April 2, 2025

INTEL471

EMERGING THREATS

VanHelsing Ransomware

In March 2025, a new ransomware-as-a-service (RaaS) program named VanHelsing was launched, quickly gaining traction within the cybercriminal community. The program has targeted and infected three victims within two weeks, demanding ransoms of $500,000 in Bitcoin for decryption and data deletion. The program allows affiliates to participate by paying a $5,000 deposit, with these affiliates retaining 80% of ransom payments while the core operators receive 20%. VanHelsing ransomware is cross-platform, capable of infecting Windows, Linux, BSD, ARM, and ESXi systems, and offers an intuitive control panel for managing attacks - notably prohibiting the targeting of entities within the Commonwealth of Independent States (CIS). Researchers have also observed this new variant already evolving in sophistication, meaning its active development and thus the need for up-to-date security measures to defend against this emerging variant.

THREAT SUMMARY

In March 2025, a new ransomware-as-a-service (RaaS) program named VanHelsing was launched, quickly gaining traction within the cybercriminal community. The program has targeted and infected three victims within two weeks, demanding ransoms of $500,000 in Bitcoin for decryption and data deletion. The program allows affiliates to participate by paying a $5,000 deposit, with these affiliates retaining 80% of ransom payments while the core operators receive 20%. VanHelsing ransomware is cross-platform, capable of infecting Windows, Linux, BSD, ARM, and ESXi systems, and offers an intuitive control panel for managing attacks - notably prohibiting the targeting of entities within the Commonwealth of Independent States (CIS). Researchers have also observed this new variant already evolving in sophistication, meaning its active development and thus the need for up-to-date security measures to defend against this emerging variant.

Intel 471 TITAN Reference:

TITAN Info Report: Actor VanHelsingRAAS recruits affiliates to join new Vanhelsing Locker ransomware-as-a-service affiliate program

HUNTER Hunt Package Collection:
https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('1f40b659-bc98-4764-a013-cda1b5c9b179'),touched:!t)

SYNOPSIS

VanHelsing Ransomware is a newly launched ransomware-as-a-service (RaaS) that was first observed in March of 2025. Within two weeks, the variant claimed three victims, demanding $500,000 in Bitcoin as ransom. Check Point Researchers identified two Windows-targeting variants compiled within five days of each other, indicating rapid development and the need to stay on top of observed TTPs (Tactics, Techniques, and Procedures).

The ransomware is designed to target multiple operating systems, including Windows, Linux, BSD, ARM, and ESXi systems. This broad compatibility enhances its effectiveness across diverse environments and maximizes its reach across environments. After infection and subsequent encryption of data, the malware appends the extensions ".vanhelsing" or ".vanlocker" to encrypted files, rendering them inaccessible without decryption. A ransom note is dropped (as README.txt in recent instances), demanding payment for the decryption key. It is also worth noting that the variant has been observed employing the common technique of deleting volume shadow copies on victim machines to inhibit system recovery.

The program provides an intuitive control panel to affiliates, simplifying the execution of ransomware attacks. Further, in its short lifespan, the malware has undergone rapid evolution - with updates introducing new command-line arguments and features, indicating active development and adaptation. As any additional information about its capabilities are discovered, Intel 471 researchers will be adding and updating content in the Hunter platform.

HUNT PACKAGE COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!(%271f40b659-bc98-4764-a013-cda1b5c9b179%27),touched:!t)

RELATED HUNT PACKAGES

Windows Management Instrumentation (WMI) Call to delete ShadowCopy via WMIC Command

https://hunter.cyborgsecurity.io/research/hunt-package/f047c78d-d761-4e34-b4fd-fc1902e4f8b1

Remote Services - SMB Share mounts/admin shares/scanning

https://hunter.cyborgsecurity.io/research/hunt-package/29b036ae-4879-4509-a0ac-65d46ea76cf1

Registry Modification of CLSIDs Pointing to Abnormal Locations - Potential COM Object Hijacking

https://hunter.cyborgsecurity.io/research/hunt-package/a7b1ec47-94ef-4df8-8728-406cdf1f1d6f

Copying a File to a Hidden Share Directory

https://hunter.cyborgsecurity.io/research/hunt-package/7d19d46f-06c8-40c6-8c91-0f924f17358d

Shadow Copies Deletion Using Operating Systems Utilities

https://hunter.cyborgsecurity.io/research/hunt-package/2e3e9910-70c1-4822-804a-ee9919b0c419

MITRE CONTEXT

Threat Name(s):

- VanHelsing Ransomware

Mitre Technique IDs:

- T1021.002
- T1546.015
- T1490
- T1565.001
- T104

Mitre Technique Names:

- Component Object Model Hijacking
- Stored Data Manipulation
- Windows Management Instrumentation
- Inhibit System Recovery
- SMB/Windows Admin Shares

Mitre Tactic Names:

- Impact
- Lateral Movement
- Privilege Escalation
- Execution
- Persistence

REFERENCES

1. https://blog.checkpoint.com/research/the-rise-of-vanhelsing-raas-a-new-player-in-the-ransomware-landscape/
2. https://www.broadcom.com/support/security-center/protection-bulletin/vanhelsing-ransomware