INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-28 13:44 UTC

Silk Typhoon Contractor Extradited: What the Xu Zewei Case Reveals About MSS Hacker-for-Hire Operations

THREAT ACTOR | HIGH | CVSS 7.5

SCC Item ID	SCC-TAC-2026-0010
Type	Threat Actor
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Exchange Server (2019 and earlier versions exploited via zero-days, February 2020 - June 2021)
Published	2026-04-27T15:56:03
Discovery Source	Rss

Executive Summary

The extradition of Xu Zewei, an alleged contractor for China's Ministry of State Security linked to the Silk Typhoon (Hafnium) APT group, marks a rare legal action against a state-affiliated cyber operator. The underlying campaign exploited Microsoft Exchange Server zero-days between February 2020 and June 2021, targeting defense contractors, COVID-19 researchers, law firms, and infectious disease institutions. This case reinforces that MSS operations rely on contractor fronts to maintain deniability, and that organizations running unpatched Exchange infrastructure remain a preferred vector for state-sponsored espionage.

Technical Analysis

Silk Typhoon (Hafnium) exploited the ProxyLogon vulnerability cluster in Microsoft Exchange Server, publicly disclosed by Microsoft in March 2021, across a campaign spanning February 2020 through June 2021. Affected versions include Exchange Server 2019 and earlier. The exploitation chain combined CWE-918 (server-side request forgery for pre-authentication access), CWE-287 (improper authentication bypass), and CWE-94 (code injection via post-authentication webshell deployment). MITRE ATT&CK techniques observed include T1190 (exploit public-facing application), T1505.003 (web shell), T1078 (valid accounts), T1021 (remote services), T1071.001 (web protocols for C2), T1041 (exfiltration over C2 channel), T1560 (archive collected data), T1083 (file and directory discovery), and T1027 (obfuscated files). The Xu Zewei extradition is the new development; the Exchange intrusion chain is well-documented. CISA maintains Exchange-specific hardening guidance.

Microsoft's current Exchange security updates (August and December 2025) address known vulnerabilities in supported versions; organizations must independently audit for undetected historical compromise from the 2020-2021 campaign period, as no patch eliminates past data exfiltration.

Action Checklist

1. Containment: Audit all Microsoft Exchange Server instances (2019 and earlier) for signs of webshell presence in IIS directories, particularly in paths such as %ExchangeInstallPath%\inetpub\wwwroot\aspnet_client\ and Exchange OWA directories. Isolate any Exchange servers showing anomalous outbound connections pending investigation.
2. Detection: Review IIS logs and Exchange HttpProxy logs for anomalous POST requests to Exchange endpoints (OWA, ECP, EWS) from unexpected source IPs, particularly during February 2020 through June 2021. Search for ASPX files written to web-accessible directories outside of planned deployments. Correlate against T1505.003 webshell indicators documented in Microsoft's March 2021 Hafnium disclosure and CISA guidance at https://www.cisa.gov/resources-tools/resources/microsoft-exchange-server-security-best-practices (T1 source, verified in item data).
3. Eradication: Apply all current Microsoft Exchange cumulative updates and security patches; reference the August 2025 (KB5063221) and December 2025 Exchange security updates documented in the item sources. Remove any unauthorized ASPX files from IIS-hosted Exchange directories. Reset credentials for all accounts with Exchange administrative access, particularly those that authenticated during the campaign window.
4. Recovery: After patching and webshell removal, validate Exchange service integrity against Microsoft's documented baseline configurations. Monitor outbound Exchange traffic for anomalous data transfer volumes (T1041, T1560). Confirm no scheduled tasks, new service accounts, or registry persistence mechanisms were introduced during potential compromise windows.
5. Post-Incident: This campaign exposed the risk of delayed patching on internet-facing Exchange infrastructure and insufficient monitoring of IIS write activity. Implement file integrity monitoring on Exchange IIS directories. Evaluate whether Exchange remains internet-facing without WAF or network-layer access controls, and consider migrating to Exchange Online if on-premises maintenance capacity is limited.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and executive notification if any Exchange server shows webshell artifacts from the Hafnium campaign window, if exfiltrated data includes PHI (HIPAA breach notification trigger), ITAR/CUI-controlled defense information (DFARS 252.204-7012 72-hour reporting to DoD), or if forensic evidence suggests the intrusion is ongoing rather than historical — the Xu Zewei extradition confirms active DOJ interest and evidence must be preserved under legal hold.

Recovery Notes	After patching to current Exchange cumulative updates and removing all webshell artifacts, maintain elevated IIS write-activity monitoring for a minimum of 90 days, as Silk Typhoon operators are known to re-establish access via secondary persistence mechanisms (transport agents, scheduled tasks) that may survive a webshell-only eradication. Validate Exchange mail flow, OWA authentication, and EWS functionality against Microsoft's Exchange Baseline Configuration documentation before returning to production, and confirm with `Test-MAPIConnectivity` and `Test-OWAConnectivity` cmdlets. Given that the Hafnium campaign ran undetected for over a year in many environments, treat any anomalous outbound HTTPS traffic from Exchange servers — particularly to non-Microsoft cloud endpoints — as a re-compromise indicator requiring immediate re-containment.
Forensic Artifacts	ASPX/ASHX webshell files in C:\inetpub\wwwroot\aspnet_client\ and Exchange OWA/ECP virtual directories — Hafnium dropped China Chopper variants and custom webshells at these exact paths; preserve with SHA-256 hashes before removal as primary evidence of Silk Typhoon tooling | IIS W3SVC access logs at C:\inetpub\logs\LogFiles\W3SVC1\ showing POST requests to /ecp/DDI/DDIService.svc/GetObject (CVE-2021-26857 exploitation path) and /owa/auth/Current/ from unexpected external IPs during the February 2020 – June 2021 window | Exchange HttpProxy logs at C:\Program Files\Microsoft\Exchange Server\V15\Logging\HttpProxy\ containing SSRF exploitation artifacts from CVE-2021-26855, specifically requests where the X-AnonResource-Backend and X-BEResource headers were abused to proxy unauthenticated requests to internal Exchange backend services | Windows Security Event Log Event ID 4688 (Process Creation) records showing w3wp.exe (IIS application pool for Exchange) spawning cmd.exe, powershell.exe, net.exe, or certutil.exe — the execution chain signature of China Chopper-style webshell interaction used by Hafnium operators for post-exploitation | Exchange transport agent registry entries at HKLM\SOFTWARE\Microsoft\ExchangeServer\v15\TransportRoles\Agents and output of Get-TransportAgent PowerShell cmdlet — Silk Typhoon-affiliated operators have used malicious Exchange transport agents to achieve persistent mail interception that survives webshell removal and patching

Per-Action IR Details

Containment — Audit all Microsoft Exchange Server instances (2019 and earlier) for signs of webshell presence in IIS directories, particularly in paths such as \inetpub\wwwroot\aspnet_client\ and Exchange OWA directories. Isolate any Exchange servers showing anomalous outbound connections pending investigation.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems to prevent further adversary access while preserving forensic state prior to eradication.

Controls: NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run the following PowerShell on each Exchange server to enumerate suspicious ASPX files dropped by Hafnium: `Get-ChildItem -Path 'C:\inetpub\wwwroot\aspnet_client\' -Recurse -Include '*.aspx','*.ashx' | Select FullName, LastWriteTime, CreationTime | Export-Csv webshell_audit.csv`. Cross-reference CreationTime against the February 2020 – June 2021 campaign window. For network isolation on a budget, implement a host-based Windows Firewall rule to block all outbound traffic except port 443 to Microsoft update endpoints: `New-NetFirewallRule -DisplayName 'Exchange Isolate' -Direction Outbound -Action Block -Enabled True`. Use Sysinternals Autoruns to check for persistence before isolation.

Evidence: Before isolating, capture a full memory image of the Exchange server using WinPmem or Magnet RAM Capture to preserve any in-memory webshell artifacts or active Silk Typhoon C2 connections. Snapshot IIS application pool process memory (w3wp.exe) specifically, as Hafnium-linked webshells such as China Chopper execute within this process. Export current netstat output (`netstat -anob > netstat_snapshot.txt`) to document live outbound connections

from the Exchange process before network isolation severs them.

Detection — Review IIS logs and Exchange HttpProxy logs for anomalous POST requests to Exchange endpoints (OWA, ECP, EWS) from unexpected source IPs, particularly during February 2020 through June 2021. Search for ASPX files written to web-accessible directories outside of planned deployments. Correlate against T1505.003 webshell indicators documented in Microsoft's March 2021 Hafnium disclosure and CISA guidance at https://www.cisa.gov/resources-tools/resources/microsoft-exchange-server-security-best-practices (T1 source, verified in item data).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: analyze log sources and network indicators to determine scope, timeline, and TTPs of the Silk Typhoon intrusion against Exchange infrastructure.

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: IIS logs are located at `C:\inetpub\logs\LogFiles\W3SVC1\`. Parse them with PowerShell for Hafnium-pattern POST requests to /ecp/ and /owa/ endpoints: `Select-String -Path 'C:\inetpub\logs\LogFiles\W3SVC1\*.log' -Pattern 'POST.*/ecp/|POST.*/owa/|POST.*/EWS/' | Where-Object { $_ -match '4[0-9][0-9]|5[0-9][0-9]' }`. Exchange HttpProxy logs are at `C:\Program Files\Microsoft\Exchange Server\V15\Logging\HttpProxy\`. Use the free Microsoft MSERT (Microsoft Safety Scanner) and the dedicated Exchange On-Premises Mitigation Tool (EOMT) released in March 2021 — both are free, no SIEM required. Additionally, deploy the Sigma rule 'win_webshell_aspx' from the SigmaHQ repository against Windows Security Event Log Event ID 4688 (Process Creation) filtering on w3wp.exe spawning cmd.exe or powershell.exe, which indicates China Chopper-style webshell execution (MITRE T1505.003).

Evidence: Collect IIS W3SVC access logs and Exchange HttpProxy logs covering the full February 2020 – June 2021 window before any log rotation or deletion occurs — archive to write-once storage immediately. Query Windows Security Event Log for Event ID 4688 (Process Creation) where ParentProcessName is w3wp.exe and NewProcessName includes cmd.exe, powershell.exe, or net.exe, which are the execution chain signatures of China Chopper and other webshells used in the Hafnium campaign. Capture Exchange Unified Messaging and OAB (Offline Address Book) virtual directory logs as Silk Typhoon leveraged CVE-2021-26855 (SSRF) specifically to reach these internal Exchange components.

Eradication — Apply all current Microsoft Exchange cumulative updates and security patches; reference the August 2025 (KB5063221) and December 2025 Exchange security updates documented in the item sources. Remove any unauthorized ASPX files from IIS-hosted Exchange directories. Reset credentials for all accounts with Exchange administrative access, particularly those that authenticated during the campaign window.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: eliminate the root cause of the incident by patching the exploited Exchange zero-days, removing implanted webshells, and invalidating credentials harvested or used during the Silk Typhoon campaign window.

Controls: NIST SI-2 (Flaw Remediation), NIST IR-4 (Incident Handling), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.2 (Use Unique Passwords), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Use Microsoft's Exchange Server Health Checker script (free, available on GitHub at https://aka.ms/ExchangeHealthChecker — search-retrieved, recommend human validation) to identify patch gaps before applying KB5063221 or December 2025 updates. For webshell removal, run `Get-ChildItem -Recurse -Path 'C:\inetpub\wwwroot' -Include '*.aspx','*.ashx' | Where-Object { $_.CreationTime -gt '2020-01-01' } | Remove-Item -WhatIf` first to preview, then execute without `-WhatIf` after manual review. For credential reset, use Active Directory bulk password reset via PowerShell: `Get-ADUser -Filter {MemberOf -RecursiveMatch (Get-ADGroup 'Exchange Organization Administrators').DistinguishedName} | Set-ADAccountPassword -Reset`. For accounts that authenticated

during the campaign window, also revoke all active Exchange tokens by running `Get-ActiveSyncDeviceStatistics` and purging sessions.

Evidence: Before removing webshell files, hash and preserve each file using `Get-FileHash -Algorithm SHA256 ` and copy to an isolated evidence share — these ASPX files constitute primary forensic evidence of Silk Typhoon tooling and may include China Chopper variants or custom implants. Export Exchange audit logs (`Search-AdminAuditLog`) for all administrative actions taken during the February 2020 – June 2021 window to document what data was accessed or exfiltrated before credentials are reset, preserving the evidentiary chain. Collect `HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeTransport` and related service registry keys before patching to detect any persistence mechanisms introduced by Silk Typhoon operators alongside the webshell.

Recovery — After patching and webshell removal, validate Exchange service integrity against Microsoft's documented baseline configurations. Monitor outbound Exchange traffic for anomalous data transfer volumes (T1041, T1560). Confirm no scheduled tasks, new service accounts, or registry persistence mechanisms were introduced during potential compromise windows.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore Exchange to a known-good operational state, verify no persistence from Silk Typhoon operators remains, and establish enhanced monitoring to detect any re-compromise or staged data exfiltration.

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysinternals Autoruns against each Exchange server and export to XML: `autorunsc.exe -a * -c -h > autoruns_output.csv` — review for any scheduled tasks or service registrations with creation timestamps falling in the February 2020 – June 2021 window, which would indicate Silk Typhoon persistence beyond webshells. For outbound traffic monitoring without a SIEM, configure Windows Firewall audit logging and parse with: `Get-WinEvent -LogName 'Security' -FilterXPath "*[System[(EventID=5156)]]" | Where-Object { $_.Message -match 'w3wp' }` to catch Exchange process making unexpected outbound connections (T1041 exfiltration via C2). Use Wireshark on a network tap or SPAN port to capture and baseline Exchange SMTP and HTTPS egress for 30 days post-recovery.

Evidence: Before declaring recovery complete, run `schtasks /query /fo CSV /v > scheduled_tasks.csv` and compare against a known-good Exchange server baseline to detect any Silk Typhoon-planted persistence tasks. Export `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` and `HKLM\SYSTEM\CurrentControlSet\Services` registry hives for timeline analysis — state-sponsored operators frequently install rogue services or modify existing Exchange transport agents as secondary persistence after webshell deployment. Pull Exchange transport agent list via `Get-TransportAgent` cmdlet and verify all entries against Microsoft's documented default agents, as Silk Typhoon-affiliated actors have used malicious transport agents to intercept mail at the server level.

Post-Incident — This campaign exposed the risk of delayed patching on internet-facing Exchange infrastructure and insufficient monitoring of IIS write activity. Implement file integrity monitoring on Exchange IIS directories. Evaluate whether Exchange remains internet-facing without WAF or network-layer access controls, and consider migrating to Exchange Online if on-premises maintenance capacity is limited.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: document lessons learned from the Silk Typhoon/Hafnium campaign, implement structural controls to prevent recurrence, and share threat intelligence consistent with organizational policy.

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SI-4 (System Monitoring), NIST AU-9 (Protection of Audit Information), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Implement file integrity monitoring on Exchange IIS directories using the free Wazuh agent (open source HIDS) configured to alert on any new file creation in `C:\inetpub\wwwroot\aspnet_client\` and Exchange virtual

directory paths — this directly addresses the webshell-drop vector used in the Hafnium campaign. Write a YARA rule targeting China Chopper ASPX webshell signatures (the `eval(Request.Item[` pattern common to variants used by Silk Typhoon-affiliated operators) and schedule a nightly scan via YARA CLI against IIS directories: `yara china_chopper.yar C:\inetpub\wwwroot\ -r`. If WAF procurement is not feasible, restrict Exchange OWA/ECP/EWS access to known IP ranges using Windows Firewall Advanced rules as a network-layer compensating control, eliminating anonymous internet access to the endpoints exploited by CVE-2021-26855.

Evidence: Conduct a formal lessons-learned review documenting the specific delay between Microsoft's March 2, 2021 emergency patch release for CVE-2021-26855/26857/26858/27065 and your organization's patch application date — this gap is the core failure mode that enabled the Hafnium campaign and must be quantified to drive SLA improvements. Preserve the complete incident timeline, all recovered webshell samples, and IIS log extracts in an evidence package aligned with NIST AU-11 (Audit Record Retention) requirements, as the Xu Zewei extradition case demonstrates these incidents may support future law enforcement actions requiring preserved evidence. Review whether any data accessed from Exchange during the campaign window triggers breach notification obligations under applicable regulations (HIPAA if COVID-19 research data, DFARS if defense contractor data), as Silk Typhoon specifically targeted those sectors.

Detection Guidance

Focus detection on Exchange IIS logs (W3SVC logs) and Exchange HttpProxy logs located at %ExchangeInstallPath%\Logging\HttpProxy. Look for POST requests to /ecp/ or /owa/ endpoints from external IPs not associated with known mail clients, particularly requests that return HTTP 200 and involve .aspx file creation events. In Windows Security logs, look for Event ID 4688 (process creation) spawning from w3wp.exe or UMWorkerProcess.exe, which indicates webshell execution (T1505.003). Search for new .aspx files in %ExchangeInstallPath%\inetpub\wwwroot\aspnet_client\ and Exchange virtual directories using file system auditing or EDR telemetry. For network-layer indicators, look for unusual outbound HTTPS connections from Exchange servers to non-Microsoft IP ranges, consistent with T1071.001 C2 over web protocols and T1041 exfiltration. CISA's Exchange hardening resource (T1 source in item data) includes additional detection recommendations. Note: specific IOCs from the Xu Zewei indictment are not yet publicly released in detail; monitor DOJ and CISA advisories for indictment-linked indicators.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Not available`	Specific IOCs from the Xu Zewei indictment have not been publicly released at time of item generation. DOJ and CISA advisories should be monitored for indictment-linked network indicators. Previously published Hafnium/ProxyLogon IOCs from Microsoft's March 2021 disclosure remain relevant for historic log review.	LOW

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1190** — Exploit Public-Facing Application
- **T1078** — Valid Accounts
- **T1071.001** — Web Protocols
- **T1505.003** — Web Shell
- **T1021** — Remote Services
- **T1027** — Obfuscated Files or Information
- **T1560** — Archive Collected Data
- **T1083** — File and Directory Discovery

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-2** — Baseline Configuration
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A10:2021** — Server-Side Request Forgery (SSRF)
- **A03:2021** — Injection

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access

- **13.4** — Perform Traffic Filtering Between Network Segments
- **16.10** — Apply Secure Design Principles in Application Architectures

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1190	Exploit Public-Facing Application	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1071.001	Web Protocols	Command-And-Control
T1505.003	Web Shell	Persistence
T1021	Remote Services	Lateral-Movement
T1027	Obfuscated Files or Information	Defense-Evasion
T1560	Archive Collected Data	Collection
T1083	File and Directory Discovery	Discovery

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/alleged-silk-typhoon...	T3
Description of the security update for Microsoft Exchange Server 2019	https://support.microsoft.com/en-us/topic/description-of-the-securi...	T1
Microsoft Exchange Server Security Best Practices - CISA	https://www.cisa.gov/resources-tools/resources/microsoft-exchange-s...	T1

Source	URL	Tier
Microsoft Exchange Server security vulnerabilities, CVEs, versions ...	https://www.cvedetails.com/product/194/Microsoft-Exchange-Server.ht...	T3
Released: December 2025 Exchange Server Security Updates	https://techcommunity.microsoft.com/blog/exchange/released-december...	T1

Generated 2026-04-28 13:44 UTC by TJS Security Command Center