Recent Malware Incidents Research Report (2023-2025)

---

1. RansomHub Ransomware (2024)

Attack Method

RansomHub is a ransomware-as-a-service (RaaS) platform that gained rapid notoriety beginning in early 2024. It is designed to provide affiliates with powerful ransomware tools, enabling widespread attacks. RansomHub operators typically distribute their ransomware through phishing emails containing malicious attachments or links. Once a victim opens the attachment and enables macros or executes malicious payloads, the ransomware encrypts the victim’s data.

What makes RansomHub particularly dangerous is its use of "triple extortion" techniques. Not only does it encrypt victim data and demand a ransom, but it also steals copies of sensitive data and threatens to leak it if payment is not made. Additionally, the attackers may target business partners or customers of the victim organization to increase pressure for payment.

Mitigation and Resolution

- **Disable Macros:** Organizations are advised to disable macros in Microsoft Office by default and train employees not to enable them from untrusted sources.
- **Patch Management:** Timely patching of vulnerabilities in software and operating systems helps prevent initial infection vectors.
- **Email Security:** Deploy advanced spam and phishing detection solutions to block malicious emails.
- **Endpoint Protection:** Use modern endpoint detection and response (EDR) systems to identify suspicious behavior early.

- **Backups:** Maintain regular, tested offline backups to restore systems without paying ransom.
- **User Training:** Educate users to recognize phishing and suspicious activity.
- **Incident Response:** Quick isolation and removal of infected systems, followed by forensic analysis to understand the breach.

---

2. BlackCat (ALPHV) Ransomware (2023)

Attack Method

BlackCat, also known as ALPHV, surfaced in 2023 as a highly sophisticated ransomware variant. Written in the Rust programming language, it is notable for its ability to target both Windows and Linux environments, setting it apart from many ransomware families. BlackCat operates as a RaaS model where affiliates lease the ransomware to launch attacks.

The attackers commonly gain initial access via vulnerabilities in Remote Desktop Protocol (RDP) services, brute force attacks, or phishing emails. Following access, they conduct extensive reconnaissance inside the victim network, escalate privileges, and deploy the ransomware. BlackCat often exfiltrates data before encryption and uses double extortion tactics.

Mitigation and Resolution

- **Multi-Factor Authentication (MFA):** Enforcing MFA on RDP and VPN access significantly reduces unauthorized access risk.
- **Patch Vulnerabilities:** Closing vulnerabilities in RDP and related services minimizes attack surface.
- **Network Segmentation:** Isolating critical systems limits lateral movement by attackers.
- **Behavioral Detection:** EDR products capable of detecting unusual activities such as privilege escalation or file encryption improves early detection.
- **Offline Backups:** Regular backup routines ensure data recovery options.
- **Threat Intelligence Sharing:** Collaborative sharing among organizations helps identify and react quickly to new attack trends.

---

3. Microsoft CLFS Zero-Day Exploit by Storm-2460 Group (April 2025)

Attack Method

In April 2025, a sophisticated cybercrime group known as Storm-2460 exploited a zero-day vulnerability (CVE-2025-29824) in the Microsoft Common Log File System (CLFS). This vulnerability allowed attackers with limited access to escalate privileges to higher levels within the system. The group used this exploit to deploy ransomware widely after gaining elevated control.

This zero-day exploit was particularly dangerous as it bypassed many traditional security measures and allowed persistent access to victim networks. The exploit was leveraged in targeted attacks on several critical infrastructure and corporate environments globally.

Mitigation and Resolution

- **Emergency Patch Deployment:** Microsoft released a security update shortly after the vulnerability was disclosed, patching the CLFS flaw.
- **Vulnerability Management:** Organizations enhanced their vulnerability scanning and patch management processes to ensure rapid update application.
- **Enhanced Monitoring:** Security teams increased monitoring for privilege escalation indicators and suspicious process behavior within networks.
- **Security Training:** IT staff was trained to recognize zero-day activity and respond to novel threats.
- **Layered Security:** Combining endpoint protection, network segmentation, and strict access control reduced the risk of such attacks succeeding.
