# Ransomware | Latest Threats | Microsoft Security Blog

Published: 2025-10-06 · Archived: 2026-04-06 00:50:31 UTC



Ransomware as a service ecosystems make it easier for attackers of any skill to launch effective attacks. Learn how these threats work—and how to detect, contain, and recover from them.

---

## Filtered by

Clear All

- ransomware

## Refine results

- **Investigating active exploitation of CVE-2025-10035 GoAnywhere Managed File Transfer vulnerability**

Storm-1175, a financially motivated actor known for deploying Medusa ransomware and exploiting public-facing applications for initial access, was observed exploiting the deserialization vulnerability in GoAnywhere MFT's License Servlet, tracked as CVE-2025-10035.

- **Storm-0501's evolving techniques lead to cloud-based ransomware**

  Financially motivated threat actor Storm-0501 has continuously evolved their campaigns to achieve sharpened focus on cloud-based tactics, techniques, and procedures (TTPs).

- **Unveiling RIFT: Enhancing Rust malware analysis through pattern matching**

  As threat actors are adopting Rust for malware development, RIFT, an open-source tool, helps reverse engineers analyze Rust malware, solving challenges in the security industry.

- **Exploitation of CLFS zero-day leads to ransomware activity**

  Microsoft Threat Intelligence Center (MSTIC) and Microsoft Security Response Center (MSRC) have discovered post-compromise exploitation of a newly discovered zero-day vulnerability in the Windows Common Log File System (CLFS) against a small number of targets.

- **Cyber Signals Issue 8 | Education under siege: How cybercriminals target our schools**

  This edition of Cyber Signals delves into the cybersecurity challenges facing classrooms and campuses, highlighting the critical need for robust defenses and proactive measures.

- **Storm-0501: Ransomware attacks expanding to hybrid cloud environments**

  August 27, 2025 update: Storm-0501 has continuously evolved to achieve sharpened focus on cloud-based TTPs as their primary objective shifted from deploying on-premises endpoint ransomware to using cloud-based ransomware tactics.

- **Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption**

  Microsoft Security researchers have observed a vulnerability used by various ransomware operators to get full administrative access to domain-joined ESXi hypervisors and encrypt the virtual machines running on them.

- **Moonstone Sleet emerges as new North Korean threat actor with new bag of tricks**

  Microsoft has identified a new North Korean threat actor, now tracked as Moonstone Sleet (formerly Storm-1789), that combines many tried-and-true techniques used by other North Korean threat actors, as well as unique attack methodologies to target companies for its financial and cyberespionage objectives.

- **Threat actors misusing Quick Assist in social engineering attacks leading to ransomware**

Microsoft Threat Intelligence has observed Storm-1811 misusing the client management tool Quick Assist to target users in social engineering attacks that lead to malware like Qakbot followed by Black Basta ransomware deployment.

- **Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction**

  Microsoft has been tracking activity related to the financially motivated threat actor Octo Tempest, whose evolving campaigns represent a growing concern for many organizations across multiple industries.

- **Automatic disruption of human-operated attacks through containment of compromised user accounts**

  User containment is a unique and innovative defense mechanism that stops human-operated attacks in their tracks.

- **Malware distributor Storm-0324 facilitates ransomware access**

  The threat actor that Microsoft tracks as Storm-0324 is a financially motivated group known to gain initial access using email-based initial infection vectors and then hand off access to compromised networks to other threat actors.

---