RAPID7

THREAT REPORT

CVE-2025-53770: TOOLSHELL EXPLOITATION

September 2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report provides an in-depth analysis of the active exploitation of Microsoft SharePoint Server vulnerability CVE-2025-53770, part of a cluster of flaws collectively referred to as ToolShell. First observed in early July 2025, exploitation campaigns have quickly escalated, with multiple security vendors (Viettel Security, LeakIX, Eye Security, Microsoft, Rapid7, WithSecure) reporting consistent targeting of on-premises SharePoint environments worldwide.

Successful exploitation enables unauthenticated remote code execution (RCE) on vulnerable servers, allowing attackers to deploy webshells, steal ASP.NET MachineKeys (for persistent access), conduct reconnaissance, move laterally, and potentially disable defenses. Evidence points to overlap with China-nexus tradecraft, though attribution remains under assessment.

Given SharePoint's role in enterprise collaboration and data storage, exploitation carries severe risk for data theft, domain compromise, and persistence even after patching. This report outlines the technical vectors, observed post-exploitation behaviors, potential attribution, and defensive measures organizations must take immediately.

- **Scope and scale:** Over 400 confirmed compromised SharePoint servers identified by independent researchers during July 17–21, 2025; more than 8,000 servers remained exposed online at that time.
- **What's new**: CVE-2025-53770/53771 are patch-bypass variants of the July 8, 2025 ToolShell chain (CVE-2025-49704/49706). Attackers quickly pivoted to the bypass and scaled exploitation.
- **Business impact:** Unauthorized access to sensitive document libraries, credential/key theft (MachineKeys), potential domain compromise, and confirmed ransomware (Warlock) in some incidents.
- **Board-level risk:** Exposure is concentrated in organizations that still operate on-prem SharePoint for collaboration and legacy workflows. Patch latency and internet exposure are key drivers.

Risk Rating:

Likelihood: High Impact: High Overall: Severe

INTRODUCTION

On July 19, 2025, Microsoft issued guidance on active exploitation of SharePoint vulnerabilities, assigning CVE-2025-53770 and related identifiers. Exploitation patterns were first observed as early as July 7, 2025, rapidly scaling across multiple geographies.

The ToolShell campaign targets on-premises SharePoint Server only (not SharePoint Online), making it particularly impactful for enterprises still operating local infrastructure. Attackers exploit the vulnerability to achieve unauthenticated RCE, deploy persistence mechanisms, and exfiltrate sensitive data.

TIMELINE OF EXPLOITATION

Time Period	Activity
July 7, 2025	First exploitation attempts recorded in telemetry by several companies
July 14, 2025	Additional exploitation observed from new attacker infrastructure
July 17, 2025 onward	Sharp increase in global exploitation attempts reported
July 19, 2025	Microsoft issues customer guidance and security updates.
Late July 2025	Rapid7, LeakIX, Eye Security, and others confirm widespread campaigns, with weaponization across multiple threat clusters.

Scope and scale (indicative): Independent scans and incident reporting identified hundreds of confirmed compromises and thousands of still-exposed SharePoint servers during the July exploitation waves.

TECHNICAL ANALYSIS

Exploit chain overview

The attack commences with a crafted HTTP POST request directed at the / _layouts/15/ToolPane.aspx?DisplayMode=Edit endpoint. A critical component of this initial phase is the spoofing of the Referer header, specifically setting it to / _layouts/SignOut.aspx.

This manipulation of the Referer header serves to bypass authentication mechanisms, creating a vulnerability that allows the attacker to proceed without proper authorization. Once authentication is circumvented, the crafted POST request triggers an unsafe deserialization path within the application. This deserialization vulnerability is the lynchpin of the attack, as it allows the attacker to inject malicious code and achieve Remote Code RCE.

Post-exploitation activities and persistence:

Upon successful exploitation and gaining RCE, attackers typically engage in a series of post-exploitation activities aimed at maintaining persistent access and expanding their control over the compromised system. A common tactic involves the deployment of an ASPX webshell, such as spinstall0.aspx. This webshell provides a persistent backdoor, enabling the attacker to execute commands and interact with the server remotely, even after the initial vulnerability might be patched or the original entry point closed.

Another prevalent post-exploitation technique is the theft of ASP.NET MachineKeys. These keys are crucial for signing and encrypting various ASP.NET components, including _VIEWSTATE payloads. By acquiring these MachineKeys, attackers can forge their own signed _VIEWSTATE payloads. This allows them to achieve persistent, unauthenticated code execution. This means that even if the underlying vulnerability is patched, and the initial RCE vector is closed, the attacker can still execute arbitrary code on the server simply by sending a request containing their forged _VIEWSTATE payload.

Observed post-exploitation TTPs

Initial access and foothold

Webshell families and payloads: Threat actors leveraged several webshell families to establish initial access and maintain persistence within compromised environments. Notably, spinstall*.aspx and info.aspx were frequently observed, indicating a potential focus on SharePoint and other IIS-based web applications. The Godzilla webshell was also a prominent tool, offering a wide range of functionalities for remote control and data exfiltration. In more targeted attacks, custom MachineKey stealer payloads were deployed, specifically designed to extract cryptographic keys, enabling decryption of sensitive data and potentially facilitating further compromise of encrypted communications or applications.

Privilege escalation

Once a foothold was established, threat actors systematically pursued privilege escalation to gain higher-level access within the compromised system. This was often achieved through the use of in-memory exploits like BadPotato, which targets Windows impersonation vulnerabilities to elevate privileges. Beyond technical exploits, the straightforward creation of local administrative users was a common tactic, providing persistent, high-level access. Scheduled tasks were also extensively utilized for privilege escalation, allowing attackers to execute malicious code with elevated permissions at predetermined intervals or in response to specific events, ensuring long-term control.

Defense Evasion

A significant aspect of these operations involved comprehensive defense evasion techniques to avoid detection by security solutions. The installation of Huorong (HRSword) was observed, indicating attempts to deploy an alternative security product, potentially to clash with or disable existing endpoint detection and response (EDR) or antivirus (AV) software. More direct impairment of EDR/AV solutions was also a consistent tactic, often involving process termination, driver manipulation, or registry modifications. Reflective module loading in IIS was a sophisticated evasion technique, where malicious code was loaded directly into memory without touching disk, making it harder for static and signature-based detections. Furthermore, rundll32 injection was frequently used to execute arbitrary DLLs within legitimate processes, masquerading malicious activity as benign system operations.

Command and control (C2) & tunneling

Maintaining resilient command and control (C2) infrastructure was critical for sustained operations. Fast Reverse Proxy (FRP), often loaded reflectively to evade detection, was a key tool for establishing robust and flexible C2 channels, allowing attackers to tunnel traffic and bypass network segmentation. A strong emphasis was placed on encrypted outbound channels, ensuring that all communication between the compromised host and the attacker's C2 server remained confidential and resistant to network-level interception and analysis. This encryption made it significantly harder for security analysts to understand the nature and content of the malicious traffic.

Lateral movement

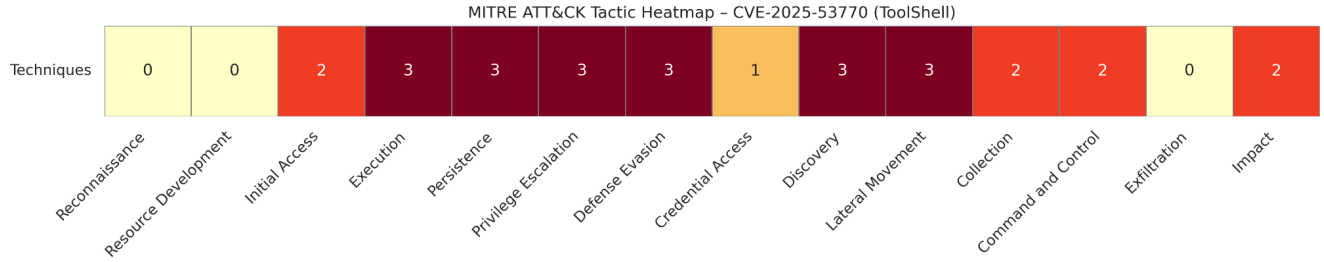
To expand their reach within the compromised network, threat actors employed a variety of lateral movement techniques. Tools like PsExec, Impacket, and WMI were routinely used to execute commands and move laterally between systems, leveraging legitimate Windows functionalities. The use of ADExplorer was a clear indicator of reconnaissance efforts within Active Directory, enabling attackers to map out the network, identify high-value targets, and locate administrative accounts. RDP pivoting allowed attackers to leverage existing Remote Desktop Protocol sessions to jump between hosts, often using compromised credentials. Finally, the SMB copy of tooling was a simple yet effective method to transfer additional malicious tools and payloads across the network using the Server Message Block protocol, often disguised as legitimate file transfers.

Attribution

IOCs and TTPs collected by Rapid7 Labs' Intelligence teams around the active exploitation of CVE-2025-53770 bear notable similarities to historic campaigns targeting edge security infrastructure, including firewalls, VPN appliances, and SSL VPN portals. This reflects a broader trend where adversaries exploit externally facing enterprise systems to gain footholds in high-value networks without requiring user interaction.

Through analysis of command-and-control infrastructure, payload staging paths, and behavioral fingerprints (such as webshell deployment cadence, directory structures, and secondary payloads), Rapid7 analysts observed a cluster of activity tied to this SharePoint vulnerability. While current intelligence does not support conclusive attribution to a single threat group, the operational tempo, tooling, and infrastructure reuse strongly suggest ties to a China-nexus threat actor, likely associated with prior cyber espionage campaigns.

ATT&CK TECHNIQUE DISTRIBUTION



The heatmap above visualizes the distribution of MITRE ATT&CK tactics involved in the exploitation of CVE-2025-53770, a critical vulnerability affecting Microsoft SharePoint servers. This vulnerability has been widely exploited in the wild, primarily using webshells such as ToolShell to gain unauthorized remote access. The most heavily leveraged tactics include:

- Initial access via exploitation of a public-facing application (T1190),
- Execution through command and scripting interpreters (T1059),
- Defense evasion using obfuscated payloads (T1027),
- Persistence via server-side components or scheduled tasks (T1505, T1053),
- and Privilege Escalation by exploiting local vulnerabilities (T1068).

This pattern of activity highlights a typical post-compromise kill chain in enterprise environments and underscores the need for layered defenses, proactive patch management, and behavioral detections aligned with MITRE ATT&CK.

RECOMMENDATIONS

- **Prioritize known-exploited vulnerabilities:** Treat CVE-2025-53770 and CVE-2025-53771 as critical, high-priority remediation items. These vulnerabilities are actively being exploited in the wild, posing an immediate and significant threat to organizational security. Establish and rigorously follow a robust known exploited vulnerability (KEV) management process to ensure rapid identification, assessment, and patching of such vulnerabilities. This process should include clear communication channels, dedicated resources, and stringent timelines for resolution.

- **Internet exposure:** Implement a strict policy requiring all access to SharePoint Server to be exclusively via a Virtual Private Network (VPN) and control your attack surface. Where technically and operationally feasible, disable direct internet reachability to SharePoint Servers entirely. This measure significantly reduces the attack surface by limiting direct exposure to malicious actors on the public internet. Regularly audit and enforce this policy to prevent accidental or unauthorized direct exposure.

- **Continuity of operations:** Develop, maintain, and regularly test comprehensive continuity of operations (COOP) and disaster recovery (DR) plans specifically addressing potential SharePoint outages and data integrity events. These plans should detail procedures for system restoration, data recovery, and maintaining essential business functions during an incident. Additionally, prepare and validate alternate collaboration paths and communication methods to ensure uninterrupted workflow and information sharing even if SharePoint services are fully compromised or unavailable.

- **Vendor/partner risk:** Establish and enforce stringent security requirements for all third-party service providers and partners handling agency SharePoint workloads. This includes requiring formal attestations from these providers confirming their adherence to security best practices, data protection regulations, and incident response protocols. Furthermore, actively verify their patch levels and ensure sufficient telemetry visibility to monitor their environments for suspicious activities and potential compromises. Conduct regular security audits and penetration tests of vendor-managed environments to proactively identify and mitigate risks.

- **Reporting and coordination:** Adhere strictly to all agency-specific incident reporting requirements. This includes timely and accurate documentation of security incidents,

their scope, impact, and remediation efforts. Crucially, establish and maintain strong coordination channels with appropriate national and sector-specific Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs). Active participation in these communities facilitates the rapid exchange of threat intelligence, best practices, and lessons learned, enhancing collective defense capabilities.

About Rapid7 Labs

Rapid7 Labs actively tracks advanced persistent threat (APT) groups such as Salt Typhoon, providing timely curated intelligence, behavioral indicators, and hunting logic to enhance detection and response capabilities across the Rapid7 platform. This intelligence directly fuels our products, including the Intelligence Hub, Managed Detection and Response (MDR), and InsightIDR (IDR), ensuring customers are equipped with actionable insights to identify and mitigate sophisticated nation-state threats.