ransom note of GlobeImposter.
- The GlobeImposter (tzw) campaign targeting South Korea companies has been discovered since February, and when infected with the ransomware, the extension of a file is changed to .tzw.
- The GlobeImposter ransomware is distributed through the RDP, and attackers scan the RDP's default port (3389) for initial infiltration and select systems with the RDP enabled as attack targets.
- After selecting an attack target, it tries to access it through a brute force attack or IAB, or a leaked account obtained from the dark web. If the access is successful, the file is encrypted through the ransomware, and it additionally uses tools like Mimikatz and the port scanner to access the internal network system and attempts to encrypt it.

## 2) Features

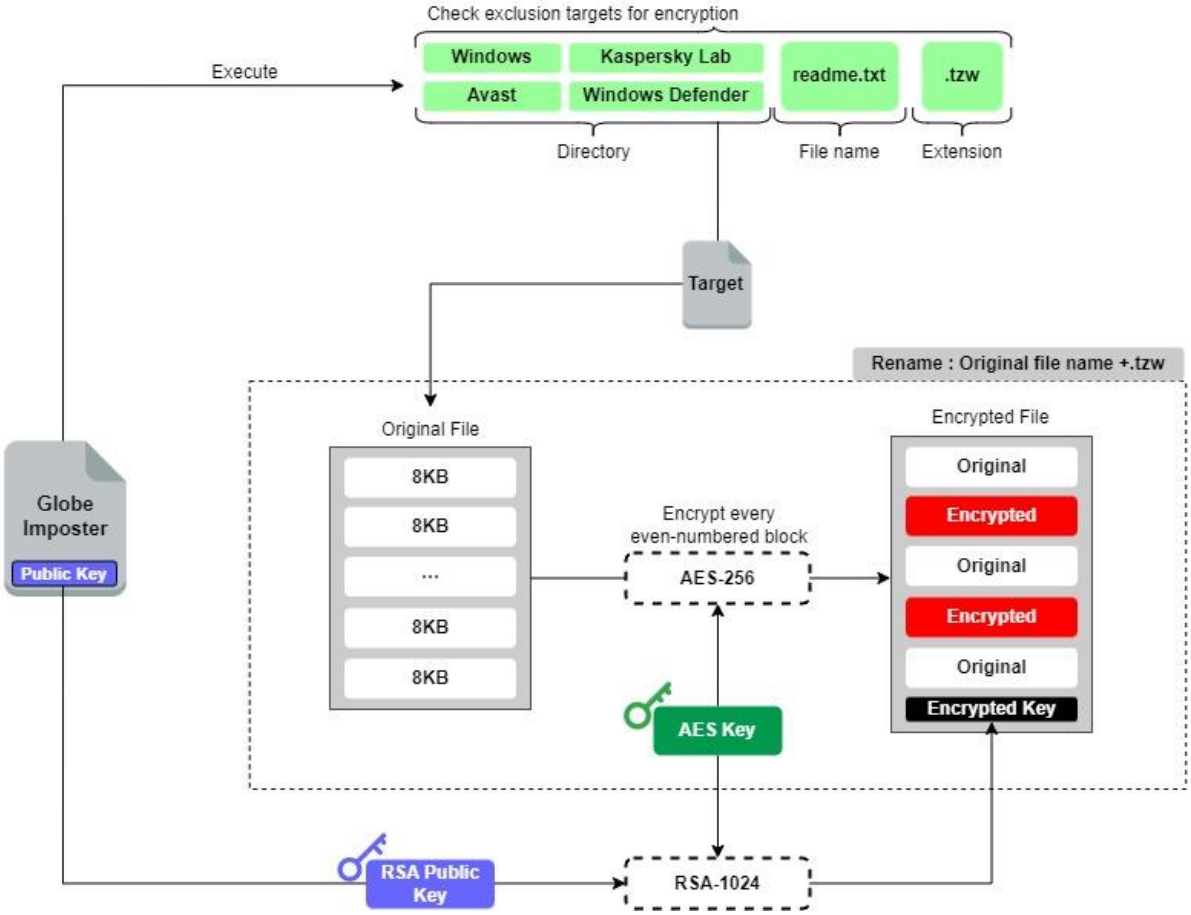



**Figure 5. GlobeImposter encryption logic**

- It uses the AES-256 algorithm to decrypt the obfuscated data inside the ransomware file. At this time, the decrypted data includes the encryption exclusion path, the encryption exclusion file name, and the extension.
- Among the encryption exclusion directories, many directories related to anti-virus products (Windows Defender, Kaspersky Lab, and Avast) are included. We guess that the purpose is to bypass detection when anti-virus related data is altered.
- After dividing each file into 8KB blocks, it uses only the AES-256 algorithm to encrypt even-numbered blocks, and protects the key value used with the RSA-1024 algorithm and stores it at the end of the file.

- After encryption is finished, it deletes the volume shadow copy[7] so that the data cannot be recovered, and additionally, it deletes the Windows event log and RDP access records, and disables the RDP function to interfere with detection and analysis.

```
// @echo off
// vssadmin.exe Delete Shadows /All /Quiet
// reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
// reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
// reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
// cd %userprofile%\documents\
// attrib Default.rdp -s -h
// del Default.rdp
// for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
```

**Figure 6. Deleting event logs and disabling RDP**

[7] Volume Shadow Copy: A snapshot or a copy at a specific point in time

### 3) IoC

| | |
|---|---|
| SHA256 | eab81d32180ddac56ed5d63e50ec4e20c0f1ceaab7e7e5f90d74883f5ae1bddc<br>6d3312e3992dc1244be5518718bb42558057f7ec59a50009892846acf58481d9<br>98e4a7b1d986cf70410dc14933dc2b3924056cb4cac52f0193cd3a93f58d6b07 |
| File name | 70.exe<br>Tzw_1.exe<br>DZ86eEu.exe |

## 3. Ransomware, awakening to non-mainstream language

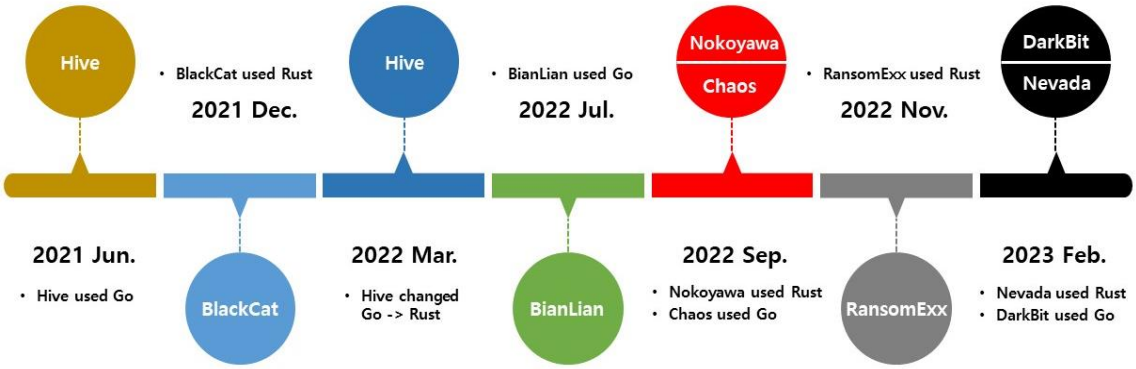



**Figure 7. When each group used the Go or Rust language**

Recently, a new trend has been discovered among ransomware groups. In particular, as ransomware produced in languages such as Go and Rust was continuously discovered last year and this year, it can be confirmed that attackers are turning their attention to non-mainstream languages. Among the ransomware groups, the Hive Group and the BlackCat Group were the first to develop ransomware using the Go and Rust languages, and after that, several ransomware groups such as BianLian, Nokyawa, and Chaos started using ransomware developed in the Go and Rust languages for their activities. As such, attempts to develop ransomware with the Go and Rust languages are constantly discovered, and we need to think about the reason.

Go is an open source programming language officially announced by Google in 2012, and has various features such as easy accessibility due to its code writing method similar to existing mainstream languages, provision of Gorutine that can implement multi-thread functions in a single core, and fast execution speed. Among them, especially noteworthy feature is that the Go language is a static compile language. Static compile means inclusion of the library information used during production of the program in binary, and inside the programs produced through this, character strings and dummy codes other than the attack codes written by the developer are included. Ransomware attackers want to increase the possibility of avoiding detection and increase the success rate of attacks by delaying analysis through complex structures created with dummy codes and obfuscation.

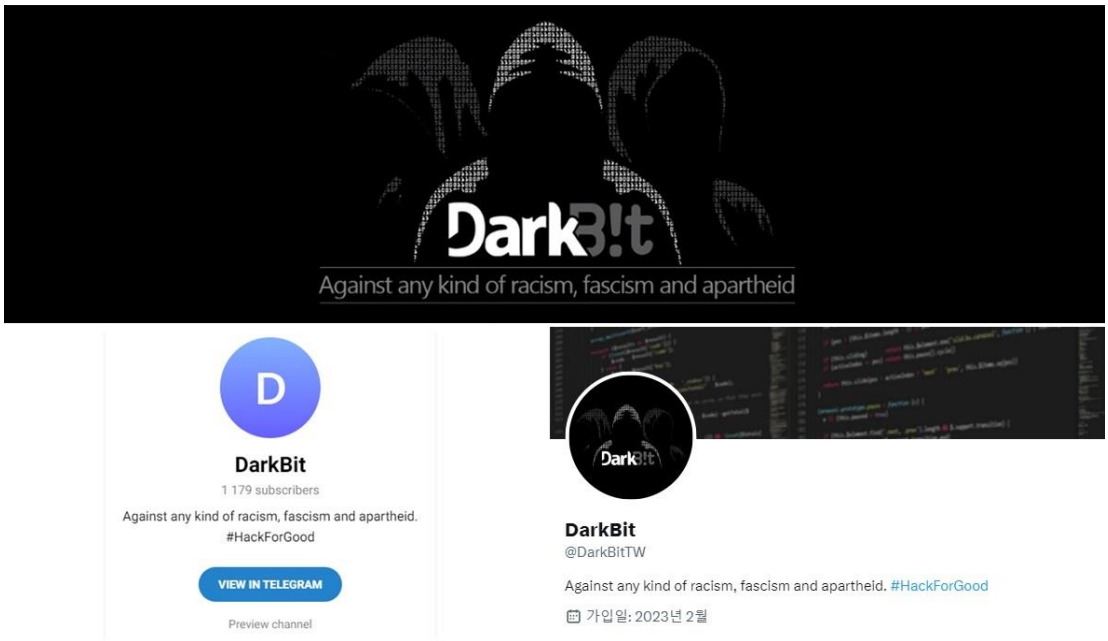
Attackers have similar reasons as above for using the Rust language. The Rust language is a language that guarantees the stability of memory. Unlike C/C++, the compiler guarantees the stability of memory during compile without the user manually managing the memory. At this time, the compiler includes various runtime codes and auxiliary functions in the code to guarantee the stability of memory. The function is included in the code, and attackers can use this to interfere with analysis, increase the possibility of avoiding detection, prevent malfunction due to memory collision, and perform encryption at high speed.

Among the non-mainstream languages used in recent ransomware development, another peculiarity is also confirmed. In the first quarter, ransomware developed in the Go and Rust languages as well as DarkPower ransomware developed in the Nim language were found. One thing to note is that all three languages support the cross compile function. The cross compile function is a function that makes it possible to create programs targeting various operating systems, and ransomware developers can efficiently perform attacks by recycling codes through this function and producing ransomware targeting various operating systems.

Ransomware developed in non-mainstream languages tends to have a lower probability of detection due to lack of analysis data than ransomware written in existing mainstream languages. While stability is guaranteed, encryption is possible quickly through excellent concurrency and parallelism. So attackers saw through this and carry out attacks accordingly. This movement has been continuously discovered for a long time, and we guess that ransomware that uses various non-mainstream languages to evade detection and hinder analysis will be continuously discovered in the future.

## ✓ DarkBit ransomware

### 1) Background




- The DarkBit Group began its activities on February 12 by attacking Technion University in Israel. In this process, a total of more than 4TB of data was leaked from 22 departments, and additional data leakage through Telegram was preannounced.
- Since the internal domain that is not accessible from the outside and the computer host names used by network experts and security experts at Technion University are included in the encryption exclusion list, we guess that attackers carried out attacks while knowing the internal structure of the attack target.
- It was speculated that it was retaliation due to personal grudge as it shows the nature of Hacktivism, e.g., raising issues about racism and layoffs through the dark web and Telegram, and showing anti-Israel tendencies, and pointed out the layoff issue inc certain industries several times through Twitter, but it turned out to be the work of MuddyWater, a hacking organization backed by Iran.
- Since 2017, the MuddyWater hacking organization has been carrying out hacking campaigns such as Static Kitten, Mercury, Seedworm, and Earth Vetala. It has particularly targeted government and private organizations in Asia, Africa, and Europe. Also, since the last quarter, it has been conducting attacks against institutions in Israel, and it is mainly using the Log4j vulnerability for initial infiltration.

## 2) Features

```
Usage of Darkbit.exe:
  -all
        run on all without timeout counter
  -domain string
        domain
  -force
        force blacklisted computers
  -list string
        list
  -nomutex
        force not checking mutex
  -noransom
        Just spread/No Encryption
  -password string
        password
  -path string
        path
  -t int
        threads (default -1)
  -username string
        username
```

- The original file includes a compressed file (.zip) and a shortcut (.lnk) file, and when the shortcut file is executed, the command of PrintBrm.exe, a printer migration tool, is used in Windows operating systems to decompress and run the ransomware.
- It was developed in the Go language and made for Windows operating systems. When the program is executed, it uses the vssadmin -delete /all /quiet command to delete the volume shadow copy, and then performs the specified operation according to the input parameters.
- It compares the host name of the PC where ransomware is running and the blacklist hardcoded inside the ransomware. If they are the same, it terminates without encryption. The blacklist includes the host names of the computers used by network experts and security experts at Technion University, as well as internal domains that are not accessible from the outside.

```
"hostnames":
[
    "TD-EF-DC.ef.technion.ac.il",
    "td-ef-main.ef.technion.ac.il",
    "td-ef-mainc.ef.technion.ac.il",
    "T-BM-DC2.bm.technion.ac.il",
    "T-BM-DC3.bm.technion.ac.il",
    "TD-SI-DC.si.technion.ac.il",
    "td-si-dc2.si.technion.ac.il",
    "td-st-dc.st.technion.ac.il",
    "TD-ST-DC2.st.technion.ac.il",
    "TD-AE-aeneid.ae.technion.ac.il",
    "td-ae-aeolus.ae.technion.ac.il",
    "TD-ME-DC01.me.technion.ac.il",
    "TD-ME-DC2.me.technion.ac.il",
    "TDSAPDC.sap.technion.ac.il",
    "tdsapdc2.sap.technion.ac.il",
    "Tech-Med-BK2019.medicine.technion.ac.il",
    "Tech-Med-DC2019.medicine.technion.ac.il",
    "Staff-DC1.staff.technion.ac.il",
    "STAFF-DC2.staff.technion.ac.il",
    "staff-dc3.staff.technion.ac.il",
    "TD-CC-ROOT.cc.technion.ac.il",
    "TD-CC-ROOTC.cc.technion.ac.il",
    "td-cc-rootd.cc.technion.ac.il",
]
```

```
"limits":
[
    {"limitMB": 25,      "parts": 1, "eachPart": -1},
    {"limitMB": 1000,    "parts": 2, "eachPart": 12000},
    {"limitMB": 4000,    "parts": 3, "eachPart": 10000},
    {"limitMB": 7000,    "parts": 2, "eachPart": 20000},
    {"limitMB": 11000,   "parts": 3, "eachPart": 30000},
    {"limitMB": 51000,   "parts": 5, "eachPart": 30000},
    {"limitMB": 1000000, "parts": 3, "eachPart": 1000000},
    {"limitMB": 5000000, "parts": 5, "eachPart": 1000000},
    {"limitMB": 6000000, "parts": 20,"eachPart": 10000000}
],
```

```
-----BEGIN RSA PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsd7nK2MlUKYZHyBgRJBf
eQ9RYuNhUuB89v/QraLJJFWVS1kl2Wkinz1Dmd8awuqiWzEYMcacVz7PHK0Gl3pe
dLgTi1cSK84hD40L7vikW/r3sRcz5LUlEc6DJwpU+NUMczUE+yTjdAXjl+eGu7qy
Iu/K4b0qYdQQv8qirOQl8XTY+2WIztDvTbOTNe1wmRvYt9JP90b/7gl5h4P83zph
4Lc1+Lrt6h0d/By0bv7Q34nPl+xJ97JqCE3kanmVzXp+exbcet+PKnAGMe/pF1le
9UsnFYQAvlesiWri8attVBumpoRPhiJyHIqoF6ST5e29cuBpPQZKxBUYRIQLwpgE
HQIDAQAB
-----END RSA PUBLIC KEY-----
```

**Figure 8. Blacklist, encryption unit, and RSA public key**

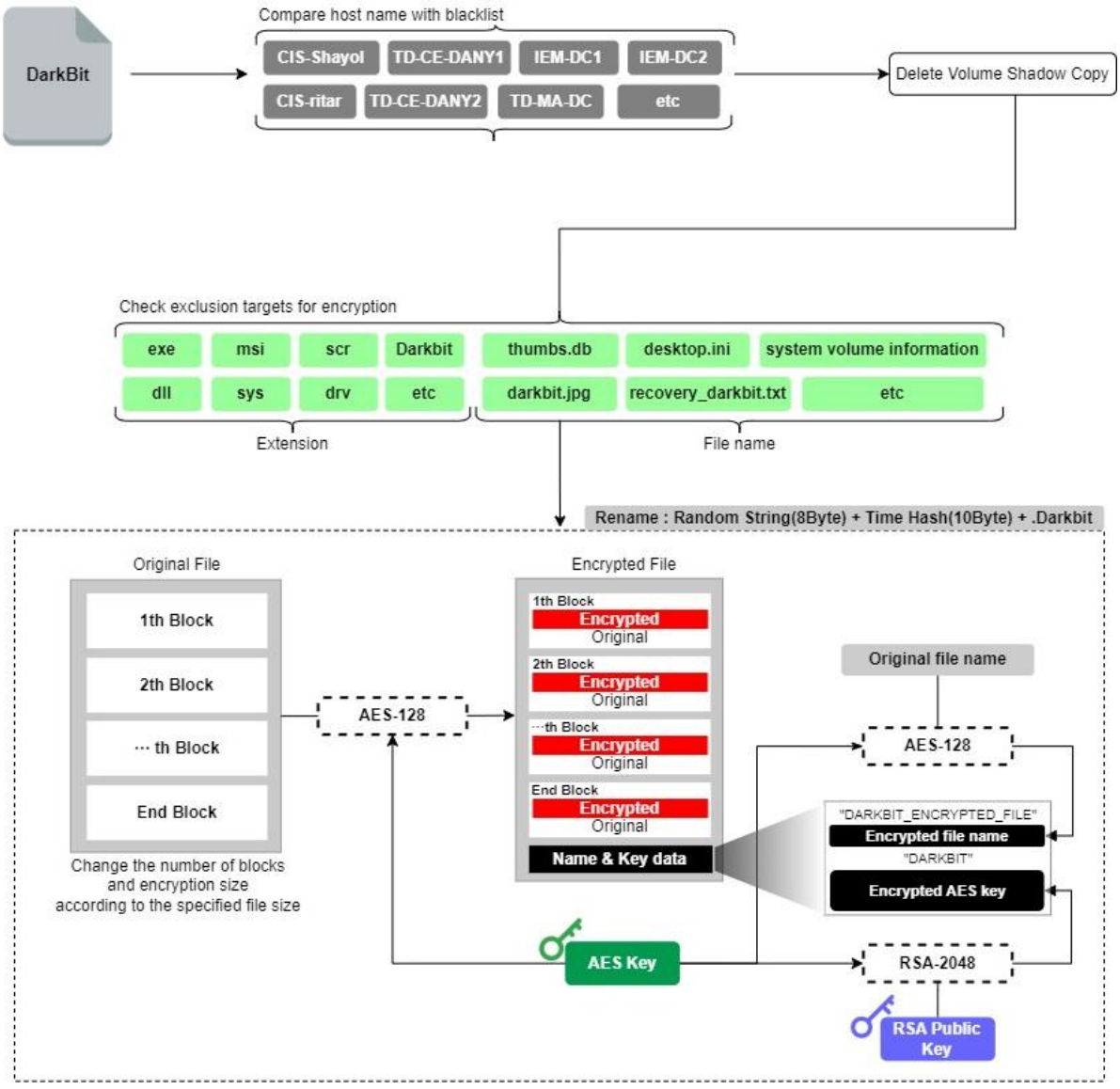



**Figure 9. DarkBit ransomware encryption logic**

- It elevates the priority of the running ransomware process before encryption so that encryption can be performed quickly, and during encryption, files are encrypted by creating Goroutines that perform encryption tasks as many as the number of processors in the computer.
- Specified extension and file name or files of 16 bits or less are excluded from encryption, and the name of the file before encryption is replaced with a random character string (8 bites) + Time hash value (10 bites), and the extension is changed to Darkbit. Afterwards, the file is divided into blocks according to the size of the file and only the designated bites within each block are encrypted using the AES-128 algorithm.

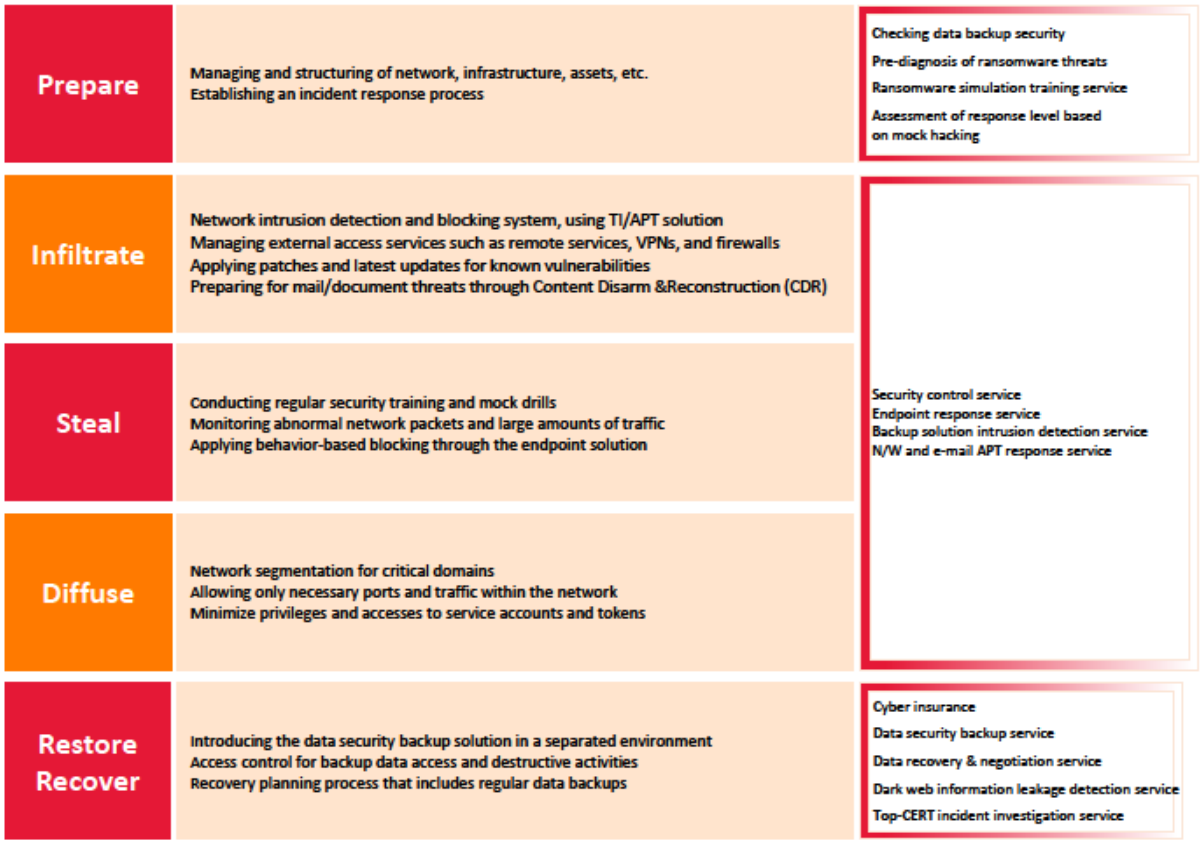
- The original file name is also encrypted with the AES-128 algorithm through the same key, and the key value used is protected with the 2,048-bit RSA public key that exists inside the ransomware, and "DARKBIT_ENCRYPTED_FILE | encrypted filename | DARKBIT" are stored in that order at the end of the file.

### 3) IoC

| | |
|---|---|
| SHA256 | 9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff<br>Bc5954d7da18a20405e994bce05d927e7599b8a9a95d4412cab6fbc6324c3558<br>81c1bf78ab59bd78f615eeb3bc9f17ec2d82ba46d0224da63c855a9e7202116b |
| File name | 8thcurse.exe<br>HR-Update.exe<br>hr-update.iso |

## Ransomware mitigations

Attackers perform reconnaissance in various ways through strategies established by the attacker groups to select attack targets, and then infiltrate internal infrastructure, encrypt files, threaten assets, and attempt blackmail through data leakage. In order to prevent such damage, it is necessary to prepare for target APT attacks and to prepare appropriate security elements and processes for each stage of intrusion to detect and block attackers before achieving their goals.



Technology for Everyday Safety | SK shieldus

23, Pangyo-ro 227beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea
https://www.skshieldus.com

Publisher : SK shieldus EQST Business Group & KARA (Korea Anti Ransomware Alliance)
Producer : SK shieldus Communication Group