

DeadLock Ransomware Group Embeds Data Leak Site Within Ransom Note

 watchguard.com/wgrd-security-hub/secplicity-blog/deadlock-ransomware-group-embeds-data-leak-site-within-ransom

By Ryan Estes

June 8, 2026

DeadLock Wallpaper

The DeadLock ransomware operation has existed since mid-2025, with most of the first reported sightings in mid-July, according to [ThreatScene](#). Their report mentioned the group “now conducts double extortion” following a [subsequent analysis](#) in September 2025, which revealed newer DeadLock payloads dropped a ransom note with an integrated web chat interface. However, almost a year later, there has been no further research on this group’s double extortion efforts. The reason for this is now clear: the newer payloads revealed the group has been embedding the data leak site into the HTML ransom note!

A recent analysis by the WatchGuard Attestation Team examined a version of DeadLock compiled at the beginning of June 2026. The analysis mimicked much of what [Cisco Talos](#), [Group-IB](#), and ThreatScene have already reported about this ransomware. These three reports covered almost every aspect of the early iterations of DeadLock, including how they embedded proxy addresses in Polygon smart contracts and how the authors used a custom stream cipher algorithm to encrypt files. What the early versions of DeadLock and these reports don’t contain is this newer ransom note.

Group-IB showed how early iterations of the ransom evolved over time, foreshadowing how this group would become a double extortion group. The first analyzed ransom note from a June 27, 2025, sample never mentioned data exfiltration, only encryption:

```
All your important files are encrypted
Your important files have been encrypted by DeadLock using military-grade encryption.
This includes all documents, photos, videos, databases, and other critical data.
You cannot access them without our decryption key.
There is only one way to get your files back:
1. Download Session to contact us https://getsession.org/
2. Contact with us (session id: 05084f9b14b02f4ffa97795a60ab1fafaf5128e3259c75459aaaaeabc80c14da78)
3. Send us 1 any encrypted your file and your personal key
4. We will decrypt 1 file for test (maximum file size - 1 MB), its guarantee what we can decrypt y
5. Pay
6. We send for you decryptor software
We accept Bitcoin/Monero
Attention
Do not rename encrypted files.
Do not try to decrypt using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their
Contact information: 05084f9b14b02f4ffa97795a60ab1fafaf5128e3259c75459aaaaeabc80c14da78
Your personal id: READ ME.F8C6A8.txt
```

Click on the image to expand

The second ransom note from July 17, 2025, added that data was also stolen in addition to being encrypted:

```
All your important files are encrypted and STOLEN
Your important files have been encrypted by DeadLock using military-grade encryption.
This includes all documents, photos, videos, databases, and other critical data.
You cannot access them without our decryption key.
There is only one way to get your files back:
1. Download Session to contact us https://getsession.org/
2. Contact with us (session id: 05084f9b14b02f4ffa97795a60ab1fafaf5128e3259c75459aaaeabc80c14da78)
3. Send us 1 any encrypted your file and your personal key
4. We will decrypt 1 file for test (maximum file size - 1 MB), its guarantee what we can decrypt )
5. Pay
6. We send for you decryptor software
We accept Bitcoin/Monero
Attention
Do not rename encrypted files.
Do not try to decrypt using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their
Contact information: 05084f9b14b02f4ffa97795a60ab1fafaf5128e3259c75459aaaeabc80c14da78
Your personal id: {_UID}
```

Click on the image to expand

A third subsequent ransom note from an August 12, 2025, sample mentioned including security reports on how they got in, an increasing trend among ransomware groups. Although this statement is used as a cover to lend legitimacy, most don't use it.

```
Your personal ID: {_UID}
Your company's network is attacked and the entire system is encrypted.
We have downloaded all the company's confidential data.
If you want your data fully decrypted and the files we stole removed from our source, you will have
We will also be able to provide a security report and explain how we did it to get in.

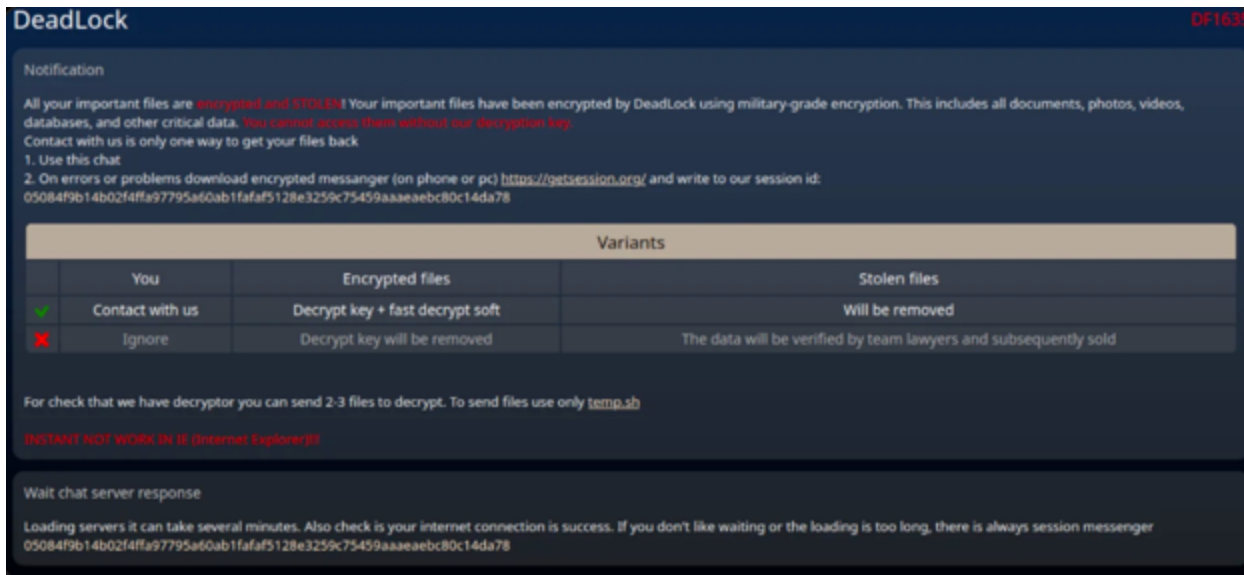
There is only one way to get your files back:
1. Contact us, open RECOVERY_CHAT.{_UID}.HTML via your browser or download Session messenger https://getsession.org/
2. Our contacts (Session id: 05084f9b14b02f4ffa97795a60ab1fafaf5128e3259c75459aaaeabc80c14da78)
3. Send us 2-3 any encrypted your files and your personal ID
4. We will decrypt few file for test (maximum file size - 5 MB), its guarantee what we can decrypt
5. Pay
6. We send for you decryptor software

After payment you will receive.
1. Decryption tool for all devices
2. Complete list of files taken from the network.
3. Proof that all your data has been deleted.
4. Information about how we got into the network.
5. Security recommendations to stop future attacks.
6. Promise that we will not attack you again in the future.
7. Guarantee that we will forget about this incident.

We accept Bitcoin/Monero
Attention
Do not rename encrypted files.
Do not try to decrypt using third party software, it may cause permanent data loss.
Contact information: 05084f9b14b02f4ffa97795a60ab1fafaf5128e3259c75459aaaeabc80c14da78
```

Click on the image to expand

The third ransom note also had the first iteration of an included HTML ransom note, which has also evolved.

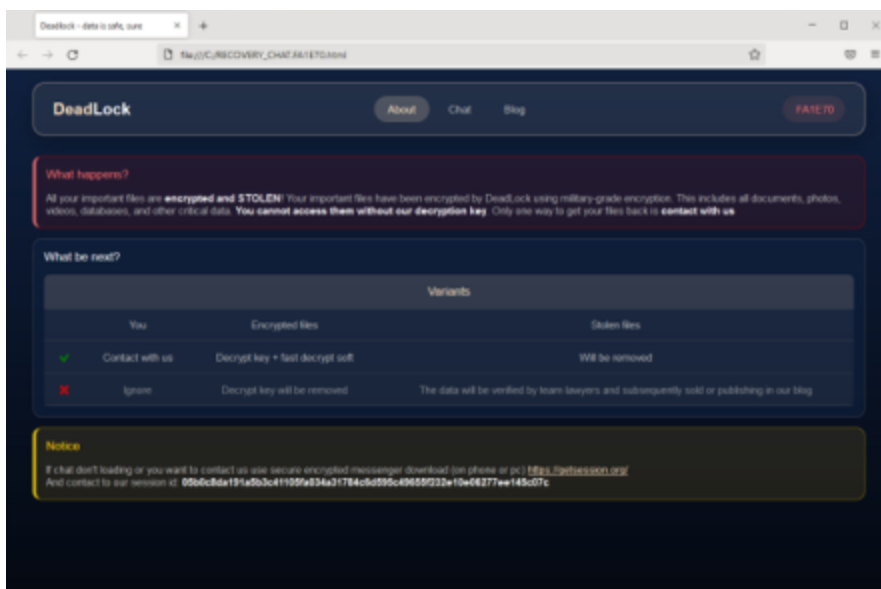


Click on the image to expand

That leads us to the current sample (SHA256:

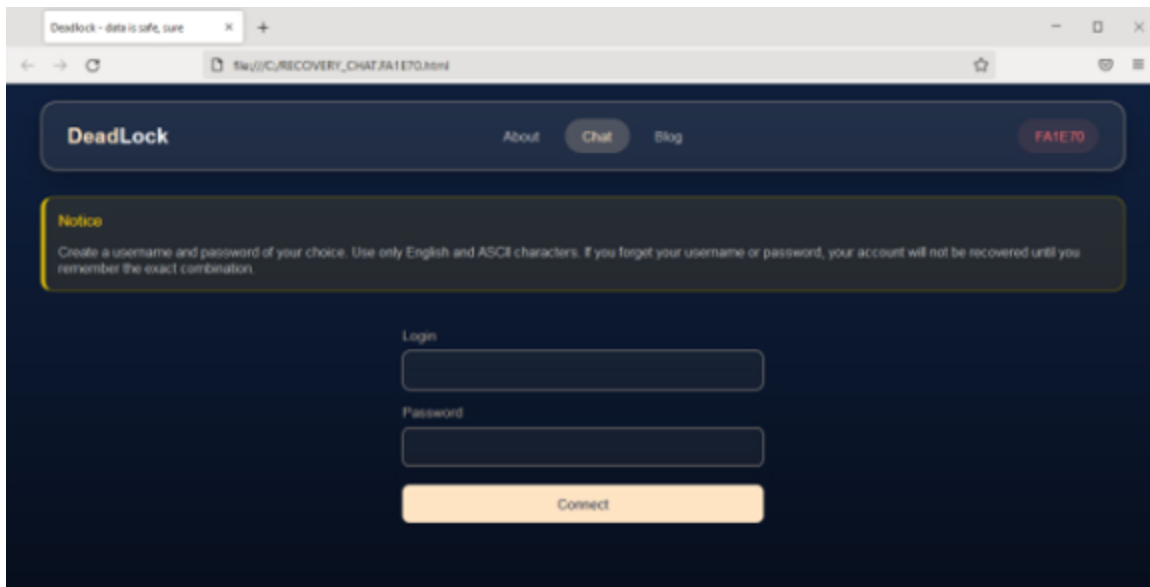
9e69862c4a5b34c12c10fbf2d345e7fd654c71adcb5f9b6524d7a54209fce343). Most behaviors matched the older samples, but the HTML ransom note differed from earlier iterations. It includes three tabs.

1. **About:** Like the original HTML ransom note from Group-IB's third sample.



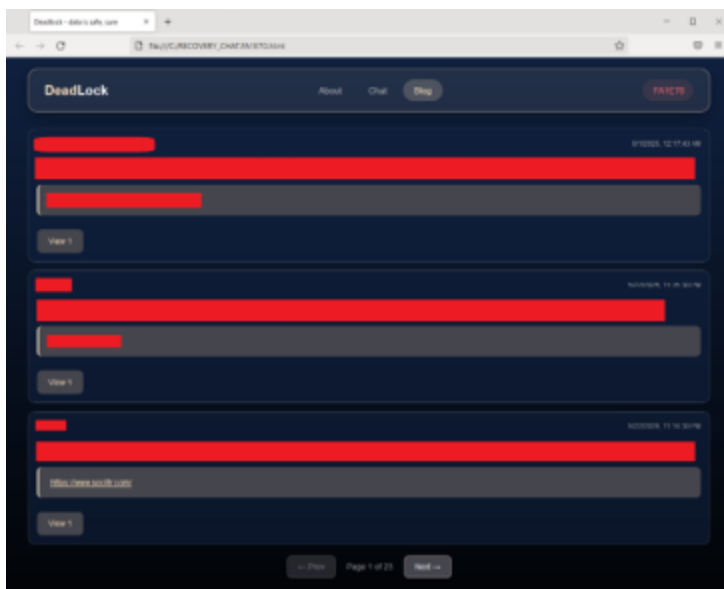
Click on the image to expand

2. **Chat:** Integrated web chat with authentication



Click on the image to expand

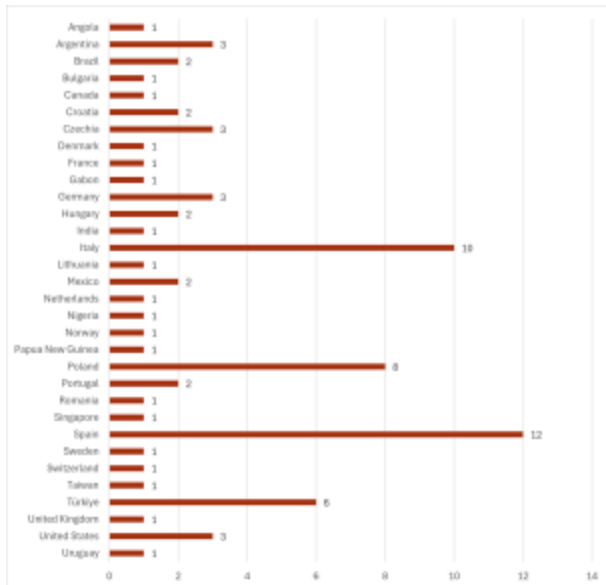
3. **Blog**: Duplicate of their current data leak site.



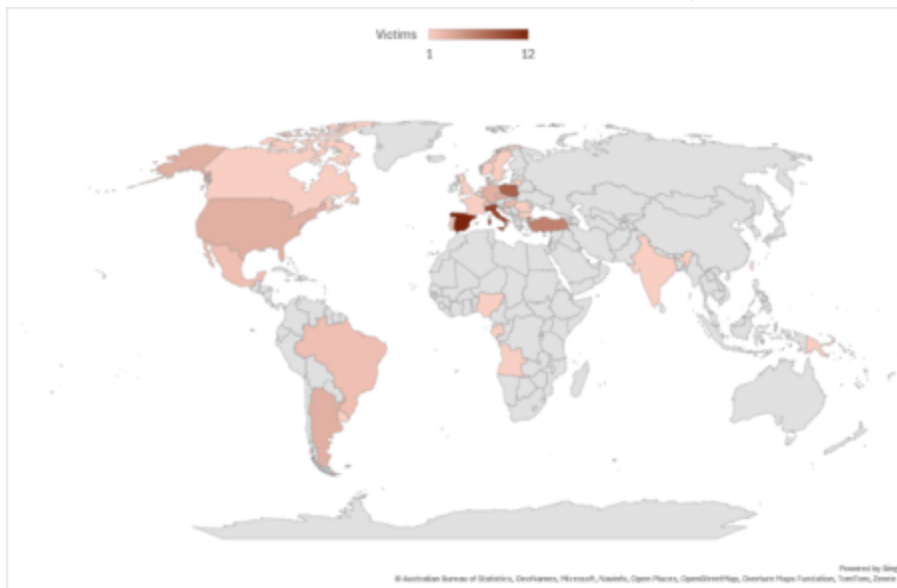
Click on the image to expand

The current data leak site has 23 pages, and many entries contain multiple organizations. We've compiled a list of all published organizations to see whether this group targets specific sectors or countries. This is also documented on the Ransomware Tracker entry: [DeadLock](#)

Most of the published victims were in Europe, specifically Spain, Italy, Poland, and Türkiye.

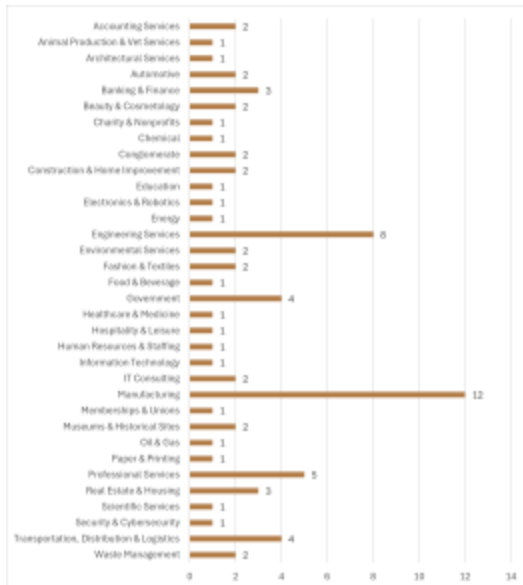


Click on the image to expand



Click on the image to expand

There is a wide variety of industries, but most victims were Engineering Services and Manufacturing organizations.



Click on the image to expand

Some of the notable inclusions on DeadLock's alleged victim list include:

- Large conglomerate in Angola
- Finance institution in Gabon
- Government agency in Papua New Guinea
- Large electronics manufacturer in Taiwan
- International veterinary pharmaceutical company

At the very end of execution, the sample drops the traditional TXT ransom note, but this version includes a link to their actual data leak site, which is on Clearnet, not the dark web.

```

HOW_RECOVER_FA1E70.txt - Notepad
File Edit Format View Help
# Your personal ID: FA1E70

# Your company's network is attacked and the entire system is encrypted.
# We have downloaded all the company's confidential data.
# If you want your data fully decrypted and the files we stole removed from our source, you will have to pay a fee.
# We will also be able to provide a security report and explain how we did it to get in.
# Our blog: https://deadlock.liveblog365.com/

# There is only one way to get your files back:
1. Contact us, open RECOVERY_ONAT.FA1E70.HTML via your browser or download Session messenger https://getsession.org/
2. Our contacts (Session id: 05b0c8da191a5b3c41105fa034a31784c6d595c49655f232e10e06277ee145c87c)
3. Send us 2-3 any encrypted your files and your personal ID FA1E70
4. We will decrypt few file for test (maximum file size - 5 MB), its guarantee what we can decrypt your files
5. Pay
6. We send for you decryptor software

# After payment you will receive.
1. Decryption tool for all devices
2. Complete list of files taken from the network.
3. Proof that all your data has been deleted.
4. Information about how we got into the network.
5. Security recommendations to stop future attacks.
6. Promise that we will not attack you again in the future.
7. Guarantee that we will forget about this incident.

# We accept Bitcoin/Monero
# Attention!
Do not rename encrypted files.
Do not try to decrypt using third party software, it may cause permanent data loss.
Contact information: 05b0c8da191a5b3c41105fa034a31784c6d595c49655f232e10e06277ee145c87c

```

Click on the image to expand

The first victim on their blog was on February 11, 2026. So, any sample on or after this date is assumed to have this embedded data leak site ransom note.

Aside from the behavior of the ransomware encryptor itself, little is known about DeadLock and its operational behaviors. For example, there is no known substantial research on how this group breaches networks. However, Cisco Talos' report mentioned that they leverage BYOVD techniques to disable defensive countermeasures. ThreatScene included some data on tools they use for lateral movement, but that's only after the initial breach. Group-IB had no telemetry on initial breach telemetry, and neither do we, unfortunately.

All IoCs, references, and artifacts can be found on the Ransomware Entry Page: [DeadLock](#)

Filed under: [Ransomware](#), [Research](#)
[Blog Home](#)