ToolShell: An all-you-can-eat buffet for threat actors

By ESET Research

Archived: 2026-04-05 15:12:09 UTC

ESET Research

ESET Research has been monitoring attacks involving the recently discovered ToolShell zero-day vulnerabilities

24 Jul 2025 • , 5 min. read

On July 19th, 2025, Microsoft confirmed that a set of zero-day vulnerabilities in SharePoint Server called ToolShell is being exploited in the wild. ToolShell is comprised of CVE-2025-53770, a remote code execution vulnerability, and CVE-2025-53771, a server spoofing vulnerability. These attacks target on-premises Microsoft SharePoint servers, specifically those running SharePoint Subscription Edition, SharePoint 2019, or SharePoint 2016. SharePoint Online in Microsoft 365 is not impacted. Exploiting these vulnerabilities enables threat actors to gain entry to restricted systems and steal sensitive information.

Starting from July 17th, ToolShell has been widely exploited by all sorts of threat actors, from petty cybercriminals to nation-state APT groups. Since SharePoint is integrated with other Microsoft services, such as Office, Teams, OneDrive, and Outlook, this compromise can provide the attackers a staggering level of access across the affected network.

As part of the attack, the threat actors often chain together four vulnerabilities: the previously patched CVE-2025-49704 and CVE-2025-49706, alongside the already mentioned CVE-2025-53770 and CVE-2025-

53771. As of July 22, CVE-2025-53770 and CVE-2025-53771 have also been patched.

Webshell payloads

Exploiting ToolShell allows the attackers to bypass multi-factor authentication (MFA), and single sign-on (SSO). After getting inside the targeted server, attackers were seen deploying malicious webshells to extract information from the compromised system. One of the scripts frequently used for this purpose is named spinstall0.aspx, which we track as MSIL/Webshell.JS.

Additionally, on July 22nd, 2025, we observed that attackers attempted to deploy other simple ASP webshells capable of executing attacker-supplied commands via cmd.exe. These webshells were deployed using the following filenames: ghostfile346.aspx, ghostfile399.aspx, ghostfile807.aspx, ghostfile972.aspx, and ghostfile913.aspx.

ESET products first detected an attempt to exploit part of the execution chain – the Sharepoint/Exploit.CVE-2025-49704 vulnerability – on July 17th in Germany. However, because this attempt was blocked, the final webshell payload was not delivered to the targeted system. The first time we registered the payload itself was on July 18th on a server in Italy. As seen in Figure 1, we have since observed active ToolShell exploitation all over the world, with the US (13.3% of attacks) being the most targeted country according to our telemetry data.

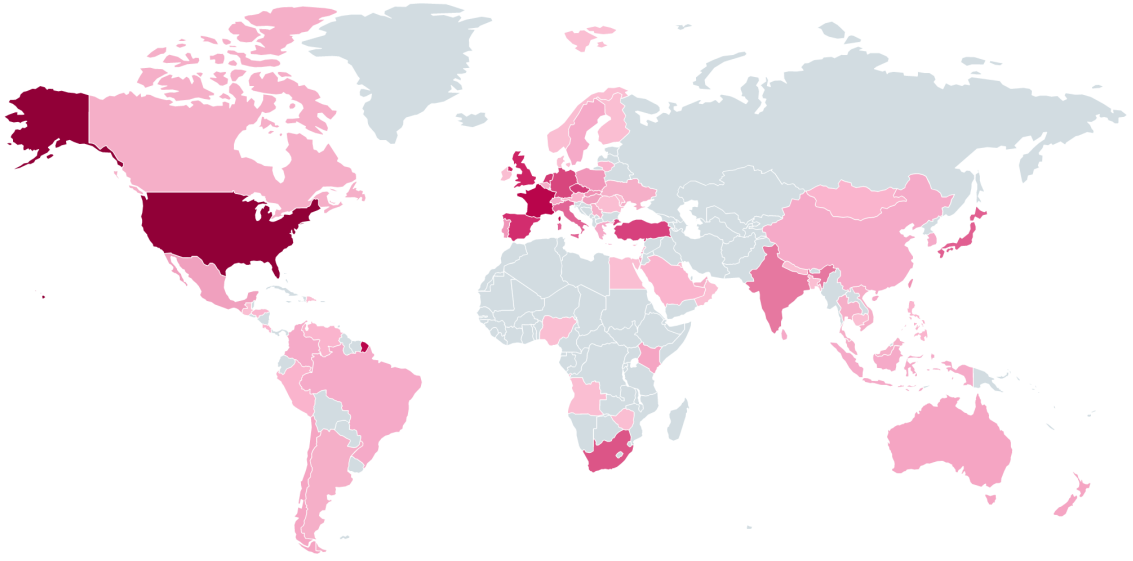

Figure 1. Geographic distribution of ToolShell attacks from July 17, 2025 to July 22, 2025

Attack monitoring

Our monitoring of the ToolShell attacks from July 17th to July 22nd revealed that they were coming from the IP addresses shown in Table 1 (all times are in UTC).

Table 1. Attacker IP addresses

IP address	Attack start date	Attack end date
96.9.125[.]147	2025-07-17 09:00	2025-07-17 16:00
107.191.58[.]76	2025-07-18 14:00	2025-07-18 20:00
104.238.159[.]149	2025-07-19 04:00	2025-07-19 09:00
139.59.11[.]66	2025-07-21 11:00	2025-07-21 16:00
154.223.19[.]106	2025-07-21 13:00	2025-07-22 18:00
103.151.172[.]92	2025-07-21 14:00	2025-07-21 16:00
45.191.66[.]77	2025-07-21 14:00	2025-07-22 07:00
83.136.182[.]237	2025-07-21 14:00	2025-07-21 16:00
162.248.74[.]92	2025-07-21 14:00	2025-07-21 17:00
38.54.106[.]11	2025-07-21 15:00	2025-07-21 15:00
206.166.251[.]228	2025-07-21 16:00	2025-07-22 16:00
45.77.155[.]170	2025-07-21 16:00	2025-07-21 19:00
64.176.50[.]109	2025-07-21 17:00	2025-07-22 17:00
149.28.17[.]188	2025-07-22 03:00	2025-07-22 03:00
173.239.247[.]32	2025-07-22 05:00	2025-07-22 05:00
109.105.193[.]76	2025-07-22 05:00	2025-07-22 16:00
2.56.190[.]139	2025-07-22 06:00	2025-07-22 07:00
141.164.60[.]10	2025-07-22 07:00	2025-07-22 18:00
124.56.42[.]75	2025-07-22 13:00	2025-07-22 18:00

Figure 2 shows the timeline of the attacks coming from the three most active IP addresses.

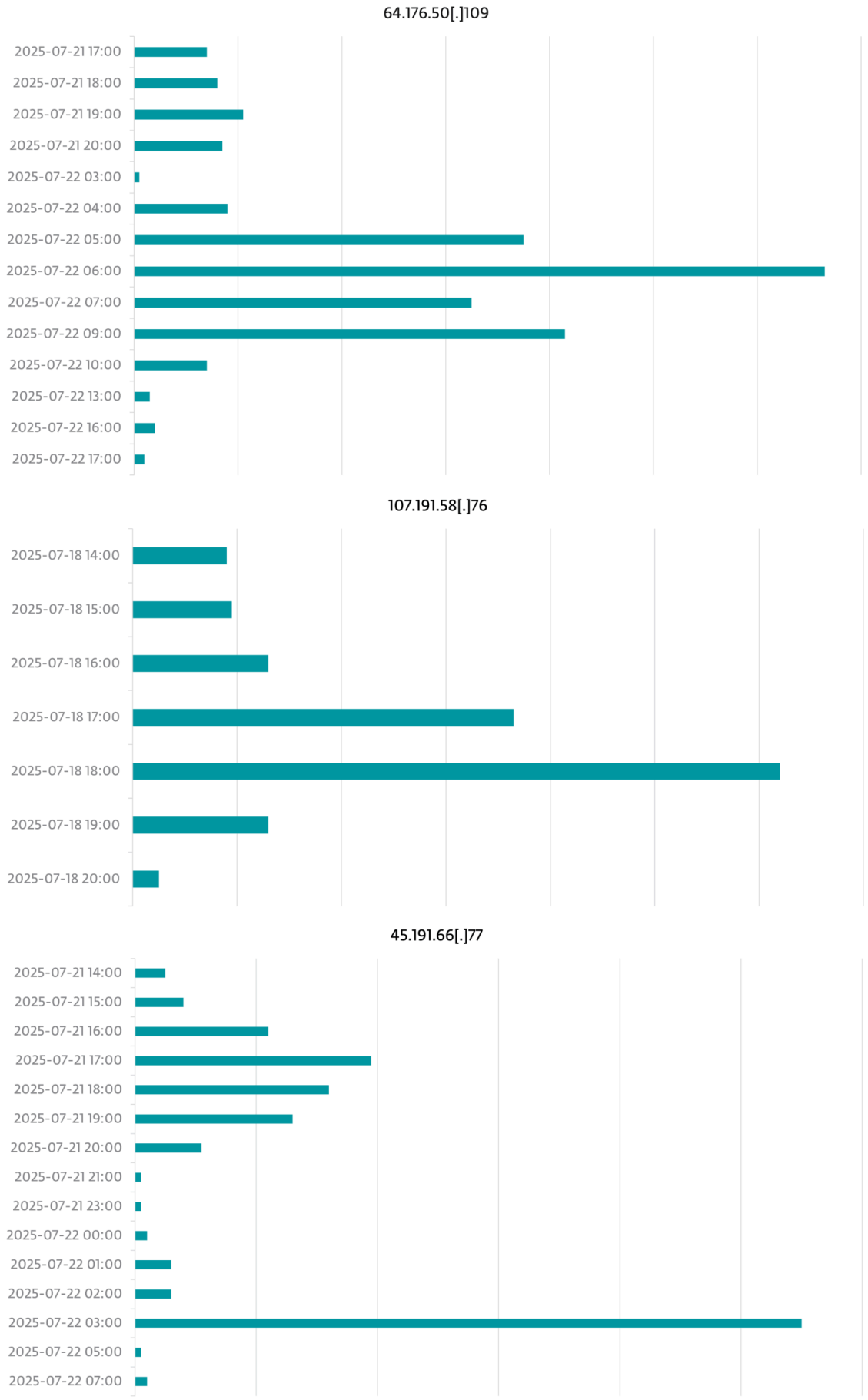

Figure 2. Attacks from the most active IP addresses seen per hour (zero values not shown)

Concerningly, Microsoft has reported that several China-aligned threat actors have joined in on the exploitation attempts. From our side, we detected a backdoor associated with LuckyMouse – a cyberespionage group that targets mainly governments, telecommunications companies, and international organizations – on a machine in Vietnam targeted via ToolShell. At this stage, it remains unclear whether the system had been previously compromised or if the backdoor was introduced during the current attack.

Nevertheless, China-aligned APT groups have certainly seized the opportunity to add the exploit chain to their arsenals: according to our telemetry, the victims of the ToolShell attacks include several high-value government organizations that have been long-standing targets of these groups.

Since the cat is out of the bag now, we expect many more opportunistic attackers to take advantage of unpatched systems. The exploit attempts are ongoing and will surely continue. Therefore, if you are using SharePoint Server, the following is recommended (as per guidance from Microsoft):

- use only supported versions,
- apply the latest security updates,
- make sure that Antimalware Scan Interface is turned on and configured properly, with an appropriate cybersecurity solution, and
- rotate SharePoint Server ASP.NET machine keys.

> *For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.*
>
> *ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.*

IoCs

A comprehensive list of indicators of compromise (IoCs) and samples can be found in our GitHub repository.

Files

SHA-1	Filename	Detection	Description
F5B60A8EAD96703080E7 3A1F79C3E70FF44DF271	spinstall0.aspx	MSIL/Webshell.JS	Webshell deployed via SharePoint vulnerabilities

Network

IP	Domain	Hosting provider	First seen	Details
96.9.125[.]147	N/A	BL Networks	2025-07-17	IP address exploiting SharePoint vulnerabilities.

IP	Domain	Hosting provider	First seen	Details
107.191.58[.]76	N/A	The Constant Company, LLC	2025-07-18	IP address exploiting SharePoint vulnerabilities.
104.238.159[.]149	N/A	The Constant Company, LLC	2025-07-19	IP address exploiting SharePoint vulnerabilities.
139.59.11[.]66	N/A	DigitalOcean, LLC	2025-07-21	IP address exploiting SharePoint vulnerabilities.
154.223.19[.]106	N/A	Kaopu Cloud HK Limited	2025-07-21	IP address exploiting SharePoint vulnerabilities.
103.151.172[.]92	N/A	IKUUU NETWORK LTD	2025-07-21	IP address exploiting SharePoint vulnerabilities.
45.191.66[.]77	N/A	VIACLIP INTERNET E TELECOMUNICAÇÕES LTDA	2025-07-21	IP address exploiting SharePoint vulnerabilities.
83.136.182[.]237	N/A	Alina Gatsaniuk	2025-07-21	IP address exploiting SharePoint vulnerabilities.
162.248.74[.]92	N/A	xTom GmbH	2025-07-21	IP address exploiting SharePoint vulnerabilities.
38.54.106[.]11	N/A	Kaopu Cloud HK Limited	2025-07-21	IP address exploiting SharePoint vulnerabilities.
206.166.251[.]228	N/A	BL Networks	2025-07-21	IP address exploiting SharePoint vulnerabilities.
45.77.155[.]170	N/A	Vultr Holdings, LLC	2025-07-21	IP address exploiting SharePoint vulnerabilities.

IP	Domain	Hosting provider	First seen	Details
64.176.50[.]109	N/A	The Constant Company, LLC	2025-07-21	IP address exploiting SharePoint vulnerabilities.
149.28.17[.]188	N/A	The Constant Company, LLC	2025-07-22	IP address exploiting SharePoint vulnerabilities.
173.239.247[.]32	N/A	GSL Networks Pty LTD	2025-07-22	IP address exploiting SharePoint vulnerabilities.
109.105.193[.]76	N/A	Haruka Network Limited	2025-07-22	IP address exploiting SharePoint vulnerabilities.
2.56.190[.]139	N/A	Alina Gatsaniuk	2025-07-22	IP address exploiting SharePoint vulnerabilities.
141.164.60[.]10	N/A	The Constant Company, LLC	2025-07-22	IP address exploiting SharePoint vulnerabilities.
124.56.42[.]75	N/A	IP Manager	2025-07-22	IP address exploiting SharePoint vulnerabilities.

MITRE ATT&CK techniques

This table was built using version 17 of the MITRE ATT&CK framework**.**

Tactic	ID	Name	Description
Initial Access	T1190	Exploit Public-Facing Application	Threat actors exploited CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, and CVE-2025-53771 to compromise on-premises Microsoft SharePoint servers.
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	The deployed webshells execute attacker-supplied commands via cmd.exe.

Tactic	ID	Name	Description
Persistence	T1505.003	Server Software Component: Web Shell	Threat actors deployed webshells to compromised servers.
Collection	T1005	Data from Local System	The deployed webshells allow the attackers to extract information from the compromised systems.

Let us keep you up to date

Sign up for our newsletters