Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

The High-Stakes Game of Vgod Ransomware

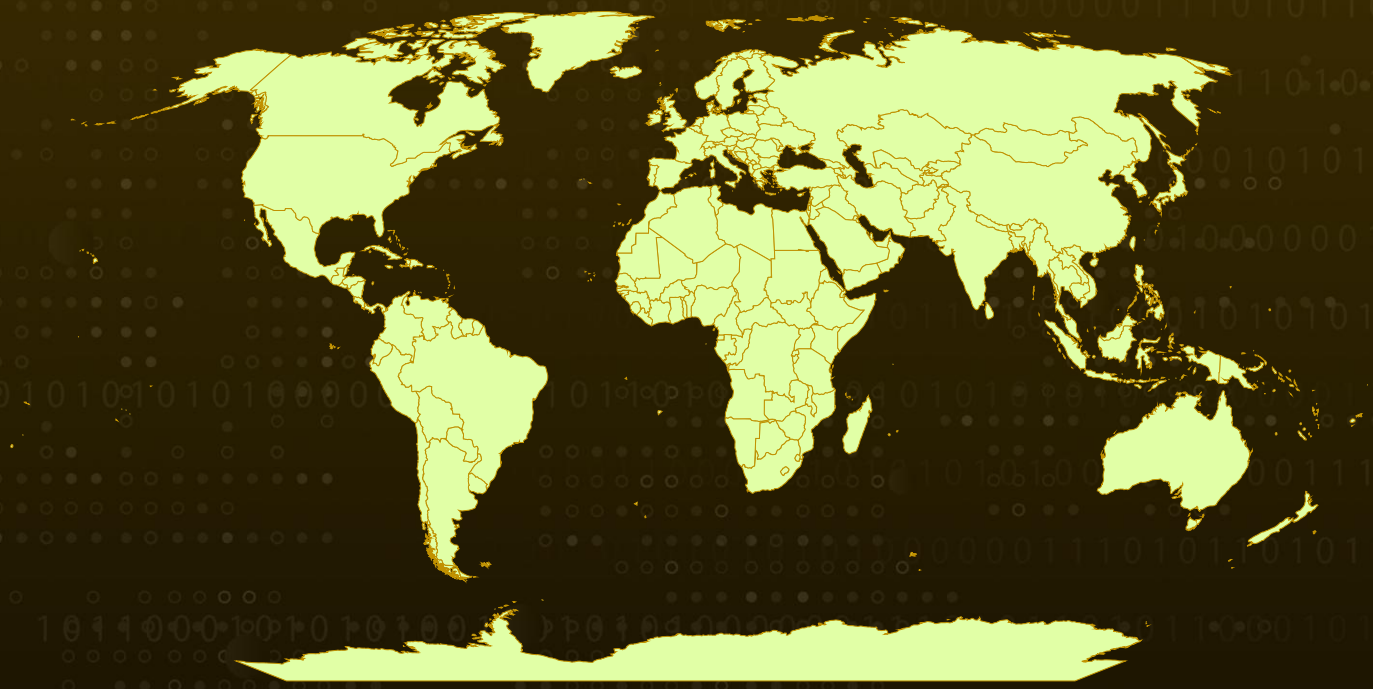
Date of Publication	Admiralty Code	TA Number
February 19, 2025	A1	TA2025048

Summary

First Seen: February 2025
Malware: Vgod Ransomware
Targeted Product: Windows
Targeted Region: Worldwide

Attack: A new and highly sophisticated ransomware strain Vgod, has surfaced posing a serious threat to Windows users. This malware employs a double extortion tactic encrypting files while stealing sensitive data leaving victims with the grim choice of paying a ransom or risking a data leak.

Attack Regions



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

Attack Details

#1 A new and formidable ransomware strain, dubbed Vgod, has recently emerged, posing a serious threat to Windows users. This malware employs a double extortion strategy, encrypting victims' files while simultaneously exfiltrating sensitive data. Failure to pay the ransom not only results in data loss but also risks the public exposure of confidential information.

#2 Vgod ransomware utilizes a hybrid encryption scheme, combining AES-256 for file encryption with RSA-4096 for key protection—an approach commonly used by advanced ransomware families such as Ryuk and LockBit.

#3 Upon infiltrating a system, Vgod swiftly encrypts files, appending the ".Vgod" extension to their original names. It then delivers a ransom note titled "Decryption Instructions.txt," detailing payment demands and recovery steps.

#4 To further intimidate victims, the malware modifies the desktop wallpaper, displaying a warning that the system has been compromised. The ransom note explicitly states that both file encryption and data exfiltration have occurred, reinforcing the severity of the attack. Threat actors behind Vgod ransomware primarily communicate with victims via email, instructing them on how to negotiate and make the ransom payment.

Recommendations

Deploy Endpoint Detection and Response (EDR) Solutions: Implement EDR tools to detect suspicious activities, such as unauthorized registry changes, process injections, and the creation of persistent tasks. Ensure rapid response and containment capabilities to neutralize threats as they occur.

Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Enhance Backup Strategies: Maintain offline, air-gapped, and immutable backups with multiple redundancy layers to ensure recovery after an attack.

Zero Trust Architecture: Implement a Zero Trust security model, where all users and devices are continuously authenticated and verified, regardless of their location within the network.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**TA0040** Impact	**T1059.001** PowerShell	**T1059** Command and Scripting Interpreter
T1106 Native API	**T1129** Shared Modules	**T1542.003** Bootkit	**T1542** Pre-OS Boot
T1574.002 DLL Side-Loading	**T1574** Hijack Execution Flow	**T1055** Process Injection	**T1548** Abuse Elevation Control Mechanism
T1014 Rootkit	**T1027.002** Software Packing	**T1027** Obfuscated Files or Information	**T1036** Masquerading
T1112 Modify Registry	**T1497.001** System Checks	**T1497** Virtualization/Sandbox Evasion	**T1564.001** Hidden Files and Directories
T1564 Hide Artifacts	**T1003** OS Credential Dumping	**T1552.001** Credentials In Files	**T1552** Unsecured Credentials

T1010 Application Window Discovery	**T1018** Remote System Discovery	**T1057** Process Discovery	**T1082** System Information Discovery
T1083 File and Directory Discovery	**T1518.001** Security Software Discovery	**T1518** Software Discovery	**T1005** Data from Local System
T1074 Data Staged	**T1114** Email Collection	**T1560** Archive Collected Data	**T1071** Application Layer Protocol
T1095 Non-Application Layer Protocol	**T1573** Encrypted Channel	**T1486** Data Encrypted for Impact	**T1496** Resource Hijacking

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	241c3b02a8e7d5a2b9c99574c28200df2a0f8c8bd7ba4d262e6aa8ed1211ba1f

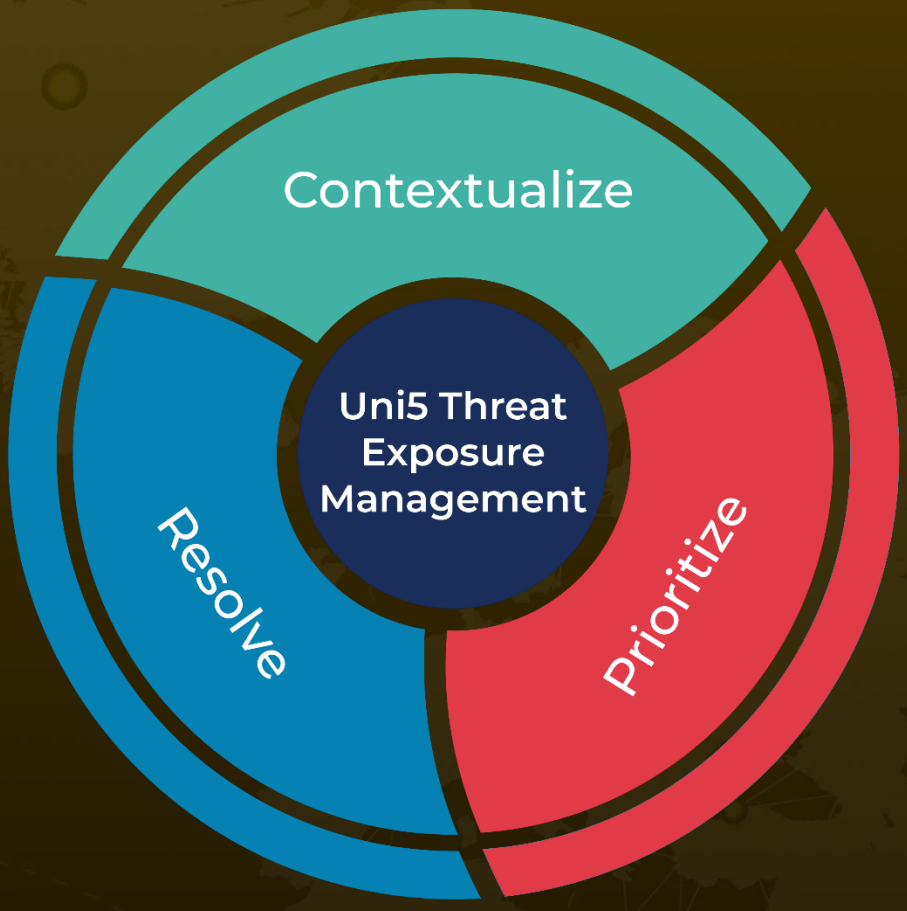
References

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

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

February 19, 2025 • 3:30 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com