Ransomware Roundup – VanHelsing

fortinet.com/blog/threat-research/ransomware-roundup-vanhelsing

May 16, 2025

Article Contents

By Shunichi Imano and Fred Gutierrez | May 16, 2025

FortiGuard Labs gathers data on ransomware variants of interest that have been gaining traction within our datasets and the OSINT community. The Ransomware Roundup report aims to provide readers with brief insights into the evolving ransomware landscape and the Fortinet solutions that protect against those variants.

This edition of the Ransomware Roundup covers the VanHelsing ransomware.

Affected platforms: Microsoft Windows
Impacted parties: Microsoft Windows
Impact: Encrypts victims' files and demands a ransom for file decryption
Severity level: High

2025 Global Threat Landscape Report

Use this report to understand the latest attacker tactics, assess your exposure, and prioritize action before the next exploit hits your environment.

VanHelsing Ransomware Overview

The first sample of the VanHelsing ransomware was made available on a publicly available file-scanning site in mid-March 2025. Like other ransomware attacks, VanHelsing demands a ransom to decrypt files via dropped ransom notes.

Infection Vector

Information on the infection vector used by the VanHelsing ransomware threat actor is unavailable. However, it is not likely to differ significantly from other ransomware groups.

Attack Method

When run, the VanHelsing ransomware (SHA2: 99959C5141F62D4FBB60EFDC05260B6E956651963D29C36845F435815062FD98) takes the following command line arguments:

- -h for help
- -v for verbose
- -sftpPassword for spreading over sftp
- -smbPassword for spreading over SMB
- -bypassAdmin for locking the target without admin
- -noLogs to stop logging
- -nopriority to stop CPU and IO priority

The VanHelsing ransomware then encrypts files on the compromised machines and adds the file extension ".vanlocker" to affected files.

Figure 1: Files encrypted by a VanHelsing ransomware variant
Note that although this VanHelsing variant

(SHA2: 99959C5141F62D4FBB60EFDC05260B6E956651963D29C36845F435815062FD98)

uses ".vanlocker" as its extension, it still belongs to the VanHelsing ransomware family because it uses the same ransom negotiation and data leak sites as another VanHelsing variant.

(SHA2: 86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17)

This other variant adds a ".vanhelsing" file extension to the files it encrypts.

Figure 2: Files encrypted by the VanHelsing ransomware
The VanHelsing ransomware exempts the following files:

boot.ini	autofun.inf	bootfont.bin	bootsect.bak
desktop.ini	ntldr	ntuser.dat	ntuser.dat.log
ntuser.ini	thumb.db	GDIPFONTCACHEV1.DAT	iconcache.db

d3d9caps.dat	LOGS.txt	README.txt	

It also avoids encrypting files with the following file extensions:

.vanlocker	.exe	.dll	.lnk	.sys	.msi	.bat
.bin	.com	.cmd	.386	.adv	.ani	.cab
.ico	.mod	.msstyles	.msu	.nomedia	.ps1	.rtp
.syss	.deskthemepack	.cur	.cpl	.diagcab	.diagcfg	.diagpke
.dll	.drv	.hlp	.pdb	.hta	.key	.lock
.ldf	.ocx	.icl	.icns	.ics	.idx	.mod
.mpa	.msc	.msp	.nls	.rom	.scr	.shs
.spl	.theme	.thempa	.wpx			

The VanHelsing ransomware avoids encrypting files in the following folders:

tmp	wiint	temp	thumb
$Recycle.Bin	$RECYCLE.BIN	System Volume Information	boot
Windows	Trend Micro	program files	program files(x86)
tor browser	Windows	intel	all users
msocache	perflogs	default	microsoft

It also creates the following mutex:

mutex: Global\\VanHelsing

It may also modify the registry key Software\Classes\.vanlocker\DefaultIcon to use a custom icon for .VANLOCKER files. However, we did not observe this VanHelsing ransomware sample change the file icon of the encrypted files in our testing.

It then drops the following ransom note in “README.txt”:

Figure 3: Ransom note dropped by the VanHelsing ransomware
The ransom note directs victims to chat sites operated by the attacker on TOR, where ransom negotiation takes place.

The ransomware also replaces the desktop wallpaper with its own.

Figure 4: Desktop wallpaper replaced by the VanHelsing ransomware

Victimology and Data Leak Site

The VanHelsing ransomware operates a TOR site where the group posts the information it has stolen from its victims. At the time of our initial investigation in late March 2025, six victims were on the data leak site, and they had added one more victim when we checked back in mid-April.

Our analysis of the VanHelsing ransomware victims listed on the data leak site found:

- The victims are spread out over four different countries.
- 50% of the victims are in the United States.
- The other victims are in Italy, France, and Australia.
- Manufacturing is the industry most affected by this, with two victims.
- One of the six victims is a municipal government organization in the U.S., which suggests that the VanHelsing ransomware group may have no restrictions on who it targets.

Note that victims who have paid the ransom may have been removed from the data leak site. As such, additional companies may have been affected by the VanHelsing ransomware.

Figure 5: A list of the VanHelsing ransomware victims on its data leak site.

Figure 6: Negotiations between the VanHelsing group and one of the victims

Figure 7: Individual page of a victim organization

Fortinet Protections

The VanHelsing ransomware described in this report is detected and blocked by FortiGuard Antivirus as:

- W32/Filecoder_VanHelsing.A!tr.ransom

- W32/PossibleThreat

FortiGate, FortiMail, FortiClient, and FortiEDR support the FortiGuard AntiVirus service. The FortiGuard AntiVirus engine is a part of each of those solutions. As a result, customers who have these products with up-to-date protections are protected.

FortiGuard Labs Guidance

Due to the ease of disruption, damage to daily operations, potential impact on an organization's reputation, and the unwanted destruction or release of personally identifiable information (PII), etc., it is vital to keep all AV and IPS signatures up to date.

Since the majority of ransomware is delivered via phishing, organizations should consider leveraging Fortinet solutions designed to train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

Our FREE Fortinet Certified Fundamentals (FCF) in Cybersecurity training. The training is designed to help end users learn about today's threat landscape and will introduce basic cybersecurity concepts and technology.

Organizations will need to make foundational changes to the frequency, location, and security of their data backups to effectively deal with the evolving and rapidly expanding risk of ransomware. When coupled with digital supply chain compromise and a workforce telecommuting into the network, there is a real risk that attacks can come from anywhere. Cloud-based security solutions, such as SASE, to protect off-network devices; advanced endpoint security, such as EDR (endpoint detection and response) solutions that can disrupt malware mid-attack; and Zero Trust Access and network segmentation strategies that restrict access to applications and resources based on policy and context, should all be investigated to minimize risk and to reduce the impact of a successful ransomware attack.

As part of the industry's leading fully integrated Security Fabric, delivering native synergy and automation across your security ecosystem, Fortinet also provides an extensive portfolio of technology and human-based as-a-service offerings. These services are powered by our global FortiGuard team of seasoned cybersecurity experts.

FortiRecon is a SaaS based Digital Risk Prevention Service backed by cybersecurity experts to provide unrivaled threat intelligence on the latest threat actor activity across the dark web, providing a rich understanding of threat actors' motivations and TTPs. The service can detect evidence of attacks in progress allowing customers to rapidly respond to and shut down active threats.

Best Practices Include Not Paying a Ransom

Organizations such as CISA, NCSC, the FBI, and HHS caution ransomware victims against paying a ransom partly because the payment does not guarantee that files will be recovered. According to a US Department of Treasury's Office of Foreign Assets Control (OFAC) advisory, ransom payments may also embolden adversaries to target additional organizations, encourage other criminal actors to distribute ransomware, and/or fund illicit activities that could potentially be illegal. For organizations and individuals affected by ransomware, the FBI has a Ransomware Complaint page where victims can submit samples of ransomware activity via their Internet Crimes Complaint Center (IC3).

How Fortinet Can Help

FortiGuard Labs' Emergency Incident Response Service provides rapid and effective response when an incident is detected. Our Incident Readiness Subscription Service provides tools and guidance to help you better prepare for a cyber incident through readiness assessments, IR playbook development, and IR playbook testing (tabletop exercises).

Additionally, FortiRecon Digital Risk Protection (DRP) is a SaaS-based service that provides a view of what adversaries are seeing, doing, and planning to help you counter attacks at the reconnaissance phase and significantly reduce the risk, time, and cost of later-stage threat mitigation.

IOCs

VanHelsing Ransomware File IOCs

SHA2	Note
86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17	VanHelsing ransomware
99959c5141f62d4fbb60efdc05260b6e956651963d29c36845f435815062fd98	