Keep up with Ransomware

Devman: A Single Group Using Assorted Ransomware

■ Overview

In May 2025, the number of ransomware incidents recorded was 484, reflecting an approximate 12% decrease compared to April's 550 cases. Although there has been a consistent downward trend in the number of incidents since March, the disclosure of the Vanhelsing ransomware source code in May has heightened the likelihood of the emergence of variants or groups exploiting this code.

In early May, the dedicated Leak Sites of LockBit was defaced with the phrase "Don't do crime CRIME IS BAD xoxo from Prague." Not only was the dedicated Leak Sites altered, but the administrative panel was also compromised, leading to the exfiltration of certain internal database files. The leaked database contained cryptocurrency wallet addresses, configuration information used by different versions of the ransomware, affiliate account details, and chat logs; however, it did not include the private keys used for decryption. This hacking incident has not only tarnished LockBit's reputation but also appears to have significantly disrupted its operations, as evidenced by the fact that the dedicated Leak Sites remained inaccessible until early June.

The source code of the Vanhelsing ransomware has been disclosed on the Russian hacking forum RAMP. A former member, known as th30c0der, uploaded a post on a related forum site indicating the sale of the Vanhelsing ransomware's source code. The Vanhelsing administrators acknowledged this and released portions of their existing ransomware and panel page source code. However, th30c0der introduced himself as the pivotal figure responsible for developing the panel, payment system, and the ransomware itself, asserting that the disclosed code does not represent the entirety of the source. He claims that the source code he is selling is the most recent version.

Meanwhile, a file presumed to be a decryption tool for Qilin ransomware has been discovered. This particular sample offers the capability to decrypt encrypted files using either the AES algorithm or the ChaCha20 algorithm. However, it has been confirmed that the decryption is not universally applicable to all Qilin ransomware variants; it functions correctly only when the files have been encrypted with specific versions or particular encryption keys.

In May, several incidents of breaches were identified domestically. The group initially operating under the name RaLord, which rebranded as Nova in May, claimed responsibility for attacking a domestic university, asserting that they exfiltrated internal documents, reports, portal site source codes, databases, and student information. In June, the exfiltrated data was disclosed; however, it did not include personal information, with only the portal site source code and database-related information being verified.

The TCR Team launched cyberattacks against two companies within the domestic finance and manufacturing sectors. These companies were categorized as having failed negotiations on a dedicated Leak Sites, leading to the partial exposure of their data. The compromised information was confirmed to include internal documents and employees' personal data. However, the data that had been disclosed was removed approximately two weeks later, and by the end of May, the dedicated Leak Sites had been deactivated, rendering it inaccessible.

A ransomware group exploiting a file upload vulnerability (CVE-2025-31324) in SAP's application integration and execution platform, NetWeaver, has been identified. Although this vulnerability was patched on April 24th, evidence has emerged indicating that the BianLian group and the RansomEXX group have exploited it. While neither group has deployed ransomware, activities have been detected involving the exploitation of the vulnerability to communicate with BianLian's command and control (C2)[1] servers or to distribute PipeMagic, a backdoor[2] commonly utilized by RansomEXX.

[1] C2 (Command and Control): A server that delivers commands to infected PCs or servers to perform attacker-specified actions.

[2] Backdoor: Malware that bypasses security mechanisms to grant access to the target system.

Ransomware News

Leak of Internal Database from LockBit Group

- Leaked intelligence indicates that the hacking incident transpired in late April while the exfiltrated data was made public in early May.
- A partial extract of the internal database was leaked, alongside a sarcastic remark "Don't do crime. CRIME IS BAD. xoxo from Prague."
- Attribution suggests that the operation was conducted by the same entity involved in the Everest group hack.

The decryption tool for the Qilin ransomware has been discovered.

- Qilin ransomware-encrypted files can be decrypted using the corresponding algorithm—either AES or ChaCha20—based on which was employed during encryption.
- The decryptor does not support all variants of the Qilin ransomware and operates successfully only when certain versions or matching keys are present.

Vanhelsing ransomware's source code has been publicly released.

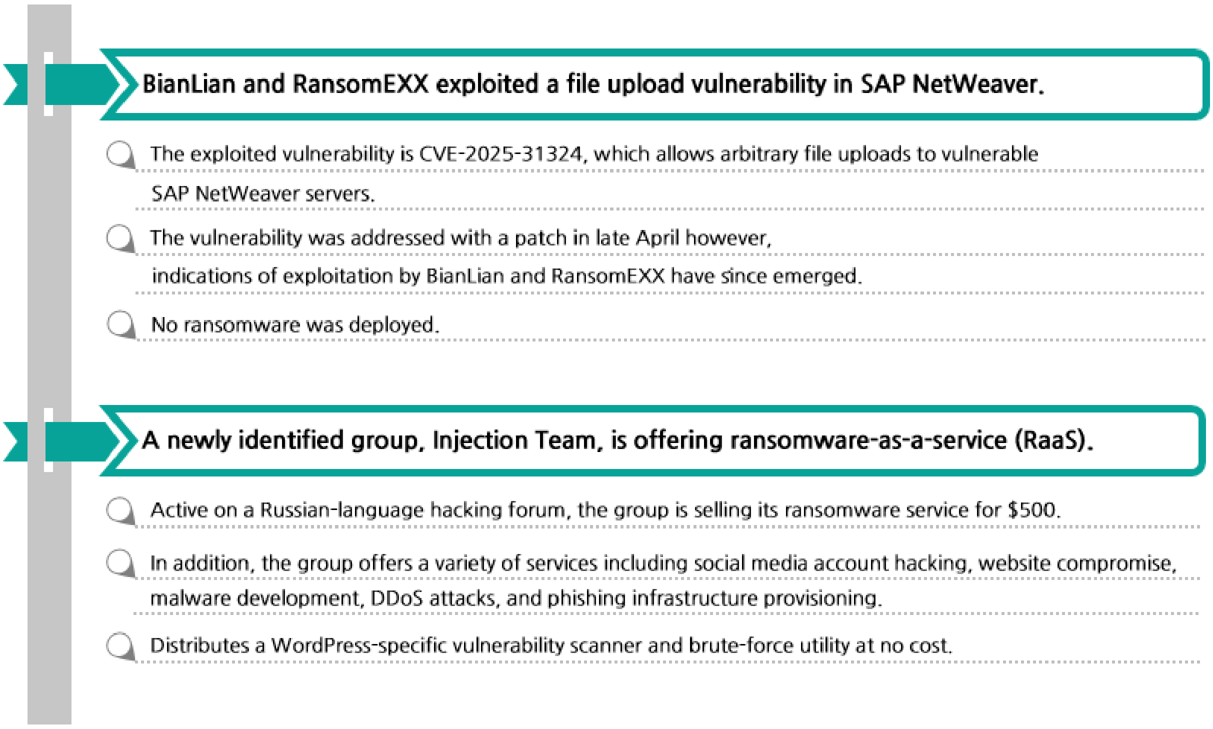
- A user operating under the alias "th30c0der" attempted to sell the source code on the RAMP forum in May.
- The Vanhelsing operators acknowledged that the user had indeed collaborated with them and subsequently released their own ransomware source code.
- "th30c0der" claimed that the publicly released code corresponds to version 1, while asserting that he is selling the latest version, v2.

The TCR Team group carried out attacks against two South Korean companies.

- The group targeted finance and manufacturing companies, stealing and leaking sensitive data.
- The leaked data included internal documents and employee personal information.
- The DLS became inactive in late May and is no longer accessible.

The Nova group carried out an attack against a South Korean university.

- The group stated that it had infiltrated a South Korean university and extracted internal documents, source code, and student records.
- Although the data was published in early June, it did not include any personal information instead, it contained the source code and database of a portal site.



BianLian and RansomEXX exploited a file upload vulnerability in SAP NetWeaver.

- The exploited vulnerability is CVE-2025-31324, which allows arbitrary file uploads to vulnerable SAP NetWeaver servers.
- The vulnerability was addressed with a patch in late April however, indications of exploitation by BianLian and RansomEXX have since emerged.
- No ransomware was deployed.

A newly identified group, Injection Team, is offering ransomware-as-a-service (RaaS).

- Active on a Russian-language hacking forum, the group is selling its ransomware service for $500.
- In addition, the group offers a variety of services including social media account hacking, website compromise, malware development, DDoS attacks, and phishing infrastructure provisioning.
- Distributes a WordPress-specific vulnerability scanner and brute-force utility at no cost.

Figure 1. Ransomware Trends

Ransomware Threats

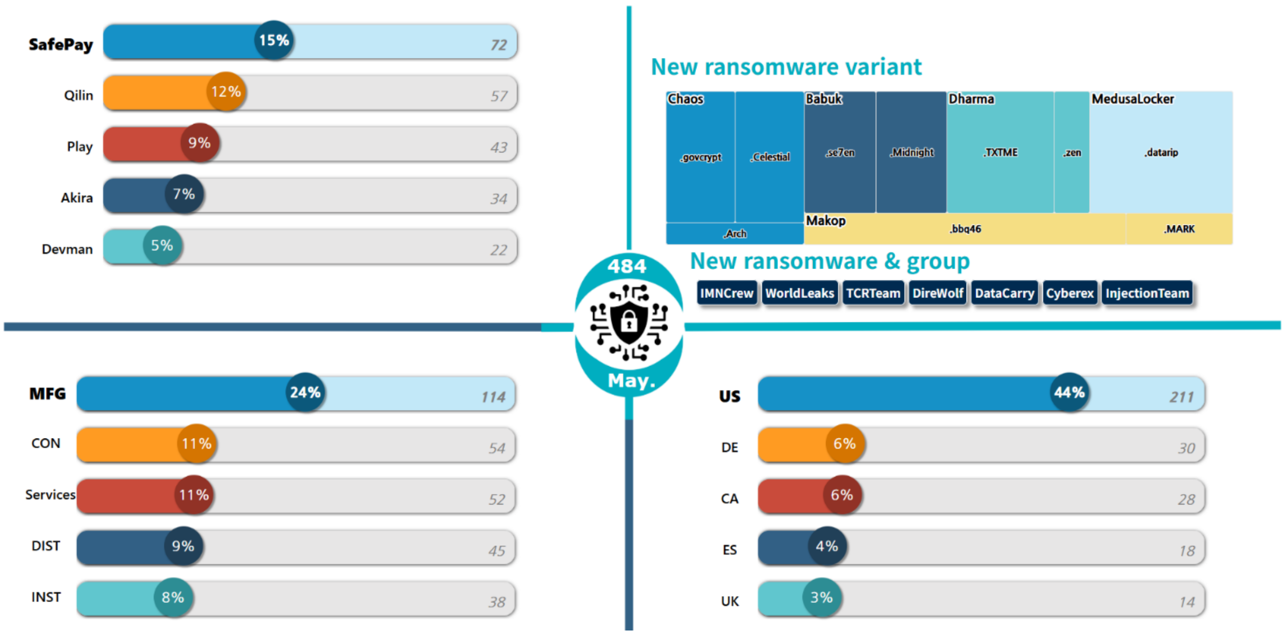
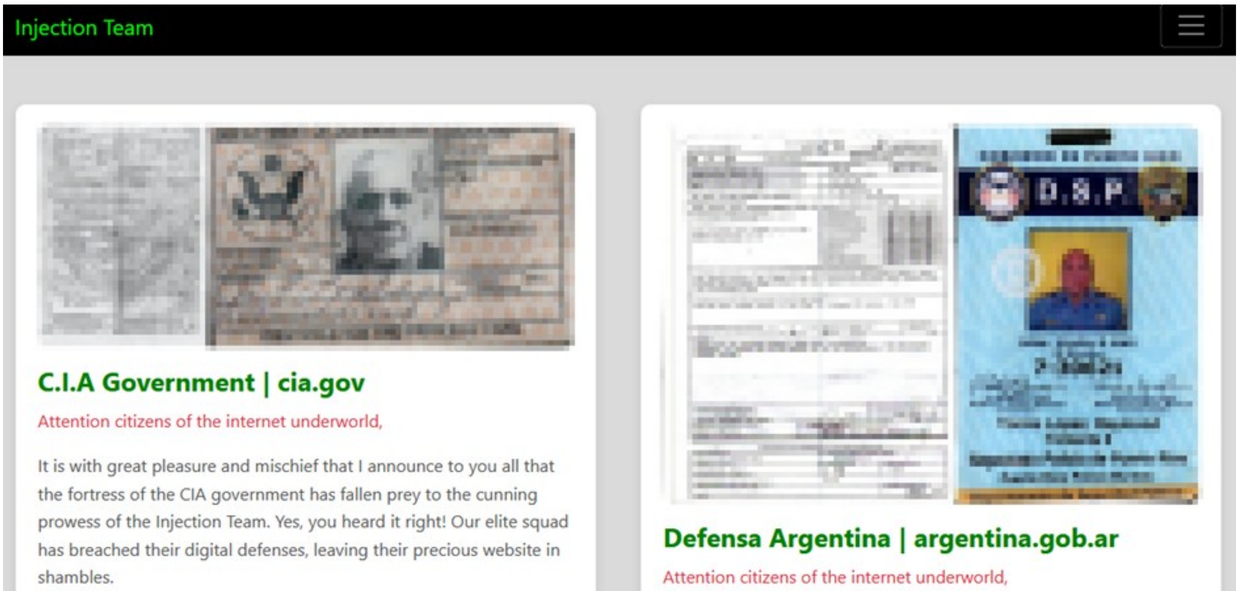


Figure 2. Status of Ransomware Threats in May 2025

New Threats

In May, a total of eight new ransomware groups were identified. It has been observed that JGroup uploaded 18 new victims, Imncrew 8, WorldLeaks 14, Direwolf 11, and DataCarry 10, each to their respective dedicated Leak Sites. Additionally, the Cyberex group does not operate a separate leak site; instead, it conducts ransom negotiations with infected victims solely through a chat site.



Injection Team

C.I.A Government | cia.gov

Attention citizens of the internet underworld,

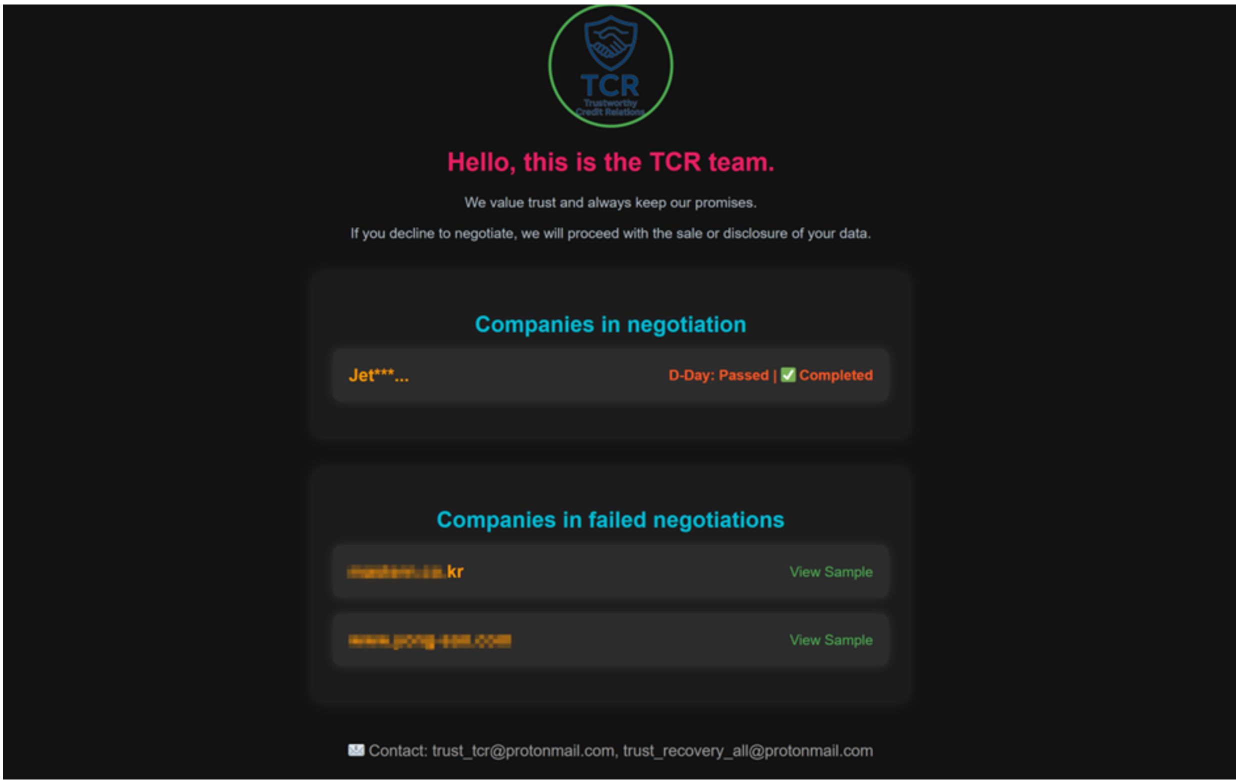
It is with great pleasure and mischief that I announce to you all that the fortress of the CIA government has fallen prey to the cunning prowess of the Injection Team. Yes, you heard it right! Our elite squad has breached their digital defenses, leaving their precious website in shambles.

Defensa Argentina | argentina.gob.ar

Attention citizens of the internet underworld,

Figure 3. Injection Team Dedicated Leak Sites

The newly emerged group, known as the Injection Team, is actively promoting itself on Russian hacking forums. This group offers a wide array of services, including ransomware-as-a-service, social media hacking, website hacking, malware development, DDoS attacks, and phishing infrastructure provision, typically priced around $1,000. In addition to these paid services, they also distribute a vulnerability scanner for WordPress environments and brute force tools free of charge.



Hello, this is the TCR team.

We value trust and always keep our promises.

If you decline to negotiate, we will proceed with the sale or disclosure of your data.

Companies in negotiation

Jet***... D-Day: Passed | ✅ Completed

Companies in failed negotiations

[redacted].kr View Sample

[redacted] View Sample

✉ Contact: trust_tcr@protonmail.com, trust_recovery_all@protonmail.com

Figure 4. TCR Team Dedicated Leak Sites

A new group targeting domestic entities has also been identified. The attacks by the TCR Team group were discovered in May, during which they targeted two domestic companies and disclosed some of their data. The affected companies were identified as a financial investment firm and an automotive parts manufacturer, with compromised documents including internal corporate files and employee personal information. By the end of May, access to sample data became unavailable, and subsequently, the dedicated Leak Sites itself was deactivated.

Top 5 Ransomware

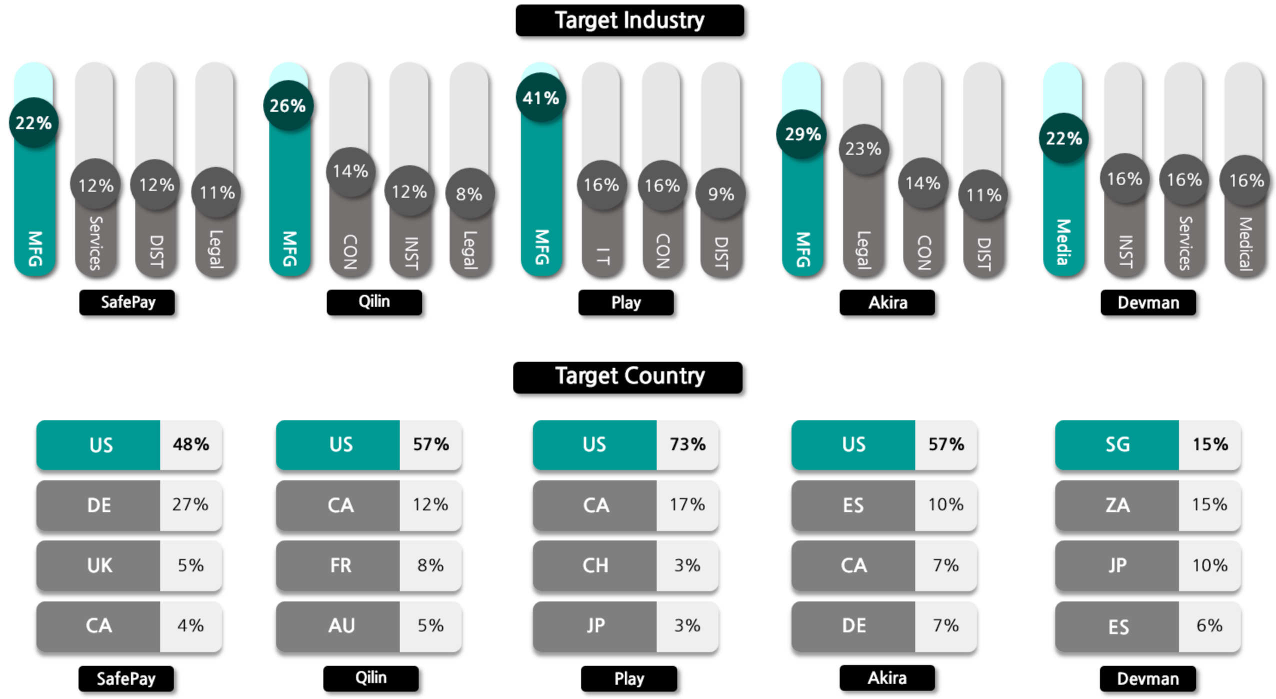


Figure 5. Overview of Major Ransomware Attacks by Industry/Country

The SafePay group launched an attack on the public high school Gymnázium a Jazyková škola Zlín, located in the Czech Republic, resulting in the exposure of approximately 30GB of internal data. This data encompassed not only internal school records but also included certain student information. Furthermore, the group targeted the Australian law firm RTB Legal, exfiltrating around 200GB of data. This breach led to the unauthorized release of a wide array of legal and administrative documents, including court documents, client information, emails, contracts, and wills.

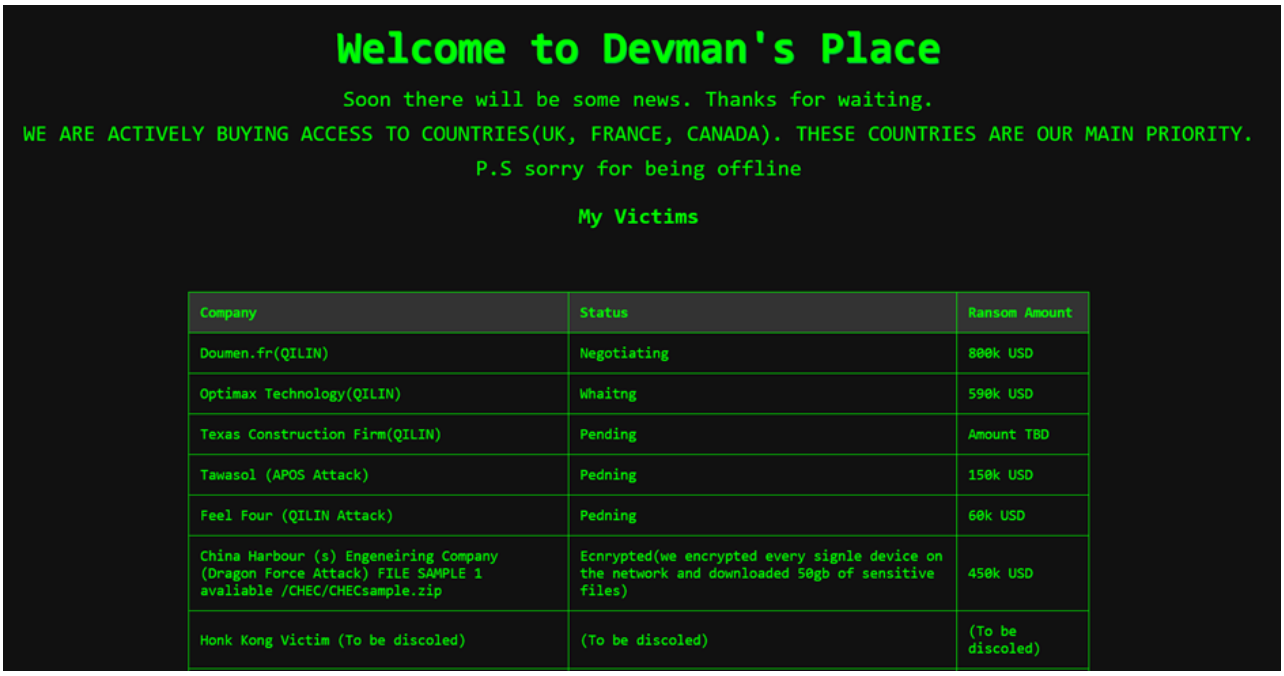
The Qilin group launched an attack on the government of Cobb County, Georgia, USA, exfiltrating approximately 150GB of data comprising 400,000 documents. The compromised data included personal information of residents and government officials, as well as images of deceased individuals. Additionally, they targeted the Army Navy Country Club, a prestigious country club in the United States, and exfiltrated 300GB of data. This breach resulted in the exposure of sensitive information such as members' names, addresses, credit card details, and credentials.

The Play group has been exhibiting a pattern of targeting American enterprises with its cyber attacks. In May, it launched an assault on the U.S. construction firm W.E. Bowers, resulting in the exfiltration of a diverse array of data, including customer documents, budgets, payroll statements, accounting records, identification credentials, and financial information. The specific extent of the damage, however, has not been disclosed. Another U.S. construction company, Greater Seattle Concrete, also fell victim to an attack, leading to the exposure of internal documents and data containing confidential information at the end of May.

The Akira Group orchestrated a cyberattack on the American energy company Pacific Summit Energy, resulting in the exfiltration of approximately 160GB of data. This compromised data encompasses employee personal information, financial audit documents, and internal operational files, all of which have been fully disclosed. Furthermore, the group targeted the U.S. financial institution Flagship Bank, seizing and releasing 40GB of data that includes customer information, detailed financial records, and contractual agreements.

In April, a newly emerged group known as Devman claimed responsibility for an attack on Kenya's National Social Security Fund (NSSF Kenya), asserting that they exfiltrated approximately 2.5 terabytes of data. The group has been consistently uploading verification screenshots via their X (formerly Twitter) account, while also detailing their reconnaissance, data exfiltration, and file encryption methodologies on a dedicated Leak Sites. The compromised data reportedly includes personal information such as names, addresses, and social security numbers, with a ransom demand set at $4.5 million USD (approximately 6.1 billion KRW).

Additionally, the Philippine media outlet GMA Network reported that their internal servers were encrypted, resulting in the exfiltration of approximately 65 gigabytes of data. The ransom demand in this instance was $2.5 million USD (approximately 3.4 billion KRW). However, GMA Network asserted that the leaked data did not contain any sensitive or personal information.



Welcome to Devman's Place

Soon there will be some news. Thanks for waiting.

WE ARE ACTIVELY BUYING ACCESS TO COUNTRIES(UK, FRANCE, CANADA). THESE COUNTRIES ARE OUR MAIN PRIORITY.

P.S sorry for being offline

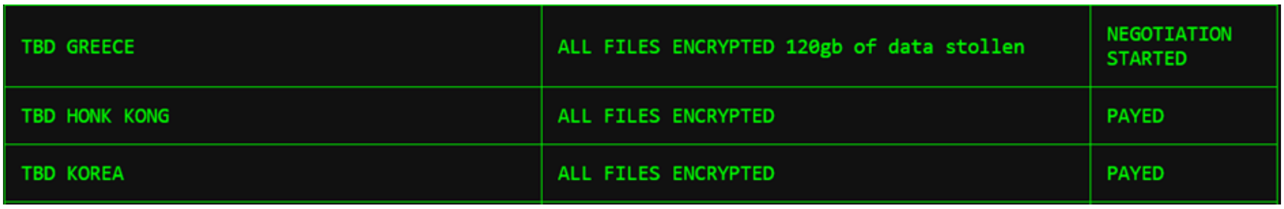
My Victims

Company	Status	Ransom Amount
Doumen.fr(QILIN)	Negotiating	800k USD
Optimax Technology(QILIN)	Whaitng	590k USD
Texas Construction Firm(QILIN)	Pending	Amount TBD
Tawasol (APOS Attack)	Pedning	150k USD
Feel Four (QILIN Attack)	Pedning	60k USD
China Harbour (s) Engeneiring Company (Dragon Force Attack) FILE SAMPLE 1 avaliable /CHEC/CHECsample.zip	Ecnrypted(we encrypted every signle device on the network and downloaded 50gb of sensitive files)	450k USD
Honk Kong Victim (To be discoled)	(To be discoled)	(To be discoled)

Figure 6. Devman Dedicated Leak Sites

The Devman group, which commenced its operations in April 2025, has thus far disclosed a total of 44 victims. Upon its initial emergence, the group exhibited a distinctive approach by meticulously detailing the software vulnerabilities or weak passwords exploited during attacks on its "My Writeups" page, delineating each phase of the attack process. Notably, instead of deploying proprietary ransomware, Devman has strategically leveraged ransomware from other groups, resulting in victims being listed not only on Devman's leak site but also on the leak sites of other ransomware collectives. The ransomware from other groups utilized in their attacks includes Apos, Qilin, DragonForce, and RansomHub. However, starting in May, they began to publish victims affected by their proprietary ransomware, known as Devman ransomware.

The Devman Group primarily operates on X (formerly Twitter), utilizing the platform predominantly for self-promotion. This includes showcasing pages for ransomware services under development, announcing impending attacks, and sharing videos demonstrating their custom-made ransomware. Furthermore, in cases involving companies with significant data breaches, the group has been observed to directly mention the victim's X account, releasing sample images of the data obtained or screenshots of the infiltrated environment as a means of mockery and intimidation.



TBD GREECE	ALL FILES ENCRYPTED 120gb of data stollen	NEGOTIATION STARTED
TBD HONK KONG	ALL FILES ENCRYPTED	PAYED
TBD KOREA	ALL FILES ENCRYPTED	PAYED

Figure 7. Victim List with Partial Information Disclosure

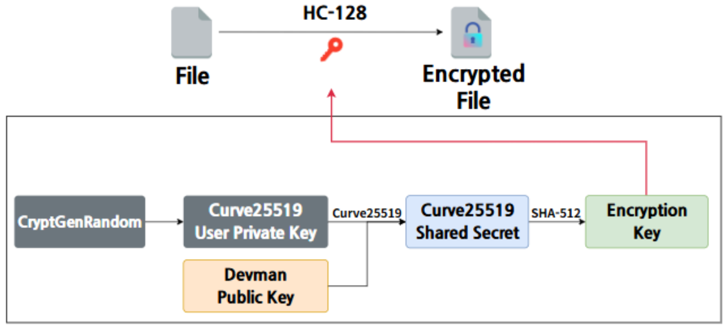
When disclosing victims, these entities do not immediately reveal the company name; instead, they first disclose the country to which the company belongs or the industry sector it operates within. Among these are domestic companies; however, the precise scale of the damage or the ransom demanded has not been disclosed, although it has been confirmed that the payment has already been made.

In May, a sample suspected to be the proprietary ransomware of the Devman Group was discovered, with the group acknowledging through their X account that this ransomware is indeed version 1. However, upon comparative analysis, it was found to be a version with additional functionalities, closely resembling the Mamona ransomware that was hacked last March. Starting in June, the group is expected to intensify its activities by launching its own ransomware service. In anticipation of this, we aim to share the analysis of the Devman ransomware to better prepare for potential threats.

Devman Ransomware

Encryption Key

Generate encryption key using Curve25519 algorithm and encrypt files with HC-128



Encryption Method

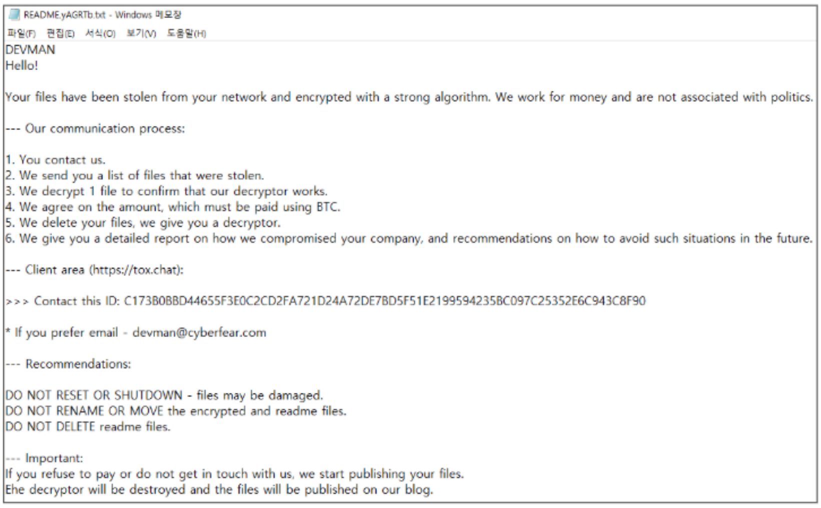
* Encryptino Method 1.
  - Files ≤ 1MB: Encrypt entire file
  - Files ﹥ 1MB and ≤ 5MB: Encrypt the first 1MB of the file
  - Files ﹥ 5MB: Encrypt from the beginning of the file up to N% of the file size (max: 70MB)

* Encryption Method 2.
  - Files ≤ 64Bytes: Encrypt entire file
  - Files ﹥ 64Bytes and ≤ 5MB: Encrypt the first 10% of the file size
  - Files ﹥ 5MB and ≤ 20MB: For every 1/6th of the file size, encrypt the first 4KB
  - Files ﹥ 20MB: For every 10MB, encrypt the first 4KB

Features

- Intermittent Encryption
- Delete VSC
- Network propagation
- Encrypt network shared folders
- HC-128 Encryption
- Kill Processes
- Change desktop and icons

Ransom Note


README.yAGRTb.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
DEVMAN
Hello!

Your files have been stolen from your network and encrypted with a strong algorithm. We work for money and are not associated with politics.

--- Our communication process:

1. You contact us.
2. We send you a list of files that were stolen.
3. We decrypt 1 file to confirm that our decryptor works.
4. We agree on the amount, which must be paid using BTC.
5. We delete your files, we give you a decryptor.
6. We give you a detailed report on how we compromised your company, and recommendations on how to avoid such situations in the future.

--- Client area (https://tox.chat):

>>> Contact this ID: C173B0BBD44655F3E0C2CD2FA721D24A72DE7BD5F51E2199594235BC097C25352E6C943C8F90

* If you prefer email - devman@cyberfear.com

--- Recommendations:

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.

--- Important:
If you refuse to pay or do not get in touch with us, we start publishing your files.
Ehe decryptor will be destroyed and the files will be published on our blog.
```

README.yAGRTb.txt

Extension

.yAGRTb

Production Language

C/C++

Figure 8. Overview of Devman Ransomware

Devman Ransomware Strategy

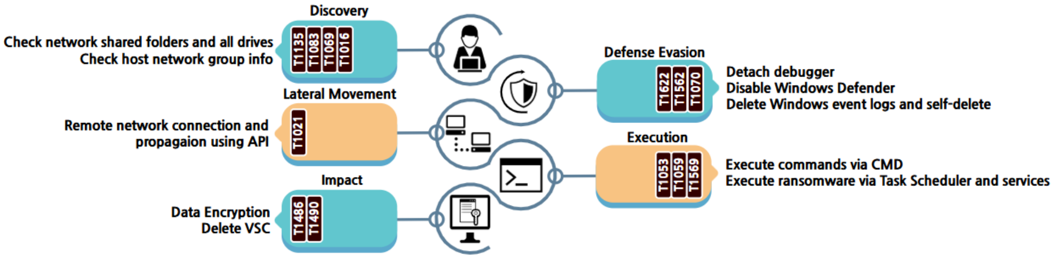


Figure 9. Devman Ransomware Attack Strategy

The Devman ransomware shares the majority of its functionalities with the Mamona ransomware. However, notable distinctions include the ability to change the icon to a specified image file, the addition of a feature to relaunch the ransomware for debugger separation, and significantly enhanced network propagation capabilities. These modifications are partially reflected in the execution parameters. In the Mamona version, the parameter -H, used to transmit the NTLM[3] hash for network authentication, has been removed in the Devman version. Additionally, new parameters have been introduced: -ldap to activate network propagation, -host to specify network propagation targets, and -detached to disable the debugger separation feature.

Type	Description
-log	Log output
-keep	Self-deletion disabled
-skip-net	Encrypt local disks only
-skip-local	Encrypt network drives only
-code {32Bytes key}	Password required to execute ransomware
-sub {subnet}	Target network range for encryption
-p {password}	Network login password
-u {username}	Network login username
-time {HH:MM}	Execute after waiting until specified time (HH:MM)
-delay {ss}	Execute after waiting for specified duration
-threads {int}	Set number of encryption threads
-path {path}	Encrypt specified folders
-host {ip_addr}	Encrypt specified hosts
-ldap	Enable network propagation
-detached	Disable ransomware re-execution

Table 1. Execution Parameters of Devman Ransomware

[3] NTLM: An authentication protocol that uses password hashes instead of plaintext passwords to grant access.

The Devman ransomware, in addition to its execution parameters, securely encrypts and stores a variety of information within a specific session. This includes encryption-related configurations, the contents of the ransom note, and the public key necessary for key generation. It subsequently decrypts this information for use. The verified details are as follows.

Offset	Description
config[0]	Partial encryption ratio
config[4]	Ransom note content
config[2056]	Enable self-deletion
config[2057]	Enable event log deletion
config[2058]	Enable service termination
config[2059]	Enable process termination
config[2060]	Enable password verification
config[2061]	Encryption mode
config[2062]	Enable ransom note printing
config[2064]	Enable icon change
config[2065]	Enable network share mounting
config[2066]	Ransomware password (32 bytes)
config[2098]	Encrypted file extension
config[2114]	Curve25519 public key (32 bytes)

Table 2. Configuration Parameters of Devman Ransomware

Ransomware also engages in the deletion of various records and traces to thwart recovery efforts and impede analysis. It completely erases data in the recycle bin and, depending on the configuration settings, deletes all event logs within the Windows environment. Furthermore, it utilizes command prompt commands to remove backup copies, and once the encryption of all files is complete, the ransomware autonomously deletes itself.

Command	Description
cmd.exe /c vssadmin delete shadows /all /quiet	VSS deletion
cmd.exe /C ping 127.0.0.7 -n 3 > Nul & Del /f /q \"%s\	Self-deletion

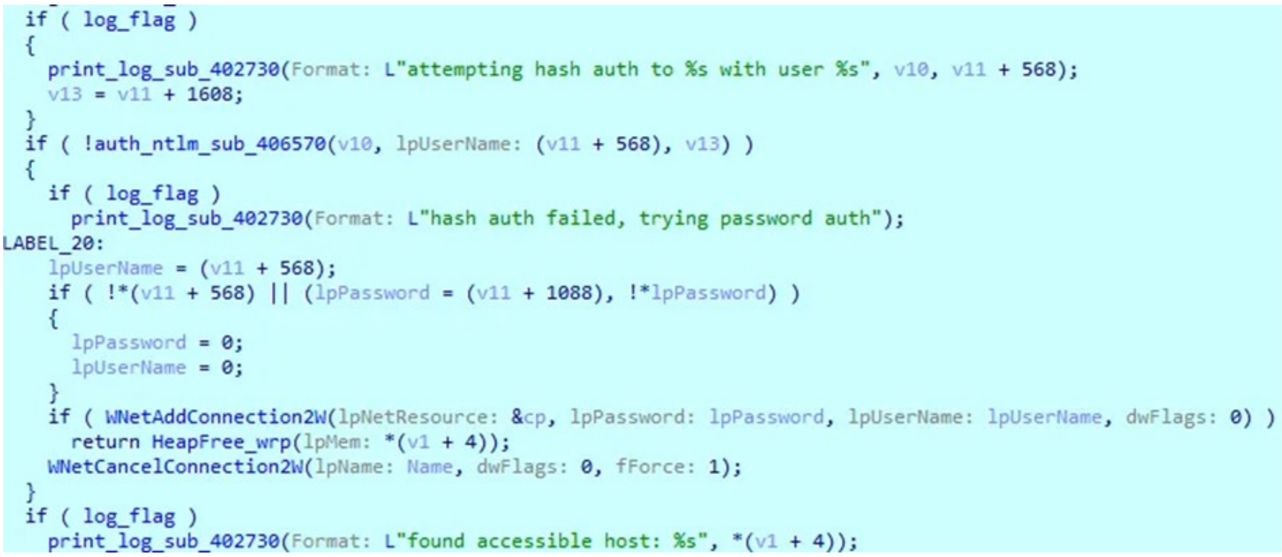
Table 3. Commands Related to Deletion

If the configuration settings include parameters related to the termination of services or processes, certain services and processes will be prioritized for termination to facilitate seamless file encryption. The services and processes targeted for termination are listed in the table below.

Service	Process
WinDefend, SecurityHealthService, wscsvc, Sense, WdNisSvc, WdNisDrv, WdFilter, WdBoot, wdnisdrv, wdfilter, wdboot, mpssvc, mpsdrv, BFE, MsMpSvc, SepMasterService, wscsvc, SgrmBroker, SgrmAgent, EventLog	MsMpEng.exe, NisSrv.exe, SecurityHealthService.exe, smartscreen.exe, SecHealthUI.exe, MpCmdRun.exe, MSASCui.exe, MpUXSrv.exe, SgrmBroker.exe, MsSense.exe, SenseIR.exe, SenseCE.exe, SenseSampleUploader.exe, SenseNdr.exe,

Table 4. Target Services and Processes for Termination

After terminating services and processes, the ransomware propagates across the network. This execution requires the use of the -ldap parameter, and additionally, propagation can be attempted to specific hosts using the -host parameter or to all hosts within a particular subnet range using the -sub parameter. In previous versions of Mamona, network connections are attempted via IPC$[4], necessitating the input of login credentials, an authentication NTLM hash, and a login password through the -u, -H, and -p parameters, respectively. Although the -H parameter receives the hash value for authentication, actual NTLM authentication is not conducted; instead, login attempts are made using the -u and -p parameters. If access is granted, the method employed encrypts files located in the network's shared resources without further propagation of the ransomware.

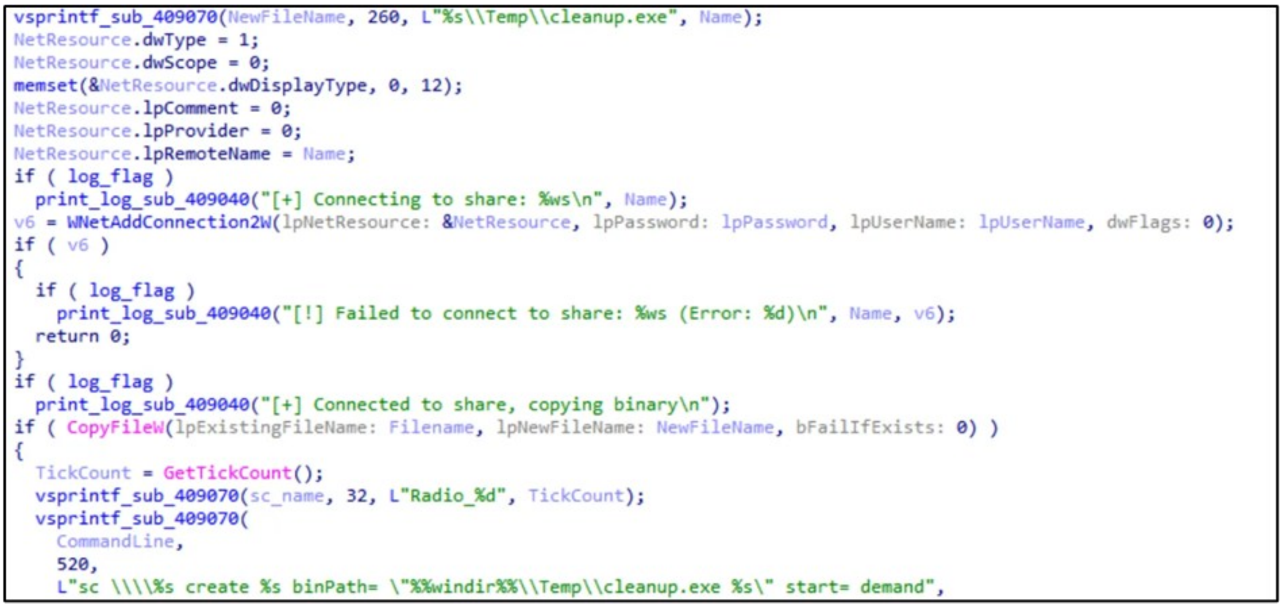


```
  if ( log_flag )
  {
    print_log_sub_402730(Format: L"attempting hash auth to %s with user %s", v10, v11 + 568);
    v13 = v11 + 1608;
  }
  if ( !auth_ntlm_sub_406570(v10, lpUserName: (v11 + 568), v13) )
  {
    if ( log_flag )
      print_log_sub_402730(Format: L"hash auth failed, trying password auth");
LABEL_20:
    lpUserName = (v11 + 568);
    if ( !*(v11 + 568) || (lpPassword = (v11 + 1088), !*lpPassword) )
    {
      lpPassword = 0;
      lpUserName = 0;
    }
    if ( WNetAddConnection2W(lpNetResource: &cp, lpPassword: lpPassword, lpUserName: lpUserName, dwFlags: 0) )
      return HeapFree_wrp(lpMem: *(v1 + 4));
    WNetCancelConnection2W(lpName: Name, dwFlags: 0, fForce: 1);
  }
  if ( log_flag )
    print_log_sub_402730(Format: L"found accessible host: %s", *(v1 + 4));
```

Figure 10. Network Authentication Method of Mamona Ransomware

[4] IPC$: shared folder used for authentication when accessing another computer over a network.

In the case of the Devman ransomware, rather than attempting network encryption through IPC$, it employs a method of propagation utilizing LDAP[5]. If the login ID provided via the -u parameter is in the form of id@domain, it extracts the domain information from this and uses it to retrieve information on all hosts connected to the Active Directory (AD)[6]. Subsequently, it verifies whether authentication is possible on each host using the ID from the -u parameter and the password from the -p parameter. Once authentication is confirmed, the ransomware is disseminated across all authenticated hosts.



```
vsprintf_sub_409070(NewFileName, 260, L"%s\\Temp\\cleanup.exe", Name);
NetResource.dwType = 1;
NetResource.dwScope = 0;
memset(&NetResource.dwDisplayType, 0, 12);
NetResource.lpComment = 0;
NetResource.lpProvider = 0;
NetResource.lpRemoteName = Name;
if ( log_flag )
  print_log_sub_409040("[+] Connecting to share: %ws\n", Name);
v6 = WNetAddConnection2W(lpNetResource: &NetResource, lpPassword: lpPassword, lpUserName: lpUserName, dwFlags: 0);
if ( v6 )
{
  if ( log_flag )
    print_log_sub_409040("[!] Failed to connect to share: %ws (Error: %d)\n", Name, v6);
  return 0;
}
if ( log_flag )
  print_log_sub_409040("[+] Connected to share, copying binary\n");
if ( CopyFileW(lpExistingFileName: Filename, lpNewFileName: NewFileName, bFailIfExists: 0) )
{
  TickCount = GetTickCount();
  vsprintf_sub_409070(sc_name, 32, L"Radio_%d", TickCount);
  vsprintf_sub_409070(
    CommandLine,
    520,
    L"sc \\\\%s create %s binPath= \"%%windir%%\\Temp\\cleanup.exe %s\" start= demand",
```

Figure 11. Propagation and Execution of Devman Ransomware

The ransomware replicates itself under the filename cleanup.exe in the temporary folder of the connected host, subsequently registering as a service or executing via the task scheduler. Additionally, to prevent multiple propagation attempts within the same network, the ransomware is executed on remote hosts with the inclusion of the -skip-net argument. The command utilized is detailed in the table below.

Command	Description
sc \\{host_ip} create Radio_[0-9]{32} binPath= "%%windir%%\\Temp\\cleanup.exe -skip-net" start= demand	Create service on remote host
sc \\{host_ip} start Radio_[0-9]{32}	Start service
schtasks /create /s {host_ip} /u {username} /p {password} /tn "CoolTask" /tr "%%windir%%\Temp\cleanup.exe -skip-net" /sc once /st 00:00	Create scheduled task
schtasks /run /s {host_ip} /u {username} /p {password} /tn	Execute scheduled task
schtasks /delete /s {host_ip} /u {username} /p {password} /tn	Delete scheduled task

Table 5. Target Services and Processes for Termination

[5] LDAP: A protocol for storing and retrieving data such as users, groups, devices, and credentials over a network.

[6] AD (Active Directory): Windows LDAP-based directory system that enables centralized management of users and computers.

Following the propagation across the network, the encryption of the local system is initiated. By employing the -skip-local parameter, only network shared folders are encrypted, whereas the -skip-net parameter restricts encryption to local disks alone. Furthermore, utilizing the -path argument allows for the encryption of specific directories and their subdirectories exclusively. Once the encryption targets have been designated, each directory is traversed to ascertain whether it corresponds to any exception items. Apart from the addition of the .bin extension to the exception list in the Devman version, the encryption exceptions remain consistent across both versions. The encryption exception targets are delineated in the table below.

Folder name	File extension, and File name
Windows, Program Files, Program Files (x86), AppData, ProgramData, All Users, NETLOGON, SYSVOL	PrintMe22.pdf, .exe, .dll, .msi, .sys, .ini, .ink, .bin

Table 6. Subjects of Encryption Exceptions

The file encryption methodology is delineated into two distinct encryption modes, contingent upon the configuration settings. These settings encompass two pivotal options: one that determines the encryption mode and another that dictates the partial encryption ratio. The first method pertains to the encryption of only the initial segment of large files. Files that are 1MB or smaller undergo full encryption, while those up to 5MB in size have only the first 1MB encrypted. For files exceeding 5MB, the encryption process involves encrypting only the initial portion of the file, as specified by the attacker's designated ratio, with the encrypted segment being capped at a maximum of 70MB.

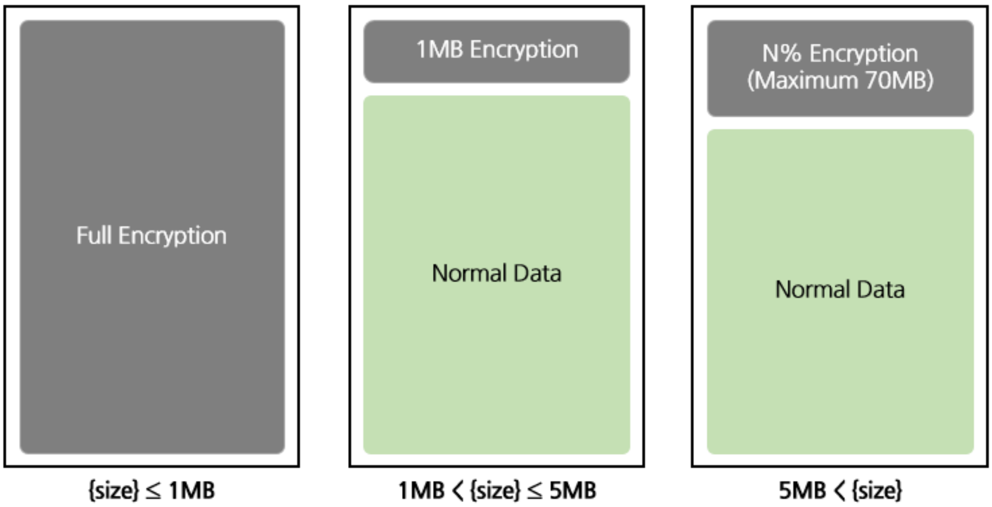


Figure 12. File Encryption Methods by Size - 1

The second method involves encrypting files at regular intervals, particularly for those of substantial size. Files that are 64 bytes or smaller undergo full encryption. For files up to 5MB, only 10% of the total size is encrypted. Files that are 20MB or smaller are divided into segments equivalent to one-sixth of the total size, with only the first 4KB of each segment being encrypted. For files exceeding 20MB, the first 4KB is encrypted for every 10MB segment.

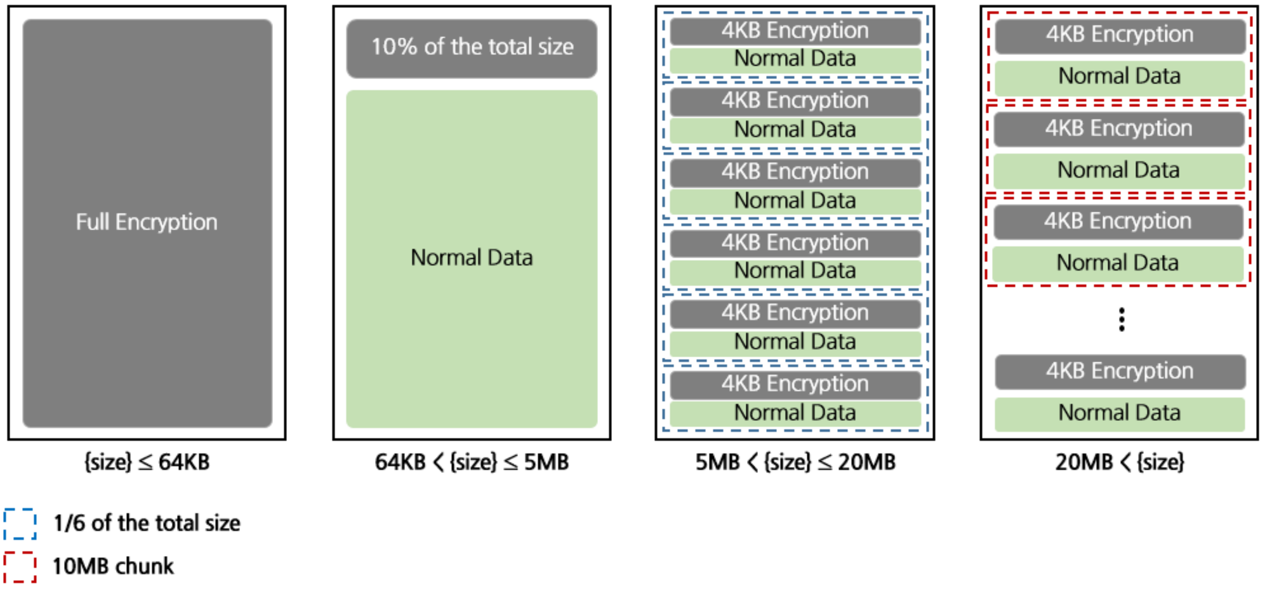
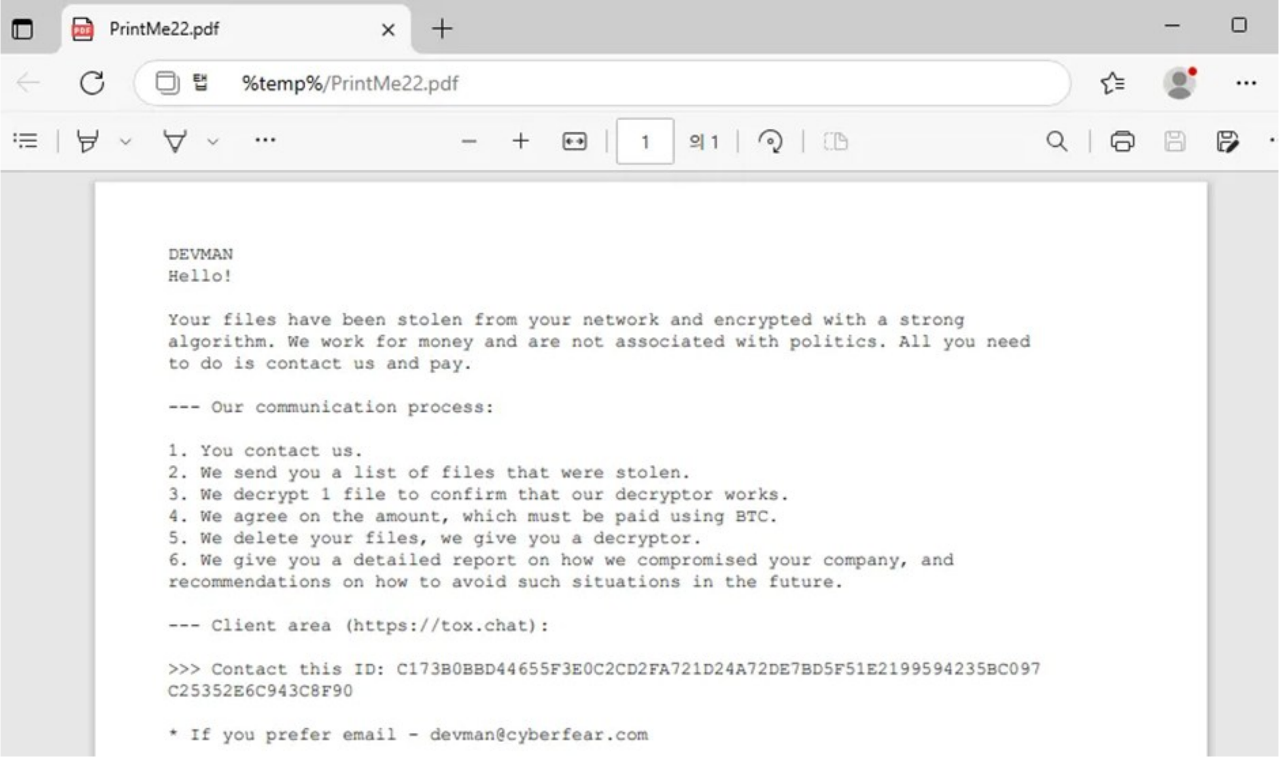


Figure 13. File Encryption Methods by Size - 2

Both encryption methods employ the same algorithm, utilizing a shared secret generated via Curve25519 for the encryption key. For each file, a random private key is generated, after which a shared secret can be established using the hardcoded public key of Devman. This process exploits the property of Curve25519, where the shared secret derived from one's private key and the counterpart's public key is identical to the shared secret obtained from one's public key and the counterpart's private key. The shared secret is then hashed using the SHA-512 algorithm, and the last 32 bytes of the hash are employed as the key for encrypting the file with the HC-128 algorithm. At the end of the file, the Curve25519 public key necessary for key recovery is stored.

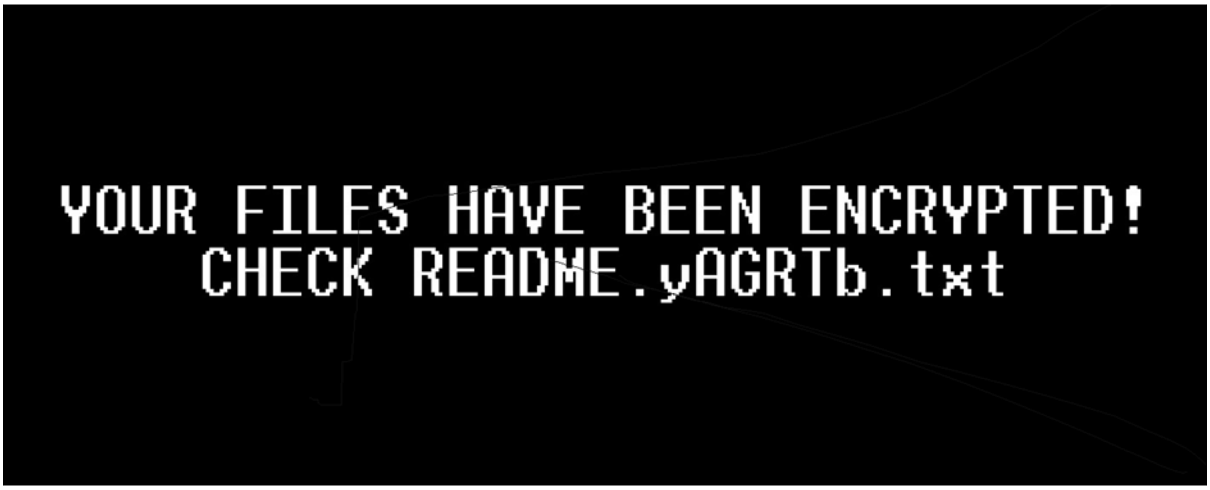
Upon the completion of file encryption, a ransom note is generated in each designated encryption path. If the option to print the ransom note is enabled, the contents of the ransom note are saved in PDF format and subsequently printed on all connected printers. The ransom note is stored in the temporary folder under the name PrintMe22.pdf.



```
DEVMAN
Hello!

Your files have been stolen from your network and encrypted with a strong
algorithm. We work for money and are not associated with politics. All you need
to do is contact us and pay.

--- Our communication process:

1. You contact us.
2. We send you a list of files that were stolen.
3. We decrypt 1 file to confirm that our decryptor works.
4. We agree on the amount, which must be paid using BTC.
5. We delete your files, we give you a decryptor.
6. We give you a detailed report on how we compromised your company, and
recommendations on how to avoid such situations in the future.

--- Client area (https://tox.chat):

>>> Contact this ID: C173B0BBD44655F3E0C2CD2FA721D24A72DE7BD5F51E2199594235BC097
C25352E6C943C8F90

* If you prefer email - devman@cyberfear.com
```

Figure 14. Ransom Note for Output

Furthermore, to alter the icons of encrypted files, the icon image file, stored in Base64 format, is temporarily saved in a designated folder. Subsequently, the registry settings are modified to arbitrarily change the icon. Additionally, the desktop wallpaper is altered to an image displaying the message, "YOUR FILES HAVE BEEN ENCRYPTED! CHECK README.yAGRTb.txt."



YOUR FILES HAVE BEEN ENCRYPTED!
CHECK README.yAGRTb.txt

Figure 15. Altered Desktop Background

Response Strategies for DragonForce Ransomware

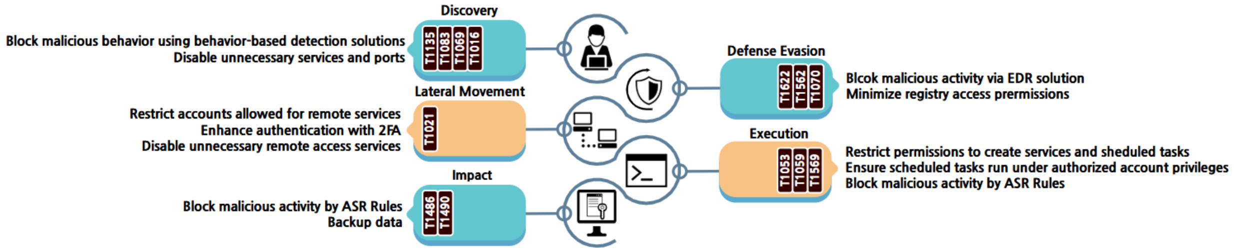

Discovery
Block malicious behavior using behavior-based detection solutions
Disable unnecessary services and ports
T1135
T1083
T1069
T1016
Lateral Movement
Restrict accounts allowed for remote services
Enhance authentication with 2FA
Disable unnecessary remote access services
T1021
Impact
Block malicious activity by ASR Rules
Backup data
T1486
T1490
Defense Evasion
T1622
T1562
T1070
Blcok malicious activity via EDR solution
Minimize registry access prermissions
Execution
T1053
T1059
T1569
Restrict permissions to create services and sheduled tasks
Ensure scheduled tasks run under authorized account privileges
Block malicious activity by ASR Rules

Figure 16. Countermeasures for Devman Ransomware

The Devman ransomware exploits various types of information, such as network shared folders and the domain to which a system belongs, to encrypt files and propagate across networks. Consequently, it is possible to thwart malicious activities by employing behavior-based detection solutions. Additionally, by eliminating or deactivating unnecessary network services, one can prevent the dissemination of damage across the network.

To evade detection of its malicious activities, ransomware disables Windows Defender, detaches debuggers, and deletes various event logs. Utilizing an Endpoint Detection and Response (EDR)[7] solution can effectively block such malicious actions as the deactivation of Windows Defender and the deletion of event logs. In particular, the deletion of event logs necessitates access to the registry; by minimizing registry access permissions, one can prevent attackers from arbitrarily deleting event logs.

Furthermore, in an attempt to disseminate ransomware within the network environment, there are efforts to gain access using login IDs and passwords. Although there has been no verified process for the collection of these IDs and passwords, it is plausible that during the preparatory phase of the attack, account information could be gathered, leaked, or exploited, particularly if the accounts are vulnerable. Consequently, it is imperative to fortify authentication mechanisms by employing two-factor authentication (2FA)[8]. Additionally, restricting accounts that can utilize remote services or deactivating unnecessary remote services altogether can serve as a deterrent, effectively preventing attackers from infiltrating the network environment.

[7] EDR (Endpoint Detection and Response): A real-time solution for detecting and mitigating malicious behavior on endpoints like computers, mobile devices, and servers.

[8] 2FA (2-factor Authentication): An authentication method that adds a second factor, such as a mobile device or OTP, in addition to ID and password.

The aforementioned malicious activities predominantly exploit the Windows Command Prompt or are executed through the registration of tasks and services. Consequently, by activating ASR (Attack Surface Reduction)[9] rules, one can effectively intercept and prevent such anomalous processes, thereby thwarting malicious actions. Furthermore, given that ransomware often stores its programs in temporary folders or replicates itself in specific locations for task registration, it is feasible to employ Anti-Virus solutions to isolate suspicious files. Additionally, it is imperative to restrict the creation permissions for services and task schedulers to prevent the remotely executed replication of ransomware. Even if scheduled tasks are executed, configuring them to run under the authority of authenticated accounts can significantly mitigate potential damage.

To prevent users from arbitrarily recovering encrypted files, all backup copies present within the system are deleted prior to file encryption. By activating ASR (Attack Surface Reduction) rules, it is possible to block processes that delete backup copies and encrypt files. Moreover, it is imperative to implement measures such as dispersing backup copies to separate networks or storage locations, ensuring recovery is feasible even if the system undergoes encryption.

[9] ASR (Attack Surface Reduction): A protection feature that blocks specific processes and executables used by attackers.

Indicators of Compromise (IoCs)

Hash(SHA-256)
1f6640102f6472523830d69630def669dc3433bbb1c0e6183458bd792d420f8e
c5f49c0f566a114b529138f8bd222865c9fa9fa95f96ec1ded50700764a1d4e7

■ Reference Websites

- GMA Network (https://www.gmanetwork.com/news/topstories/nation/945481/gma-network-statement-on-cybersecurity-incident)

- RELIAQUEST (https://reliaquest.com/blog/threat-spotlight-reliaquest-uncovers-vulnerability-behind-sap-netweaver-compromise/)