ultraviolet

THREAT ADVISORY

The Ongoing Threat of Anubis Ransomware

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
July 29, 2026
TLP:GREEN

Executive Snapshot

Anubis is a ransomware-as-a-service (RaaS) operation that has been active since December 2024, when it emerged under an earlier test name, "Sphinx," before rebranding. It has since built out a functioning affiliate program on Russian-language cybercrime forums, offering negotiable revenue splits and multiple monetization paths beyond a standard ransom, including separate programs for data extortion and access sales. This flexible business model, combined with technical capabilities that go beyond typical encryption (namely, an optional file-wiping feature) makes Anubis a more destructive and adaptable threat than many of its RaaS peers.

The group gained significant attention in July 2026 after publicly claiming an attack on Coca-Cola's Fairlife dairy subsidiary, alleging theft of roughly 1 TB of data and later publishing that data after Coca-Cola did not meet its ransom deadline. The incident disrupted U.S. dairy production, required SEC disclosure, and ultimately led to confirmed data theft. This illustrates how a mid-sized subsidiary can become the entry point for an attack with enterprise-wide consequences. Looking at the victimology, it is worth noting that Anubis's victims are broken out across multiple, unrelated, sectors with seemingly no geographic boundaries. That spread, consistent with many RaaS operations, points to opportunistic targeting and indicates that organizations should not assume they are at a lower risk for Anubis attacks based on their individual industry.

- **Backups alone won't save you**: Anubis's wiper can permanently destroy files even after encryption, so offline, immutable backups are essential rather than optional.
- **Phishing is the entry point:** The group relies on spear-phishing for initial access, making email/web filtering and user training a frontline defense.
- **Watch for privilege escalation and shadow-copy deletion**: These are the clearest early warning signs of an active Anubis intrusion and should be tuned into EDR/SIEM alerting.
- **Assume dual extortion from day one:** Plan incident response, legal, and communications playbooks around both an operational outage and a data leak, since paying (or refusing to pay) doesn't guarantee data stays private.

TIDE Team Analysis

Anubis first appeared under the name "Sphinx" in late 2024 before rebranding; analysis found the Sphinx and Anubis binaries were nearly identical aside from the ransom-note generation function, suggesting a rebrand rather than a new codebase. By early 2025, the group was actively recruiting affiliates on Russian-language cybercrime forums (RAMP and XSS), offering negotiable revenue-share terms and additional monetization paths beyond standard ransom payments, including a data-extortion affiliate program and an access-monetization affiliate program.

Technically, Anubis operates as a command-line executable requiring parameters for its encryption key, privilege elevation, target/exclusion paths, and an optional destructive mode. The malware checks for administrative privileges and attempts to elevate itself to SYSTEM level, prompting the user interactively when elevation fails. This is behavior that suggests the tool is still under active development. Once running, it deletes Volume Shadow Copies via vssadmin to prevent file restoration, stops security-relevant services, and encrypts files using an Elliptic Curve Integrated Encryption Scheme implementation drawn from a public Go library. This code overlaps with other ransomware families such as EvilByte/Prince. Encrypted files are marked with the ".anubis" extension and a custom icon. Additionally, a ransom note ("RESTORE FILES.html") is dropped and contains threats to publicly leak data.

What separates Anubis from typical double-extortion crews is its optional wiper: a "/WIPEMODE" parameter permanently erases file contents rather than encrypting them, leaving files listed at 0 KB with no possibility of recovery. This capability apparently is reserved as leverage against victims who refuse to pay.

ADVERSARY PROFILE

Anubis

Anubis Ransomware / Sphinx

ALSO	superSonic, Anubis__media
ATTRIBUTION	**Russia-linked (unattributed to a state),** Not applicable, financially motivated criminal group
ACTIVE SINCE	2024 (2+ years)
MOTIVES	**Financial extortion** **Data theft** **Data destruction**
INDUSTRIES	Largely indiscriminate like many RaaS operations
COUNTRIES	United States, United Kingdom, Australia, Canada, France, the Netherlands, and New Zealand

NOTABLE TTPs	
01	Spear-phishing for initial access
02	Command-line execution with configurable parameters
03	Privilege escalation to SYSTEM level
04	Valid account abuse for defense evasion
05	File and directory discovery before encryption
06	Volume shadow copy deletion to block recovery
07	ECIES-based file encryption
08	Optional wipe mode for irreversible data destruction

In the Coca-Cola Fairlife case, Coca-Cola disclosed on July 16, 2026 that a ransomware incident had disrupted Fairlife's U.S. dairy production, without naming the actor at the time. Days later, the Anubis gang placed Fairlife on its dark web leak site, claimed to have stolen roughly 1 TB of corporate data, and stated it had fully encrypted Fairlife's Nutanix infrastructure. The actor gave the company until the end of the week to negotiate. Anubis told BleepingComputer it had breached the network roughly a week before Coca-Cola's public disclosure and that Coca-Cola reported the incident rather than following the extortion instructions left on the network. Coca-Cola confirmed data theft after the leak deadline passed and Anubis published the files.

Why It Matters

The Fairlife incident demonstrates how the impact from ransomware attacks does not end once systems are restored. Even when a victim recovers operations quickly, the parallel threat of published stolen data extends legal, regulatory, and reputational exposure well beyond the technical outage. This includes potential SEC disclosure obligations, customer/employee notification duties, and litigation risk. For any organization, Anubis's blended model (encryption, exfiltration, and optional destructive wipe) means that backup strategy alone is insufficient; data governance, third-party/subsidiary security posture, and incident communication planning are equally critical. Their targeting pattern (multiple sectors, multiple countries) means no organization or industry should assume it is out of scope.

Beyond the immediate technical disruption, the Fairlife case highlights how ransomware has become a business continuity problem as much as a security one. Coca-Cola's ability to keep Canadian operations running while U.S. production was halted demonstrates the value of segmentation and contingency planning, but it also shows how quickly an attack on one subsidiary can ripple into supply chain and production concerns for a much larger parent company. Stakeholders should recognize that brand and consumer trust are now directly tied to how a company handles the data-theft side of an incident, not just how fast IT can bring systems back online. A slow or unclear public response can do as much reputational damage as the breach itself.

In alignment with the FBI, UltraViolet Cyber does not recommend paying ransoms. However, organizations should have contingency plans in place to deal with the risk of subsequent data leakage. Leadership teams need to have this conversation before an attack happens, not during one, since decisions made under a ransom deadline are rarely as sound as those made in advance. Cyber insurance terms, legal counsel availability, and law enforcement coordination should all be worked out ahead of time rather than figured out on the fly.

Finally, the involvement of a major public company's SEC filing over what began as a subsidiary-level IT disruption is a reminder that materiality thresholds for cyber incidents are lower than many boards assume. Even attacks that don't touch the parent company's core systems directly can trigger disclosure obligations and investor scrutiny, making this a governance issue as well as a technical one.

How to Respond

- **Harden identity and access controls:** Enforce least privilege, monitor for anomalous privilege-escalation attempts, and restrict access to core infrastructure (e.g., hypervisor/virtualization platforms such as Nutanix).
- **Maintain immutable, offline backups:** Critical given Anubis's wiper capability, which can destroy data beyond recovery even after encryption.
- **Strengthen email/web filtering and user training:** Phishing remains the primary initial access vector.
- **Deploy EDR/SIEM tuned for ransomware precursors:** Specifically shadow-copy deletion (vssadmin), mass service stops, and suspicious command-line parameters resembling Anubis's known syntax (e.g., "/KEY=", "/WIPEMODE", and "/elevated").
- **Prepare a joint legal/communications/incident-response playbook:** Assume dual extortion (encryption + leak) and pre-plan regulatory disclosure, customer notification, and negotiation-refusal procedures.
- **Extend scrutiny to subsidiaries and less-visible business units**: Fairlife, a Coca-Cola subsidiary, was the entry point, illustrating that smaller or less centrally managed units can be the weak link.
- **Do not assume payment guarantees data deletion or non-disclosure:** Treat every exfiltration as a permanent breach for planning purposes.

What UltraViolet Cyber is Doing

- Tracking new CVEs and high impact vulnerabilities, analyzing and deploying public Proof-Of-Concept code against custom built targets.
- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber