DevMan Ransomware Threat Actor Report

TLP: CLEAR
July 2025

INCD
Israel National
Cyber Directorate

Table of Contents

Part I

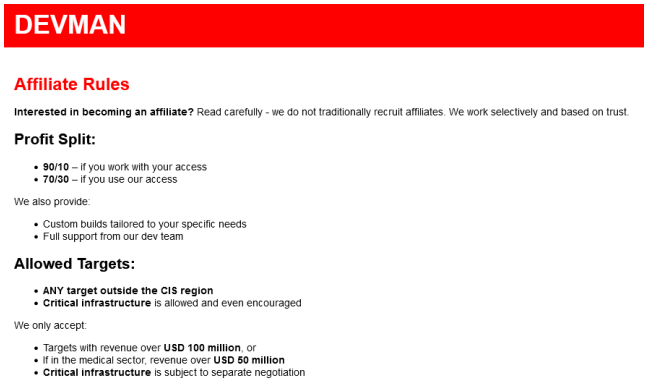
Threat Actor Intelligence Brief

INCD
Israel National
Cyber Directorate

In early April 2025, an actor presenting itself as “DevMan” has claimed on X[1] to gain access and perform a ransomware attack against the French transport company “doumen”. Since then, the threat actor has proved itself as being highly prolific and was named as one of the top active ransomware attackers in the following months.[2] As of July 2025, DevMan has claimed at least 54 victims.

DevMan is an affiliate of several RaaS programs, mainly Qilin, APOS and also Dragon Force.[3] As it seems, the first victims were indeed victims of those ransomware strains, but as time passed, DevMan has become more independent and claimed to use their own ransomware, eponymously named “DevMan”. Later on, they have announced their private ransomware will become a RaaS program as well (advertised on their onion DLS site to be officially active in late June 2025). The threat actor has claimed on their X account that DevMan is a group and not a sole actor.[4]

As part of their RaaS program, DevMan offers 90% profit per victim and 70% profit if the affiliate uses an access provided by DevMan. They claimed they only accept attacks on targets with over 100M$ revenue or over 50M$ in the medical sector while critical infrastructure is supposed to be negotiated differently, they encourage attacks on the critical infrastructure and show little to no guidelines on which victims are allowed. They advertise full support for affiliates with custom builds for each specific victim and attack.



Affiliate rules from DevMan’s DLS

The threat actor is operating with a high-profile online presence and updating about developments, updates and general statements mainly in English and sometimes in Russian as well. They operate the aforementioned X account and a DLS page on the TOR network.[5] They often “brag” about their achievements, to the point where they post write-ups that describe the way they gained access and performed the attack.

Up until June 2025, a DLS platform was hosted on TOR[6] and featured posts where the threat actor detailed how they gained access and performed the ransomware attacks, the aforementioned “write-ups”. Those posts could shed light on the threat actor’s MO and TTPs if they come back online on the newer DLS.

[1] https://x.com/Inifintyink/status/1908042147887988883
[2] https://www.ransomware.live/group/devman
[3] https://cyble.com/blog/qilin-tops-april-2025-ransomware-report/
[4] https://x.com/Inifintyink/status/1910036251140305179
[5] https://wugurgyscp5rxpihef5vl6b6m5ont3b6sezhl7boboso2enib2k3q6qd.onion
[6] https://qljmlmp4psnn3wqskkf3alqquatymo6hntficb4rhq5n76kuogcv7zyd.onion

Part II

Technical Malware Analysis

INCD
Israel National
Cyber Directorate

Malware Sample Analysis

The following sample was analyzed:

`1f6640102f6472523830d69630def669dc3433bbb1c0e6183458bd792d420f8e`

The sample has a lot of code overlap with a relatively new ransomware strain that open-source reporting refers to as Mamona.

The ransomware starts by setting the priority class of the process to `HIGH_PRIORITY_CLASS` and resolves the necessary APIs at runtime, using API hashing. It parses the arguments and creates a mutex named `Global\\Fxo16jmdgujs437`. Next, DevMan empties the recycle bins on every drive by calling the function `SHEmptyRecycleBinA` and deletes existing shadow copies using the following command:

```
cmd.exe /c vssadmin delete shadows /all /quiet
```

Finally, it starts the encryption process according to the provided arguments and the configuration and sets a custom wallpaper displaying the following text:

```
YOUR FILES HAVE BEEN ENCRYPTED!
Check README.yAGRTb.txt
```

DevMan ransomware accepts the following command-line arguments:

Argument	Description
`-log`	Enables extensive logging output
`-force`	Executes even if an instance is already running
`-detached`	Runs without a window and sets the handles for all standard devices (stdin, stdout and stderr) to NUL
`-path`	Provides a specific path to be encrypted
`-threads`	Specifies the number of threads used for encryption (1-256; default is the number of logical processors returned by SystemInfo.dwNumberOfProcessors)
`-delay`	Waits the specified amount of seconds before starting the encryption process (maximum 24 hours)
`-time`	Defines when to start the encryption process (HH:MM)
`-skip-local`	Disables local drive encryption
`-skip-net`	Disables network encryption
`-keep`	Disables self-deletion
`-ldap`	Enables spreading to LDAP domains - -u and -p are required
`-u`	Specifies the username for the LDAP spreading
`-p`	Specifies the password for the LDAP spreading
`-code`	Provides the password needed to execute the ransomware (depends on the configuration)
`-host`	Targets a specified host
`-sub`	Specify a subnet for spreading

The sample contains an encrypted configuration that is 0x864 bytes in size. It is stored in a dedicated PE section named `.config` which the ransomware decrypts during runtime. The following Python snippet implements the decryption routine:

```
def decrypt_config(data):
      result = bytearray(data)
      current_key = 0x52D8FC7D

      for i in range(0x219):
            result[i*4] ^= current_key & 0xFF
            result[i*4+1] ^= (current_key >> 8) & 0xFF
            result[i*4+2] ^= (current_key >> 16) & 0xFF
            result[i*4+3] ^= (current_key >> 24) & 0xFF
            current_key = (0x9A8B7C6D * ((current_key << 13) |
            (current_key >> 19))) & 0xFFFFFFFF
            current_key ^= 0x5E4F3D2C
      return bytes(result)
```

For this sample, the decrypted configuration starts with the bytes `14 00 00 00` followed by the ransom note that is written to each processed directory and named README.<extension>.txt. The value for <extension> is read from the configuration and is set to yAGRTb in the submitted sample. Notably, the ransomware also tries to print the ransom note on all available printers.
Additionally, the configuration holds multiple flags that control specific features of the ransomware. For example, the byte at the offset `0x80c` represents a switch for the password protection feature. If it is enabled, the ransomware expects to be provided a password via the `-code` command line argument. The expected password is stored in the encrypted configuration.
The configuration also holds flags determining if the Windows event log should be deleted and a flag that toggles the termination of hardcoded services and processes. It also contains a hardcoded public key for ECDH using Curve25519 that is later used in context of the encryption.
Notably, although the ransom note states that the actor will start to publish the files in case the victim does not pay, no extraction capabilities were identified.

For each file, the ransomware generates 32 random bytes that it uses to create a key-pair using the ECDH algorithm on Curve25519. The generated public key is appended at the end of each encrypted file. Next, DevMan creates a shared key using the initially created private key and the following hardcoded public key from the configuration:

```
C6 00 6E 2C 29 F7 CB 5C C5 59 99 84 F6 5F 4D EF 04 0E B4 84 B9 FC C5
A1 C2 3E 8C FD 97 13 E3 79
```

The Blake2 hash of the generated shared key is then used to initialize a HC-256 stream cipher to ultimately encrypt the current file. Finally, it appends the following hardcoded file marker to indicate that the file has already been encrypted:

`xcrydtednotstill_amazingg_time!!`
Generally, the ransomware fully encrypts files that are up to 5 MB large. For larger files, DevMan encrypts a percentage of the file that is defined in the configuration. If the configuration does not define the percentage, a default value of 20% is used.

Indicators

Over the weeks following the launching of their activity, a few researchers have posted about technical OPSEC mistakes by the group that led to exposing IP addresses behind the DLS site and their activity.[7]
The following IPs were detected as hosting the threat actor's DLS onion site:

- `38.132.122[.]213`
- `38.132.122[.]214`
- `83.217.209[.]210`

Hashes of DevMan ransomware samples (partly from AlienVault[8]):

- `018494565257ef2b6a4e68f1c3e7573b87fc53bd5828c9c5127f31d37ea964f8`
- `df5ab9015833023a03f92a797e20196672c1d6525501a9f9a94a45b0904c7403`
- `1f6640102f6472523830d69630def669dc3433bbb1c0e6183458bd792d420f8e`

The mutex `Global\\Fxo16jmdgujs437` was found in 6 more files submitted to VirusTotal that seem like different samples with various extensions used:

SHA-256 file hash	Extension
232f86e26ced211630957baffcd36dd3bcd6a786f3d307127e1ea9a8b31c199f	vEHdfmA
c7b91de4b4b10c22f2e3bca1e2603160588fd8fd829fd46103cf536b6082e310	EeUfy
13b82f4ac62faf87a105be355c82bacfcbdd383050860dfa93dfbb7bb2e6c9ba	YtKMI
c5f49c0f566a114b529138f8bd222865c9fa9fa95f96ec1ded50700764a1d4e7	HAes
28f3de066878cb710fe5d44f7e11f65f25328beff953e00587ffeb5ac4b2faa8	LDIdQm
94180cac48ba76bbcb7ef672f7f6a1e5afffb51da1e094f8f8391ca10ffa4b37	vEHdfmA

[7] https://x.com/karol_paciorek/status/1909197870877622457
https://x.com/RakeshKrish12/status/1924716514202288232
[8] https://otx.alienvault.com/pulse/68535853fe15cff17229577d

Part III

Appendices

INCD
Israel National
Cyber Directorate

Ransom note

```
DEVMAN
Hello!
Your files have been stolen from your network and encrypted with a strong algorithm.
We wo
rk for money and are not associated with politics. All you need to do is contact us
and pa
y.
 ---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 o
n how to avoid such situations in the future.
 ---Client area (https[:]//tox[.]chat):
 <<<Contact this ID:
C173B0BBD44655F3E0C2CD2FA721D24A72DE7BD5F51E2199594235BC097C25352E6C9
43C8F90
 *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.
```

List of services to be terminated

- WinDefend
- SecurityHealthService
- Wscsvc
- Sense
- WdNisSvc
- WdNisDrv
- WdFilter
- WdBoot
- wdnisdrv
- wdfilter
- wdboot
- mpssvc
- mpsdrv
- BFE
- MsMpSvc
- SepMasterService
- wscsvc
- SgrmBroker
- SgrmAgent
- EventLog

List of processes to be killed

- 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
- SenseCncProxy.exe

Known TOX IDs

9D97F166730F865F793E2EA07B173C742A6302879DE1B0BBB03817A5A04B572FBD82F984981D
C173B0BBD44655F3E0C2CD2FA721D24A72DE7BD5F51E2199594235BC097C25352E6C943C8F90