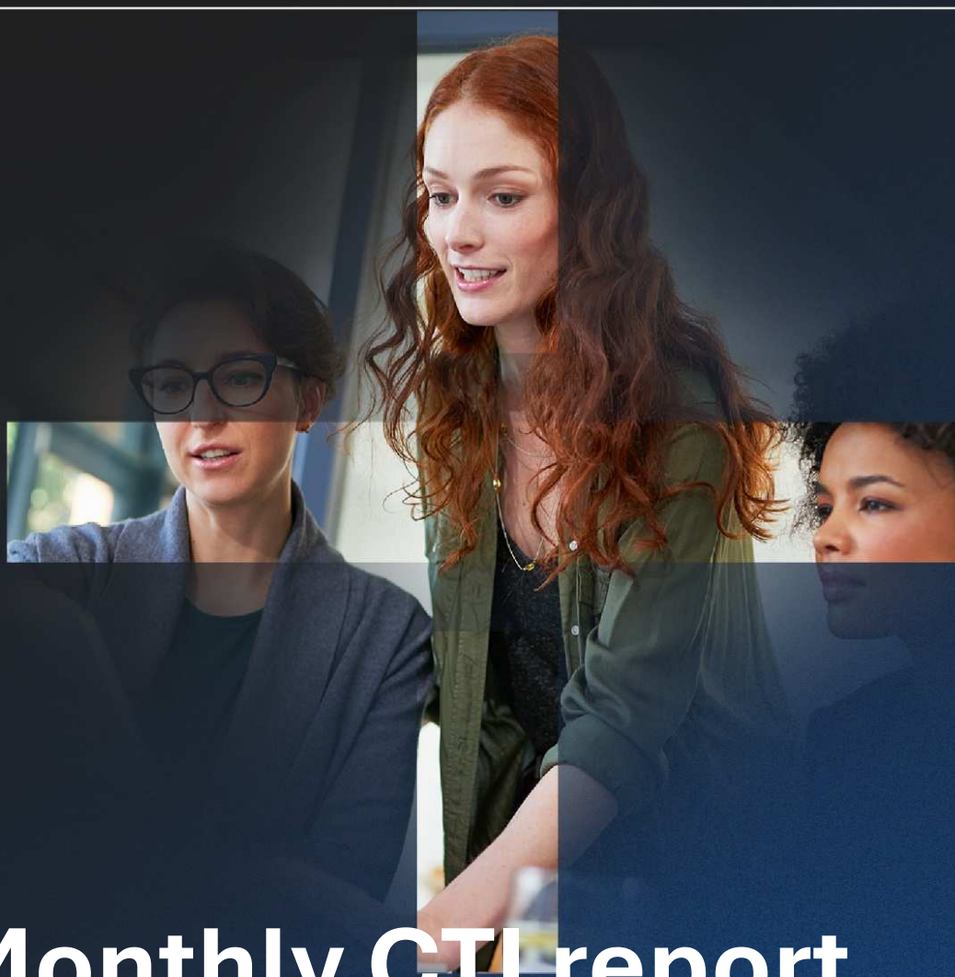
aDvens

For cyber, people & planet



Monthly CTI report

May 2026

CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

TABLE OF CONTENT

1. EXECUTIVE SUMMARY

This month, CERT aDvens brings you an overview of emerging threats and recently identified vulnerabilities:

- Three new security vulnerabilities have been detected, including one critical vulnerability with a CVSSv3.1 score of 10. These are in addition to the vulnerabilities previously identified.
- An analysis of the Medusa ransomware, used in October 2025 by the North Korean APT Lazarus against a Saudi group specialised in the textile and food trade.

These topics aim to help you anticipate risks and strengthen your cybersecurity posture.

2. VULNERABILITIES

This month, the CERT aDvens highlights **three** vulnerabilities affecting commonly used technologies within companies.

They are sorted by severity (proofs of concept available, exploitation...). Applying their patches or workarounds is highly recommended.

2.1. Cisco - CVE-2026-20223

An access control flaw in Cisco Secure Workload's REST APIs allows an unauthenticated attacker, by sending specially crafted requests, to access sensitive data or make configuration changes with the privileges of a *Site Admin* user.

2.1.1. Type of vulnerability

- **CWE-306**: Missing Authentication for Critical Function

2.1.2. Risks

- Security bypass
- Information disclosure
- Integrity breach

2.1.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.1.4. Impacted Products

Cisco Secure Workload:

- versions prior to 3.10.8.3
- versions 4.x prior to 4.0.3.17

2.1.5. Recommendations

Update Cisco Secure Workload to version 3.10.8.3, 4.0.3.17 or later.

Migrate Cisco Secure Workload versions 3.9 and earlier to a patched version.

Cloud-hosted Cisco Secure Workload SaaS deployments have already been patched by Cisco.

Additional information is available in Cisco's advisory.

2.1.6. Proof of concept

To date, no proof of concept is available in open source.

2.2. Fortinet - CVE-2026-44277

An improper access control of the Fortinet FortiAuthenticator API allows an unauthenticated attacker to execute arbitrary code by sending specially crafted requests.

2.2.1. Type of vulnerability

- **CWE-284**: Improper Access Control

2.2.2. Risk

- Remote code execution

2.2.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.2.4. Impacted Products

Fortinet FortiAuthenticator:

- versions 6.5.x prior to 6.5.7
- versions 6.6.x prior to 6.6.9
- versions 8.0.0 and 8.0.2

2.2.5. Recommendations

Update Fortinet FortiAuthenticator to version 6.5.7, 6.6.9, 8.0.3 or later.

FortiAuthenticator Cloud is not affected and no user action is required.

It is possible to disable API access for exposed interfaces via the *Network → Interfaces → Access Rights* menu.

Additional information is available in Fortinet's advisory.

2.2.6. Proof of concept

To date, no proof of concept is available in open source.

2.3. SAP - CVE-2026-34260

An improper validation of user input in SAP S/4HANA allows an authenticated attacker, using specially crafted SQL queries, to access sensitive data in the database or cause the application to crash.

2.3.1. Type of vulnerability

- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

2.3.2. Risks

- Information disclosure
- Denial of service

2.3.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	None
User Interaction	None	Impact on availability	High

2.3.4. Impacted Products

- SAP S/4HANA (SAP Enterprise Search for ABAP) versions SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758 and SAP_BASIS 816

2.3.5. Recommendations

Apply the May 2026 security patches to SAP S/4HANA.

Additional information is available in SAP's advisory.

2.3.6. Proof of concept

To date, no proof of concept is available in open source.

3. CYBER-VIROLOGY: ANALYSIS OF A SAMPLE OF THE MEDUSA RANSOMWARE

Author: Samuel De Cruz

3.1. A new affiliation

During 2025, a ransomware cyberattack attributed to the North Korean APT Lazarus was identified. This cyberattack targeted a major textile and food trading group, one of whose main offices is located in Saudi Arabia. According to available information, the initial intrusion phase began in March 2025. For nearly seven months, the attackers reportedly conducted reconnaissance, espionage, and lateral movement activities within the targeted organisation's systems and network. In October 2025, the operators launched the second phase of the operation by deploying and executing the Medusa ransomware via an executable named gaze.exe. The investigative work carried out by Breakglass researchers highlights an unprecedented collaboration between the Ransomware-as-a-Service (RaaS) franchise Medusa, acting as franchisor, and the APT Lazarus, which allegedly operated as an affiliate.

This article offers a further analysis of the portable executable gaze.exe, corresponding to the Medusa ransomware recently used by APT Lazarus. It also sheds light on the use of ransomware by North Korean state actors, as well as the strategic and operational implications that these new criminal alliances may have for organisations.

3.2. APT Lazarus and ransomware

Since its emergence, APT Lazarus has conducted numerous ransomware attacks, notably using its own arsenal of malware, including WannaCry in 2017, Maui in 2022, and H0lyGh0st the same year. Operators have also used ransomware based on the Ransomware-as-a-Service (RaaS) model, such as PLAY and Qilin.

In most documented cases, these tools are used in cyber extortion campaigns aimed at financial gain. In collaboration with the North Korean units APT 38 and APT TEMP Hermit, APT Lazarus also deployed ransomware belonging to other criminal groups following cyber heists to disrupt investigations and complicate attribution. For example, attackers used the HERMES ransomware to cover their tracks during the cyber heist of the Central Bank of Bangladesh in February 2016.

3.3. Lazarus and Medusa

APT LAZARUS

Active since 2007, APT Lazarus is a North Korean advanced persistent threat (APT) group specialising in cyber espionage, cyber extortion, cyber robberies, and cyber sabotage operations. Composed of highly skilled attackers, the group is considered an elite cyber unit whose level of technical sophistication, operational capabilities, and ingenuity are widely recognised within the threat intelligence community.

MEDUSA

Although initially associated with a relatively small collective, Medusa has gradually evolved into a structured criminal franchise based on the RaaS model, specialising in ransomware crime. The franchisors are believed to be the actors grouped under the name Spearwing, active since at least 2021 and likely originating from the Russian-speaking cybercrime sphere. To date, the operators of Medusa primarily employ double extortion strategies combining data exfiltration and encryption. Investigations also show that they frequently favor the use of legitimate tools already present on compromised systems, following a so-called Living-off-the-Land (LotL) approach, in order to reduce their malicious footprint and complicate detection.

3.4. Dissection of the gaze.exe code (Medusa)

Several methods, including malicious artifacts, were used during the cyberattack to achieve intrusion, lateral movement, and privilege escalation. This article focuses primarily on the analysis of the ransomware code gaze.exe, deployed and executed by the attackers during the impact phase.

	Artifact: gaze.exe and dft7aw3f.exe Aliases: Medusa (Medusa Locker) Virology: Ransomware - Trojan horse Virology - Intelligence: Ransomware:Win/Medusa.A Virology - Popular label: Ransomware.medusa/medusalocker Type: PE32 executable Intel 80386, MS Windows Size: 624 kB MD5: 60aaafce354ae5e0b8115729464a8b24 SHA1: 53948d9596ebab5c4cf2ac04e7fb70c429e0cbbf SHA256: 15208030eda48b3786f7d85d756d2bd6596ef0f465d9c8509a8f02c53fad9a10

3.4.1. Static Analysis - EXIF

Static analysis of the code reveals interesting information such as the "TimeSTamp": **2025:10:17 13:48:31+00:00**. The ransomware binary appears to have been created during the month of phase 2 of the attack.

EXIF

EXE

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	2025:10:17 13:48:31+00:00
ImageFileCharacteristics:	Executable, 32-bit
PEType:	PE32
LinkerVersion:	14.27
CodeSize:	488960
InitializedDataSize:	192512
UninitializedDataSize:	-
EntryPoint:	0x37bfa
OSVersion:	6
ImageVersion:	-
SubsystemVersion:	6
Subsystem:	Windows command line

Figure 1. ANY RUN : EXIF.

3.4.2. Disruption of the defense

To circumvent antivirus solutions, Medusa launches numerous parent **net.exe** processes with the **/y** (force) parameter, resulting in a multitude of child **net1.exe** and **conhost.exe** processes generated to execute malicious commands. These commands allow to disable the following elements, including:

- Acronis VSS
- Sophos sercices (Message router, MCS Agent, MCS Client, File Scanner, Safestore, Clean Service...)
- Symantec System Recovery
- Services SQLsafe

Below is an example of parent (**net.exe**) and child (**net1.exe** and **conhost.exe**) processes observed in virtualisation:

```
net.exe (PID: 6920 cmdline: net stop "Acronis VSS Provider" /y MD5: 31890A7DE89936F922D44D677F681A7F)
conhost.exe (PID: 6888 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5:
0D698AF330FD17BEE3BF90011D49251D)
net1.exe (PID: 7100 cmdline: C:\Windows\system32\net1 stop "Acronis VSS Provider" /y MD5:
2EFE6ED4C294AB8A39EB59C80813FEC1)
```

```
net.exe (PID: 7028 cmdline: net stop "Enterprise Client Service" /y MD5: 31890A7DE89936F922D44D677F681A7F)
conhost.exe (PID: 7008 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5:
0D698AF330FD17BEE3BF90011D49251D)
net1.exe (PID: 5244 cmdline: C:\Windows\system32\net1 stop "Enterprise Client Service" /y MD5:
2EFE6ED4C294AB8A39EB59C80813FEC1)
```

```
net.exe (PID: 2592 cmdline: net stop "Sophos Agent" /y MD5: 31890A7DE89936F922D44D677F681A7F)
conhost.exe (PID: 5508 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5:
0D698AF330FD17BEE3BF90011D49251D)
net1.exe (PID: 4224 cmdline: C:\Windows\system32\net1 stop "Sophos Agent" /y MD5:
2EFE6ED4C294AB8A39EB59C80813FEC1)
```

```
net.exe (PID: 2124 cmdline: net stop "Sophos AutoUpdate Service" /y MD5: 31890A7DE89936F922D44D677F681A7F)
conhost.exe (PID: 6440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5:
0D698AF330FD17BEE3BF90011D49251D)
net1.exe (PID: 6956 cmdline: C:\Windows\system32\net1 stop "Sophos AutoUpdate Service" /y MD5:
2EFE6ED4C294AB8A39EB59C80813FEC1)
```

```
net.exe (PID: 7160 cmdline: net stop "Sophos Clean Service" /y MD5: 31890A7DE89936F922D44D677F681A7F)
conhost.exe (PID: 4992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5:
0D698AF330FD17BEE3BF90011D49251D)
net1.exe (PID: 1772 cmdline: C:\Windows\system32\net1 stop "Sophos Clean Service" /y MD5:
2EFE6ED4C294AB8A39EB59C80813FEC1)
```

```
net.exe (PID: 6624 cmdline: net stop "Sophos Device Control Service" /y MD5: 31890A7DE89936F922D44D677F681A7F)
conhost.exe (PID: 7012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5:
0D698AF330FD17BEE3BF90011D49251D)
net1.exe (PID: 3368 cmdline: C:\Windows\system32\net1 stop "Sophos Device Control Service" /y MD5:
2EFE6ED4C294AB8A39EB59C80813FEC1)
```

```
net.exe (PID: 2636 cmdline: net stop "Sophos File Scanner Service" /y MD5: 31890A7DE89936F922D44D677F681A7F)
conhost.exe (PID: 4652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5:
0D698AF330FD17BEE3BF90011D49251D)
net1.exe (PID: 2588 cmdline: C:\Windows\system32\net1 stop "Sophos File Scanner Service" /y MD5:
2EFE6ED4C294AB8A39EB59C8
```

The static analysis helps to identify "kill" functions:

```
                    s_kill_services_processes_004... XREF[...FUN_00413500:004...
...488008 6b 69        ds       "kill_services processes\n"
          6c 6c
          5f 73 ...
...488021 00           ??       00h
...488022 00           ??       00h
...488023 00           ??       00h

                    s_kill_services_%s_00488024   XREF[...FUN_00413500:004...
...488024 6b 69        ds       "kill_services %s\n"
          6c 6c
          5f 73 ...
...488036 00           ??       00h
...488037 00           ??       00h

                    s_kill_processes_%s_00488038 XREF[...FUN_00413500:004...
...488038 6b 69        ds       "kill_processes %s\n"
          6c 6c
          5f 70 ...
...48804b 00           ??       00h
```

Figure 2. GHIDRA: Code browsing.

Services and processes killed (non-exhaustive list)

Acronis VSS Provider	Enterprise Client Service	Sophos Agent
Sophos AutoUpdate Service	Sophos Clean Service	Sophos Device Control Service
Sophos File Scanner Service	Sophos Health Service	Sophos MCS Agent
Sophos MCS Client	Sophos Message Router	Sophos Safestore Service
Sophos System Protection Service	Sophos Web Control Service	SQLsafe Backup Service

During virtualisation, it was observed that Medusa does not appear to impact Windows Defender. Indeed, it is not stopped and functions correctly even after restarting the infected and encrypted system. Without an update to the antivirus database, Windows Defender does not appear to detect the sample on the system. The attackers seem to be paying particular attention to **Sophos**, **Symantec**, and **SQL** solutions.

3.4.3. Deleting backups

To prevent victims from using Shadow Copies backups, these are deleted by Medusa. The command used is as follows:

```
gaze.exe, 00000001.00000002.3719575753.000000000053E000.00000004.00000001.01000000.00000003.sdmp
vssadmin Delete Shadows /all /quietSQLAgent$ECWDB2macmnsvcY
```

The instruction is found in the code below:

```
                    s_delete_shadow_copies_0048...  XREF[...FUN_004137c0:0041...
...48804c 64 65     ds      "delete_shadow_copies\n"
          6c 65
          74 65 ...
...488062 00        ??      00h
...488063 00        ??      00h
```

Figure 3. GHIDRA: Code browsing.

3.4.4. Program database

The Program Database (PDB) is a file format (developed by Microsoft) used to store debugging information about a program. PDB files typically have a .pdb extension. An address was identified during code analysis using Ghidra, indicating an OPSEC ("Operations Security") error: the attackers worked on the sample in a folder named **Release**, itself located in **Medusa** on a storage space with the letter **G**:

```
G:\\Medusa\\Release\\gaze.pdb
```

```
0048983b    ?? 48h   H                                                    "HkJoTHG\\KHAVMA@HGI"
0048d640    ds "G:\\Medusa\\Release\\gaze.pdb" (DotNetPdbInfo.pdbpath)   "G:\\Medusa\\Release\\gaze.pdb"
0048d67c    ?? 2Eh   .                                                    ".text$di"
```

Figure 4. GHIDRA: Code browsing.

This information has also been identified and reported in open-source analyses, which indicate the use of these malicious samples by the APT Lazarus (North Korea):

```
rule Lazarus_Medusa_Gaze_Ransomware {
meta:
author = "Breakglass Intelligence"
date = "2026-03-09"
description = "Detects Lazarus-deployed Medusa ransomware (gaze.exe) via PDB path, XOR config, and BCrypt encryption imports"
hash = "15208030eda48b3786f7d85d756d2bd6596ef0f465d9c8509a8f02c53fad9a10"
tlp = "TLP:CLEAR"
severity = "CRITICAL"
reference = "https://intel.breakglass.tech"
strings:
$pdb = "G:\\Medusa\\Release\\gaze.pdb" ascii
```

Figure 5. LAZARUS DAY: The exact address is found.

3.4.5. Encryption

To perform its encryption task, Medusa uses the **BCryptEncrypt API**. This is a modern Windows cryptographic API called CNG (Cryptography Next Generation). It is provided by Microsoft in the **bcrypt.dll** system library and allows for data encryption. The attackers' choice of this function is not arbitrary: it is efficient, stable, and officially recognised, which consequently makes it less suspicious.

- The added extension is: .MEDUSA
- Other extensions observed (Medusa in general): .encrypted, .bomber, .boroff, .breakingbad, .locker16, .newlock, .nlocker, and .skynet.
- Combined use of **AES** et **RSA-2048**.

  Below, the image import descriptor table in the PE Medusa describes the functions imported from a specific target DLL. The DLL **bcrypt.dll** is identified in the code:

```
                        * IMAGE_IMPORT_BY_NAME      *
                        ********************************
...49250a 06 00         dw      6h
...49250c 42 43         ds      "BCryptCreateHash"
          72 79
          70 74 ...
...49251d 00            ??      00h
                        ********************************
                        * IMAGE_IMPORT_BY_NAME      *
                        ********************************
...49251e 1f 00         dw      1Fh
...492520 42 43         ds      "BCryptGenerateSymmetricKe...
          72 79
          70 74 ...
...49253b 00            ??      00h
                        ********************************
                        * IMAGE_IMPORT_DESCRIPTOR...  *
                        ********************************
...49253c 62 63         ds      "bcrypt.dll"
          72 79
          70 74 ...
...492547 00            ??      00h
                        ********************************
                        * IMAGE_IMPORT_BY_NAME      *
                        ********************************
...492548 85 00         dw      85h
...49254a 43 72         ds      "CryptDecodeObjectEx"
          79 70
          74 44 ...
                        ********************************
                        * IMAGE_IMPORT_BY_NAME      *
                        ********************************
...49255e e3 00         dw      E3h
...492560 43 72         ds      "CryptStringToBinaryA"
          79 70
          74 53 ...
```

Figure 6. GHIDRA: Code browsing.

3.5. Virtualisation / Sandboxing

3.5.1. JoeSandBox

- Virtualisation date: 26/02/2026 20H14
- Time before impact after detonation: approximately 120 seconds

In the screenshot below, the ransomware is deployed and executed. The files visible on the desktop will soon be encrypted.

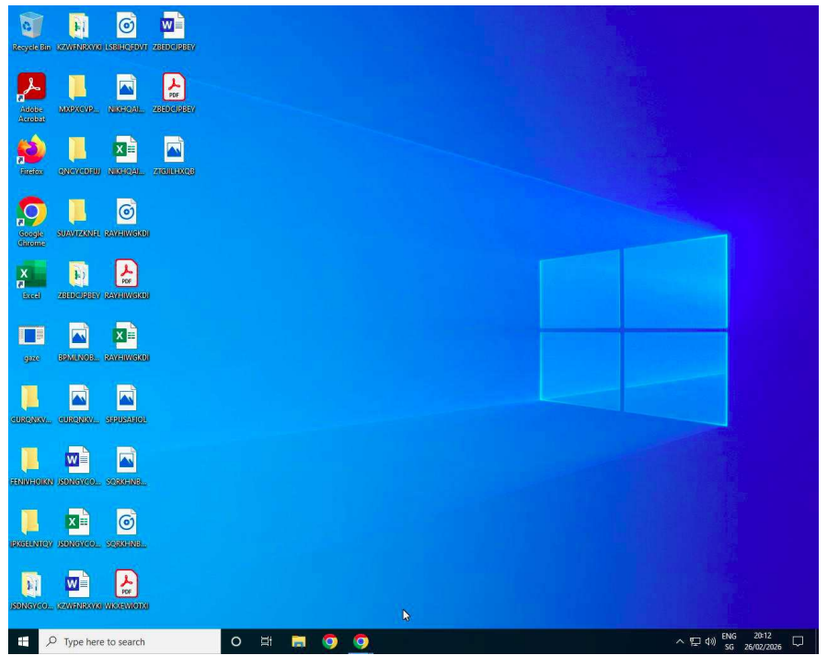


Figure 7. Joesandbox: before encryption.

In the screenshot below, the ransomware successfully completed its data encryption task.

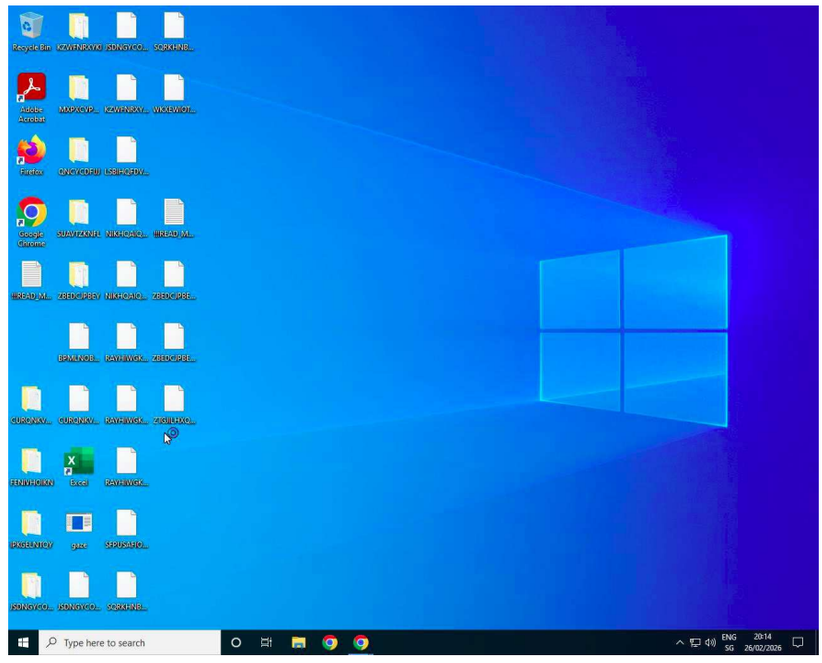


Figure 8. Joesandbox: after encryption.

3.5.2. aDvens - CTI analysis

- Virtualisation date: 11/05/2026 15H10
- Time before impact after detonation: approximately 60 secondes

In the screenshot below, the ransomware is deployed and executed. The files visible on the desktop will soon be encrypted.

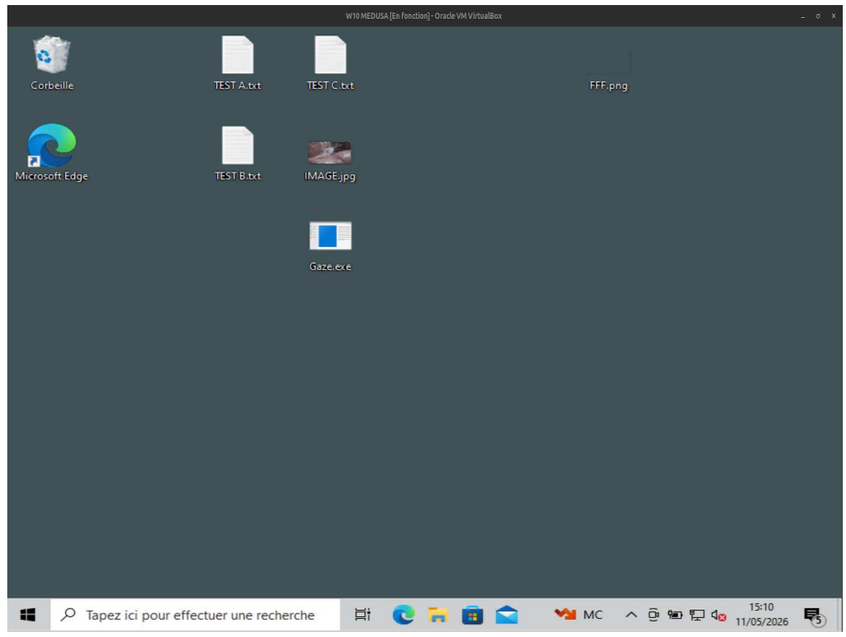


Figure 9. Virtualisation: before encryption.

Approximately 60 seconds after detonation, the first signs of encryption became visible. Some files now had the extension **.MEDUSA**. The background image changed. It is now completely black, seemingly containing neither text nor images.

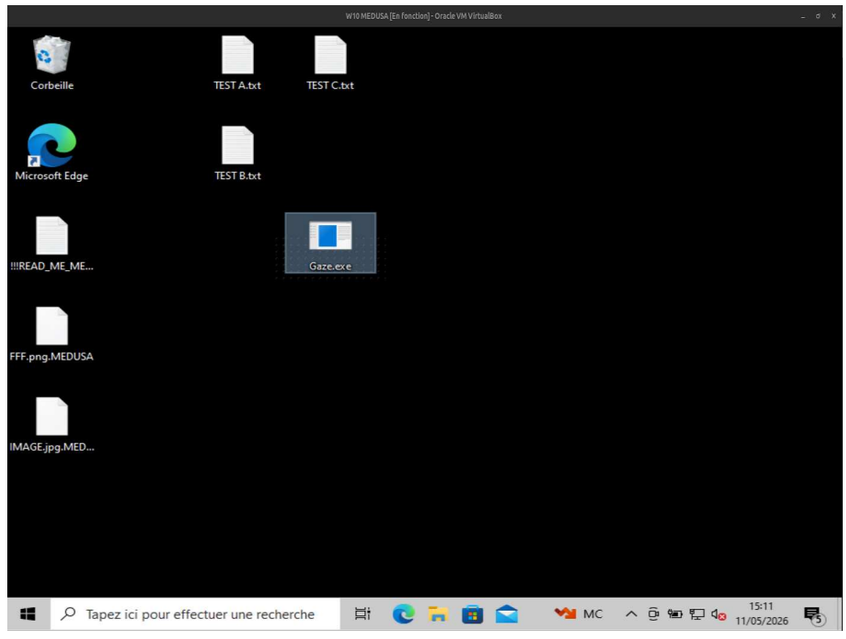


Figure 10. Virtualisation: after encryption.

A ransom note is now available on the desktop. Approximately two seconds after it appeared, the ransomware strain gaze.exe self-deleted and is no longer visible on the desktop. Below is the ransom note on the infected virtual machine (the name of the victim organisation has been removed for security reasons):

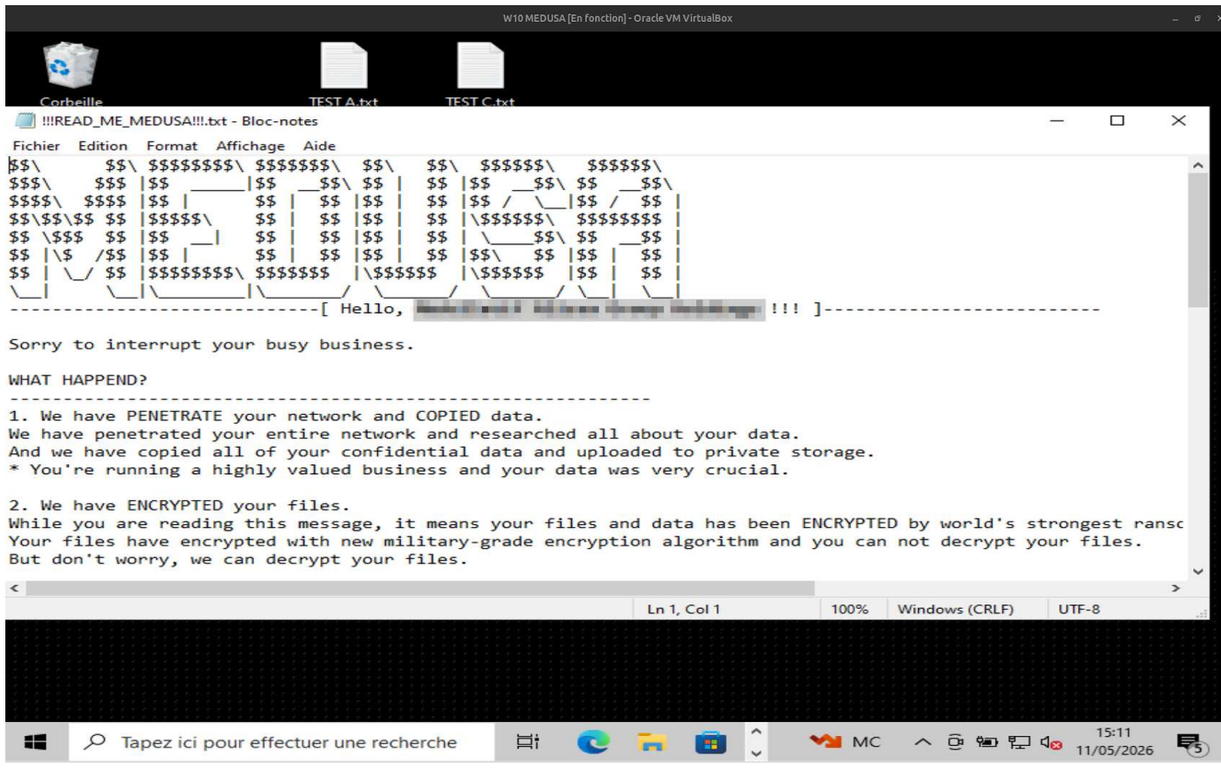


Figure 11. Virtualisation: after encryption.

In the task manager, it is possible to see that gaze.exe has configured the ransom note (!!!READ_ME_MEDUSA!!!.txt) to be read at system startup:

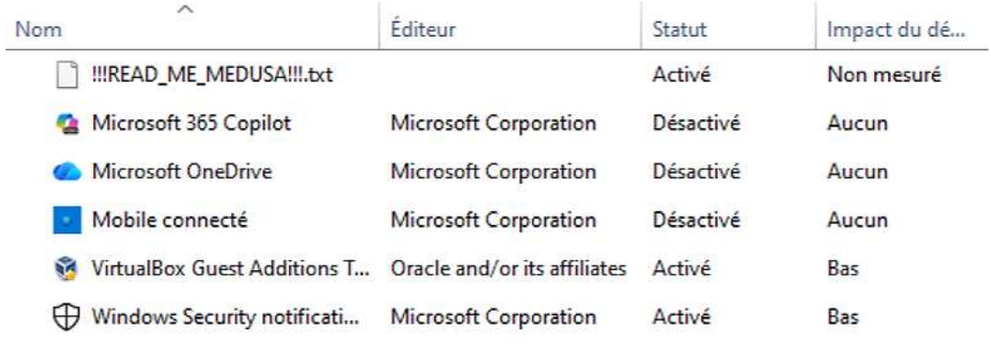


Figure 12. Virtualisation: after encryption.

3.5.3. Ransom note

Below is the ransom note retrieved during virtualisation.

```
$$\      $$\ $$$$$$$$\ $$$$$$$\  $$\   $$\  $$$$$$\   $$$$$$\
$$$\    $$$ |$$  _____|$$  __$$\ $$ |  $$ |$$  __$$\ $$  __$$\
$$$$\  $$$$ |$$ |      $$ |  $$ |$$ |  $$ |$$ /  \__|$$ /  $$ |
$$\$$\$$ $$ |$$$$$\    $$ |  $$ |$$ |  $$ |\$$$$$$\  $$$$$$$$ |
$$ \$$$  $$ |$$  __|   $$ |  $$ |$$ |  $$ | \____$$\ $$  __$$ |
$$ |\$  /$$ |$$ |      $$ |  $$ |$$ |  $$ |$$\   $$ |$$ |  $$ |
$$ | \_/ $$ |$$$$$$$$\ $$$$$$$  |\$$$$$$  |\$$$$$$  |$$ |  $$ |
\__|     \__|\________|\_______/  \______/  \______/ \__|  \__|
-----------------------------[ Hello, [REDACTED] !!! ]--------------------------
Sorry to interrupt your busy business.
```

```
WHAT HAPPEND?
-------------------------------------------------------------
1. We have PENETRATE your network and COPIED data.
We have penetrated your entire network and researched all about your data.
And we have copied all of your confidential data and uploaded to private storage.
* You're running a highly valued business and your data was very crucial.
2. We have ENCRYPTED your files.
While you are reading this message, it means your files and data has been ENCRYPTED by world's strongest
ransomware.
Your files have encrypted with new military-grade encryption algorithm and you can not decrypt your files.
But don't worry, we can decrypt your files.
There is only one possible way to get back your computers and servers, keep your privacy safe - CONTACT us via
LIVE CHAT and pay for the special
MEDUSA DECRYPTOR and DECRYPTION KEYs.
This MEDUSA DECRYPTOR will restore your entire network 24 hours.
```

```
WHAT GUARANTEES?
-------------------------------------------------------------
We can post all of your critical data to the public and send emails to your competitors.
We have professional OSINTs and media team for leak data to telegram, facebook, twitter channels and top news
websites. You can easily search about us.
You can suffer significant problems due to disastrous consequences, leading to loss of valuable intellectual
property and other sensitive information,
costly incident response efforts, information misuse/abuse, loss of customer trust, brand and reputational
damage, and legal and regulatory issues.
After paying for the data breach and decryption, we guarantee that your data will never be leaked and make
everything silent, this is also for our reputation.
```

```
YOU should be AWARE!
-------------------------------------------------------------
We will speak only with an authorized person. It can be the CEO, top management etc.
In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in serious harm to
your company!
Inform your supervisors and stay calm!
If you do not contact us within 48 hours, We will start publish your case to our official blog and everybody
will start notice your incident!
--------------------[ Official blog tor address ]--------------------
Using TOR Browser(hxxps[:]//www[:]torproject.org/download/):
hxxp[:]//xfv4jzckytb4g3ckwemcny3ihv4i5p4lqzdpi624cxisu35my5fwi5qd.onion/
hxxp[:]//7aqabivkwmpvjkyefonf3gpy5gsubopqni7kcirsrq3pflckxq5zz4id.onion/
hxxp[:]//s7lmmhlt3iwnwirxvgjidl6omcblvw2rg75txjfduy73kx5brlmiulad.onion/
```

```
CONTACT US!
----------------------[ Your company live chat address ]---------------------------
Using TOR Browser(hxxps[:]//www[:]torproject.org/download/):
hxxp[:]//uyku4o2yg34ekvjtszg6gu7cvjzm6hyszhtu7c55iyuzhpr4k5knewyd.onion/00b4f860f1798b62b3531f1b4e8bb6e0
--------------------[ Or Use Tox Chat Program(hxxps[:]//utox.org/uTox_win64.exe) ]--------------------
Add user with our tox ID : AEA72DFCF492037A6D15755A74645C7D8E674E342BACA9F9070A3FB74117EC3143FD6E29BEAC
Company identification hash:
830bf59642b7eed598d78b10277b32f8c31329bd7bb798fe57aed286f6ccd46b
```

Several interesting points are raised.

First, DLS (Dedicated Leak Site) addresses belonging to the Medusa group are identified. These are hardcoded and encrypted using XOR in the ransomware's source code. They are decrypted by the ransomware when the ransom note is generated.

- hxxp[:]//7aqabivkwmpvjkyefonf3gpy5gsubopqni7kcirsrq3pflckxq5zz4id.onion/
- hxxp[:]//xfv4jzckytb4g3ckwemcny3ihv4i5p4lqzdpi624cxisu35my5fwi5qd.onion/
- hxxp[:]//s7lmmhlt3iwnwirxvgjidl6omcblvw2rg75txjfduy73kx5brlmiulad.onion/

Secondly, the name of the targeted organisation (a group specialising in the textile and food trade) is written at the top of the ransom note. For security reasons, the name itself is not displayed. What makes this interesting is that the name is the same regardless of the environment in which the ransomware appears to be executed. The attackers seem to have customised the ransomware for a specific attack targeting only this organisation.

```
[ Hello, [REDACTED] !!! ]
```

An address is provided to confirm this information:

```
hxxp[:]//uyku4o2yg34ekvjtszg6gu7cvjzm6hyszhtu7c55iyuzhpr4k5knewyd.onion/00b4f860f1798b62b3531f1b4e8bb6e0
```

This is the address for negotiations; the segment **00b4f860f1798b62b3531f1b4e8bb6e0** corresponds to the victim. Since these elements are hard-coded and encrypted in the ransomware's source code, this last segment reveals that the attack was specific and predetermined. It is not an "identifier" generated on the fly during ransomware execution. **Virtualisation repeatedly detected the same segment**.

3.5.4. Reflections on cybercrime and cyberpsychology

3.5.5. Cybercriminology

From a cybercrime perspective, this ransomware operation resulting from an affiliation between a state unit and a non-state cybercriminal organisation presents several strategic and operational advantages for the attackers.

Concealment of activities

By operating within the traditional cybercrime ecosystem and blending into the large volume of attacks carried out by non-state criminal groups, the APT Lazarus benefits from a dilution effect. This proximity to "classic" cybercrime activities helps to obscure the attribution of operations and reduces the likelihood of quickly identifying the state actors involved.

Resource optimisation

By leveraging the already operational infrastructure of the Medusa franchise, including the ransomware itself, trading platforms and DLS sites, North Korean cyberwarriors can reduce development costs, save time and focus their resources on the intrusion and exploitation phases.

Access to specialised criminal networks

Affiliation with a RaaS franchise such as Medusa also allows Lazarus to benefit from established relationships with various players in the underground economy, particularly Initial Access Brokers (IABs). These intermediaries, specialising in compromising and reselling access, facilitate obtaining initial access to targeted environments, thereby increasing the operational efficiency of campaigns.

Diversification of illicit income

Beyond the massive and exceptional cryptocurrency theft operations traditionally associated with North Korean units, the use of RaaS franchises allows for increased illicit revenue streams through classic cyber extortion campaigns. This financial combination of exceptional and conventional activities offers attackers additional benefits.

Pooling of criminal skills

This type of collaboration also fosters an exchange of expertise between state actors and non-state cybercriminals. RaaS groups contribute their infrastructure and business models, while state-sponsored APTs contribute their advanced expertise in intrusion, persistence, and defensive evasion, thereby enhancing the overall sophistication of operations.

3.5.6. Cyberpsychology

From a cyberpsychological perspective, this ransomware operation resulting from an affiliation between a state unit and a non-state cybercriminal organisation presents several advantages in terms of **cognitive resistance**, more specifically: **psychological counter-countermeasures (PCCM)**.

Psychological disempowerment and dilution of identity

By operating through a RaaS franchise already active in "traditional" cybercrime, cyebrwarriors of APT Lazarus can benefit from a phenomenon of identity dilution. This dissociation fosters a reduction in the feeling of individual responsibility, a better rationalisation of actions, and a decrease in the psychological pressure linked to the risk of geopolitical attribution.

Normalisation of criminal behavior

Integration, to varying degrees, into the RaaS ecosystem also allows for a form of social normalisation of cybercrime. RaaS platforms function as veritable criminal communities with their own codes, services, reputations, and cooperation mechanisms. For state actors, operating within this environment can contribute to trivialising certain criminal practices by presenting them as "ordinary" economic activities within contemporary cybercrime.

Reduction of operational cognitive load

The RaaS model outsources a significant portion of the technical and logistical tasks: leak infrastructure, negotiation, payment management, and ransomware maintenance. Psychologically, this reduces the mental workload and allows the cyberwarriors of Lazarus to focus their attention on specific tasks (intrusion, lateral movement, etc.). This specialisation potentially improves the attackers' cognitive performance by reducing the dispersion of their efforts.

Increased sense of impunity

Using an existing criminal franchise creates a psychological camouflage effect. Attackers know that attribution is more complex, investigators may focus on traditional cybercrime, and state responsibility may remain ambiguous. This context can thus reinforce feelings of impunity, risk-taking, and operational audacity. In criminal science, this mechanism is similar to the theory of criminal opportunity: the lower the perceived risk, the easier it is to commit a crime.

3.6. Conclusion

The cyberattack carried out by the APT Lazarus, acting as an affiliate of the Medusa franchise, against an organisation specialising in the trade of textiles and food products raises several major points of attention.

First, this operation concretely illustrates the high level of sophistication that ransomware attacks can reach when they benefit from the expertise and operational capabilities of state-sponsored cybercrime. This sophistication is manifested in particular by an attack chain adapted to the targeted environment, as well as by the application of consistent, discreet, and perfectly controlled tactics, techniques, and procedures (TTPs).

Secondly, this intelligence confirms that North Korean units are continuing their offensive activities well beyond the Korean Peninsula and that all sectors of activity, including those traditionally perceived as less strategic such as textiles, can represent a source of economic or operational interest for these actors.

Third, unlike many non-state cybercriminal groups, which generally prioritise rapid operations to maximise profits, Lazarus cyberwarriors continue to employ a "slow burning espionage" strategy, characterised by a prolonged and discreet presence within compromised environments before the impact phase is triggered. This operational patience is a significant advantage, as it allows attackers to thoroughly study the targeted infrastructure, identify critical assets, and adapt their actions accordingly. This observation underscores the importance of continuous, detailed, and proactive monitoring of systems and networks to detect both rapid intrusions and long-term, latent compromises.

Finally, the observed evidence shows that the Lazarus unit applies a level of precision to its ransomware campaigns comparable to that of its cyberespionage operations. This convergence between criminal logic and state capabilities contributes to increasing the danger of this type of attack.

Ultimately, this operation demonstrates that no organisation, regardless of its geographic location or sector of activity, can be considered beyond the reach of the APT Lazarus. Furthermore, it is likely that the phenomena of affiliation and cooperation between state and non-state cybercriminal actors will continue to develop, given the financial, strategic, and operational benefits generated by these malicious activities.

3.7. Diamond Model

APT Lazarus (aka Plutonium, Dark Seoul, Whois Team, Guardians of Peace...) is an advanced and persistent threat of North Korean origin.

3.8. Matrixes

3.8.1. Mitre ATT&CK

REFERENCES	TACTICS	TECHNIQUES
T1059	Execution	Command and Scripting Interpreter
T1106	Execution	Native API
T1129	Execution	Shared Modules
T1569.002	Execution	System Services - Service Execution
T1543.003	Persistence	Create or Modify System Process - Windows Service
T1543	Privilege Escalation	Create or Modify System Process
T1027.005	Stealth	Obfuscated files or information - Indicator Removal from Tools
T1027.009	Stealth	Obfuscated files or information - Embedded Payloads
T1107	Stealth	File Deletion
T1140	Stealth	Deobfuscate/Decode Files or Information
T1202	Stealth	Indirect Command Execution
T1497.001	Stealth	Virtualization/Sandbox Evasion - System Checks
T562	Stealth	Impair Defenses
T564	Stealth	Hide Artifacts
T1012	Discovery	Query Registry
T1063	Discovery	Security Software Discovery
T1082	Discovery	Security Information Discovery
T1497.001	Discovery	Virtualization/Sandbox Evasion - System Checks
T1518	Discovery	Software Discovery
T1614	Discovery	System Location Discovery
T1560	Collection	Archive Collected Data
T1071	Command and Control	Application Layer Protocol
T1105	Command and Control	Ingress Tool Transfer
T1592	Reconnaissance	Gather Victim Host Information
T1222	Defense Impairment	File and Directory Permissions Modification
T1486	Impact	Data Encrypted for Impact
T1491.001	Impact	Defacement: Internal Defacement
T1490	Impact	Inhibit System Recovery
T1489	Impact	Service Stop

3.8.2. Psychology / Cyberpsychology

Two concepts are used; they are essential for a proper understanding of the psychological dimension.

- **PCM: Psychological Countermeasure**, this refers to the set of manipulation tactics and techniques used **in an offensive logic** in order to impose a superiority of mind ("*mind superiority*") over a target.

- **PCCM: Psychological Counter-Countermeasure**, the set of cognitive resistance mechanisms mobilised **in a defensive logic** to limit the impact of opposing PCMs and preserve one's capacity for reasoning, judgment and decision-making in the face of an attempt at destabilisation or psychological domination.

3.8.3. DECEPTION Matrix

The table below lists the tactics and techniques of **psychological countermeasures (PCM)** used for manipulation by attackers. These PCMs are derived from the **DECEPTION model 5.0**.

REFERENCES	TACTICS	TECHNIQUES
T2.11.4	Resource	Resource for manipulation: Text
T6.09	Impact	Restricted choice
T6.08	Impact	Intimidation and threats
T6.14	Impact	Emergency effect
T7.17	Evasion	Confusion
T7.36	Evasion	Concealment

3.8.4. Cognitive resistance

The table below lists the cognitive resistance efforts of attackers. These are the **psychological counter-countermeasures (PCCM)** used by attackers to maintain effectiveness, resilience, and psychological defense in the face of adversity.

COGNITIVE RESISTANCE	DESCRIPTION
Dilution of identity	Identity dissociation allows for a reduction in the feeling of individual responsibility.
Normalisation of behavior	The activities are part of a collective dynamic perceived as ordinary, which helps to legitimise and reassure the actions taken.
Cognitive unloading	The efforts undertaken build upon a set of actions already carried out, thereby reducing the mental load and freeing up attention for other tasks..
Psychological camouflage	The complex nature of the cooperation makes attributing responsibility more difficult. The responsible entity is not necessarily the one that is first exposed.
Increased sense of impunity	Certain configurations (geographical distance, state protection, technological advantage, etc.) reinforce the feeling of impunity by limiting perceived risks, which in particular reduces the fear of consequences.
Shared motivation	In addition to contributing collectively to the entity's activity, a portion of the benefits is allocated individually, thereby reinforcing the motivation to act through an operant conditioning mechanism (Skinner: reinforcement by positive reward).

3.8.5. Indicators of Compromise (IoC)

3.8.6. IOC - aDvens Analysis

Below are the indicators from the analysis:

TLP	TYPE	VALUE	DESCRIPTION
TLP:CLEAR	MD5	60aaafce354ae5e0b8115729464a8b24	Gaze.exe
TLP:CLEAR	SHA1	53948d9596ebab5c4cf2ac04e7fb70c429e0cbbf	Gaze.exe
TLP:CLEAR	SHA256	15208030eda48b3786f7d85d756d2bd6596ef0f465d9c8509a8f02c53fad9a10	Gaze.exe
TLP:CLEAR	MD5	66bc4a9fb7303b213c94e6e46dc71422	!!!READ_ME_MEDUSA!!!.txt
TLP:CLEAR	SHA1	9cc0da7aacb04a8df6409381ad8596ed3ecf17d7	!!!READ_ME_MEDUSA!!!.txt
TLP:CLEAR	SHA256	1e835185378a988cc9dbb3ac30c2da79b068f6723602cbc37b9975fe7da1722c	!!!READ_ME_MEDUSA!!!.txt
TLP:CLEAR	URL	hxxp[:]//xfv4jzckytb4g3ckwemcny3ihv4i5p4lqzdpi624cxisu35my5fwi5qd.onion	MEDUSA - DLS
TLP:CLEAR	URL	hxxp[:]//7aqabivkwmpvjkyefonf3gpy5gsubopqni7kcirsrq3pflckxq5zz4id.onion	MEDUSA - DLS
TLP:CLEAR	URL	hxxp[:]//s7lmmhlt3iwnwirxvgjidl6omcblvw2rg75txjfduy73kx5brlmiulad.onion	MEDUSA - DLS

3.8.7. YARA

YARA aDvens

```
rule MEDUSA_detection {
meta:
author = "ADVENS"
source = "ADVENS"
status = "RELEASED"
sharing = "TLP:CLEAR"
malware = "MEDUSA-gaze"
description = "Yara_rule_that_detects_MEDUSA-gaze-Lazarus-ransomware."
info = "MEDUSA-Ransomware"
Sample_SHA256 = "15208030eda48b3786f7d85d756d2bd6596ef0f465d9c8509a8f02c53fad9a10"
Sample_SHA1 = "53948d9596ebab5c4cf2ac04e7fb70c429e0cbbf"
Sample_MD5 = "60aaafce354ae5e0b8115729464a8b24"
//HEXA
strings:
$MEDUSA_HEXA1 = {7d 08 33 db 89 5d f0 85}
$MEDUSA_HEXA2 = {73 01 43 8b cf c6 45 db}
$MEDUSA_HEXA3 = {00 00 00 00 59 5f 5e 5b}
$MEDUSA_HEXA4 = {ff 55 8b ec 83 ec 10 ff}
$MEDUSA_HEXA5 = {08 6a 00 51 51 dd 1c 24}
$MEDUSA_HEXA6 = {16 eb 58 85 db 75 c5 e8}
$MEDUSA_HEXA7 = {f8 33 ff 50 0f b7 c2 25}
$MEDUSA_HEXA8 = {03 d1 72 0e 3b 54 24 0c}
$MEDUSA_HEXA9 = {3b d3 72 e8 33 c0 5f 5e}
//STRINGS
$MEDUSA_string1 = "CRYPT32.dll"
$MEDUSA_string2 = "kill_processes"
$MEDUSA_string3 = "TerminateProcess"
$MEDUSA_string4 = "encrypt"
$MEDUSA_string5 = "powershell"
$MEDUSA_string6 = "bcrypt.dll"
$MEDUSA_string7 = "Medusa"
$MEDUSA_string8 = "gaze"
condition:
filesize > 600KB and filesize < 650KB and all of ($MEDUSA_HEXA*) and all of ($MEDUSA_string*)
}
```

YARA rules available in open sources

Source : Breakglass

```
rule Lazarus_Medusa_gaze_Ransomware {
meta:
       author = "Breakglass Intelligence"
       date = "2026-03-09"
       description = "Detects Lazarus-deployed Medusa ransomware (gaze.exe) via PDB path, XOR config, and
BCrypt encryption imports"
       hash = "15208030eda48b3786f7d85d756d2bd6596ef0f465d9c8509a8f02c53fad9a10"
       tlp = "TLP:CLEAR"
       severity = "CRITICAL"
       reference = "https://intel.breakglass.tech"
strings:
       $pdb = "G:\\Medusa\\Release\\gaze.pdb" ascii
       $ransom_note = "!!!READ_ME_MEDUSA" ascii wide
       $shadow1 = "vssadmin Delete Shadows" ascii wide nocase
       $shadow2 = "vssadmin resize shadowstorage" ascii wide nocase
       $bcrypt1 = "BCryptImportKeyPair" ascii
       $bcrypt2 = "BCryptGenerateSymmetricKey" ascii
       $bcrypt3 = "BCryptEncrypt" ascii
       $svc1 = "Sophos" ascii wide
       $svc2 = "Veeam" ascii wide
       $svc3 = "McAfee" ascii wide
       $svc4 = "BackupExec" ascii wide
condition:
       uint16(0) == 0x5A4D and
       ($pdb or $ransom_note) and
       1 of ($shadow*) and
       2 of ($bcrypt*) and
       2 of ($svc*)
}
```

```
rule Lazarus_TSMSISrv_IME_Loader {
meta:
       author = "Breakglass Intelligence"
       date = "2026-03-09"
       description = "Detects Lazarus IME SDK-based DLL sideloading loader via IME version strings, expected
exports, and RTTI class names"
       hash = "aeebcd8c8b15645d7e71b68ac05e21e9a4c94f832c64044725d870b87b9573c7"
       tlp = "TLP:CLEAR"
       severity = "HIGH"
       reference = "https://intel.breakglass.tech"
strings:
       $ime1 = "SampleIME" ascii wide
       $ime2 = "The Sample code of Windows 8 IME" ascii wide
       $ime3 = "SampleIM.dll" ascii wide
       $exp1 = "OnSessionChange" ascii
       $exp2 = "StartComponent" ascii
       $exp3 = "StopComponent" ascii
       $exp4 = "DllRegisterServer" ascii
       $rtti1 = "CSampleIME" ascii
       $rtti2 = "CCompositionProcessorEngine" ascii
       $msft = "MSFT" ascii wide
condition:
       uint16(0) == 0x5A4D and
       uint16(0x18) != 0x0040 and  // Not a .NET assembly
       2 of ($ime*) and
       3 of ($exp*) and
       1 of ($rtti*) and
       filesize > 500KB and filesize < 2MB
}
```

```
rule Lazarus_Medusa_Campaign_XOR_Config {
meta:
       author = "Breakglass Intelligence"
       date = "2026-03-09"
       description = "Detects XOR-encoded Medusa configuration block with known Tor onion patterns and campaign
identifiers"
       tlp = "TLP:CLEAR"
       severity = "HIGH"
       reference = "https://intel.breakglass.tech"
strings:
       $onion1_xor = { 56 42 5A 4E 66 4A 44 5B }  // "xfv4jzck" XOR 0x2E
       $tox_marker = "AEA72DFCF492037A6D15755A74645C7D" ascii
       $victim_id = "00b4f860f1798b62b3531f1b4e8bb6e0" ascii
condition:
       uint16(0) == 0x5A4D and
       any of them
}
```

4. SOURCES

Vulnerabilities

- https://www.cve.org/CVERecord?id=CVE-2026-20223
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csw-pnbsa-g8WEnuy

- https://www.cve.org/CVERecord?id=CVE-2026-44277
- https://fortiguard.fortinet.com/psirt/FG-IR-26-128

- https://www.cve.org/CVERecord?id=CVE-2026-34260
- https://me.sap.com/notes/3724838
- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2026.html

Cyber-virology: Analysis of a sample of the MEDUSA ransomware

- ANY RUN. (2026). *Gaze.exe Analysis*. https://app.any.run/tasks/4c242e38-5c5b-468b-951f-3ad42a724b9f/

- Bleeping Computer. (2026). *North Korean Lazarus group linked to Medusa ransomware attacks*. https://www.bleepingcomputer.com/news/security/north-korean-lazarus-group-linked-to-medusa-ransomware-attacks/

- Breakglass. (2026). *When Nation-States Become Ransomware Affiliates: Lazarus Group Deploys Medusa via a Custom IME-Based Loader*. https://intel.breakglass.tech/post/when-nation-states-become-ransomware-affiliates-lazarus-group-deploys-medusa-via-a-custom-ime-based-loader#what-we-found

- CheckPoint. (2025). *Medusa Ransomware Group: A Rising Threat in 2025*. https://www.checkpoint.com/fr/cyber-hub/threat-prevention/ransomware/medusa-ransomware-group/

- Cyber Fortress. (2026). *Gaze.exe Analysis*. https://cyber-fortress.com/docs/result/index.php?id=69a092a4c950ab5d9ab1e49f

- DarkTrace. (2026). *Under Medusa's Gaze: How Darktrace Uncovers RMM Abuse in Ransomware Campaigns*. https://www.darktrace.com/fr/blog/under-medusas-gaze-how-darktrace-uncovers-rmm-abuse-in-ransomware-campaigns

- DOJ. (2018). *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- FBI. (2025). *StopRansomware: Medusa Ransomware*. https://www.fbi.gov/file-repository/cyber-alerts/stopransomware-medusa-ransomware-031225.pdf/view

- Fire Eye. (2018). *APT 38 Un-usual Suspect*. https://services.google.com/fh/files/misc/apt38-un-usual-suspects.pdf

- GTR - Global Trade Review (2018). *North Korea APT 38 the biggest cyber threat to global trade finance*. https://www.gtreview.com/news/asia/north-koreas-apt38-the-biggest-cyber-threat-to-global-trade-finance/

- Hunt&Hackett. (2026). *Threat Actor Profile LAZARUS*. https://www.huntandhackett.com/threats/actors/apt38

- Hybrid Analysis. (2026). *Gaze.exe Analysis*.
https://hybrid-analysis.com/sample/15208030eda48b3786f7d85d756d2bd6596ef0f465d9c8509a8f02c53fad9a10

- JoeSandbox. (2026). *Windows Analysis Report: gaze.exe*.
https://www.joesandbox.com/analysis/1875550/0/html

- Kaspersky. (2022). *Les attaques du groupe Andariel : DTrack et Maui*.
https://www.kaspersky.fr/blog/andariel-dtrack-maui/19280/

- Lazarus Day. (2026). *When Nation-States Become Ransomware Affiliates: Lazarus Group Deploys Medusa via a Custom IME-Based Loader*.
https://lazarus.day/reports/post/when-nation-states-become-ransomware-affiliates-lazarus-group-deploys-medusa-via-a-custom-ime-based-loader-TyM01

- LeMagIT. (2026). *Quand un acteur malveillant persistant se met au ransomware*.
https://www.lemagit.fr/actualites/366639324/Quand-acteur-malveillant-persistant-se-met-au-ransomware

- Malpedia. (2026). *LAZARUS Group*.
https://malpedia.caad.fkie.fraunhofer.de/actor/lazarus_group

- MalwareBazaar Database. (2026). Sample: *Gaze.exe*.
https://bazaar.abuse.ch/sample/15208030eda48b3786f7d85d756d2bd6596ef0f465d9c8509a8f02c53fad9a10/

- Medium. (2024). *[CyberThreat] APT — Lazarus Group overview*.
https://medium.com/@tribal.secberet/cyberthreat-apt-lazarus-group-overview-da4e898f1244

- Microsoft. (2026). *BCryptEncrypt function (bcrypt.h)*.
https://learn.microsoft.com/en-us/windows/win32/api/bcrypt/nf-bcrypt-bcryptencrypt

- MITRE. (2026). *MEDUSA Group*.
https://attack.mitre.org/groups/G1051/

Cyberpsychology

- DECEPTION Model. Psychological countermeasures (PCM).
https://deceptionmodel.sitew.fr/