TIR-20250730 ToolShell - Chinese State Threat Actors Breach U.S. Agencies via SharePoint Zero-Days

7/30/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

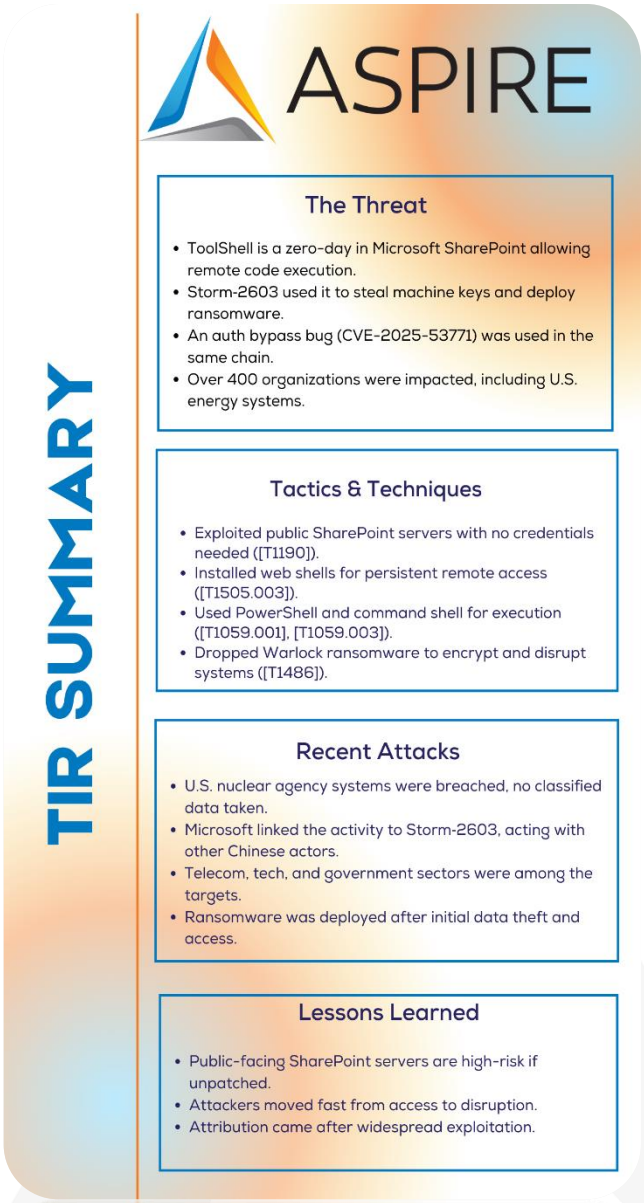
TABLE OF CONTENTS

EXECUTIVE SUMMARY

In July 2025, Microsoft disclosed that multiple Chinese state-linked threat actors exploited zero-day vulnerabilities in Microsoft SharePoint Server to conduct a widespread cyber campaign. The attackers used a custom backdoor known as **"ToolShell"** to quietly compromise hundreds of systems across public and private sectors, including multiple U.S. government agencies. While the activity initially focused on credential theft and lateral movement, it later escalated into ransomware attacks.

This campaign stands out not just for its technical execution, but for its boldness. The threat actors didn't try to hide their tracks and infrastructure, payloads, and tactics all linked back to known Chinese APT groups. The targets were not random and included agencies tied to national security, public health, and critical infrastructure. The attackers weren't just after access, and the attacks were deliberate in how and where the threat actors used it. The threat actors appeared to focus on targets that would draw attention, including agencies tied to national security and public health.

SharePoint is a widely used enterprise tool and using it as the entry point is a calculated choice. Many organizations still run on-premises instances, often without



actively monitoring or patching, which makes them an ideal target. Let's break down ToolShell, the fallout, and the threat actors behind the exploitation.

TOOLSHELL

ToolShell was deployed through chained exploitation of three SharePoint vulnerabilities. Those vulnerabilities are CVE-2025-53770, CVE-2025-53771, CVE-2025-48704, and CVE-2025-49706. Together, these vulnerabilities allowed for remote code execution with no authentication, allowing attackers to gain a strong foothold inside targeted networks. The backdoor itself blended into SharePoint's native processes and used PowerShell for persistence and remote command execution. This made it appear benign on the surface while granting full control to the attackers behind the scenes.

The real threat of ToolShell came from how seamlessly it hid in plain sight, not just the flaws it abused. The malware relied on trusted internal services and legitimate scripting tools, making it difficult for traditional security products to catch. Infected systems didn't show obvious signs of compromise, and in many cases, defenders didn't detect the breach until days or weeks later. The campaign worked because it didn't draw attention. By the time it was noticed, the damage was done.

CVE-2025-49706

- A spoofing (authentication bypass) vulnerability allowing an attacker to craft a malicious request to the ToolPane.aspx endpoint with a manipulated Referer header, bypassing authentication checks.
- **CVSS Score** - 6.3 (Medium)

CVE-2025-49704

- A code-injection (Remote Code Execution) vulnerability in SharePoint's unsafe deserialization logic, enabling execution of arbitrary payloads when chained with CVE-2025-49706.
- CVSS Score - 8.8 (High)

CVE-2025-53770

- A patch-bypass variant of CVE-2025-49704: unsafe deserialization remains exploitable due to incomplete remediation in initial fixes. This direct zero-day allows unauthenticated RCE via hidden data deserialization on ToolPane.aspx.
- CVSS Score - 9.8 (Critical)

CVE-2025-53771

- A path-traversal/spoofing bypass of CVE-2025-49706: attackers evade the prior patch by appending a slash or crafting paths to bypass authentication logic. Frequently used in conjunction with CVE-2025-53770.
- CVSS Score - 6.3 (Medium)

Microsoft's investigation revealed that the attackers may have had early access to vulnerability information, perhaps through a leak within Microsoft's own ecosystem or a partner program. The speed of the attacks and how quickly they bypassed early patches raised alarms about how zero-day knowledge may be getting into the hands of state-aligned groups before the public ever sees it. ToolShell wasn't built overnight and likely took months of planning and testing to perfect.

Threat Actors Exploit ToolShell

Violet Typhoon and Linen Typhoon

Microsoft attributed the broader ToolShell campaign to a group of Chinese state-affiliated threat actors - Storm-2603, Violet Typhoon (formerly Zirconium), and Linen Typhoon. Each group brought a different strength to the table. Violet Typhoon and Linen Typhoon have long focused on political targets, NGOs, and diplomatic entities. The groups often use subtle, stealthy techniques to avoid detection. Take a look at Violet Typhoon's and Linen Typhoon's tools, as well as their tactics, techniques, and procedures (TTPs):

Violet Typhoon (aka Bronze Vinewood, APT31, Judgment Panda)

Tools

- Custom PowerShell loaders
- DLL side-loading techniques
- Living-off-the-land binaries (LOLBins)
- Credential harvesting utilities (undisclosed)
- ToolShell – initial access and backdoor control

TTPs in ToolShell Attacks

- [T1190] Exploit Public-Facing Application – SharePoint exploitation
- [T1059.001] Command and Scripting Interpreter: PowerShell – used in scripts and payloads
- [T1071.001] Application Layer Protocol: Web Protocols – C2 communication over HTTP/S
- [T1055] Process Injection – used for stealth and evasion
- [T1070.004] Indicator Removal on Host: File Deletion – to remove logs/artifacts
- [T1087] Account Discovery – used for privilege mapping

Linen Typhoon (aka APT27, Emissary Panda, Bronze Union)

Tools

- Custom .NET backdoors
- Web shells
- Exploit frameworks (custom)
- LOLBins (e.g., CertUtil, bitsadmin)
- ToolShell – initial foothold

TTPs in ToolShell Attacks

- [T1190] Exploit Public-Facing Application – for gaining access to SharePoint

- [T1505.003] Server Software Component: Web Shell – persistent access
- [T1059] Command and Scripting Interpreter – general execution
- [T1082] System Information Discovery – environment profiling
- [T1036] Masquerading – blending in with system processes
- [T1562.001] Impair Defenses: Disable or Modify Tools – tampering with AV or EDR

Storm-2603

Storm-2603, on the other hand, is known for shifting into destructive mode once the window for stealth closes. This group has previously used LockBit in similar scenarios, where ransomware was deployed to destroy evidence or drive media coverage away from espionage.

Their tactics in ToolShell reflect this same playbook. The threat actors get in quietly and pivot when caught. This strategy causes enough damage to delay response. Take a look at Storm-2603's tools, as well as TTPs below:

Tools

- Mimikatz – credential dumping
- PsExec – lateral movement
- Impacket – lateral movement, remote execution
- Windows Management Instrumentation (WMI) – remote command execution
- Group Policy Objects (GPO) – mass ransomware deployment
- Warlock ransomware – encryption and impact phase
- PowerShell – script-based execution
- ToolShell – backdoor access

TTPs in ToolShell Attacks

- [T1190] Exploit Public-Facing Application – SharePoint zero-day exploit for initial access
- [T1059.001] Command and Scripting Interpreter: PowerShell – execution of ToolShell and other commands

- [T1003.001] OS Credential Dumping: LSASS Memory – credential harvesting using Mimikatz
- [T1021.002] Remote Services: SMB/Windows Admin Shares – lateral movement via PsExec/Impacket
- [T1047] Windows Management Instrumentation – remote execution across hosts
- [T1486] Data Encrypted for Impact – Warlock ransomware used to encrypt files

Storm-2603 is assessed with moderate confidence to be a China-based threat actor. Microsoft observed Storm-2603 operating alongside Violet Typhoon and Linen Typhoon during the ToolShell campaign but there is currently no public evidence directly linking the group to the Chinese government or military.

However, Microsoft has stated that Storm-2603 does not appear to be affiliated with Violet Typhoon and Linen Typhoon and has not shown signs of direct control or command alignment with Chinese government entities. While the group's geographic origin and operational overlap raise suspicion, attribution remains limited to geographic association, not confirmed state sponsorship.

APT31

APT31 is also relevant here. Though not publicly linked to ToolShell, APT31 was recently blamed for a separate campaign targeting the Czech Ministry of Foreign Affairs and its critical infrastructure. That campaign also involved long-term access and information theft and may have shared tactics or coordination with the ToolShell attackers. Taken together, these incidents show how various China-based intelligence units are linked and working in parallel (and sometimes in tandem) against Western governments and infrastructure.

WARLOCK RANSOMWARE

Warlock ransomware became a key phase in the ToolShell campaign only after Storm-2603 joined the operation. Prior to their involvement, activity was limited to quiet

backdoor access and data theft. Around July 18, Storm-2603 began using their foothold to deploy Warlock across compromised networks, marking a shift from espionage to ransomware.

The group delivered the payload by modifying Group Policy Objects and using previously established administrative access to spread the ransomware laterally. Microsoft noted that Storm-2603 has used LockBit in past operations, often to obscure attribution or destroy forensic evidence. Warlock may have served a similar dual role by disrupting systems while also masking the campaign's broader objectives.

Ransom notes appeared on infected systems demanding payment in cryptocurrency, but technical details of the malware are limited. So far, there is no evidence that any impacted U.S. agencies paid the ransom. The appearance of Warlock ransomware in the later stages of the operation marked a shift in intent and showed that the attackers were not just after information. They wanted to leave lasting damage.

Attacks and Global Impact

The impact of the ToolShell campaign was global, and the impact continues to grow. Confirmed U.S. victims included high-value federal agencies, education organizations, healthcare organizations, and telecommunications organizations. Regions impacted so far are North America (with the U.S logging the highest number of attacks), Europe, Africa, the Middle East, and Asia Pacific Take a look at some of the campaign's targets below:

National Nuclear Security Administration (NNSA)

Beginning around July 18, 2025, the threat actor Storm-2603 leveraged the ToolShell exploit chain (CVE-2025-49704 and CVE-2025-49706) to target on-premises Microsoft SharePoint servers used by NNSA. Despite targeting infrastructure tied to U.S. nuclear weapons oversight, no classified information was accessed.

According to the Department of Energy, only a very small number of systems were affected. Because NNSA primarily uses cloud-hosted SharePoint Online (M365) and maintains strong cybersecurity controls, the breach was contained quickly. The

department stated that the breach had minimal impact and that affected systems were in the process of being restored.

National Institutes of Health (NIH)

The National Institute of Health (NIH) was one of several U.S. agencies breached during the SharePoint zero-day attacks that began around July 18, 2025. As a precaution, NIH officials disconnected eight internal servers after suspicious activity was detected. One server was confirmed compromised, while two others showed signs of attempted intrusions that were ultimately blocked. At that stage, there was no indication that sensitive research data or patient information was stolen.

The NIH launched a full investigation into the incident and is currently continuing efforts to restore affected systems. Security teams are still working to keep the breach contained and stop any future attempts of getting back in.

Other Attacks

Outside the U.S., reports stated that there were successful compromises of government entities across Europe and the Middle East. While the exact identities of those victims haven't been disclosed, Eye Security and Microsoft both confirmed that more than 400 SharePoint servers were compromised in total. Many of the victims were still running older, unpatched versions of SharePoint exposed directly to the internet.

Cybersecurity and Infrastructure Security Agency

On July 20, 2025, the Cybersecurity and Infrastructure Security Agency (CISA) responded to ToolShell by issuing an emergency directive and adding CVE-2025-53770 to its Known Exploited Vulnerabilities catalog. However, by the time they issued the warning, the damage was done. The delayed response is a good example of the lag between vulnerability disclosure and active exploitation. Many organizations didn't realize they'd been breached until it was too late - systems were locked, credentials were stolen, and the attackers had already created backdoors.

RECOMMENDATIONS

If your organization uses SharePoint, secure it now. The attackers exploited specific flaws and tools, and these recommendations will help keep your organization safe:

ToolShell Recommendations

- Install the latest SharePoint patches addressing CVE-2025-49704, CVE-2025-49706, and CVE-2025-53770. These were directly exploited in the ToolShell campaign.
- Look for signs of compromise, including unusual service activity, modified Group Policy Objects (GPOs), or suspicious behavior in SharePoint's native processes.
- Monitor for tools like Mimikatz that extract credentials from LSASS memory. Any abnormal access to LSASS should trigger investigation.
- Look for use of PsExec, Impacket, and Windows Management Instrumentation (WMI), which were used to spread ransomware after initial access.
- Review system GPOs and startup folders for unauthorized changes or scheduled tasks that may maintain attacker access.
- Update EDR/AV solutions to detect activity related to PowerShell abuse, WMI execution, and SharePoint exploitation patterns.
- Limit access to tools like PsExec and segment SharePoint environments from critical systems to contain lateral movement.

Now that Warlock ransomware is involved in the ToolShell attacks, it is also important to follow ransomware best practices:

- Make sure backups are segmented from the network and tested regularly for restoration.
- Limit admin rights and restrict lateral movement opportunities.
- Use EDR tools capable of detecting ransomware behavior like file encryption and privilege escalation.

- Watch for sudden changes to Group Policy and remote execution via WMI.
- Segment systems that hold sensitive data to reduce ransomware blast radius.
- Run tabletop exercises to ensure readiness for a ransomware attack.

CONCLUSION

The ToolShell attack started quietly but quickly escalated into something far more disruptive, showing how fast things can spiral once attackers gain a foothold. It started with backdoor access through SharePoint zero-days and escalated when Storm-2603 deployed Warlock ransomware across networks. The attack campaign blended data theft with operational interference, forcing defenders to handle both exposure and recovery at once.

This is a clear example of why detection needs to go beyond patch status. Attackers aren't waiting around. They move fast and often use normal-looking behavior to hide their next step. Every organization still running on-prem systems should be treating this campaign as a warning of what's likely to come next.

MITRE MAP

ToolShell

- Initial Access
  - Exploit Public-Facing Application [T1190] – The attacker exploited a zero-day vulnerability in Microsoft SharePoint to gain unauthorized access without valid credentials.
- Execution

  - Command and Scripting Interpreter: PowerShell [T1059.001] – PowerShell scripts were used to execute follow-on payloads and maintain control.
  - Command and Scripting Interpreter: Windows Command Shell [T1059.003] – The attacker used the command shell to run system commands and interact with compromised machines.
- Persistence
  - Web Shell [T1505.003] – A malicious web shell was deployed to maintain access and allow remote command execution over an extended period.
- Privilege Escalation
  - Abuse Elevation Control Mechanism: Bypass User Access Control [T1548.002] – The attacker bypassed user access controls to escalate privileges and run administrative tasks.
- Defense Evasion
  - Obfuscated Files or Information [T1027] – Scripts and payloads were obfuscated to avoid detection by endpoint and network security tools.
  - Masquerading [T1036] – Files and processes were renamed to mimic legitimate system components.
  - Indicator Removal on Host [T1070] – Logs were cleared to erase signs of intrusion.
- Credential Access
  - Credential Dumping [T1003] – The attacker attempted to collect cached credentials and authentication material for further lateral movement.
- Discovery
  - System Network Connections Discovery [T1049] – Commands were run to map out network connections and identify other reachable systems.
  - Account Discovery [T1087] – The attacker enumerated user accounts and group memberships.
- Lateral Movement
  - Remote Services: SMB/Windows Admin Shares [T1021.002] – Compromised credentials were used to move laterally via shared administrative services.
- Collection
  - Data from Information Repositories [T1213] – The attacker accessed stored digital machine keys and other SharePoint configuration files.
- Command and Control
  - Application Layer Protocol: Web Protocols [T1071.001] – The web shell communicated over HTTP/S for command and control.
  - Ingress Tool Transfer [T1105] – Additional tools and payloads were uploaded to compromised systems from remote servers.

- Impact
  - Data Encrypted for Impact [T1486] – Warlock ransomware was deployed to encrypt files and disrupt operations after data theft.

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

ToolShell

CVEs

- CVE-2025-49704
- CVE-2025-49706
- CVE-2025-53770
- CVE-2025-53771

SHA256

- 0548fad567c22ccf19031671f7ec1f53b735abf93dc11245bc9ea4dfd463fe40
- 10e01ce96889c7b4366cfa1e7d99759e4e2b6e5dfe378087d9e836b7278abfb6
- 3adbebbc2093615bb9210bfdb8ebb0841c62426bee8820f86ff0a64d15206041
- 7e3fff35ef909c556bdf6d9a63f0403718bf09fecf4e03037238176e86cf4e98

IPv4

- 165[.]154[.]196[.]91
- 203[.]160[.8]0[.]77
- 203[.]160[.]86[.]111
- 205[.]198[.]84[.]197

Warlock

IPV4

- 65[.]38[.]121[.]198
- 104[.]238[.]159[.]149
- 131[.]226[.]2[.]6
- 134[.]199[.]202[.]205
- 188[.]130[.]206[.]168

MD5

- 02b4571470d83163d103112f07f1c434
- 2bae4487ccb7cb14ea48947725c452ac

SHA1

- f5b60a8ead96703080e73a1f79c3e70ff44df271
- ffe18db834403070a7e5ab8c0a19637c64f32a4d

SHA256

- 24480dbe306597da1ba393b6e30d542673066f98826cc07ac4b9033137f37dbf
- 445a37279d3a229ed18513e85f0c8d861c6f560e0f914a5869df14a74b679b86
- 4c1750a14915bf2c0b093c2cb59063912dfa039a2adfe6d26d6914804e2ae928
- 567cb8e8c8bd0d909870c656b292b57bcb24eb55a8582b884e0a228e298e7443
- 62881359e75c9e8899c4bc9f452ef9743e68ce467f8b3e4398bebacde9550dea
- 6753b840cec65dfba0d7d326ec768bff2495784c60db6a139f51c5e83349ac4d
- 6b273c2179518dacb1218201fd37ee2492a5e1713be907e69bf7ea56ceca53a5
- 6f6db63ece791c6dc1054f1e1231b5bbcf6c051a49bad0784569271753e24619
- 7ae971e40528d364fa52f3bb5e0660ac25ef63e082e3bbd54f153e27b31eae68
- 83705c75731e1d590b08f9357bc3b0f04741e92a033618736387512b40dab060
- 92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514
- b180ab0a5845ed619939154f67526d2b04d28713fcc1904fbd666275538f431d
- b5a78616f709859a0d9f830d28ff2f9dbbb2387df1753739407917e96dadf6b0
- c27b725ff66fdfb11dd6487a3815d1d1eba89d61b0e919e4d06ed3ac6a74fe94
- c2c1fec7856e8d49f5d49267e69993837575dbbec99cd702c5be134a85b2c139
- d6da885c90a5d1fb88d0a3f0b5d9817a82d5772d5510a0773c80ca581ce2486d
- f54ae00a9bae73da001c4d3d690d26ddf5e8e006b5562f936df472ec5e299441
- ffbc9dfc284b147e07a430fe9471e66c716a84a1f18976474a54bee82605fa9a

SUPPORTING DOCUMENTATION

Inside The ToolShell Campaign - LevelBlue - Open Threat Exchange

Exploitation of SharePoint Vulnerabilities to Deploy Warlock Ransomware - LevelBlue - Open Threat Exchange

Disrupting active exploitation of on-premises SharePoint vulnerabilities | Microsoft Security Blog

Customer guidance for SharePoint vulnerability CVE-2025-53770 | MSRC Blog | Microsoft Security Response Center

Active Exploitation of Microsoft SharePoint Vulnerabilities

UPDATE: Microsoft Releases Guidance on Exploitation of SharePoint Vulnerabilities | CISA

Ransomware Actors Pile on 'ToolShell' SharePoint Bugs

What we know about the Microsoft SharePoint attacks | Cybersecurity Dive

Storm-2603 Exploits SharePoint Flaws to Deploy Warlock Ransomware on Unpatched Systems

SharePoint 'ToolShell' Vulnerabilities Exploited by Chinese Hackers - Infosecurity Magazine

Microsoft SharePoint attack now sees victim count rises to 400 organizations, including US nuclear agency | TechRadar

Microsoft confirms SharePoint vulnerabilities have been exploited by suspected Chinese hackers, as reports indicate the US Nuclear Security Administration may have been among those compromised | PC Gamer

Microsoft knew of SharePoint security flaw but failed to effectively patch it, timeline shows | Reuters

Microsoft SharePoint compromise pinned on potential leak | SC Media

Disrupting active exploitation of on-premises SharePoint vulnerabilities | Microsoft Security Blog

ToolShell Exploit: Critical SharePoint Zero-Day Threatens Global Enterprises

CVE Record: CVE-2025-49704

CVE Record: CVE-2025-49706

Microsoft Links Ongoing SharePoint Exploits to Three Chinese Hacker Groups

Statement by the Government of the Czech Republic | Ministry of Foreign Affairs of the Czech Republic

Czech Republic Blames China-Linked APT31 Hackers for 2022 Cyberattack

Emerging Threat Actor: Warlock Ransomware

New ransomware gang Warlock strikes government agencies worldwide - Comparitech

DHS impacted in hack of Microsoft SharePoint products, people familiar say - Nextgov/FCW

Storm-2603 Threat Intelligence for Damovo Customers - Damovo

China behind vast global hack involving multiple US agencies - POLITICO

New ransomware gang Warlock strikes government agencies worldwide - Comparitech

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.