TIR-20250626 Anubis Ransomware

6/26/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

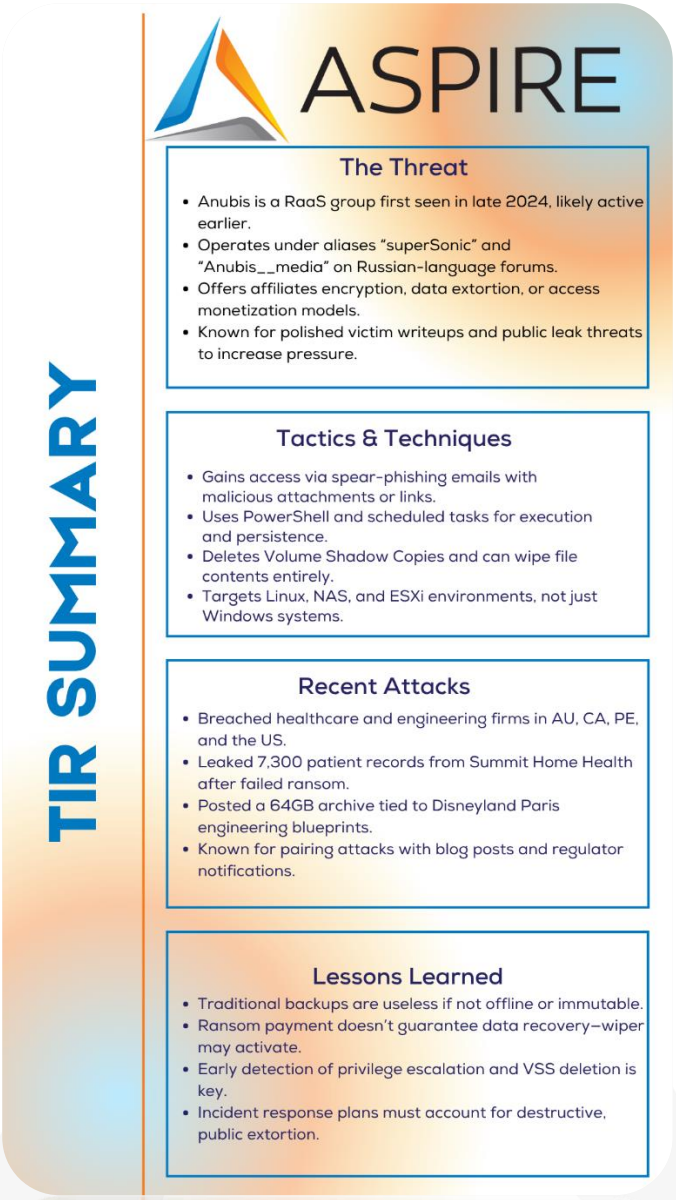
TABLE OF CONTENTS

EXECUTIVE SUMMARY

Anubis is an aggressive ransomware-as-a-service operation first observed in late 2024. It quickly gained traction by offering affiliates multiple monetization tracks, including data theft, encryption, and access brokering. What sets it apart is its destructive "wipe mode," which permanently deletes file contents (even after encryption) making data recovery impossible and increasing the pressure on victims to pay ransoms.

The group communicates in Russian on underground forums and actively recruits affiliates through RAMP and XSS, promising flexible revenue splits and tools that support both Windows and Linux environments, including ESXi and NAS. The ransomware has been linked to attacks across healthcare, engineering, and construction sectors in the U.S., Canada, Australia, and Peru.

Recent attacks, including a 64 GB breach of Disneyland Paris blueprints, show how Anubis focuses on reputational damage and public pressure. The threat actor uses a combination of double extortion, destructive encryption, and calculated media tactics, and the group's goal is to leave victims with few options and less time to respond. Let's look at Anubis, its tactics and techniques, and what to expect next from the threat actor.



ANUBIS RANSOMWARE

The first public sign of Anubis landed on X (formerly Twitter) in late December 2024, but evidence of compromise at an Australian healthcare clinic in mid-November hints at pilot attacks weeks earlier. Researchers soon tied the threat actor to forum aliases “superSonic” on RAMP and “Anubis__media” on XSS, both posting in Russian and pushing an aggressive marketing pitch that promised “non-standard methods” for getting as much as they can out of victims.

Forum ads say the malware uses ChaCha and ECIES, spreads on Windows networks, and ships with a web panel. That hints at builders with strong reverse-engineering chops, or code borrowed from the short-lived “Sphinx” ransomware.

Unlike older one-size-fits-all ransomware groups, Anubis rolled out an explicit multi-model business plan. Track one is classic ransomware - encrypt the data and demand payment for the key. Track two skips the encryption. Anubis bundles the stolen files into an “investigative article,” locks it behind a password, and waves the link at executives and customers to drum up public pressure. Track three moves further upstream, inviting access brokers to hand over valid credentials in exchange for half the eventual payout, after Anubis analysts craft custom pressure points.

Throughout early 2025 the operators refined their attack technique. Each leak notice is paired with a Q&A aimed at executives (“How do we remove our data?”) and journalists (“Will you grant an exclusive?”). This kind of message control shows the group knows how to work the media. It helps Anubis cut through the noise, even when bigger ransomware names are making headlines. By mid-June, their leak site featured a revamped blog, scheduled social media posts, and ticking countdowns. This was all designed to crank up the pressure on companies that weren’t responding.

Behind the theatrics is a setup built to stay online. They’ve got test decryption tools, Tor-based chat portals, and backup blogs that kick in if surface sites get taken down. To affiliates, it looks stable and reliable. To defenders, it means taking them down won’t be quick or easy. The speed with which new victims appear suggests that either recruitment is quick or individual affiliates churn through soft targets rapidly, banking on the wipe feature to boost payment odds.

TACTICS AND TECHNIQUES

Anubis ransomware operations follow a modular, multi-stage process designed for flexibility across diverse environments. After initial infection, the ransomware does not immediately execute encryption or destruction routines. Instead, it performs extensive environment reconnaissance to assess system configurations and active defenses. This includes checking for virtualization, endpoint detection agents, and domain membership, allowing the malware to tailor its actions based on the target's architecture and security posture. This adaptive behavior reduces the chances of early detection and increases operational effectiveness.

The malware is capable of disabling or bypassing a range of defensive controls before it begins its core functions. Samples have demonstrated the use of command-line execution flags that suppress errors and warnings, as well as kill-switches for endpoint agents and data protection tools. Certain variants have built-in logic to delay execution based on system uptime or CPU usage, an evasion strategy meant to outlast sandbox analysis.

Anubis also has a distinct focus on control and customization. Affiliates can toggle parameters to choose between encryption-only deployments, wipe-mode destructive attacks, or data exfiltration without encryption. In some samples, configuration files are fetched from remote command-and-control (C2) servers in real time, allowing operators to change payload behavior mid-operation. The malware can be deployed in stages—initial reconnaissance tools followed by the locker and wiper, which depends on the access level obtained and the affiliate's goals.

In Linux environments, particularly those involving NAS and ESXi infrastructure, the ransomware has a strong understanding of system internals. It interacts directly with mounted drives, uses shell scripts for automation, and takes advantage of weak access controls on shared volumes. Rather than relying on GUI-based escalation, it manipulates permission bits and uses cron jobs for persistence and timed execution. These tactics are specifically chosen to minimize noise in environments where GUI activity might be nonexistent or unmonitored.

Anubis also makes use of multiple persistence techniques depending on the operating system. In Windows systems, scheduled tasks and registry entries tied to user login are commonly used. On the other hand, Linux variants often modify system initialization

files or drop payloads into startup directories with obfuscated filenames. These platform-aware persistence methods allow infections to survive reboots or administrative cleanup attempts. Combined with the ability to run fully fileless in some configurations, this makes the malware harder to detect and remove once imbedded.

Recent Attacks

Anubis first showed up in healthcare. On November 13, 2024, Pound Road Medical Centre in Australia reported a breach after staff discovered systems locked and patient records stolen. Within six weeks the same campaign hit Summit Home Health in Canada, where 7,300 detailed medical records were leaked for free on a criminal forum when the firm allegedly refused to pay the demanded ransom. That early release showed how Anubis moves - full data publication rather than the partial leaks favored by older groups.

Construction and engineering companies followed. In Peru, Comercializadora S&E reported ransomware-related outages that matched artefacts later posted under the Anubis name. The group then attacked a U.S. contractor in February 2025; though unnamed in public feeds, evidence of blueprint exfiltration and a stalled negotiation timer appeared on the leak portal. Each breach notice came paired with an article dissecting the victim's market profile, compliance liabilities and even board-level contacts. This is all a part of the Anubis pressure playbook.

The biggest case hit in June 2025, when Anubis claimed it stole 64 GB of files from Disneyland Paris, including engineering plans for rides like Pirates of the Caribbean and Ratatouille. Screenshots of backstage maintenance tunnels and water-line schematics surfaced hours later. The incident showed Anubis isn't afraid to hit big-name brands and leak sensitive insider data to stir up public drama. Disneyland has yet to confirm details, but the episode pushed Anubis into mainstream coverage and sparked urgent audits across entertainment and theme-park operators.

In February 2025, there were 956 reported ransomware victims. A number that was up 87% from January. Analysts say newer groups like Anubis helped drive that spike with

aggressive leak-first tactics. Threat actors like Clop and Play still lead in volume, but Anubis stands out for how damaging each attack can be.

CONCLUSION

Anubis is not like older ransomware groups and it's not just locking files and asking for money. It's stealing data, encrypting systems, and in some cases, wiping everything out completely. That kind of damage is something no organization wants. Paying the ransom won't help if the data has already been destroyed. This group is pushing victims into a corner, and it's forcing security teams to rethink how they prepare and respond.

The group's operational maturity is evident in both its technical capabilities and its messaging tactics. Each attack is treated as a campaign, with coordinated leaks, and investigative-style writeups designed to attract media attention and embarrass targeted organizations. Their leaks are timed to spark legal trouble and draw unwanted attention from customers. For companies that rely on reputation or operate under strict compliance rules, the damage can escalate quickly.

Anubis blurs the line between straightforward cybercrime and something more deliberate. Its structure makes it easy for different types of affiliates to get involved and target organizations using a variety of systems, including Linux, NAS, and ESXi. The speed at which it's spreading points to a larger shift. More threat actors are likely to adopt this kind of operation, where extortion is combined with destruction to push past even well-prepared security teams.

Organizations must prepare for the possibility that some attacks will offer no viable recovery path. This requires shifting focus from encryption-only response to scenarios involving permanent data loss. Defenses should prioritize offline and immutable backups, widespread user phishing awareness, and early detection of privilege escalation or file manipulation behaviors.

ASPIRE'S RECOMMENDATIONS

Anubis can wipe systems completely and move across both Windows and Linux environments, including ESXi and NAS. Defenders need to plan for the possibility that nothing will be left to recover. The following recommendations are directly aligned with Anubis's tactics and infrastructure:

- **Deploy immutable and offline backups** – Ensure critical backups cannot be altered or deleted by ransomware. Anubis's wipe mode makes traditional backups ineffective if they remain connected or accessible during an attack.
- **Detect and block vssadmin usage** – Monitor endpoints for unauthorized use of vssadmin delete shadows, a known technique used by Anubis to eliminate restore points.
- **Restrict lateral movement in hybrid environments** – Harden ESXi, NAS, and Linux systems with strong segmentation, credential isolation, and audit logging. Anubis affiliates have demonstrated awareness of gaps in these often-overlooked areas.
- **Harden initial access points** – Enforce phishing-resistant multi-factor authentication and restrict macros and scripting languages that enable payload execution. Anubis typically gains entry via spear-phishing with malicious attachments or links.
- **Apply behavioral detection for file wiping and zero-byte writes** – Configure EDR or SIEM solutions to alert on patterns that match /WIPEMODE behavior, such as sudden file-size reductions across multiple directories.
- **Monitor for domain-wide propagation** attempts – Anubis attempts self-spreading across networks; detecting unusual credential use or rapid file access patterns can help flag early-stage propagation.
- **Flag abuse of built-in scripting tools** – Anubis often uses PowerShell, WMIC, and scheduled tasks to maintain persistence and disable defenses. Limit

scripting access to trusted users and monitor script execution across high-privilege accounts.

MITRE MAP

Anubis

Initial Access	T1566.001 - Phishing: Spearphishing Attachment
Execution	T1059.001 – Command and Scripting Interpreter: PowerShell
Persistence	T1547.001 – Boot or Logon Autostart Execution: Registry Run Key/ Startup Folder
Privilege Escalation	T1134.002 – Access Token Manipulation: Create Process with Token
Defense Evasion	T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control T1027 – Obfuscated Files or Information T1490 - Inhibit System Recovery
Discovery	T1083 – File and Directory Discovery T1018 – Remote System Discovery
Lateral Movement	T1021.001 - Remote Services: Remote Desktop Protocol
Impact	T1486 – Data Encrypted for Impact T1485 – Data Destruction

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Indicators of Compromise (IoCs)

MD5

- 06edda688a05fd0eaf3a14aba20568c4

SHA1

- 2137eeaa84e961b71f281bfc4c867e417253ad5f

SHA256

- 98a76aacbaa0401bac7738ff966d8e1b0fe2d8599a266b111fdc932ce385c8ed

Supporting Documentation

Beauty and the breach: Disneyland Paris data allegedly stolen by threat actors - Cyber Daily

Ransomware Groups Evolve Affiliate Models | Secureworks

Inside Anubis Ransomware: Tactics, Impact & Protection

Unboxing Anubis: Exploring the Stealthy Tactics of FIN7's Latest Backdoor

Anubis Ransomware Adds File-Wiping Capability - Infosecurity Magazine

Defending Linux Against Anubis Ransomware - JumpCloud

Anubis ransomware's wiper feature escalates risk for victims

Anubis: A New Ransomware Threat | KELA Cyber

Anubis Ransomware-as-a-Service Kit Adds Data Wiper

[Anubis Ransomware Lists Disneyland Paris as New Victim]

[Anubis Ransomware Packs a Wiper to Permanently Delete Files - SecurityWeek]

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.