Threat Intelligence Report

Prepared by SOClogix Threat Intelligence

Coverage period: Aug 11–17, 2025

⚠️ URGENT: Multiple critical vulnerabilities under active exploitation ⚠️

This intelligence brief provides analysis of the week's most significant cyber threats, including the Microsoft Patch Tuesday releases, multiple zero-day vulnerabilities under active exploitation, and specific recommendations for immediate action.

Staying ahead of cyber adversaries is paramount. This weekly Threat Intelligence Report from SOClogix is meticulously curated to provide small and medium businesses (SMBs) with timely, relevant, and actionable insights into the most pressing cybersecurity challenges.

Our aim is to empower your organization to proactively defend against emerging threats, minimize risk, and enhance overall cyber resilience.

Within these pages, you will find a comprehensive overview of the current threat environment, including detailed analysis of newly identified vulnerabilities, significant threat actor activities, and critical Patch Tuesday updates. Crucially, we also provide a concise section of 'SMB Recommendations (Do These This Week)' designed for immediate implementation to strengthen your defenses against the highlighted risks.

Thank you for reading,

SOClogix Cyber Threat Recon Unit (TRU) | tru@soclogix.com

Executive Summary

Microsoft Patch Tuesday (Aug 12)

Microsoft addressed over 107 vulnerabilities, including a Windows Kerberos zero-day (CVE-2025-53779), with 13 flaws rated Critical. This requires immediate updates to domain controllers and core infrastructure to prevent potential domain compromise.

WinRAR Zero-Day (CVE-2025-8088)

Under active exploitation by the RomCom/Storm-0978 threat group in spear-phishing campaigns, pushing malware via weaponized archives. Users are urged to update to WinRAR 7.13 without delay to mitigate this critical path traversal vulnerability.

MSP Tool Vulnerabilities

Active exploitation warnings emerged for both N-able N-central (CVE-2025-8875/8876) and Citrix NetScaler (CVE-2025-6543), with confirmed breaches reported. This presents an especially severe risk to MSPs and the SMBs that depend on them, potentially enabling cascading compromises.

The cyber threat landscape this week has shown a concerning convergence of critical vulnerabilities affecting core infrastructure, everyday business applications, and managed service tools. Organizations must take immediate action to patch, mitigate, and monitor for signs of compromise.

Top Cyber Threats

This week's landscape is dominated by critical vulnerabilities under active exploitation, requiring immediate attention from security teams:

Threat	Impact/Severity
Microsoft August Patch Tuesday — Kerberos zero-day & 13 Critical CVEs	⚠️ Critical Potential domain compromise via Kerberos EoP; numerous RCEs across Windows stack. Apply August updates now; prioritize DCs.
WinRAR CVE-2025-8088 (active exploitation)	⚠️ Critical Path traversal lets archives drop files outside intended folders; used by RomCom to deploy backdoors (SnipBot, RustyClaw, Mythic). Upgrade to 7.13; disable auto-extract; block .rar in email.
N-able N-central RMM zero-days (CVE-2025-8875/8876)	⚠️ Critical Active attacks against MSP RMM platforms could cascade to many SMB tenants. Patch immediately; audit RMM accounts & tokens; monitor for anomalous push jobs.
Citrix NetScaler CVE-2025-6543 (exploited)	🔒 High Memory overflow → potential control flow/DoS; confirmed breaches in NL critical orgs. Patch/mitigate; restrict management plane; inspect internet-exposed ADCs.
Dell "ReVault" ControlVault3 firmware flaws	✅ Medium (enterprise exposure varies) 5-bug chain on >100 Dell models enables login bypass & persistent implants. Apply DSA-2025-053; review use of fingerprint auth; protect physical access.

Patch Management

Phishing Attacks

SMBs & MSPs Risk

Vulnerability Spotlight

These vulnerabilities are high-value targets for attackers—timely patching and monitoring are the difference between prevention and compromise.

CVE-2025-53779 — Windows Kerberos Elevation of Privilege (0-day)

- Affected: Windows Server/Domain environments (Kerberos)
- Severity: ⚠️ Critical (domain takeover risk)
- Details: Publicly disclosed; attackers with specific attribute write access can escalate to Domain Admin
- Fixed in August 2025 patches

Action: Patch Domain Controllers first; review msds-groupMSAMembership / msds-ManagedAccountPreceededByLink ACLs; monitor for abnormal TGS/TGT activity.

Source: BleepingComputer

CVE-2025-8088 — WinRAR Path Traversal (actively exploited)

- Affected: WinRAR < 7.13 on Windows
- Severity: ⚠️ Critical (malware drop on extract)
- Details: Enables malicious code execution when archive is extracted
- Under active exploitation by RomCom/Storm-0978

Action: Update to 7.13, block inbound .rar attachments, open archives in sandbox/VM, enable application allow-listing.

Source: The Hacker News

CVE-2025-8875 / CVE-2025-8876 — N-able N-central

- Affected: N-central RMM (MSPs & internal IT)
- Severity: ⚠️ Critical (active exploitation)
- Details: Authentication bypass and remote code execution vulnerabilities in a popular MSP remote management platform
- Provides attackers with "keys to the kingdom" across multiple client networks

Action: Patch; rotate credentials/API keys; review job history; restrict RMM to VPN/allow-lists.

Source: BleepingComputer

Threat Actor Activity

RomCom / Storm-0978 (Russia-linked)

Actively leveraging CVE-2025-8088 via targeted phishing campaigns with these themes:

- Job applications and resumes
- Official government documents
- Industry conference registrations
- Financial reports and invoices

Payloads include sophisticated malware families:

- SnipBot — information stealer with keylogging
- RustyClaw — remote access trojan
- Mythic — modular C2 framework

Primary targeting: Financial services, manufacturing, defense contractors, and logistics companies in EU and Canada.

Sources: BleepingComputer, eset.com

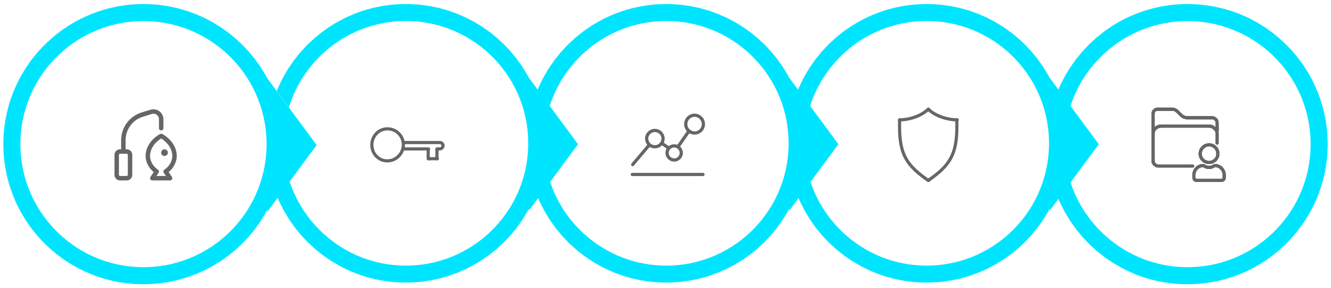
Ransomware Landscape

BlackSuit: Infrastructure dismantled by international law enforcement operation (servers, domains, ~$1M seized); expect rebrand/regroup (reports suggest connection to Chaos ransomware variant).

Source: Axios, IT Pro

Akira: Activity remains elevated with a focus on MSP environments; claims indicate successful compromise of managed service providers with SonicWall-adjacent intrusion vectors reported in multiple cases.

Source: IT Pro, The Hacker News



Exfiltration

SMB Recommendations (Do These This Week)

Focus on rapid patching, phishing defense, and RMM hardening this week to reduce immediate exposure to active threats.

Patch with Urgency

Deploy Microsoft August 2025 updates, prioritizing Domain Controllers; reboot and verify Kerberos service is running correctly. Monitor for any anomalous authentication events post-patching.

Source: BleepingComputer

Eliminate WinRAR Exposure

Upgrade to WinRAR 7.13 immediately; temporarily block .rar attachments at email gateway; implement processes to detonate archives in sandbox before opening in production environments.

Source: The Hacker News

Secure MSP/RMM Stack

Patch N-central immediately; enforce MFA and least-privilege for all RMM users; implement IP allowlists for management console access; review automated jobs and scripts for signs of tampering.

Source: BleepingComputer

Harden Edge Appliances

Patch/mitigate Citrix NetScaler vulnerabilities without delay; restrict administrative interfaces to internal networks only; enable WAF and geographical IP blocking where appropriate; inspect internet-exposed ADCs for indicators of compromise.

Source: BleepingComputer

Verify Backups & Recovery

Confirm offline/immutable backups are functioning properly and test restoration procedures; ensure EDR coverage extends to servers and RMM endpoints to detect lateral movement.

(General best practice aligned to current ransomware activity)

Source: IT Pro

Enhance Phishing Resilience

Refresh user security awareness training with focus on archive attachments; implement special flagging for emails with archives; disable macros and risky file associations in productivity applications.

About SOClogix

SOClogix provides **cyber threat intelligence, 24/7 monitoring, and managed detection and response (MDR)** tailored for SMBs and mid-market organizations. Our mission is to help businesses stay ahead of evolving threats with actionable intel, proactive defense, and rapid incident response.

Our Services Include:

Threat Intelligence

Weekly reports and real-time alerts on emerging threats relevant to your industry

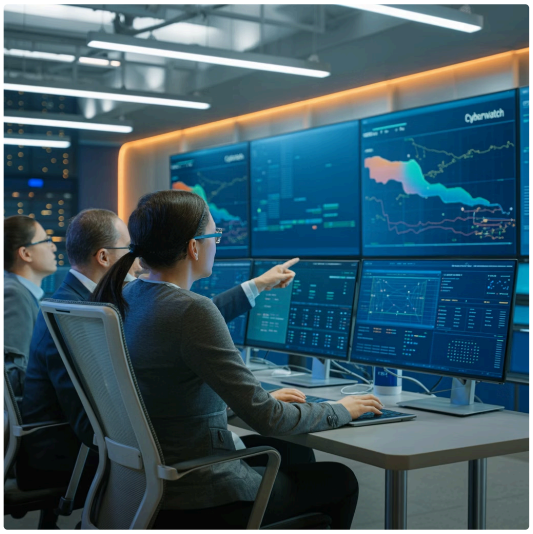
24/7 Monitoring

Continuous security event monitoring with human analysis and verification

Incident Response

Rapid containment and remediation of security incidents with detailed forensics

If you have questions about this week's report—or need support addressing any of the highlighted vulnerabilities—contact the SOClogix team at **support@soclogix.com** or call our 24/7 hotline at **(443) 409-5426**. Visit **www.soclogix.com** for more resources.



Need Emergency Assistance?

Our incident response team is available 24/7 to help contain and remediate active threats. Call our emergency hotline for immediate support.

Contact IR Team