IMPORTANT CYBERSECURITY NEWS: ANUBIS RANSOMWARE ADDS WIPER TO DESTROY FILES BEYOND RECOVERY

Vairav Cyber Security News Report

Date: June 16, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A recent evolution in the Anubis ransomware-as-a-service (RaaS) operation has seen the addition of a destructive file-wiping capability. Beyond encrypting files and demanding a ransom, the malware now includes a wiper module activated via a /WIPEMODE flag. When triggered, it erases the contents of targeted files—reducing them to 0 KB—while preserving directory structure. This tactic ensures that even if victims pay, file recovery is impossible. The move significantly elevates pressure on victims and makes Anubis a more dangerous threat.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: Anubis is a relatively new ransomware strain, first seen December 2024, operating under a RaaS model. Initially used for file encryption and extortion, affiliates receive an 80% revenue share. According to Trend Micro, a wiper module was discovered in recent variants, designed to destroy file contents beyond recovery

Identification: It was identified by Trend Micro analysts in samples analyzed June 2025. A technical write-up confirmed the file-wiping feature under a specific command-line flag

Affected Entities/Industries: RaaS programs are opportunistic—potential targets include healthcare, critical infrastructure, SMBs, and enterprises. Recent dark-web listings show only eight named victims so far, but expansion is expected.

Potential Impact:

- Encrypted files cannot be recovered even with ransom payment.
- Loss of vital data, operational downtime, reputational damage, and regulatory as well as financial repercussions.

Exploitation Methods:

- Common initial access via phishing emails with malicious links or attachments.

- Uses ECIES encryption and deletes shadow copies, terminates interfering processes, avoids encrypting vital system directories.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Block execution of anomalous processes containing the string “wipe” or the /WIPEMODE flag.
- Monitor for abrupt deletion of file contents and use of vssadmin.exe or similar shadow-copy commands.
- Quarantine or isolate suspicious phishing email attachments.

Security Best Practices

- Enforce multi-layer phishing awareness training.
- Maintain offline, immutable backups (3-2-1 strategy).
- Ensure regular patching, disable macros via group policy, and limit removable media usage.

For Advanced Security Teams

- Deploy Endpoint Detection and Response (EDR) to flag deletion activity following encryption.
- Use SIEM to cross-correlate phishing attempts, privilege elevation logs, and wipe operations.
- Threat hunt for IOCs like missing VSS snapshots or unexpected .anubis extensions.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://www.bleepingcomputer.com/news/security/anubis-ransomware-adds-wiper-to-destroy-files-beyond-recovery/
- https://www.trendmicro.com/en_us/research/25/f/anubis-a-closer-look-at-an-emerging-ransomware.html

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com