Ransomware in July 2025 Report

ThreatMon
Under Cyber Wings

Executive Summary

Ransomware attacks remain one of the most critical threats to modern businesses, leading to severe operational disruptions, data breaches, and substantial financial losses. These incidents often necessitate costly infrastructure overhauls. However, early detection and proactive countermeasures can significantly mitigate these risks.

The insights presented here aim to empower organizations across industries to better anticipate, prevent, and respond to ransomware threats, ensuring business continuity and data integrity in an ever-changing threat landscape.

This report provides a comprehensive overview of ransomware trends, offering actionable insights for businesses to enhance their cybersecurity strategies. By analyzing the evolving tactics of threat actors and identifying vulnerabilities in organizational infrastructures, we emphasize the critical importance of proactive defense mechanisms and regular security assessments.

June's Most Significant Ransomware Attacks

China Harbour Engineering Company

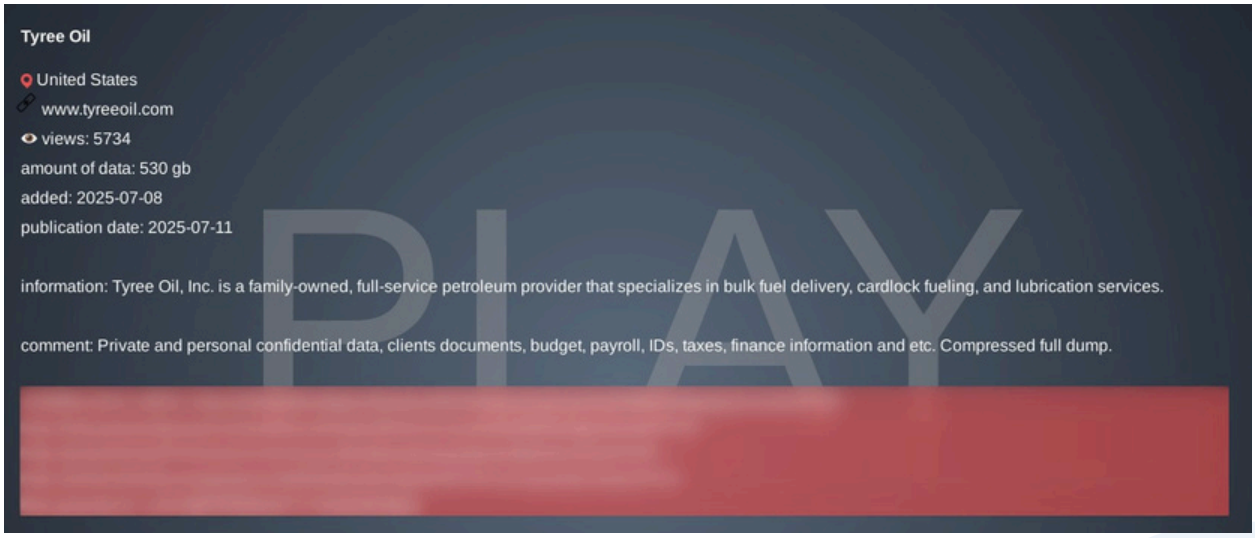
On July 5, 2025, China Harbour Engineering Company (CHEC), one of the leading companies in the international construction and engineering sector, was hit by a cyberattack carried out by the Devman ransomware group. As a result of the ransomware attack, sensitive data was stolen from the company's systems, and it was announced that some documents would be disclosed on the ransomware blog page.

Devman's blog post following the ransomware attack on China Harbour Engineering Company.

Tyree Oil

Tyree Oil, Inc., a family-owned company based in the United States that provides large-scale fuel deliveries, fueling services with card locks, and lubrication services, was targeted by the Play ransomware group. Following the attack on July 8, 2025, 530 GB of sensitive data was stolen, and the Play group threatened to disclose the data.

Among the stolen data are personal and confidential information, customer documents, budget and payroll information, identification details, tax information, and other financial data.

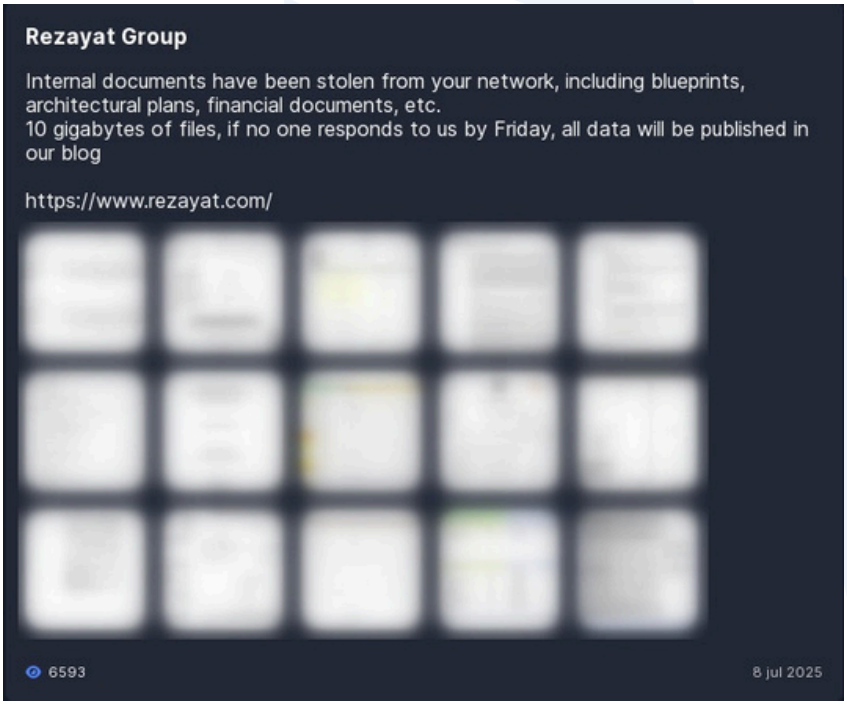


The Play ransomware group published a blog post following its ransomware attack on Tyree Oil.

Rezayat Group

On July 8, 2025, Rezayat Group was hit by a ransomware attack by the Everest ransomware group. According to the group's blog post, various sensitive documents were stolen from the company's internal network. The attackers stated that they had obtained critical data such as engineering plans, architectural drawings, and financial documents.

The total size of the stolen data is reported to be 10 GB. The Everest group threatened to publish all of this data on the company's blog if the company did not respond to their ransom demand.

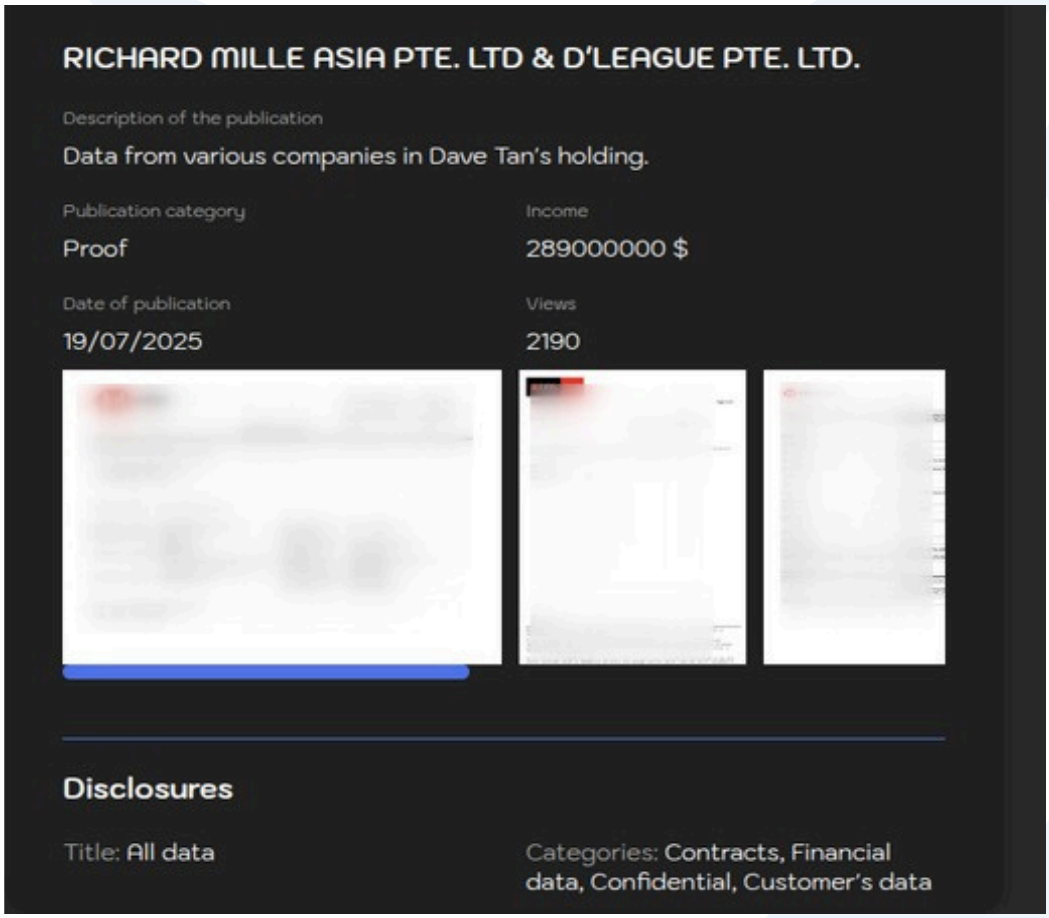


Everest Group blog post following ransomware attack on Rezayat Group.

Richard Mille Asia & D'League

On July 19, 2025, the ransomware group known as Lynx publicly disclosed a cyberattack targeting RICHARD MILLE ASIA PTE. LTD and D'LEAGUE PTE. LTD. According to the publication, the attackers obtained and leaked sensitive data from multiple companies associated with Dave Tan's holding. The exposed information includes contracts, financial records, and customer data, demonstrating the impact and scale of the breach.

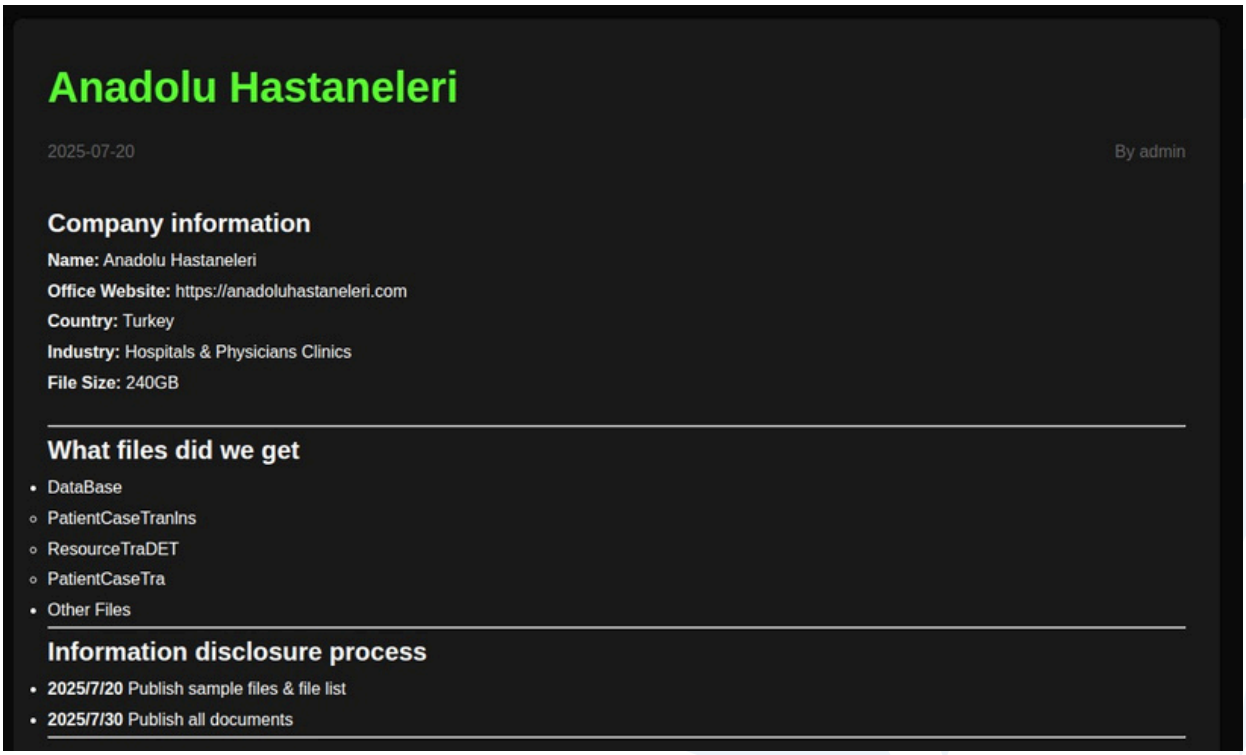
The attackers published a set of proof documents, including HSBC payment advices and transaction records, to substantiate their claims. The disclosed materials indicate an income figure of $2,890,000,000, underscoring the financial significance of the targeted entities.



Blog post by the Everest group following the ransomware attack on Mailchimp.

Anadolu Hastaneleri

On July 20, 2025, the ransomware group Direwolf announced that they had carried out an attack against Anadolu Hastaneleri, a hospital network based in Turkey. According to the published information, the attackers obtained approximately 240 GB of data, including databases, patient records, and various internal documents such as files labeled PatientCaseTranIns, ResourceTraDET, and PatientCaseTra.

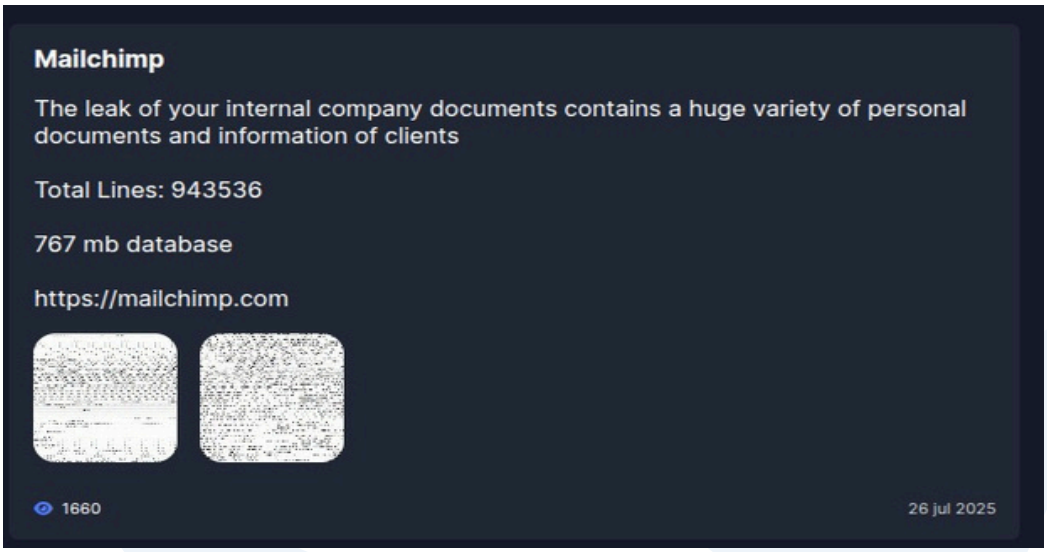


Lynx group's data made public after ransomware attack on Richard Mille Asia & D'League.

Mailchimp

On July 26, 2025, the ransomware group Everest announced that it had carried out a successful cyberattack against Mailchimp. According to the published statement, the attackers leaked a significant amount of information from the company's internal documents, including a 767 MB database containing a wide variety of personal information and customer records.

The leak was reported to span 943,536 lines of data, illustrating the scale of the attack. The attackers shared evidence of the breach and threatened to publish or monetize the stolen data.



Everest group's data made public after ransomware attack on Mailchimp.

Threat Actors Analysis

Devman

Devman (a.k.a. Devman 2.0) is a ransomware group known for its data extortion operations. The group is believed to have emerged in 2025 as a successor or rebranding of a former affiliate of the RansomHub and INC Ransom operations. Since its first recorded victim on April 6, 2025, Devman has claimed at least 62 attacks, showing a notable focus on technology, construction, public sector, healthcare, and consumer services industries.

While the exact tools and malware strains used by the group remain largely undisclosed, roughly 29.2% of their victims show signs of infostealer activity, suggesting credential theft is a significant part of their tactics. Additionally, their infrastructure includes multiple known IP addresses and TOX identifiers, which are commonly used for anonymous communication and extortion.

Key Characteristics:

- Double extortion is presumed to be the primary method: data is both encrypted and exfiltrated, with ransom demands made under the threat of public leaks.

- Victims are spread across several regions, with South Africa, Thailand, Japan, Singapore, and China among the most targeted countries.

- The group shows an average delay of 15 days between breaching a system and publicly claiming responsibility, likely allowing time for internal negotiation or silent extortion efforts.

Tactics and Behavior:

- Devman has been linked to infostealer deployment, likely to harvest credentials and sensitive information before file encryption.
- While the group has not publicly disclosed its ransom notes or negotiation chat logs, evidence suggests professional-grade operational security.
- The group operates without publicly known YARA rules or extensive threat intelligence footprints, indicating a stealth-focused approach.

As of August 2025, Devman remains active, with its most recent known victim dated August 1, 2025.

IoC's

MD5:e84270afa3030b48dc9e0c53a35c65aa

SHA-256 :df5ab9015833023a03f92a797e20196672c1d6525501a9f9a94a45b0904c7403

FileName:hsfjuukjzloqu28oajh727190

FileName:e47qfsnz2trbkhnt.devman

SHA-256:018494565257ef2b6a4e68f1c3e7573b87fc53bd5828c9c5127f31d37ea964f8

Play

Play Ransomware first appeared in June 2022. Unlike other ransomware groups, it uses a specially developed encryption module. It gets its name from the .play extension it adds to encrypted files. The group has a highly organized and technically competent structure.

One of the most notable features of the Play group is its adherence to the principles of privacy and simplicity. The ransom notes they publish are brief and lack detailed information. Communication with victims typically occurs through .onion-extended (Tor network-based) portals.

Attack Methods and Tactics, Techniques, and Procedures (TTPs)

1. Initial Access
- Vulnerability Detection: Targets critical vulnerabilities (e.g., FortiOS SSL-VPN CVE-2018-13379) in Fortinet, Exchange, and VPN devices in particular.
- Brute-force and Credential Stuffing: Targets weak or reused passwords.
- Phishing: Sends malicious links and attachments via spear phishing emails.

2. Lateral Movement
- RDP Propagation: Spreads across the network using RDP connections with stolen credentials.
- Mimikatz and LSASS Dump: Used to steal usernames and passwords.
- NTDS.dit Access: Extensive credential collection via Active Directory.

3. Payload Delivery
- Encryption Algorithm: Uses a double encryption mechanism; both file contents and file names can be encrypted.
- Proprietary Ransomware: Often uses specially written variants that are difficult to detect with conventional solutions.

4. Data Exfiltration
- Double Extortion: Data is exfiltrated before being encrypted. If the ransom is not paid, the stolen data is threatened to be leaked by the group.
- Exfiltration tools: Open source tools such as FileZilla, RClone, and WinSCP are used.

Ransom Notes

PLAY

news portal, tor network links:

mbrlkbtq5jonaqkurjwmxftytyn2ethqvbxfu4rgjbkkknndqwae6byd.onion
k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion

*****arikucisv@gmx.de

IoC's

SHA-256:

- 47B7B2DD88959CD7224A5542AE8D5BCE928BFC986BF0D0321532A7515C244A1E
- 75B525B220169F07AECFB3B1991702FBD9A1E170CAF0040D1FCB07C3E819F54A
- 453257C3494ADDAFB39CB6815862403E827947A1E7737EB8168CD10522465DEB
- C59F3C8D61D940B56436C14BC148C1FE98862921B8F7BAD97FBC96B31D71193C
- 1409E010675BF4A40DB0A845B60DB3AAE5B302834E80ADEEC884AEBC55ECCBF7
- 0E408AED1ACF902A9F97ABF71CF0DD354024109C5D52A79054C421BE35D93549
- 90040340EE101CAC7831D7035230AC8AD4224D432E5636F34F13AA1C4A0C2041
- 6DE8DD5757F9A3AC5E2AC28E8A77682D7A29BE25C106F785A061DCF582A20DC6
- 75404543DE25513B376F097CEB383E8EFB9C9B95DA8945FD4AA37C7B2F226212
- 7A42F96599DF8090CF89D6E3CE4316D24C6C00E499C8557A2E09D61C00C11986
- 7DEA671BE77A2CA5772B86CF8831B02BFF0567BCE6A3AE023825AA40354F8ACA
- 967DAFF362E63FF45526F585B7944488ACE1BB5BB5B30FA40D56557F1C538D09
- 859165041D75FBA3759C5533E324225F355C8A07B4645B984192AD6BEF06DB1A
- 511F63455CA4F83B0347B65DDA17585AD02591A9F23D8E234E5CE1321AA3381A
- 372F7B45A141BB0709D578BC716CBCA03104258822C4290CCBEB600223850158

SHA-1:

- 3D86555ACAA19AEDDB5896071D1E3711B062EDBE

Everest

Everest is a threat actor known in the cybersecurity world for its ransomware and data extortion activities. The group has been active since the early 2020s. Like other ransomware gangs, they infiltrate systems, encrypt data, and then demand a ransom for decryption and to prevent data leaks.

Tools and Techniques Used:

Credential Theft: They can steal user passwords and credentials with tools like ProcDump.

Discovery/Enumeration: They perform internal network reconnaissance with network scanning tools such as SoftPerfect NetScan.

Attack and Infiltration: They use advanced pen-testing and attack tools such as Cobalt Strike, Metasploit, Meterpreter.

Remote Management: They can use remote management software such as AnyDesk, Atera, Splashtop in their infiltrations in a legitimate-looking way.

Key Characteristics:

- They use the double extortion technique:
  - They encrypt the victim's files.
  - They exfiltrate data and threaten to publish it if the ransom is not paid.
- They operate leak sites, usually on the dark web, to release stolen data if victims refuse to pay.
- Their typical targets include:
  - Government agencies
  - Large private corporations
  - Education and healthcare institutions

Sometimes, even if the ransom is not paid, they attempt to sell the stolen data on dark web forums.

Tactics, Techniques, and Procedures (TTPs):

- Initial access is often gained through phishing campaigns.
- After gaining access, they move laterally across the network to find and target critical systems.
- They may use popular cyberattack tools such as Cobalt Strike or Mimikatz.
- File encryption is typically done using either their own custom malware or open-source encryption tools.

Lynx

Lynx is a cybercrime group that started operating in the ransomware world in 2024, specifically targeting Windows platforms. According to research, Lynx ransomware is considered a successor to INC ransomware, which emerged in 2023.

Activities and Attacks:

- Electrica Group Breach (January 2025): Electrica Group, a leading electricity supplier in Romania, was targeted by the Lynx ransomware gang in January 2025. While critical power supply systems were not affected during the attack, the company's other IT infrastructures were.
- Other Attacks: Lynx ransomware has added more than 78 victims to the data leak site since August 2024. Among these victims, companies in the US are the majority.

Methods Used:

Lynx ransomware demands ransom from victims by encrypting files. The encrypted files are appended with the “.LYNX” extension and the desktop background is replaced with a ransom note. It also has features such as printing the ransom note via connected printers. By avoiding encrypting certain file types and directories, Lynx preserves system operability and increases the likelihood of paying the ransom.

IoC's

SHA-256:

- 31de5a766dca4eaae7b69f807ec06ae14d2ac48100e06a30e17cc9acccfd5193
- 3e68e5742f998c5ba34c2130b2d89ca2a6c048feb6474bc81ff000e1eaed044e
- 432f549e9a2a76237133e9fe9b11fbb3d1a7e09904db5ccace29918e948529c6
- 468e3c2cb5b0bbc3004bbf5272f4ece5c979625f7623e6d71af5dc0929b89d6a
- 4e5b9ab271a1409be300e5f3fd90f934f317116f30b40eddc82a4dfd18366412
- 571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b
- 589ff3a5741336fa7c98dbcef4e8aecea347ea0f349b9949c6a5f6cd9d821a23
- 80908a51e403efd47b1d3689c3fb9447d3fb962d691d856b8b97581eefc0c441
- 85699c7180ad77f2ede0b15862bb7b51ad9df0478ed394866ac7fa9362bf5683
- 97c8f54d70e300c7d7e973c4b211da3c64c0f1c95770f663e04e35421dfb2ba0
- 9a47ab27d50df1faba1dc5777bdcfff576524424bc4a3364d33267bbcf8a3896
- b378b7ef0f906358eec595777a50f9bb5cc7bb6635e0f031d65b818a26bdc4ee
- d5ca3e0e25d768769e4afda209aca1f563768dae79571a38e3070428f8adf031
- eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc
- ecbfea3e7869166dd418f15387bc33ce46f2c72168f571071916b5054d7f6e49
- f71fc818362b1465fc1deb361de36badc73ac4dd9e815153c9022f82c4062787

SHA-1:

- 89d84ab72b2e5116f4a46b19f4d8096a0a9c7a88
- 558f259459d0ed1b30cbeaee71aa46eb5e40b090
- d0a3ae172c7c79ea3d964dae03e46cd67514ed0d
- d758d1f048ace4547dd3c22357aa2cf223426a50
- 67217e5c6859afb1b2c736625fcf8bee9ad158cc
- c632223f5f7a8a469bbf07eb017863bb83564b84
- f22bda5fa8a632e7d2dd2982300b4374168f8f32
- 3dd215876039ebee144e18ecb84d8702697db94b
- 5ef327b0154f7936ec185135a589fe2e19298d6f
- c1929f7f0ecda46baa1a1a97acc5e6f15f7075b3
- 01376fdcbd0e2063836ec2b075241587d7a56cdb
- 5338cae40e5419a0567b8162c52484f390284f15
- 6732c71c51a2ad68771984231f696f6e46708297
- 672553c79db2a3859a8ea216804d4ff8d2ded538
- 2424cf1f1c612c548345023db1a44d91dd3bf942
- 4182106fbec3d3fcecde5056b8246b6db317c2a3

MD5:

- a20886a5b378624d16972db66bd4e7e1
- f16238836909d07f86154c5ccbade96a
- 30656c737338818bee8cc3591e3f3dcc
- 571684f28ce1cf4d8236dbd46ef6f7f0
- 65c0c7c9fe6bc1d5296447aae6c6c14c
- d972bbbb3edb0e5ab5751b911f3dda17
- 146d350fd6271b4411714c630d8cda87
- 67a44a38cc36becd6e2e9c20c27fd9ad
- b47cdcdc179c5949ce18f4d161603901
- 2348b069647af0a714ae1e005f73b522
- 14a0ecf45aa72adb2b1f2ccca99f6faa
- 57f45c0738af9cd49c61984ea99f83ca
- 31a77e0d1c1b91eebec1f7cdcc1ab8b8
- 7e851829ee37bc0cf65a268d1d1baa7a
- 74ae58a716aa834949388ee1574788e0
- 0e521e0452f113cdf8b5c2fa6580db1f

Direwolf

Dire Wolf is a ransomware group that emerged in 2025 and quickly gained attention among threat actors. It is particularly notable for its double extortion method, target-specific ransom notes, advanced system manipulation, and data exfiltration platforms. The group's name is derived from the file extension it leaves behind (.direwolf) and the encryption mechanism it uses.

Tactics, Techniques, and Procedures (TTPs)

1. Pre-attack Preparation (Initial Access)

In Dire Wolf attacks, initial access is usually gained through the following methods:

- Phishing Emails: Fake payment receipts or human resources documents with ZIP or ISO attachments.
- RDP Brute Force: Especially weak RDP connections that are open to the outside world.
- Zero-Day and N-Day Vulnerabilities: Especially known vulnerabilities in Fortinet, Ivanti, and VPN devices.
- Legitimate Remote Management Tools: Tools such as AnyDesk, Atera, and ConnectWise (ScreenConnect) are manually installed on victim systems.

2. Lateral Movement & Preparation

- EDR/AV disabling: Defender and third-party security software are stopped using Powershell, WMI, and service management.
- File Search & Encryption: Specifically targets extensions such as .docx, .pdf, .xls, .csv, and .sql. Certain system files (.exe, .dll, .sys) are excluded.

3. Encryption Methods and Technical Details

Encryption Algorithm:
Asymmetric: Curve25519
Symmetric: ChaCha20
File Extension: .direwolf
Network folders are also encrypted (including UNC paths)
UPX-Packed Golang Binary: UPX compression and embedded string encryption are used to make reverse engineering more difficult.
Self-destruction capability: If certain files and mutexes are present, the software will uninstall itself.

Ransom Notes

Dear Mr or Ms,
If you are reading this message, it means that:
- your network infrastructure has been compromised
- critical data was leaked
- We decrypted your encrypted files. The anti-leakage system is useless to us. We can provide proof.
- files are encrypted

The best and only thing you can do is to contact us
to settle the matter before any losses occurs.

We can maintain confidentiality for 3 days for you, during which we will not disclose any information about your intrusion or data leakage.
We can extend the confidentiality period free of charge until we reach an agreement if you contact us within 3 days and communicate effectively with us.
If the confidentiality period expires, we will disclose the relevant information.
We provide complimentary decryption testing services. For specific details, please contact us.

We have provided a sample document as proof of our possession of your files and you can download and check it:
- https://gofile.io/d/[snip]
Please be advised that your files are scheduled for public release after 30 working days.
If you want to secure your files, we urge you to reach out to us at your earliest convenience.

Contact Details:
- live chat room:
-
url:http://direwolf3ddtab5anvhulcelauvoxu2a7l264hqs6vtxtgrqsjfvodid.onion/
- roomID: [snip]
- username: [snip]
- password: [snip]

Our official website:
-
url:http://direwolfcdkv5whaz2spehizdg22jsuf5aeje4asmetpbt6ri4jnd4qd.onion/

How to access .onion website:
1.Download and install TOR Browser https://torproject.org
2.Open it and try to access our onion address
3.Maybe you need to use VPN if it can not open our onion address

IoC’s

MD5:

- A71dbf2e20c04da134f8be86ca93a619
- aa62b3905be9b49551a07bc16eaad2ff

SHA-1:

- Ed7c9fbd42605c790660df86b7ec325490f6d827
- 4a5852e9f9e20b243d8430b229e41b92949e4d69

Conclusion

The analysis reveals that by July 2025, ransomware attacks will reach levels that pose significant threats to critical sectors in terms of both complexity and frequency. Sectors such as engineering, oil/energy, and healthcare have become the primary targets of ransomware groups such as Devman, Play ,Everest, Lynx, and Direwolf. These groups employ a wide range of sophisticated methods, including phishing, RDP exploits, double extortion, and infrastructure-focused attacks.

These developments underscore the urgency of organizations strengthening their cybersecurity frameworks. Continuous risk assessments, regular cybersecurity awareness training for employees, timely patch management, and the use of advanced threat detection systems play a critical role in this process. Additionally, cross-industry collaboration, information sharing, and effective communication with law enforcement are crucial to preventing the global spread of ransomware threats.

ThreatMon
Under Cyber Wings

More Information About ThreatMon

One Platform for all intelligence needs.

ThreatMon End-to-end intelligence is a cutting-edge, cloud-based SaaS platform that continuously monitors the dark and surface web, providing early warnings and actionable insights into emerging threats.

We are a SaaS platform designed to help businesses proactively detect and address threats before a cyber attack occurs. Unlike traditional cyber threat intelligence, we provide comprehensive and holistic cyber intelligence.

- *Attack Surface Intelligence*
- *Fraud Intelligence*
- *Dark and Surface Web Intelligence*
- *Threat Intelligence*

APPLY

FREE ACCESS

Contact Us:

Email Address
team@threatmonit.io

https://x.com/MonThreat

https://www.linkedin.com/company/threatmon