



Monthly Intelligence Report

August 19, 2025

Date prepared: 08/19/25

Prepared by: Kayla Hodge

Prepared for: Full Sail CISO, Professor McQuiggan

Summary

Recent cyber incidents reveal a clear trend of attackers moving faster to exploit vulnerabilities, leveraging trusted platforms to spread malware, and expanding their reach into new regions. No sector or environment is immune, whether they are government, enterprise, or consumer. The emerging pattern shows adversaries blending technical exploits with strategic delivery methods, making detection and prevention more difficult. These developments emphasize the need for stronger patch management, proactive monitoring, and awareness that personal and organizational risks are increasingly interconnected.

US Nuclear Weapons Agency Hacked in Microsoft SharePoint Attacks

Assessment: The attack on the U.S. National Nuclear Security Administration (NNSA) through a Microsoft SharePoint vulnerability shows the critical risk posed by widely used collaboration platforms. Exploiting an unpatched SharePoint vulnerability gave attackers a foothold inside one of the most sensitive government agencies. The threat extends beyond espionage. Compromised systems tied to nuclear management could threaten national security, disrupt critical defense operations, and destroy public trust. Organizations relying on Microsoft environments face a heightened risk when patching cycles lag or visibility into cloud and on-prem applications is limited. While the NNSA had layered defenses in place, the attackers leveraged stealthy intrusion tactics that bypassed standard detection, raising concerns about zero-day exploitation and vendor supply chain reliance.

Recommendations: Organizations should immediately review and apply Microsoft's latest SharePoint security patches and confirm that critical systems are prioritized in patch management programs. Enhanced monitoring of user activity within SharePoint, particularly around privilege escalation and abnormal data access, is essential. Security teams should consider implementing behavioral analytics to detect suspicious usage patterns. Leadership should be briefed on the



significance of this incident to stress the importance of vulnerability management in critical systems. Given the potential scale of impact, coordination with law enforcement or federal cybersecurity agencies is advised for any organization that suspects compromise.

Next Steps: The Cyber Threat Intelligence (CTI) team needs to close several intelligence gaps to build a complete picture of the SharePoint breach. Adapt Forward (2025) notes that this incident shows how quickly attackers can weaponize newly released vulnerabilities before organizations apply patches. Understanding the exact timeline of exploitation compared to patch deployment is critical to assessing how long the attackers had access. It's also necessary to determine whether backdoors or persistence mechanisms, such as web shells, were installed to maintain access even after the patches were applied. Another key gap is clarifying the adversary's intent, whether the breach was limited to reconnaissance and data theft or if it was designed to prepare for the disruption of critical systems. Enterprise platforms should now represent critical infrastructure. The team must expand monitoring beyond this event to assess whether similar tactics are being used against other sensitive agencies or contractors.

MITRE ATT&CK Model

<i>Reconnaissance</i>	Targeted identification of government agencies using Microsoft SharePoint (T1595 – Active Scanning).
<i>Resource Development</i>	Possible development of exploit tools for SharePoint vulnerabilities (T1587 – Develop Capabilities).
<i>Initial Access</i>	Exploitation of public-facing SharePoint application (T1190 – Exploit Public Facing Application).
<i>Execution</i>	Remote code execution via crafted SharePoint payloads (T1203 – Exploitation for Client Execution).
<i>Persistence</i>	Potential use of web shells or SharePoint service account modifications to maintain access (T1505.003 – Web Shell).
<i>Privilege Escalation</i>	Abuse of SharePoint service accounts or system misconfigurations to gain elevated privileges (T1068 – Exploitation for Privilege Escalation).
<i>Defense Evasion</i>	Obfuscation of malicious scripts within SharePoint directories (T1027 – Obfuscated Files or Information).
<i>Credential Access</i>	Possible credential harvesting from SharePoint's authentication services (T1002.001 – LSASS Memory).
<i>Discovery</i>	Enumeration of internal systems connected to SharePoint (T1087 – Account Discovery, T1083 – File and Directory Discovery).
<i>Lateral Movement</i>	Using harvested credentials or remote service exploitation to move into adjacent systems (T1021 – Remote Services).



<i>Collection</i>	Gathering documents, files, and communications stored in SharePoint (T1114 – Email Collection, T1005 – Data from Local System).
<i>Command and Control</i>	Encrypted channels or tunneled communications to external servers (T1071 – Application Layer Protocol).
<i>Exfiltration</i>	Transfer of sensitive defense-related data out of the environment (T1041 – Exfiltration Over C2 Channel).
<i>Impact</i>	Compromise of critical national defense information and disruption of secure communication channels (T1489 – Service Stop, T1499 – Endpoint Denial of Service).



Hacker Sneaks Infostealer Malware into Early Access Steam Game

Assessment: A threat actor known as EncryptHub, also known as Larva-208, compromised the early-access Steam game *Chemia* to deliver multiple info-stealing payloads. According to reports, the attacker added HijackLoader to the game files to establish persistence and fetch the Vidar infostealer. Hours later, it then introduced Fickle Stealer via a malicious DLL that used PowerShell to pull the main payload from an external domain. The malware runs in the background without affecting gameplay, exploiting user trust in the Steam platform rather than traditional lures. This creates real risk for any organization with employees who game on corporate BYOD systems. Browser-stored credentials, cookies, autofill data, and cryptocurrency wallet information are prime targets, enabling account takeover and follow-on intrusions. It remains unclear how the malicious binaries were inserted. An insider assist is one possibility. At the time of reporting, the game was still available. It is no longer available on the Steam platform as of today. This is the third case of malware being slipped into Steam as of this year.

Recommendations: Treat consumer platforms as untrusted software sources in enterprise risk models. Enforce application control on corporate endpoints, restrict execution to approved publishers, and block game clients where appropriate. Strengthen your browser and password manager policies, disable credential storing where possible, require MFA, and monitor for unusual cookie reuse. Push EDR detections for HijackLoader, Vidar, and Fickle Stealer behaviors and watch for PowerShell-based staging from unknown domains. For BYOD, require up-to-date EPP/EDR, isolate corporate access with managed browsers, and educate users that playtests and early-access titles can be weaponized even when hosted on trusted platforms. Use published IOCs to hunt across telemetry and quarantine any host that executed the *Chemia* binaries or reached related C2, then switch exposed credentials.

Next Steps: Confirm if any endpoints in your environment downloaded or executed *Chemia* during the reported window, and associate with network logs for connections to Telegram-sourced C2 or the referenced download domain. Determine if persistence remains after game removal and whether additional payloads were staged via HijackLoader. Assess for theft or misuse of browser cookies and tokens and issue re-authentication with MFA for affected accounts. Track Steam early-access and playtest installs in software inventories to evaluate exposure and monitor for further developments on the game's status and any updated IOCs.



RECONNAISSANCE

Attackers identified Steam's early-access titles as trusted but less monitored. Targeted the *Chemia* game to blend malicious payloads with normal gameplay.



DELIVERY

Distributed the infected game through Steam's official platform. Leveraged User trust in Steam.



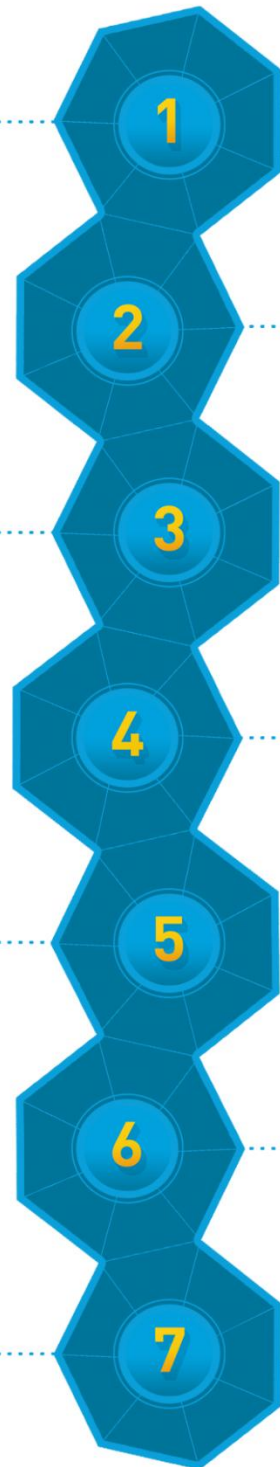
INSTALLATION

HijackLoader established persistence. PowerShell commands fetched and installed additional malware payloads.



ACTIONS ON OBJECTIVES

Collected browser credentials, cookies, and autofill data.
Exfiltrated cryptocurrency wallet details for financial gain.



WEAPONIZATION

Embedded HijackLoader into the game build. Used a malicious DLL to load Fickle Stealer.



EXPLOITATION

Execution triggered automatically when the game was launched. Malicious code ran without requiring additional interaction.



COMMAND & CONTROL (C2)

Vidar used Telegram channels for C2. Fickle Stealer communicated with an external malicious domain.



China-Backed APT41 Cyberattack Surfaces in Africa

Assessment: APT41 is a well-known Chinese state-sponsored group that has recently expanded its operations by targeting government and telecom organizations in Africa. According to an article by Vijayan (2025), the group exploited unpatched vulnerabilities in public-facing systems to gain access and then deployed customized malware to establish persistence and exfiltrate sensitive data. This signals a shift in APT41's targeting strategy, displaying Africa as an emerging target for nation-state cyber operations. The attack indicates the risk to organizations that leave critical systems exposed without timely patching and monitoring. Beyond the regional impact, this campaign demonstrates how state-backed groups can use strategic entry points to pursue espionage, influence operations, and potentially disrupt national infrastructure.

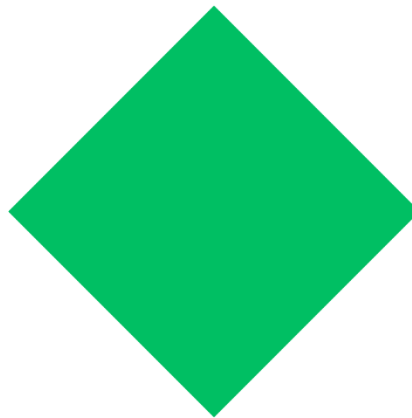
Recommendations: Organizations should immediately prioritize patch management for all public-facing systems. Continuous monitoring and threat hunting should be in place to detect lateral movement or suspicious outbound traffic, especially from systems that handle sensitive government data. Security teams should implement network segmentation to limit the reach of intrusions and deploy endpoint detection tools to identify behaviors linked to APT41, such as custom malware and credential theft techniques. This incident is a reminder for leaders to factor geopolitical motivations into risk assessments, especially when partnering with organizations or operating in regions where nation-state activity is increasing.

Next Steps: The CTI team must work to identify the exact vulnerabilities exploited in this attack and confirm whether any systems in the environment remain exposed. It is also imperative to investigate whether APT41's malware families overlap with previously reported toolsets, which could guide detection engineering. Intelligence gaps remain regarding the main objectives of the campaign, whether the focus was entirely espionage or if disruption capabilities were embedded for future use. Expanding collection on APT41's activity in Africa, as well as corresponding indicators of compromise across regional partners, will be critical for building a more complete threat picture.



APT 41 - Chinese State-Sponsored Group

- Custom Malware
- Credential Theft
- Lateral Movement
- Exploited Unpatched Applications



- Unpatched, public-facing systems
- External Command-and-Control Server
- Compromised Web Servers

Government and
Telecommunications Organizations in
Africa



Report Sources:

1. Gatlan, S. (2025, July 23). *US nuclear weapons agency hacked in Microsoft SharePoint attacks*. Bleeping Computer. <https://www.bleepingcomputer.com/news/security/us-nuclear-weapons-agency-hacked-in-microsoft-sharepoint-attacks/>
 2. [Bloomberg Television]. (2025, July 23). *Microsoft Hack: US National Nuclear Security Administration Among the Victims* [Video]. Youtube. <https://www.youtube.com/watch?v=wrzqBIWnp7M>
 3. Adapt Forward (2025, July 29). *Lessons from the Nuclear Weapons Agency Breach*. Adapt Forward, Cyber Security. <https://www.adaptforward.com/news-center/lessons-from-the-nuclear-weapons-agency-breach>
 4. Toulas, B. (2025, July 24). *Hacker sneaks infostealer malware into early access Steam game*. <https://www.bleepingcomputer.com/news/security/hacker-sneaks-infostealer-malware-into-early-access-steam-game/>
 5. Ophetek (2025, August 12). *Infostealers Hidden Inside Steam Early Access Title*. Ophetek LLC. <https://ophtek.com/infostealers-hidden-inside-steam-early-access-title/>
 6. Vijayan, J. (2025, July 22). *China-Backed APT41 Cyberattack Surfaces in Africa*. Dark Reading. <https://www.darkreading.com/cyberattacks-data-breaches/china-backed-apt41-attack-africa>
-