Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

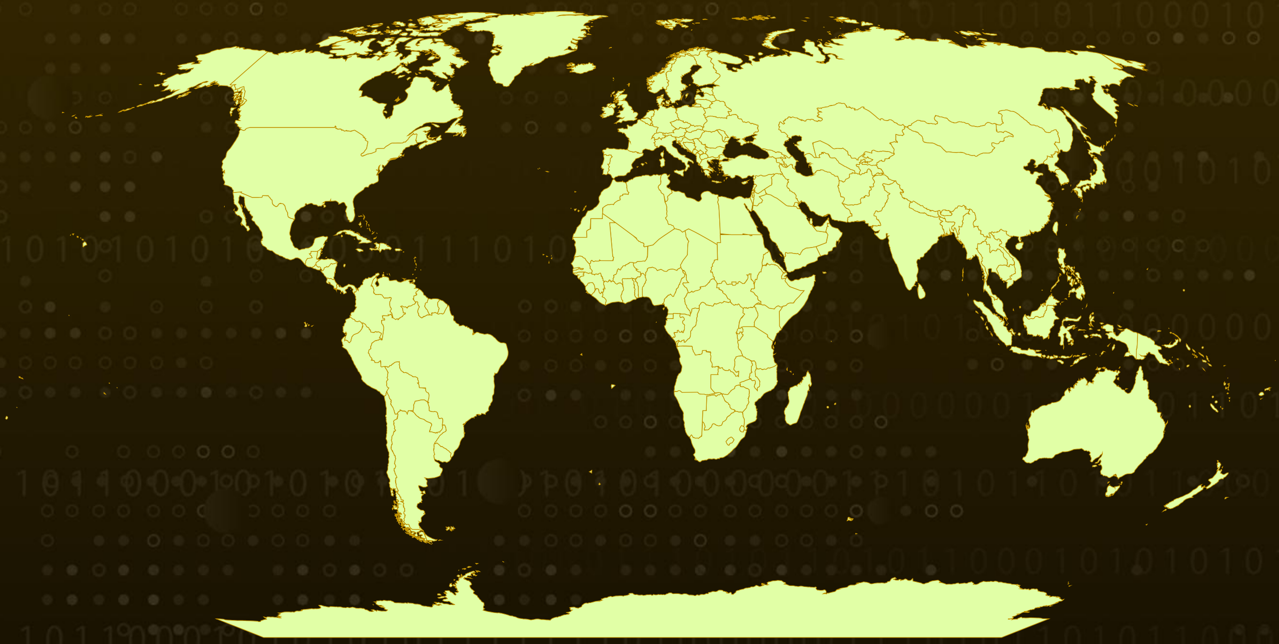
Cybercriminals Exploit VHD Files to Deploy VenomRAT and Steal Data

Date of Publication	Admiralty Code	TA Number
March 21, 2025	A1	TA2025089

Summary

Attack Discovered: February 2025
Targeted Countries: Worldwide
Malware: VenomRAT
Attack: A new malware campaign is exploiting virtual hard disk (VHD) files to stealthily deliver VenomRAT. The attack begins with phishing emails posing as purchase orders, tricking users into opening an archive containing a VHD file. Once mounted, the VHD deploys a heavily obfuscated batch script that leverages PowerShell to execute malicious actions, stealing sensitive data and exfiltrating it to attacker-controlled C2 servers hosted on Pastebin.

Attack Regions



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

Attack Details

#1

Threat actors are leveraging virtual hard disk (VHD) files to stealthily distribute VenomRAT malware, targeting large communities through phishing emails. These emails, disguised as purchase orders, contain archive attachments that extract a .vhd file, which mounts itself as a disk drive. Inside, an obfuscated batch script executes malicious PowerShell commands to steal sensitive data and communicate with command-and-control (C2) servers.

#2

Once executed, the script creates a copy of itself in C:\Users%userprofile%\dwm.bat and modifies system registry entries for persistence. It also drops additional files into the Startup folder, ensuring the malware runs at every reboot. To evade detection, it connects to Pastebin.com, a legitimate service repurposed as a storage hub for malicious payloads and exfiltrated data.

#3

The batch script performs multiple actions, such as establishing a malicious TCP connection, creating a DataLogs_keylog_online.txt file to record keystrokes, and deploying a .NET compiled executable with AES decryption techniques. If PowerShell is running, it further manipulates system settings to maintain its foothold.

#4

VenomRAT 6.0.3, the malware variant used in this campaign, includes Hidden Virtual Network Computing (HVNC) capabilities, allowing attackers to control infected systems remotely. It also drops a DataLogs.conf file to capture sensitive data, further increasing its stealth and effectiveness. This attack highlights the evolving tactics of cybercriminals, who exploit VHD files as a delivery mechanism to bypass traditional security measures.

Recommendations

Prevent Untrusted VHD File Execution: Block virtual hard disk (VHD) files from running if they come from unknown sources, reducing the risk of malware sneaking in through mounted drives.

Strengthen Email Security Measures: Implement advanced filtering and anti-phishing solutions to identify and block malicious attachments, particularly archive files that may contain VHD-based malware.

Restrict PowerShell and Monitor System Changes: Enforce Group Policy to allow only signed PowerShell scripts and enable logging to detect suspicious executions. Simultaneously, track registry changes, Startup folder modifications, and unexpected file creations to identify signs of malware persistence.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0009 Collection	**TA0010** Exfiltration	**TA0011** Command and Control	**T1566** Phishing
T1566.001 Spearphishing Attachment	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.003** Windows Command Shell
T1140 Deobfuscate/Decode Files or Information	**T1132** Data Encoding	**T1132.001** Standard Encoding	**T1056** Input Capture
T1056.001 Keylogging	**T1005** Data from Local System	**T1112** Modify Registry	**T1041** Exfiltration Over C2 Channel

T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1027** Obfuscated Files or Information	**T1102** Web Service
T1204 User Execution	**T1204.002** Malicious File		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	74262a750437b80ed15aeca462172b50d87096e5, df9fb41bffbb7479776d1d9a1eecdbb94abdf99b, ae467b8593e340194dc73dc3db6363c3e73ca970, ddc7315a3903974624dfd750a374c37c9c67c6dd
URL	hxxps[:]//Pastebin[.]com/raw/i3NzmwEg
IPv4:Port	81[.]19[.]131[.]153[:]50037, 217[.]64[.]148[.]159[:]50037
Domain	ggggg[.]gettt:50037

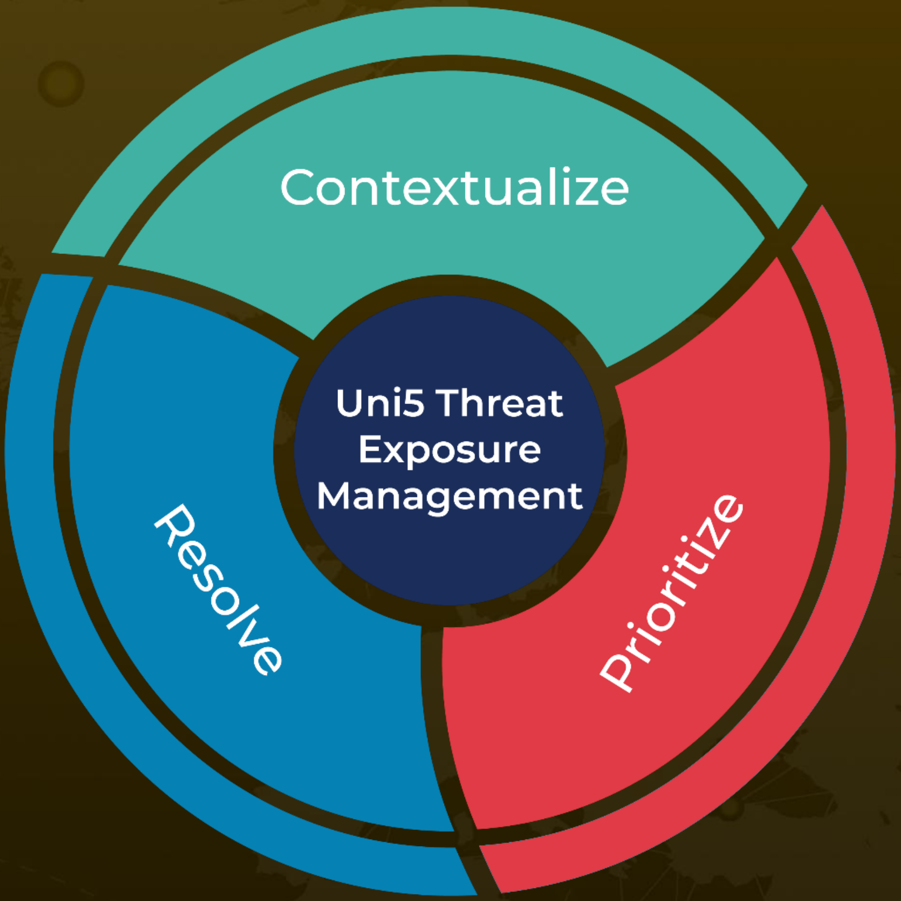
References

https://www.forcepoint.com/blog/x-labs/venomrat-malware-uses-virtual-hard-drives

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 21, 2025 • 4:30 AM

More at www.hivepro.com