Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

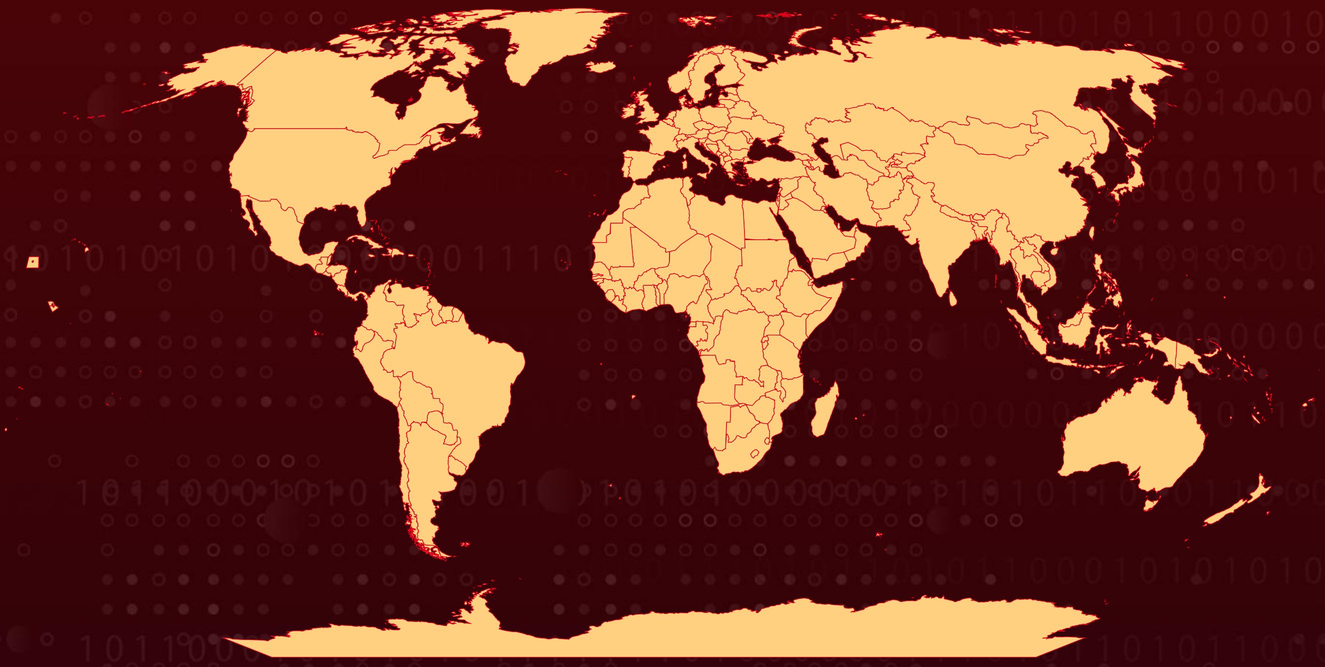
A New Ransomware Threat: VanHelsing’s Rapid Expansion

Date of Publication	Admiralty Code	TA Number
March 25, 2025	A1	TA2025094

Summary

Attack Commenced: March 7, 2024
Targeted Countries: Worldwide
Malware: VanHelsing
Targeted Platforms: Windows, Linux, BSD, ARM, and VMware ESXi
Ransom Demand: $500,000
Targeted Industries: Government, Manufacturing, and Pharmaceuticals
Attack: VanHelsing is a ransomware-as-a-service (RaaS) operation that emerged on March 7, 2025, quickly gaining attention in the cybercrime world. It uses double extortion tactics, encrypting files while threatening to leak stolen data, with ransom demands reaching up to $500,000 per victim. Operating on an affiliate model, it allows cybercriminals to join with a $5,000 deposit, offering them 80% of the ransom while operators take 20%. Primarily targeting Windows, it also claims compatibility with Linux, BSD, ARM, and VMware ESXi. Within two weeks, it had already infected three organizations, highlighting its rapid spread and the urgent need for strong cybersecurity defenses.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

VanHelsing ransomware is a newly emerged ransomware-as-a-service (RaaS) operation that first appeared in early March 2025. It is primarily designed to target Windows systems, although its creators claim it also supports other operating systems such as Linux, BSD, ARM, and VMware ESXi. This multi-platform capability broadens its potential reach, but most documented infections have so far been on Windows machines.

#2

The ransomware employs a double extortion tactic where it not only encrypts files, appending a ".vanhelsing" extension, but also exfiltrates sensitive data from the victim. The attackers then threaten to leak this stolen information if the ransom demands are not met, increasing the pressure on victims to pay. This strategy has already resulted in high ransom demands, reportedly reaching up to $500,000 per incident.

#3

A notable feature of VanHelsing is its affiliate-based business model. Experienced cybercriminals can join the program at no cost, while new affiliates must pay a $5,000 deposit to participate. Once an attack is carried out, the revenue is split between the affiliates and the core operators, with affiliates receiving 80% of the ransom payments and the operators taking the remaining 20%. This low barrier to entry is attracting a diverse group of threat actors, thereby amplifying the overall threat.

#4

From a technical standpoint, VanHelsing is written in C++ and leverages sophisticated encryption techniques. It uses the ChaCha20 algorithm in combination with a Curve25519 public key to secure encrypted files. In addition, the malware is programmed to delete volume shadow copies, a key step in preventing victims from easily restoring their data, and employs a stealth mode to delay the file renaming process and avoid early detection. These technical choices make it a resilient and adaptable threat.

#5

Furthermore, the ransomware's operators enforce a geographic restriction by prohibiting attacks on systems located within the Commonwealth of Independent States (CIS), a common trait among Russian-linked cybercriminal groups. Initial attacks have predominantly affected organizations in sectors such as government, manufacturing, and pharmaceuticals in the United States and France. Given the rapid evolution and increasing sophistication of VanHelsing, organizations are advised to bolster their cybersecurity defenses with regular, isolated backups, timely patch management, robust endpoint protection, and strict access controls to mitigate the risk of infection.

Recommendations

Apply Security Patches and Updates Promptly: Regularly update all software, operating systems, and applications to address known vulnerabilities that VanHelsing can exploit. Automated patch management systems can assist in ensuring timely updates.

Deploy Endpoint Detection and Response (EDR) Solutions: Utilize EDR tools to monitor and analyze endpoint activities, enabling the detection and swift response to suspicious behaviors indicative of ransomware attacks.

Restrict User Privileges and Network Access: Apply the principle of least privilege by limiting user access rights to only what is necessary for their roles. Implement network segmentation to contain potential ransomware spread and regularly audit privileged accounts.

Strengthen Email Security and Filtering: Implement advanced email filtering solutions to block malicious attachments, links, and phishing attempts. Technologies such as SPF, DKIM, and DMARC can authenticate senders and reduce the risk of email-based attacks.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of an VanHelsing ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0002 Execution
TA0007 Discovery	TA0040 Impact	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0010 Exfiltration	T1490 Inhibit System Recovery	T1496 Resource Hijacking

T1083 File and Directory Discovery	T1135 Network Share Discovery	T1518 Software Discovery	T1005 Data from Local System
T1047 Windows Management Instrumentation	T1053 Scheduled Task/Job	T1059 Command and Scripting Interpreter	T1129 Shared Modules
T1542 Pre-OS Boot	T1543.003 Windows Service	T1543 Create or Modify System Process	T1547.001 Registry Run Keys / Startup Folder
T1542.003 Bootkit	T1547 Boot or Logon Autostart Execution	T1574.002 DLL Side-Loading	T1574 Hijack Execution Flow
T1055 Process Injection	T1486 Data Encrypted for Impact	T1548 Abuse Elevation Control Mechanism	T1006 Direct Volume Access
T1014 Rootkit	T1027.002 Software Packing	T1027 Obfuscated Files or Information	T1036 Masquerading
T1070 Indicator Removal	T1112 Modify Registry	T1202 Indirect Command Execution	T1222 File and Directory Permissions Modification
T1564.001 Hidden Files and Directories	T1564.003 Hidden Window	T1564 Hide Artifacts	T1003 OS Credential Dumping
T1552.001 Credentials In Files	T1012 Query Registry	T1057 Process Discovery	T1082 System Information Discovery
T1114 Email Collection	T1213 Data from Information Repositories	T1518.001 Security Software Discovery	T1071 Application Layer Protocol
T1090 Proxy	T1105 Ingress Tool Transfer	T1485 Data Destruction	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	3e063dc0de937df5841cb9c2ff3e4651, 5c254d25751269892b6f02d6c6384aef, cd9563b4cbc415b3920633b93c0d351b
SHA1	4211cec2f905b9c94674a326581e4a5ae0599df9, 79106dd259ba5343202c2f669a0a61b10adfadff, e683bfaeb1a695ff9ef1759cf1944fa3bb3b6948
SHA256	86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17, 99959c5141f62d4fbb60efdc05260b6e956651963d29c36845f435815062fd98
Tor Address	vanhelcbxqt4tqie6fuevfng2bsdtxgc7xslo2yo7nitaacdfrlpxnqd[.]onion, vanhelqmjstkvlhrjwzgjzpq422iku6wlggiz5y5r3rmfdeiaj3ljaid[.]onion, vanhelsokskrlaacilyfmtuqqa5haikubsjaokw47f3pt3uoivh6cgad[.]onion, vanheltarnbfjhuvggbncniap56dscnzz5yf6yjmxqivqmb5r2gmllad[.]onion, vanhelvuuo4k3xsiq626zkqvp6kobc2abry5wowxqysibmqs5yjh4uqd[.]onion, vanhelwmbf2bwzw7gmseg36qqm4ekc5uuhqbsew4eihzcahyq7sukzad[.]onion, vanhelxjo52qr2ixcmtjayqqrcodkuh36n7uq7q7xj23ggotyr3y72yd[.]onion
Tox Address	FEE914521FB507AB978107ACE3B69B4CA41DA89859408BAE23E1512E8C2E614A26C5FFD482A3
Bitcoin Wallet	bc1q0cuvj9eglxk43v9mqmyjzzh6m8qsvsanedwrru

Recent Breaches

https://studiocdlvallone.it
https://www.atos-racks.com
https://atos.net
https://www.medsrx.com
https://atos-racks.com
https://www.cityofbellville.com

References

https://research.checkpoint.com/2025/vanhelsing-new-raas-in-town/

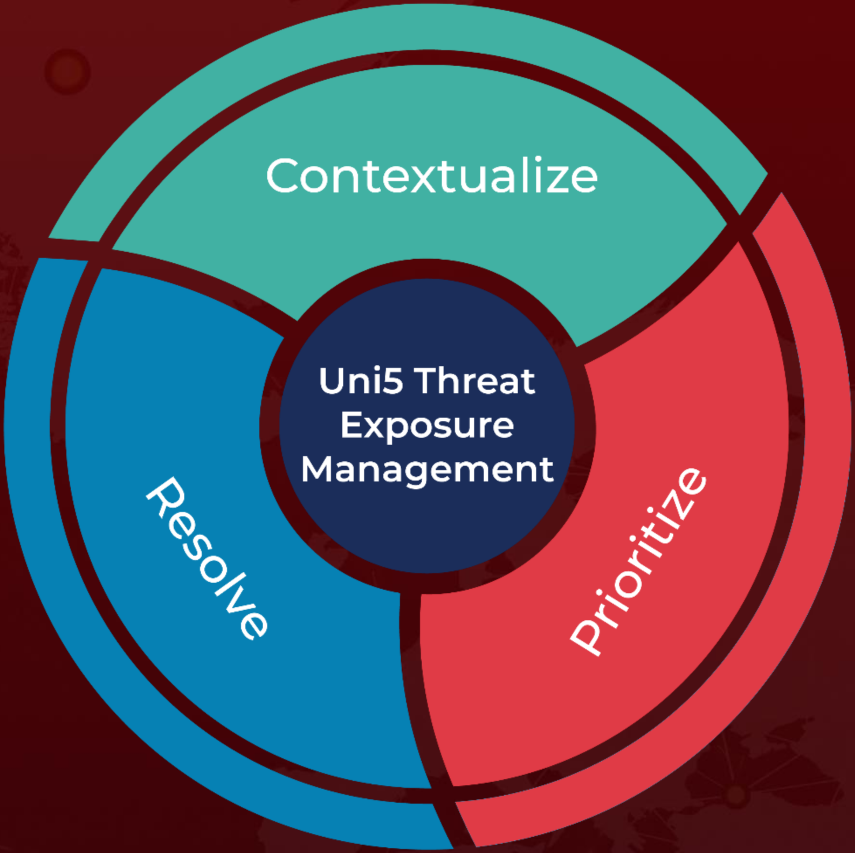
https://www.cyfirma.com/research/vanhelsing-ransomware/

https://industrialcyber.co/ransomware/vanhelsing-ransomware-uses-double-extortion-on-us-french-government-manufacturing-pharma-sectors/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 25, 2025 • 7:30 AM

More at www.hivepro.com