K logix
Be confident.

AUGUST 2025 | THREAT INTEL NEWSLETTER

Don’t Just Patch, Learn and Strengthen

C-Suite level threat review by applicable business area addressing active threats.

Organizations are facing a surge in zero-day exploits targeting widely used enterprise platforms and tools. In July, a critical Microsoft SharePoint Server vulnerability became the focus of a large-scale campaign. Attackers exploited a zero-day, now identified as ToolShell, through a chained attack combining CVE-2025-53770 and CVE-2025-53771 to execute code remotely and, in some cases, deploy ransomware. Around the same time, researchers uncovered a WinRAR zero-day, CVE-2025-8088, that gives attackers a way to compromise systems without requiring elevated privileges. While zero-days strike without warning, understanding attacker patterns can help your organization strengthen defenses and anticipate threats.

Microsoft SharePoint Zero-Day:

Over 400 organizations globally have been affected by this vulnerability, including multiple U.S. federal agencies and organizations in the telecommunications, healthcare, and software sectors. China-linked groups Linen Typhoon, Violet Typhoon, and Storm-2603 are actively exploiting the vulnerability, with Storm-2603 observed deploying ransomware. *This vulnerability does not affect Microsoft 365 SharePoint Online.

WinRAR Zero-Day:

The WinRAR zero-day impacted organizations in the financial, manufacturing, and defense industries in Europe and Canada. The Russian-linked RomCom group (also known as Storm-0978 and Tropical Scorpius) carried out the exploits with the intent of cyber espionage.

Microsoft SharePoint Zero-Day

Threat Level: Medium

Attack:

For initial access, threat actors exploit the ToolShell zero-day in Microsoft SharePoint. They begin by abusing CVE-2025-53771 to bypass authentication by sending crafted requests that trick SharePoint into treating them as authorized requests. This grants attackers access to admin-only pages without requiring a login (MITRE T1190). Once inside, the attackers upload a web shell to establish persistent remote control of the server (MITRE T1505.003). Next, the attackers extract sensitive machine keys from SharePoint configuration files (MITRE T1552.004). SharePoint commonly uses these keys to sign and validate data, but attackers use them to create malicious ViewState payloads, triggering CVE-2025-53770 and giving the attacker full server control. With this access, the attackers collect system and user data, delete logs to evade detection, and harvest credentials from LSASS memory (MITRE T1082, T1087, T1070.001, T1003.001). Finally, threat actors, specifically Storm-2603, deploy Warlock ransomware, encrypting business-critical data and disrupting operations (MITRE T1486).

Remediation:

- Patch CVE-2025-53770 and CVE-2025-53771 immediately.
- Rotate machine keys regularly to prevent attackers from using stolen keys for unauthorized access.
- Enforce least privilege on SharePoint servers and across all organization systems to reduce lateral movement and limit the impact of a compromised account.

WinRAR Zero-Day

Threat Level: Medium

Attack:

RomCom uses spear-phishing emails disguised as job applications or legitimate documents to deliver malicious RAR archives (MITRE1566.001). The zero-day vulnerability, CVE-2025-8088, is triggered when the victim opens the document, which automatically executes code without requiring elevated privileges or additional user actions. The malware then drops files into the Windows Startup folder to maintain access, ensuring persistence by automatically running the malware each time the user logs in (MITRE T1547.001). To evade detection, the malware checks for virtual environments and obfuscates its code to hide from security tools (MITRE T1497.001, T1027). Attackers install backdoors like SnipBot and Mythic Agent, which enable them to collect system information, harvest user credentials, exfiltrate emails and browser data, take screen captures of the system, and perform network reconnaissance (MITRE T1082, T1555.001, T1555.003, T1114, T1539, T1113, T1016). Using their access, RomCom attackers move laterally across the network and gather information for espionage, and in some cases, financial theft (MITRE TA009, T1657).

Remediation:

- Patch CVE-2025-8088 immediately.
- Review Windows Startup folders to detect unauthorized entries that may indicate attackers establishing persistence.
- Train employees to recognize spear-phishing emails, specifically those disguised as job applications or attachments, which have been on a rise since 2024.

Microsoft SharePoint Zero-Day:

- **SharePoint Exploit Outline:** https://safe.security/resources/blog/toolshell-fallout-from-cve-to-crisis-in-48-hours/
- **Microsoft Update:** https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/

WinRAR Zero-Day:

- **WinRAR Exploit Walkthrough:** https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/
- **RomCom Involvement in CVE-2025-8088:** https://socradar.io/cve-2025-8088-winrar-zero-day-exploited-targeted/

ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.

How K logix Can Help

Technology Advisory

- Email Security
- Endpoint Detection and Response (EDR)
- Identity and Access Management (IAM)
- Managed Security Service Provider (MSSP)
- Security Information and Event Management (SIEM)
- Cloud Security Posture Management (CSPM)
- SaaS Security Posture Management (SaaS)

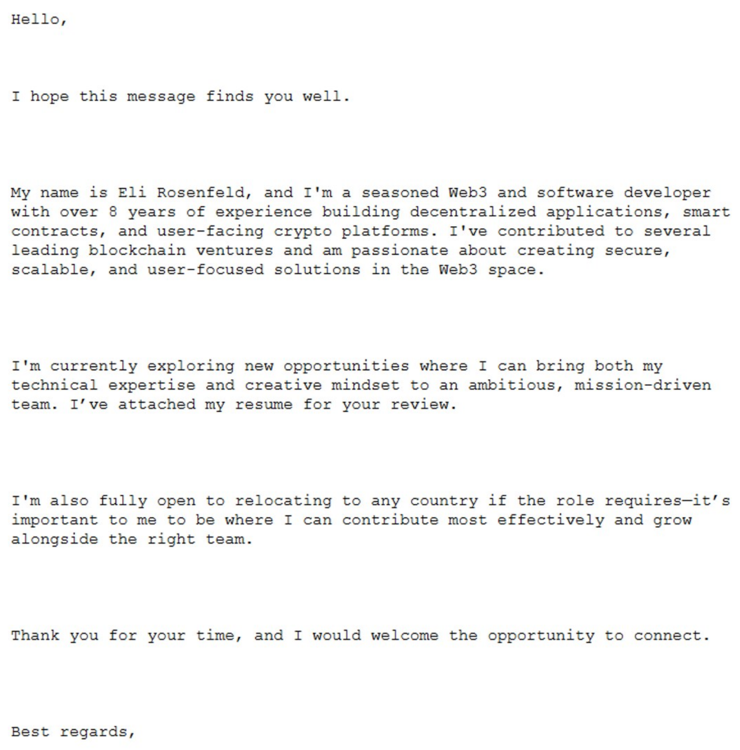
Program Advisory

- Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
- Cloud Security Maturity
- Identity and Access Management Program Maturity

Threat Intelligence

- Notification to customers of threats
- On-demand briefings
- Threat exposure workshops
- User awareness training seminars
- Monthly and quarterly threat intelligence reports

Spear-Phishing Email connected to WinRAR Vulnerability



Hello,

I hope this message finds you well.

My name is Eli Rosenfeld, and I'm a seasoned Web3 and software developer with over 8 years of experience building decentralized applications, smart contracts, and user-facing crypto platforms. I've contributed to several leading blockchain ventures and am passionate about creating secure, scalable, and user-focused solutions in the Web3 space.

I'm currently exploring new opportunities where I can bring both my technical expertise and creative mindset to an ambitious, mission-driven team. I’ve attached my resume for your review.

I'm also fully open to relocating to any country if the role requires—it’s important to me to be where I can contribute most effectively and grow alongside the right team.

Thank you for your time, and I would welcome the opportunity to connect.

Best regards,