ADVISORY FOR ICM SECTOR

# Storm-2603 exploits SharePoint vulnerabilities to deliver backdoor and Warlock ransomware

Original report published on: Aug 2025[1]

## Executive Summary

Since July 2025, Storm-2603 and CL-CRI-1040, believed to be related, are primarily financially motivated to use ToolShell and exploit internet-facing on-premise Sharepoint Servers (CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, and CVE-2025-53771). The threat actor then conducts remote execution, drop web shells, steal machine keys, move laterally and in many cases deploy malware toolkit named Project AK47, which includes a modular backdoor, WarLock ransomware and loaders.

## Background

Palo Alto Unit 42 researchers have identified a financially motivated threat cluster known as CL-CRI-1040, which overlaps with Microsoft's previously reported Storm-2603 activity. This group has been exploiting recently disclosed SharePoint vulnerabilities, collectively referred as "ToolShell" (CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, and CVE-2025-53771) to deploy a specialised malware toolkit named Project AK47. This toolkit includes a modular backdoor, warlock ransomware, and loaders.

The primary backdoor, AK47C2 supports both DNS and HTTP protocols for command-and-control communications, encrypts data, terminates processes, and demands ransom. Malicious loaders are deployed using DLL side loading enabling the attackers to evade signature-based detection.

This campaign highlights how financially motivated actors are increasing adopting advanced modular toolkits and exploiting trusted infrastructure including SharePoint vulnerabilities to launch complex, widespread ransomware attack. Organisations should prioritize patching these SharePoint vulnerabilities and implement robust security measures to detect and mitigate potential exploitation attempts.

Cisco Talos also reported on threat actors exploiting the same SharePoint vulnerabilities to deploy Velociraptor (open source EDR) for command and control (C2) and Visual Studio Code Tunnel for maintaining persistence. [2]

## Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the Microsoft Sharepoint attacks identified in this advisory:

- Scan for Indicators of Compromise listed in Annex A to detect potential threat activities.
- Refer to the MITRE ATT&CK techniques in Annex B to create, test, and validate detection rules against the observed threat behaviours.

- Apply the latest Microsoft security updates immediately and/or upgrade to supported SharePoint versions.
- Rotate cryptographic keys (e.g. ASP.NET machine keys), restart SharePoint-related services, and deploy EDR (Endpoint Detection Response).
- Enable AMSI (Anti-Malware Scan Interface) on Windows OS to detect any suspicious DLL side-loading behavior and anomalous process injection.
- Implement detection rules for suspicious Visual Studio Code tunnel installations and traffic.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

## Annex A - Indicators of Compromise

| SHA256 | Description |
|---|---|
| 4147a1c7084357463b35071eab6f4525a94476b40336ebbf8a4e54eb9b51917f | AK47 Ransomware |
| 79bef5da8af21f97e8d4e609389c28e0646ef81a6944e329330c716e19f33c73 | AK47 Ransomware |
| a919844f8f5e6655fd465be0cc0223946807dd324fcfe4ee93e9f0e6d607061e | AK47 Ransomware |
| f711b14efb7792033b7ac954ebcfaec8141eb0abafef9c17e769ff96e8fecdf3 | AK47 Ransomware / Warlock link |
| 55a246576af6f6212c26ef78be5dd8f83e78dd45aea97bb505d8cee1aeef6f17 | AK47 Ransomware / X2anylock |
| abb0fa128d3a75e69b59fe0391c1158eb84a799ddb0abc55d2d6be3511ef0ea1 | AK47 Ransomware / X2anylock |
| ceec1a2df81905f68c7ebe986e378fec0805aebdc13de09a4033be48ba66da8b | AK47C2 dnsclient |
| 1eb914c09c873f0a7bcf81475ab0f6bdfaccc6b63bf7e5f2dbf19295106af192 | AK47C2 dnsclient |
| 257fed1516ae5fe1b63eae55389e8464f47172154297496e6f4ef13c19a26505 | AK47C2 dnsclient |
| b5a78616f709859a0d9f830d28ff2f9dbbb2387df1753739407917e96dadf6b0 | AK47C2 dnsclient |
| c27b725ff66fdfb11dd6487a3815d1d1eba89d61b0e919e4d06ed3ac6a74fe94 | AK47C2 dnsclient |
| 24480dbe306597da1ba393b6e30d542673066f98826cc07ac4b9033137f37dbf | AK47C2 httpclient |
| 268ddfa3f7ea9324ae6305824e5dbb32b7f0810d55165f67bbff26b633038172 | create_dump.exe |
| f6ee01303cf1d68015eee49f7dc7f26151a04ae642a47e49c70806931ce652d3 | googleApiUtil64.sys (BYOVD) |
| 7638069eeccf3cd7026723d794a7fd181c9fe02cecc1d1a98cf79b8228132ef5 | IIS_backdoor |
| 6f6db63ece791c6dc1054f1e1231b5bbcf6c051a49bad0784569271753e24619 | IIS_backdoor |
| 1d85b18034dc6c2e9d1f7c982a39ca0d4209eb6c48ace89014924eae6532e6bc | Loader |
| 7e9632ab1898c47c46d68b66c3a987a0e28052f3b59d51c16a8e8bb11e386ce8 | Loader |
| 7c31d43b30bda3a891f0332ee5b1cf610cdc9ecf772cea9b073ac905d886990d | Loader |
| 3b013d5aec75bf8aab2423d0f56605c3860a8fbd4f343089a9a8813b15ecc550 | LockBit 3.0 Dropper |
| dbf5ee8d232ebce4cd25c0574d3a1ab3aa7c9caf9709047a6790e94d810377de | LockBit 3.0 Loader |
| f06fe1c3e882092a23002bed3e170da7b64e6b4475acdedea1433a874b10afdf | LockBit Black / Warlock-linked |
| 5cc047a9c5bb2aa6a9581942b9d2d185815aefea06296c8195ca2f18f2680b3e | masscan |
| 078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b | PsExec |

| | |
|---|---|
| edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef | PsExec64 |
| 0f4b0d65468fe3e5c8fb4bb07ed75d4762e722a60136e377bdad7ef06d9d7c22 | PyPyKatz |
| 040d7ee5b7bb0b978220be326804fa827f6284c8478a27af88c616fcacfeb423 | SecurityCheck.exe |
| f01675f9ca00da067bdb1812bf829f09ccf5658b87d3326d6fddd773df352574 | SharpAdidnsdump |
| d6da885c90a5d1fb88d0a3f0b5d9817a82d5772d5510a0773c80ca581ce2486d | SharpHostInfo |
| 86a6cb73840dfef8542387e4a6e68c65b47afd6bf3dda11e00e53836eb7d6a0f | TrickDump |
| f9fa3b2e2404c2016d4d6f0ff1d6e511ed741c0ba8d9e32cf71935e7d1d548a3 | vmtools.exe (EDR killer) |

| Domain | Description |
|---|---|
| update.updatemicfosoft.com | Fake C2 domain |
| files.qaubctgg.workers.dev | Cloudflare Workers C2 domain |
| velo.qaubctgg.workers.dev | Cloudflare Workers C2 domain |

| Hostname | Description |
|---|---|
| DESKTOP-C1N9M | Threat actor host |

| Regex Domain | Description |
|---|---|
| /^[^.]+\.[a-zA-Z0-9]{8}\.workers\.dev/i | Pattern for Cloudflare Workers C2 domains |

## Annex B - MITRE ATT&CK Tactics and Techniques

| Tactic | Technique ID | Technique Name |
|---|---|---|
| Initial Access | T1190 | Exploit Public-Facing Application |
| Execution | T1059.001 | Command and Scripting Interpreter: PowerShell |
| Execution | T1059.003 | Command and Scripting Interpreter: Windows Command Shell |
| Persistence | T1136.001 | Create Account: Local Account |
| Persistence | T1505.003 | Server Software Component: Web Shell |
| Privilege Escalation | T1068 | Exploitation for Privilege Escalation |
| Defense Evasion | T1078.003 | Valid Accounts: Local Accounts |
| Defense Evasion | T1218.007 | System Binary Proxy Execution: Msiexec |
| Defense Evasion | T1218.011 | System Binary Proxy Execution: Rundll32 |
| Defense Evasion | T1562.001 | Impair Defenses: Disable or Modify Tools |
| Credential Access | T1003.001 | OS Credential Dumping: LSASS Memory |
| Credential Access | T1003.002 | OS Credential Dumping: Security Account Manager |
| Discovery | T1016 | System Network Configuration Discovery |
| Discovery | T1049 | System Network Connections Discovery |
| Discovery | T1057 | Process Discovery |
| Discovery | T1087.001 | Account Discovery: Local Account |
| Discovery | T1482 | Domain Trust Discovery |
| Lateral Movement | T1021.001 | Remote Services: Remote Desktop Protocol |

| | | |
|---|---|---|
| Lateral Movement | T1021.002 | Remote Services: SMB/Windows Admin Shares (PsExec) |
| Command and Control | T1071.001 | Application Layer Protocol: Web Protocols |
| Command and Control | T1090 | Proxy |
| Command and Control | T1105 | Ingress Tool Transfer |

**References**

1. Project AK47: Uncovering a Link to the SharePoint Vulnerability Attacks
2. Velociraptor leveraged in ransomware attacks