Smarttech
YOUR 24/7 SECURITY PARTNER

THREAT ACTOR SPOTLIGHT

Published 4 September 2026
Threat Intelligence Team

ANUBIS

Ransomware-as-a-service operation that rebranded from "Sphinx" in late 2024. Combines standard double extortion with an optional, irreversible data-wipe mode, and pairs both with a media pressure campaign rather than a plain leak-site posting.

Sphinx (former name) | .anubis extension | RaaS, flexible affiliate splits

RISK RATING	ACTIVE SINCE	BUSINESS MODEL	PRIMARY VECTOR	DISTINCTIVE FEATURE
Critical	2024	RaaS, negotiable affiliate splits	CitrixBleed 2, infostealer credentials	Optional data-wipe mode, no decryption

ATTACK CHAIN

1. **Initial Access**
   Exploits CitrixBleed 2 and other edge vulnerabilities, or buys infostealer-harvested credentials.
2. **Access Brokering**
   Runs a flexible affiliate model supporting encryption, data-theft-only, or access-resale as separate monetization paths.
3. **Data Theft**
   Exfiltrates sensitive records first, before deciding whether to encrypt, wipe, or simply extort.
4. **Optional Destruction**
   Can trigger an irreversible wipe mode instead of encryption, removing recovery as a guaranteed outcome.
5. **Media Pressure Campaign**
   Publishes a styled "investigative article" on stolen data, then promotes it to journalists and on X if unpaid.

MITRE ATT&CK MAPPING

ID	TECHNIQUE
T1190	Exploit public-facing application (CitrixBleed 2)
T1078	Valid accounts (infostealer-purchased credentials)
T1567	Exfiltration over web service
T1486	Data encrypted for impact (standard mode)
T1485	Data destruction (optional wipe mode)
T1591.001	Gather victim org information (media/journalist pressure campaign)

SECTOR BY SECTOR Summary

Healthcare
Its most-hit sector, headlined by a 293GB breach of a US health system that exposed surgical images and Social Security numbers.

Manufacturing
A steady secondary target, consistent with the group's broad, opportunistic targeting rather than a specific niche.

Consumer Goods & Beverage
Landed its highest-profile hit here, claiming roughly 1TB stolen from a major beverage brand's dairy subsidiary.

Smarttech
YOUR 24/7 SECURITY PARTNER

ANUBIS

ORIGIN & EVOLUTION

Rebranded from an earlier operation called Sphinx in late 2024, and runs a flexible affiliate model that lets partners choose encryption, data-theft-only, or access-resale as separate paths rather than one fixed playbook. Recent trackers show activity dropping roughly 50% month over month, suggesting the group may be past its peak.

THREAT LANDSCAPE CONTEXT

A rebrand of Sphinx rather than a clean-slate group, which explains the operational maturity behind its flexible affiliate model. Its "wipe mode" pressure tactic distinguishes it from most peers, who rely on encryption or leak threats alone.

SIGNATURE TRADECRAFT

Exploits CitrixBleed 2 and similar edge vulnerabilities, or buys infostealer-harvested credentials, then exfiltrates data before deciding whether to encrypt, wipe, or simply extort. Its most unusual feature is an optional, irreversible wipe mode instead of encryption, paired with a media pressure campaign that offers journalists early access to stolen data.

ANALYST OUTLOOK

Reported activity has dropped roughly 50% month over month on at least one tracker recently, suggesting Anubis may be past its peak. Its wipe-mode threat remains a real differentiator worth monitoring even if overall victim counts continue declining.

NOTABLE INCIDENTS

Coca-Cola's Fairlife subsidiary

July 2026

Claimed roughly 1TB of stolen data and encryption of Nutanix infrastructure at the dairy subsidiary, disrupting US production and forcing an SEC disclosure.

Singing River Health System

Exploited a React2Shell vulnerability to breach the legal data provider, exposing records tied to government and judicial staff.

Winn-Dixie

August 2026

Claimed responsibility for a breach of the US grocery retailer, threatening to expose sensitive data unless paid.