CSAI Foundation

Cloud Security Alliance AI Safety Initiative

Storm-1175: Zero-Day Exploit Chains in Medusa Ransomware Attacks

China-Linked Affiliate Leverages Nation-State-Grade Capability Against Healthcare Infrastructure

Unofficial AI-assisted Research

2026-04-07

Key Takeaways

- Microsoft Threat Intelligence has publicly attributed Storm-1175 as a China-based, financially motivated cybercriminal group operating as an affiliate of the Medusa ransomware-as-a-service (RaaS) platform, targeting healthcare, education, professional services, and finance organizations across Australia, the United Kingdom, and the United States [1].
- Storm-1175 has demonstrated zero-day exploitation capability, weaponizing CVE-2025-10035 (Fortra GoAnywhere MFT, CVSS 10.0) and CVE-2026-23760 (SmarterTools SmarterMail) approximately one week before public disclosure — a capability that Microsoft and other researchers have characterized as historically associated with state-sponsored actors rather than financially motivated criminal groups [1][6].
- The group's operational tempo appears to significantly exceed typical ransomware timelines: intrusion timelines span five to six days from initial access to ransomware deployment, with some incidents completing in under 24 hours [2].
- Healthcare organizations have been prominent and repeatedly confirmed Medusa targets, with incidents in 2025 and 2026 including an estimated 1.27 million patients exposed through the SimonMed breach alone, alongside additional victims whose full patient impact has not yet been publicly disclosed [3][7][4].
- CSA assesses that this actor's profile — a China-nexus group combining rapid zero-day weaponization with a mature RaaS platform — represents a meaningful escalation in the ransomware threat landscape and warrants immediate attention from healthcare and critical infrastructure security teams [1][3].

Background

On April 6, 2026, Microsoft Threat Intelligence published a detailed profile of Storm-1175, a China-based financially motivated cybercriminal group that has operated as an affiliate of the Medusa ransomware platform since at least 2023 [1]. The publication arrived against a backdrop of escalating Medusa activity: a joint advisory from CISA, the FBI, and MS-ISAC issued on March 12, 2025 documented more

than 300 Medusa victims across critical infrastructure sectors, and noted that the group claimed more than 40 victims in January and February 2025 alone — nearly double the volume recorded during the same period in 2024 [3][5].

The Medusa ransomware ecosystem itself is a mature, double-extortion RaaS platform first identified in June 2021. Microsoft assesses Medusa's core developers to be Russia-linked, based on behavioral indicators including avoidance of Commonwealth of Independent States targets and Russian-language forum activity [1] — a classification distinct from Storm-1175, which represents one of multiple affiliated operators deploying the platform [2]. This division between infrastructure provider and operational affiliate is an important analytical distinction: Storm-1175 is not Medusa's developer, but a capable and high-tempo operator that has recently demonstrated access to exploit capabilities that go beyond what typical RaaS affiliates have historically deployed.

Storm-1175 follows Microsoft's "Storm" naming taxonomy, which the company reserves for emerging or unattributed threat actors. The China-based classification reflects operational infrastructure and behavioral indicators rather than a confirmed nexus to the People's Liberation Army or the Ministry of State Security, and Microsoft characterizes the group as financially motivated rather than state-directed [1][2]. Nevertheless, the actor's apparent access to zero-day vulnerabilities — and the precision and velocity with which it deploys them — has led Microsoft's threat intelligence team to examine whether Storm-1175 may be sourcing exploits from specialized brokers who serve both state-sponsored and criminal markets [1].

Security Analysis

Exploit Chain Architecture and Zero-Day Capability

Storm-1175's defining operational characteristic is the systematic targeting of internet-facing web applications at extreme velocity. Since 2023, the group has exploited more than 16 vulnerabilities across at least 10 distinct products, including Microsoft Exchange Server, PaperCut NG/MF, Ivanti Connect Secure, ConnectWise ScreenConnect, JetBrains TeamCity, SimpleHelp, CrushFTP, and SmarterMail [1][2]. The breadth and currency of this exploit inventory is, as researchers at Microsoft and BleepingComputer have characterized it, unusual for a RaaS affiliate [1][2], and suggests a level of resourcing — whether through internal development, exploit broker procurement, or state-adjacent access — that distinguishes Storm-1175 from conventional ransomware operators.

The group's two confirmed zero-day exploitations represent the most significant escalation in its profile. CVE-2025-10035, a maximum-severity (CVSS 10.0) deserialization vulnerability in Fortra's GoAnywhere Managed File Transfer product, was exploited by Storm-1175 on or around September 10–11, 2025. Fortra did not disclose the vulnerability or release a patch until September 18, 2025, placing the actor's exploitation approximately one week ahead of public knowledge [1]. CISA subsequently added CVE-2025-10035 to its Known Exploited Vulnerabilities catalog on September 29, 2025. A second zero-day, CVE-2026-23760 — an authentication bypass in SmarterTools SmarterMail — was similarly exploited before public disclosure, again by roughly one week [2]. Pre-disclosure exploitation of internet-accessible enterprise software at this scale has historically been associated with nation-state-sponsored actors with dedicated vulnerability research programs — a characterization Microsoft and other researchers have applied to contextualize this development [1][6] — and its appearance in the toolset of a financially motivated affiliate marks a notable shift.

The broader context reinforces the significance: security researchers have documented a marked increase in zero-day exploitation throughout 2025, with financially motivated threat actors — including ransomware operators — exploiting zero-days at nearly double the rate observed in 2024 [6]. Whether Storm-1175's capability stems from direct state support, black-market exploit procurement, or an informal connection to China's extensive domestic vulnerability research ecosystem remains an open analytical question. Microsoft's April 2026 reporting describes an "evolution toward exploit brokers or expanded development capability" [1], suggesting the company assesses the zero-day access as a relatively recent development rather than a longstanding capability.

Post-Compromise Tradecraft

Once initial access is established via exploit, Storm-1175 moves with deliberate efficiency. The actor creates unauthorized user accounts and deploys web shells within compromised applications to establish persistent footholds [1]. For lateral movement and remote access, it leverages a wide array of legitimate remote monitoring and management (RMM) tools — including Atera, Level, N-able, DWAgent, MeshAgent, ConnectWise ScreenConnect, AnyDesk, and SimpleHelp — as well as Cloudflare tunnels for covert command-and-control communications. This heavy reliance on legitimate tooling blends into normal administrative traffic, complicating detection based on process or network signatures alone [1] [2].

Credential harvesting forms a central component of Storm-1175's lateral movement strategy. The actor employs Mimikatz, direct LSASS memory dumping via Task Manager, WDigest registry manipulation to force cleartext credential caching, and Veeam password recovery scripts — a combination that effectively grants access to domain-wide credentials and backup infrastructure simultaneously [1]. Prior to ransomware deployment, the group exfiltrates data using Rclone (synchronized to attacker-controlled

cloud storage) and Bandizip (for archive compression), establishing the evidentiary basis for subsequent extortion demands. Defense evasion measures include configuring Microsoft Defender Antivirus exclusions and modifying Windows Firewall policies to enable RDP access across the network [1]. The ransomware payload itself — Medusa's `gaze.exe` encryptor, using AES-256 encryption and appending the `.medusa` extension — is distributed across the network via PDQ Deployer [3].

Healthcare Sector Impact

Healthcare organizations have emerged as prominent Medusa targets, a pattern that the CISA advisory and subsequent reporting have documented in considerable detail. The sector's combination of legacy infrastructure, federated IT environments, and operationally critical systems — in which service disruption directly affects patient safety — makes it a high-value target both for extortion leverage and for the likelihood that organizations will pay rather than endure extended downtime [3][4].

Confirmed Medusa victims in the healthcare sector include SimonMed Imaging, one of the largest U.S. medical imaging providers, from which Medusa operators claimed to have exfiltrated approximately 2 terabytes of data affecting an estimated 1.27 million patients in January 2025, with a reported ransom demand of $1 million [7]. Bell Ambulance, a Wisconsin-based ambulance services provider, was struck in February 2025 with approximately 219.5 GB of data stolen and a $400,000 demand [12]. In the United Kingdom, HCRG Care Group, an independent healthcare services company, suffered the exfiltration of approximately 2.3 terabytes of data in February 2025, with a demand of $2 million [13]. The University of Mississippi Medical Center — the state's largest hospital, with 10,000 employees and 35 clinic locations — experienced a Medusa ransomware incident in late February 2026 that forced nine days of system outages, the closure of all outpatient clinics, and the rescheduling of cancer infusion patients; the institution reverted to paper-based operations throughout the incident [8]. Medusa publicly claimed the UMMC attack on March 13, 2026, posting a $800,000 ransom demand with a deadline of March 20 [8].

The Medusa platform's extortion model adds a layer of complexity beyond standard double extortion. The FBI's March 2025 advisory documented at least one instance of triple extortion, in which a victim who had paid the ransom was subsequently contacted by a purportedly separate Medusa actor claiming the original negotiator had stolen the payment — and demanding additional funds for the "true decryptor" [3]. This tactic undermines victim confidence in payment as a recovery mechanism and increases the imperative for organizations to maintain offline, tested backups as their primary recovery posture.

The Nation-State–Criminal Convergence

Storm-1175 is not an isolated case. The broader ransomware ecosystem in 2025 and 2026 has demonstrated a meaningful convergence between the exploit capabilities historically associated with state-sponsored actors and the monetization models of criminal RaaS platforms. Microsoft has separately documented Storm-2603, a China-backed group that exploited SharePoint zero-day vulnerabilities (the "ToolShell" chain) and subsequently deployed LockBit Black and Warlock ransomware, blending state-sponsored intrusion tradecraft with direct ransomware monetization [9]. North Korea's Lazarus Group has similarly been documented operating as a Medusa RaaS affiliate, deploying Medusa ransomware against Middle Eastern and U.S. healthcare organizations and nonprofits between November 2025 and February 2026, combining custom backdoor tooling with the Medusa platform [10].

The significance of this convergence extends beyond attribution complexity. When financially motivated ransomware operations can access pre-disclosure vulnerability intelligence — whether through state-adjacent exploit markets, informal intelligence sharing, or direct state support — the effective warning time available to defenders is significantly compressed. The assumption that a disclosed vulnerability will be exploited over a period of weeks or months no longer reliably holds for high-value internet-facing products, as this case suggests. Healthcare organizations and other critical infrastructure operators must now treat their internet-facing perimeter as potentially exposed to zero-day conditions at all times, not merely in the period following a CVE announcement.

Recommendations

Immediate Actions

Organizations running any of the products identified in Storm-1175's documented exploit inventory should treat patch application as emergency priority. This includes Fortra GoAnywhere MFT (CVE-2025-10035), SmarterTools SmarterMail (CVE-2026-23760), ConnectWise ScreenConnect (CVE-2024-1709), Ivanti Connect Secure (CVE-2023-46805, CVE-2024-21887), JetBrains TeamCity (CVE-2024-27198, CVE-2024-27199), and SimpleHelp (CVE-2024-57726, CVE-2024-57727, CVE-2024-57728). Organizations should also review CISA's Known Exploited Vulnerabilities catalog as an authoritative, continuously updated reference for vulnerabilities under active exploitation.

Internet-facing systems that cannot be immediately patched should be isolated behind additional network controls or taken offline if operationally feasible. Given Storm-1175's documented exploitation of managed file transfer, email server, and remote access products, these categories deserve particular scrutiny. Web application firewall rules and IDS/IPS signatures for the known CVEs should be deployed or refreshed immediately.

Short-Term Mitigations

Security teams should prioritize detection engineering for the tools and techniques Storm-1175 is known to deploy after gaining initial access. Behavioral detection of Mimikatz, LSASS memory access via Task Manager, WDigest registry modification, and Rclone data staging should be enabled and alerting on. Legitimate RMM tools including AnyDesk, SimpleHelp, ConnectWise ScreenConnect, and Atera should be subject to strict allowlisting, with any instance running outside of approved administrative workflows treated as a high-severity alert. Cloudflare tunnel processes running on servers that do not normally use them warrant immediate investigation.

Network segmentation between internet-facing systems and internal infrastructure can meaningfully slow Storm-1175's lateral movement, even if initial access cannot be prevented. Given the actor's documented use of PDQ Deployer for network-wide ransomware distribution, strict controls on administrative deployment tooling — including multi-factor authentication and session logging for all privileged access — are warranted. Backup systems, including Veeam infrastructure, should be hardened with distinct credential sets that are not accessible from domain administrator accounts, given the actor's specific targeting of Veeam credential recovery.

Strategic Considerations

The convergence of zero-day capability with financially motivated ransomware operations requires a recalibration of how organizations assess their vulnerability window. The evidence presented in this note suggests the traditional patch cadence assumption — that a vulnerability disclosed today will be exploited in weeks or months — no longer reliably holds for high-value internet-facing products. Healthcare organizations in particular should evaluate whether compensating controls (network segmentation, web application firewalls, behavior-based detection) can reduce the effective attack surface for critical perimeter systems during the period between a vulnerability's existence and its remediation.

Incident response planning should account for Medusa's documented triple extortion tactic and the possibility that payment does not guarantee recovery or confidentiality. Offline, air-gapped backup environments tested for healthcare-specific recovery scenarios — including electronic health record

systems, medical imaging infrastructure, and patient scheduling — represent a highly reliable recovery mechanism and substantially improve organizations' negotiating posture against extortion pressure [3]. This approach is directly recommended in the CISA, FBI, and MS-ISAC advisory on Medusa ransomware.

Finally, the healthcare sector should engage with the H-ISAC and HHS HC3 (Health Sector Cybersecurity Coordination Center) for sector-specific threat intelligence sharing. The CISA and FBI have released formal advisories on Medusa ransomware, and the American Hospital Association has issued direct warnings to member organizations [4][11]. These resources represent the current frontier of publicly available threat intelligence on this actor and should be integrated into security program awareness and tabletop exercise scenarios.

CSA Resource Alignment

This incident and the threat actor pattern it represents connect directly to several active CSA research and framework initiatives.

The **MAESTRO framework** (Agentic AI Threat Modeling) offers a modeling approach that parallels the challenge Storm-1175 presents for detection: the group's combination of automated exploit deployment, living-off-the-land lateral movement, and use of legitimate RMM tooling as a command-and-control layer reflects the broader challenge of detecting adversarial action within trusted operational flows that MAESTRO was designed to model for agentic systems.

CSA's **Healthcare Cybersecurity Playbook** and **Medical Device Incident Response Playbook** provide directly applicable guidance for the operational continuity challenges demonstrated in the UMMC and SimonMed incidents, including the transition to paper-based operations and the recovery prioritization of patient-critical systems.

The **AI Controls Matrix (AICM)** and **Cloud Controls Matrix (CCM)** together provide the governance scaffolding for the compensating control strategies recommended above. CCM control families for vulnerability and patch management, privileged access management, and incident response are directly implicated, and AICM's additional layer of AI-system risk management is relevant given the increasing role of AI-assisted threat detection in reducing dwell time for high-velocity actors like Storm-1175.

CSA's **Zero Trust Guidance for Critical Infrastructure** addresses the segmentation and least-privilege access principles that are most effective against Storm-1175's lateral movement and credential harvesting tradecraft. The zero trust principle of treating every internal session as potentially compromised — and requiring continuous re-authentication for privileged operations — directly counters the actor's reliance on harvested domain credentials for network-wide ransomware deployment.

References

[1] Microsoft Threat Intelligence. "Storm-1175 focuses gaze on vulnerable web-facing assets in high-tempo Medusa ransomware operations." Microsoft Security Blog, April 6, 2026.

[2] Gatlan, Sergiu. "Microsoft links Medusa ransomware affiliate to zero-day attacks." BleepingComputer, April 6, 2026.

[3] CISA, FBI, and MS-ISAC. "#StopRansomware: Medusa Ransomware (AA25-071A)." CISA Cybersecurity Advisory, March 12, 2025.

[4] Heilweil, Rebecca. "Medusa ransomware group using zero-days to launch attacks within 24 hours of breach, Microsoft says." The Record, April 6, 2026.

[5] Kovacs, Eduard. "Medusa ransomware claims 40+ victims in early 2025." Infosecurity Magazine, March 2025.

[6] Google Cloud Threat Intelligence. "2025 Zero-Day Trends." Google Cloud Blog, April 7, 2026.

[7] "Ransomware gang Medusa hits SimonMed Imaging in one of 2025's largest healthcare breaches." Enterprise Security Tech, January 2025.

[8] Lyngaas, Sean. "Medusa claims Mississippi's largest hospital and NJ county as victims." The Record, March 2026.

[9] Check Point Research. "Before ToolShell: Exploring Storm-2603's Previous Ransomware Operations." Check Point Research, 2025.

[10] Lakshmanan, Ravie. "Lazarus Group Uses Medusa Ransomware in Middle East and U.S. Healthcare Attacks." The Hacker News, February 2026.

[11] American Hospital Association. "Advisory: Medusa Ransomware Activity Warning." AHA Cybersecurity Advisory, March 14, 2025.

[12] "235,000 affected by cyberattack on ambulance provider Bell Ambulance." The Record, 2025.

[13] Whittaker, Zack. "UK healthcare giant HCRG confirms hack after ransomware gang claims theft of sensitive data." TechCrunch, February 20, 2025.

