Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

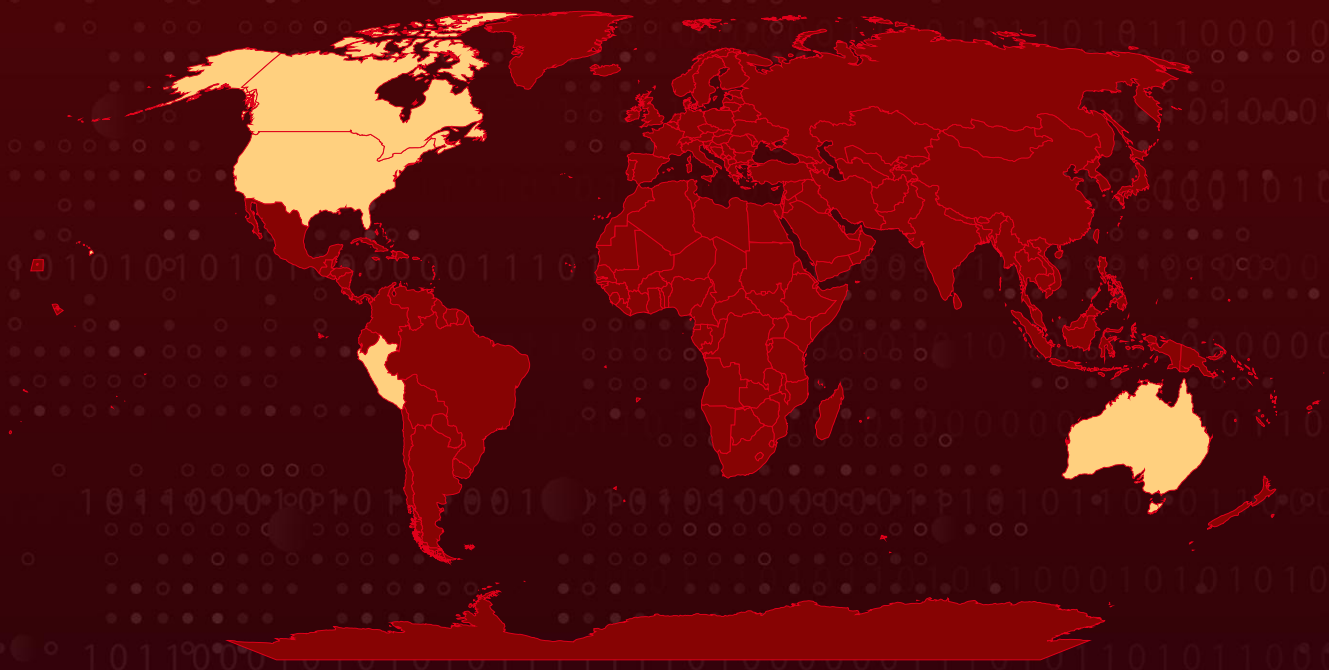
Anubis Ransomware Emerges with Destructive Encryption and Data Wiping

Date of Publication	Admiralty Code	TA Number
June 16, 2025	A1	TA2025189

Summary

First Seen: December 2024
Targeted Countries: United States, Canada, Australia, and Peru
Malware: Anubis Ransomware
Targeted Platforms: Windows, Linux, NAS, and ESXi (VMware) environments
Targeted Industries: Healthcare, Engineering, Construction, Manufacturing
Attack: Anubis is a destructive ransomware threat that emerged in December 2024, offering both file encryption and an optional wiper mode that renders data unrecoverable. Distributed via phishing, stolen credentials, and access brokers, it operates under a ransomware-as-a-service (RaaS) model. It uses ECIES encryption and customizable execution commands to target victims primarily in healthcare, construction, and engineering sectors. Its dual-purpose design suggests motives beyond financial gain, including sabotage or espionage.

Attack Regions



Attack Details

#1

Anubis is an emerging ransomware threat first observed in December 2024, notable for its dual-mode operation that includes both traditional file encryption and optional wiper functionality. It operates under a ransomware-as-a-service (RaaS) model, offering a customizable and destructive toolkit to affiliates and cybercriminals. It is primarily written in the Go (Golang) programming language, with some components and loaders observed in Python. Unlike conventional ransomware, Anubis includes a file-wiping mode, making it uniquely destructive and significantly increasing the impact level of its attacks.

#2

The ransomware is distributed primarily through spear-phishing campaigns, compromised credentials, and access purchased from initial access brokers. Once inside a network, it executes with elevated privileges and begins encrypting or destroying files, depending on the chosen payload mode. In its default encryption mode, Anubis uses ECIES (Elliptic Curve Integrated Encryption Scheme) to lock files. In wipe mode, it overwrites file contents, reducing them to 0 KB, rendering recovery impossible, even if the ransom is paid.

#3

During execution, Anubis deletes system shadow copies and disables various services to prevent recovery. It avoids specific system-critical directories to maintain OS stability long enough to deliver its ransom note and display its branding across the system, including desktop wallpaper changes. Attackers can customize execution using various command-line arguments, including /WIPEMODE, /KEY=, /PFAD=, /PATH=, and /elevated.

#4

The ransomware group promotes itself on darknet forums, offering flexible partnerships with high revenue shares to affiliates. It has primarily targeted organizations in the United States, Canada, Australia, and Peru, focusing on industries such as healthcare, engineering, and construction. The combination of its dual-threat model and wiper capability suggests that Anubis may be used not only for financial gain but also for data sabotage, potentially serving dual purposes in espionage or destructive operations.

Recommendations

Restrict access and patch systems: Grant administrative privileges sparingly and keep all security software up to date. Regularly scan for vulnerabilities and ensure endpoint protection can identify or block unknown malware.

Endpoint and Server Hardening: Deploy advanced endpoint detection and response (EDR) or extended detection and response (XDR) tools that can identify and block suspicious behaviors, including command-line flags such as /WIPEMODE and /elevated. Implement application control mechanisms like AppLocker to prevent execution of unauthorized binaries. Monitor for anomalies such as sudden file size reduction or mass file extensions being changed to .anubis.

Network Segmentation and Traffic Control: Segment the internal network to limit lateral movement between endpoints, especially for privileged and critical systems. Apply strict firewall rules and network policies to restrict outbound traffic, particularly to known malicious domains, Tor exit nodes, and suspected command-and-control (C2) infrastructure.

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 Anubis ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0004 Privilege Escalation
TA0007 Discovery	TA0040 Impact	T1485 Data Destruction	T1057 Process Discovery
T1566 Phishing	T1059 Command and Scripting Interpreter	T1078 Valid Accounts	T1059.003 Windows Command Shell

T1083 File and Directory Discovery	T1134.002 Create Process with Token	T1134 Access Token Manipulation	T1490 Inhibit System Recovery
T1486 Data Encrypted for Impact	T1489 Service Stop		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	98a76aacbaa0401bac7738ff966d8e1b0fe2d8599a266b111fdc932ce385c8ed
TOR Address	hxxp://om6q4a6cyipxvt7ioudxt24cw4oqu4yodmqzl25mqd2hgllymrgu4aqd[.]onion

Recent Breaches

https://pkwycon.com
https://twokingscasinokingsmountain.com
https://dg2design.com
https://gaynors.co.uk
https://summithhc.net
https://https://www.sye.com.pe
https://firstdefensefireprotection.com
https://poundroadmc.com.au

References

https://www.trendmicro.com/en_us/research/25/f/anubis-a-closer-look-at-an-emerging-ransomware.html

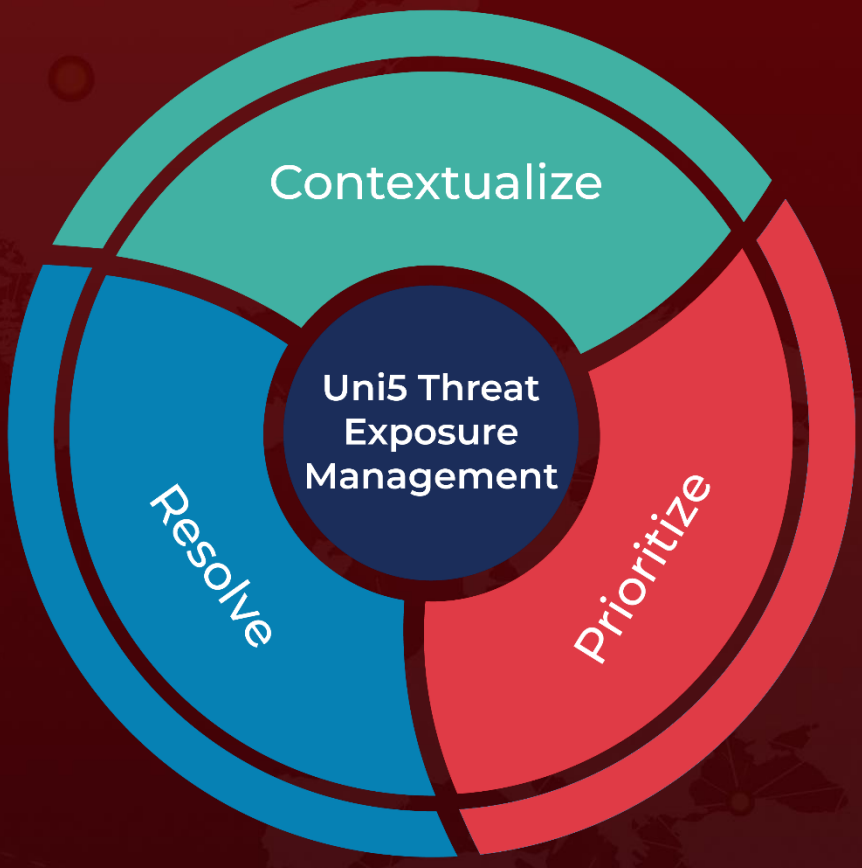
https://www.kelacyber.com/blog/anubis-a-new-ransomware-threat/

https://jumpcloud.com/blog/defending-linux-against-anubis-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

June 16, 2025 • 6:30 AM

More at www.hivepro.com