CIRT.GY Guyana National Computer Incident Response Team

AL2025_32 Anubis Ransomware Adds Wiper to Destroy Files Beyond Recovery (June 17, 2025)

Description

The Anubis ransomware-as-a-service (RaaS) operation, first identified in December 2024, has evolved into a more destructive threat by incorporating a wiper module that permanently destroys targeted files, rendering recovery impossible even if the ransom is paid. This dual-threat approach combines traditional file encryption with a devastating file-wiping capability, significantly increasing pressure on victims to comply with ransom demands. The ransomware has primarily targeted industries such as healthcare, construction, and engineering across Australia, Canada, Peru, and the United States, with eight victims listed on its dark web extortion site as of June 2025.

Attack Details

Anubis gains initial access through spear-phishing emails, leveraging social engineering to trick users into executing malicious payloads. Once inside a system, the ransomware escalates privileges, conducts reconnaissance, and executes commands to delete Volume Shadow Copies using ‘vssadmin delete shadows /for=norealvolume /all /quiet’, eliminating built-in Windows recovery options. It employs the Elliptic Curve Integrated Encryption Scheme (ECIES) for file encryption, appending the “.anubis” extension to encrypted files and altering system icons with its logo. Additionally, it may change the desktop wallpaper to a custom image named wall.jpg. The standout feature of Anubis is its “wipe mode,” activated via the /WIPEMODE parameter. When enabled, this feature permanently erases file contents, reducing them to zero-byte shells while preserving filenames and directory structures. This ensures that even professional data recovery tools cannot restore the affected files, making Anubis not only a ransomware but also a wiper. The wiper functionality is designed to maximize damage and coerce victims into paying quickly by eliminating any hope of recovery without ransom payment. Anubis operates a flexible affiliate program, offering ransomware affiliates an 80% share of proceeds, data extortion affiliates 60%, and initial access brokers 50%. The ransomware is still under active development, with early samples identified as “Sphinx” before rebranding, suggesting potential for further enhancements.

Indicators of Compromise (IoCs)

A list of IoCs including file hash, and list of processes and services terminated can be found here: https://www.trendmicro.com/content/dam/trendmicro/global/en/research/25/f/anubis--a-closer-look-at-an-emerging-ransomware-with-built-in-wiper/Anubis_A_Closer_Look_at_a_Emerging_Ransomware_with_Built-in_Wiper_IOCs.txt

Remediation

To mitigate the threat posed by Anubis ransomware, organizations should adopt the following measures:

- User Awareness and Training
  - Educate employees on recognizing spear-phishing emails and suspicious attachments.
  - Train staff to avoid executing unknown files or scripts from unverified sources.
- Email Filtering and Security Gateways
  - Implement advanced email filters to detect phishing emails with malicious payloads.
  - Block emails containing suspicious URLs or attachments from unverified senders.
- Endpoint Protection
  - Deploy Endpoint Detection and Response (EDR) solutions to identify and block ransomware behaviors, such as file encryption or wiper activity.
  - Ensure real-time monitoring for unauthorized file modifications.
- Data Backup and Recovery
  - Maintain offline and immutable backups to ensure data recovery in case of wiping.
  - Regularly test backup and restoration processes to verify integrity.
- Network Monitoring
  - Monitor outbound traffic for connections to known malicious domains or dark web sites.
  - Detect and block unauthorized privilege escalation attempts.
- Incident Response Readiness
  - Develop and test an incident response plan to isolate infected systems and limit lateral movement.
  - Prepare for rapid containment and eradication of ransomware infections.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Trend Micro. (2025, June 13). Anubis: A Closer Look at an Emerging Ransomware with Built-in Wiper. Retrieved from https://www.trendmicro.com/en_us/research/25/f/anubis-a-closer-look-at-an-emerging-ransomware.html
- Toulas, B. (2025, June 14). Anubis ransomware adds wiper to destroy files beyond recovery. Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/security/anubis-ransomware-adds-wiper-to-destroy-files-beyond-recovery/