SharePoint ToolShell Exploitation, Campaign C0058

Archived: 2026-04-05 16:23:00 UTC

Enterprise T1583 .001 Acquire Infrastructure: Domains

During SharePoint ToolShell Exploitation, threat actors registered C2 domains to spoof legitimate Microsoft domains.[1][2]

Enterprise T1595 .002 Active Scanning: Vulnerability Scanning

During SharePoint ToolShell Exploitation, threat actors scanned for SharePoint servers vulnerable to CVE-2025-53770.[2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

During SharePoint ToolShell Exploitation, threat actors issued HTTP `POST` requests to web shells with spoofed or empty Referrer headers, to circumvent authorization controls.[1][3][5][6][2]

Enterprise T1119 Automated Collection

During SharePoint ToolShell Exploitation, threat actors used a command shell to automatically iterate through web.config files to expose and collect machineKey settings.[5][2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

During SharePoint ToolShell Exploitation, threat actors used PowerShell to execute attacker-controlled encoded commands.[1][3][6][2]

.003 Command and Scripting Interpreter: Windows Command Shell

During SharePoint ToolShell Exploitation, threat actors utilized `cmd.exe` and batch scripts within the victim environment.[1][4][3][6]

Enterprise T1486 Data Encrypted for Impact

During SharePoint ToolShell Exploitation, threat actors deployed ransomware including 4L4MD4R and Warlock.[1][2]

Enterprise T1005 Data from Local System

During SharePoint ToolShell Exploitation, threat actors extracted information from the compromised systems.[1][4][6][2]

Enterprise T1074 .001 Data Staged: Local Data Staging

During SharePoint ToolShell Exploitation, threat actors staged stolen data from web.config files to debug_dev.js.[2][5]

Enterprise T1140 Deobfuscate/Decode Files or Information

During SharePoint ToolShell Exploitation, threat actors decrypted scripts prior to execution.[2]

Enterprise T1484 .001 Domain or Tenant Policy Modification: Group Policy Modification

During SharePoint ToolShell Exploitation, threat actors, including Storm-2603, modified group policy to enable ransomware distribution.[1]

Enterprise T1585 .002 Establish Accounts: Email Accounts

During SharePoint ToolShell Exploitation, threat actors created Proton mail accounts for communication with organizations infected with ransomware.[2]

Enterprise T1041 Exfiltration Over C2 Channel

During SharePoint ToolShell Exploitation, threat actors exfiltrated stolen credentials and internal data over HTTPS to C2 infrastructure.[1]

Enterprise T1190 Exploit Public-Facing Application

During SharePoint ToolShell Exploitation, threat actors exploited authentication bypass and remote code execution vulnerabilities (CVE-2025-49706 and CVE-2025-49704) against on-premises SharePoint servers. This activity was characterized by crafted `POST` requests to the ToolPane endpoint `/_layouts/15/ToolPane.aspx`.[1][4][3][5][6][2]

Enterprise T1083 File and Directory Discovery

During SharePoint ToolShell Exploitation, threat actors leveraged commands to locate accessible file shares, backup paths, or SharePoint content.[1]

Enterprise T1657 Financial Theft

During SharePoint ToolShell Exploitation, threat actors demanded ransom payments to unencrypt filesystems and to refrain from publishing sensitive data exfiltrated from victim networks.[2]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

During SharePoint ToolShell Exploitation, threat actors disabled Microsoft Defender through Registry settings and real-time monitoring via PowerShell.[1][2]

Enterprise T1105 Ingress Tool Transfer

During SharePoint ToolShell Exploitation, threat actors used a loader to download and execute ransomware.[2]

Enterprise T1570 Lateral Tool Transfer

During SharePoint ToolShell Exploitation, threat actors used Impacket to remotely stage and execute payloads via WMI.[1]

Enterprise T1112 Modify Registry

During SharePoint ToolShell Exploitation, threat actors, including Storm-2603, disabled security services via Registry modifications.[1]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

During SharePoint ToolShell Exploitation, threat actors UPX-packed malicous payloads including 4L4MD4R ransomware.[2]

.010 Obfuscated Files or Information: Command Obfuscation

During SharePoint ToolShell Exploitation, threat actors executed Base64-encoded PowerShell commands.[1][3][5][6][2]

Enterprise T1588 .002 Obtain Capabilities: Tool

During SharePoint ToolShell Exploitation, threat actors leveraged tools including Impacket, PsExec, and Mimikatz.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

During SharePoint ToolShell Exploitation, threat actors used Mimikatz to dump LSASS memory.[1]

Enterprise T1572 Protocol Tunneling

During SharePoint ToolShell Exploitation, threat actors utilized ngrok tunnels to deliver PowerShell payloads.[1]

Enterprise T1090 Proxy

During SharePoint ToolShell Exploitation, threat actors used Fast Reverse Proxy to communicate with C2.[1][4]

Enterprise T1620 Reflective Code Loading

During SharePoint ToolShell Exploitation, threat actors reflectively loaded payloads using `System.Reflection.Assembly.Load`.[1][3][5][6][2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

During SharePoint ToolShell Exploitation, threat actors used scheduled tasks to help establish persistence.[1]

Enterprise T1505 .003 Server Software Component: Web Shell

During SharePoint ToolShell Exploitation, threat actors followed exploitation of SharePoint servers with installation of a malicious .aspx web shell (spinstall0.aspx) that was written to the `_layouts/15/` directory, granting persistent HTTP-based access.[1][4][3][5][6][2]

.004 Server Software Component: IIS Components

During SharePoint ToolShell Exploitation, threat actors modified Internet Information Services (IIS) components to load suspicious .NET assemblies for persistence.[1]

Enterprise T1082 System Information Discovery

During SharePoint ToolShell Exploitation, threat actors fingerprinted targeted SharePoint servers to identify OS version and running processes.[1]

Enterprise T1033 System Owner/User Discovery

During SharePoint ToolShell Exploitation, threat actors executed `whoami` on victim machines to enumerate user context and validate privilege levels.[1][6]

Enterprise T1569 .002 System Services: Service Execution

During SharePoint ToolShell Exploitation, threat actors leveraged PsExec for command execution and used `services.exe` to disable Microsoft Defender via Registry keys.[1]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

During SharePoint ToolShell Exploitation, threat actors accessed web.config and machine.config to extract MachineKey values, enabling them to forge legitimate VIEWSTATE tokens for future deserialization payloads.[1][3][5][6][2]

Enterprise T1047 Windows Management Instrumentation

During SharePoint ToolShell Exploitation, threat actors used WMI for execution.[1]
