



BRIEF FOCUS · MEDUSA · RANSOMWARE

Medusa Ransomware: Why Rapid Exploitation and Data Theft Demand a Prevention-First Strategy

An updated joint advisory from CISA, the FBI, and HHS reports that Medusa has now impacted more than 500 victims across critical infrastructure sectors. Affiliates exploit exposed systems and steal data before encryption begins.

THREAT ACTOR

**Medusa (first identified
June 2021)**

ATTRIBUTED TO

**Ransomware-
as-a-Service
Double extortion**

PLATFORMS

**Vulnerable internet-
facing systems
Initial access brokers**

ADVISORY

**CISA · FBI · HHS
Updated Aug 18, 2026**

SECTORS AT RISK

Medical · Education · Legal · Insurance · Technology · Manufacturing

THE ACTOR

Who Is Medusa?

On August 18, 2026, CISA, the FBI, and the U.S. Department of Health and Human Services updated their joint Cybersecurity Advisory on Medusa ransomware. As of April 2026, Medusa developers and affiliates had impacted more than 500 victims across critical infrastructure sectors, up from more than 300 reported as of February 2025. Affected industries include medical, education, legal, insurance, technology, and manufacturing.

First identified in June 2021, Medusa has evolved into a ransomware-as-a-service (RaaS) operation supported by affiliates and initial access brokers. Medusa uses double extortion, encrypting victim systems while threatening to publish stolen data if payment is not made. It should not be confused with MedusaLocker or Medusa mobile malware, which are separate threats.

INITIAL ACCESS

Rapid Exploitation Increases the Risk

Exploiting Vulnerabilities Before Defenders Can Respond: Medusa actors opportunistically target organizations running vulnerable internet-facing systems and services. Rather than relying on a single method of entry, affiliates exploit known

vulnerabilities and can also obtain access through initial access brokers. This approach allows Medusa to capitalize on exposed infrastructure and unpatched systems while reducing the time defenders have to identify and contain an intrusion.

THREAT SNAPSHOT

JUN 2021

First identified, before evolving into a RaaS operation

500+

Victims impacted as of April 2026, up from 300+ in February 2025

6 SECTORS

Affected industries named in the updated advisory

EVOLVING TTPs

What Makes Medusa Dangerous

Medusa actors commonly obtain initial access through vulnerable internet-facing systems and access purchased from initial access brokers. Once inside, they use credential-stealing tools, PowerShell obfuscation, remote monitoring and management software, and tunneling utilities to establish persistence and move laterally while attempting to evade detection.

The updated advisory identifies tools including Mimikatz, Ligolo-ng, Nezha, MeshAgent, AnyDesk, Atera,

BeyondTrust, ConnectWise, SimpleHelp, Splashtop, and other legitimate remote administration utilities. Actors have also hidden payloads in folders excluded from Windows Defender scanning, deleted command history, installed web shells, and used legitimate Windows functionality during post-compromise activity. Data is exfiltrated before encryption, giving Medusa additional leverage even when organizations are able to restore affected systems.

TECHNOLOGIES TARGETED IN OBSERVED QTFY ACTIVITY

Mimikatz

Ligolo-ng

Nezha

MeshAgent

AnyDesk

Atera

BeyondTrust

ConnectWise

SimpleHelp

Splashtop

PowerShell

THE BLACKFOG PERSPECTIVE

BlackFog's Real-Time Defense For Risk Mitigation

Stops data theft before encryption

Medusa relies on stolen information as leverage during extortion. BlackFog's anti data exfiltration (ADX) technology helps prevent unauthorized outbound data transfers before attackers can use sensitive information against the organization.

Detects abuse of legitimate applications

Medusa regularly uses legitimate remote administration and system management tools to blend into normal enterprise activity. Behavioral analysis helps identify suspicious use of trusted applications rather than relying solely on known malware signatures.

Responds to evolving attack techniques

Medusa's exploitation of vulnerable internet-facing infrastructure means organizations cannot rely exclusively on traditional signature-based detection. BlackFog's behavioral approach focuses on abnormal activity and data movement as attacks evolve.

Limits the impact of compromised credentials

Credential theft and remote access play an important role in Medusa intrusions. Behavioral monitoring helps identify unusual activity associated with compromised accounts and devices before attackers can extend their reach across the network.

SIDE BY SIDE

BlackFog Vs Medusa Ransomware

THREAT VECTOR	MEDUSA TACTIC	BLACKFOG COUNTERMEASURE
Initial Access	Exploitation of vulnerable internet-facing systems and purchased access	Behavioral detection, access anomaly monitoring
Credential Theft	Mimikatz and credential harvesting techniques	Behavioral monitoring, credential abuse detection
Lateral Movement	RDP, remote management tools, tunneling and administrative utilities	Behavioral analytics, traffic control, rapid containment
Data Exfiltration	Theft of sensitive information before encryption	Anti data exfiltration (ADX)
Ransom & Extortion	Theft of sensitive information before encryption	Data loss prevention, incident containment, forensic readiness

ABOUT BLACKFOG

BlackFog is the category-defining vendor in anti data exfiltration (ADX). Founded in 2015, the company invented ADX on the thesis that the endpoint is the only control point capable of stopping data from leaving an organization, an architectural bet that has now been validated across three exfiltration vectors: ransomware, Shadow AI, and autonomous AI agents. BlackFog's endpoint-native platform protects more than 500 enterprises, government agencies, and critical infrastructure operators worldwide. The company is the publisher of the annual [State of Ransomware report](#) and the BlackFog/Sapio [Shadow AI Research](#), the most-cited primary research in the category. BlackFog's recognition includes the teiss Awards 2026, the AI Excellence Award 2026, the Cybersecurity Excellence Awards 2026, and the Cybersecurity Breakthrough Award 2026. BlackFog is headquartered in San Francisco, with international operations in London and Belfast. Learn more at blackfog.com.