Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

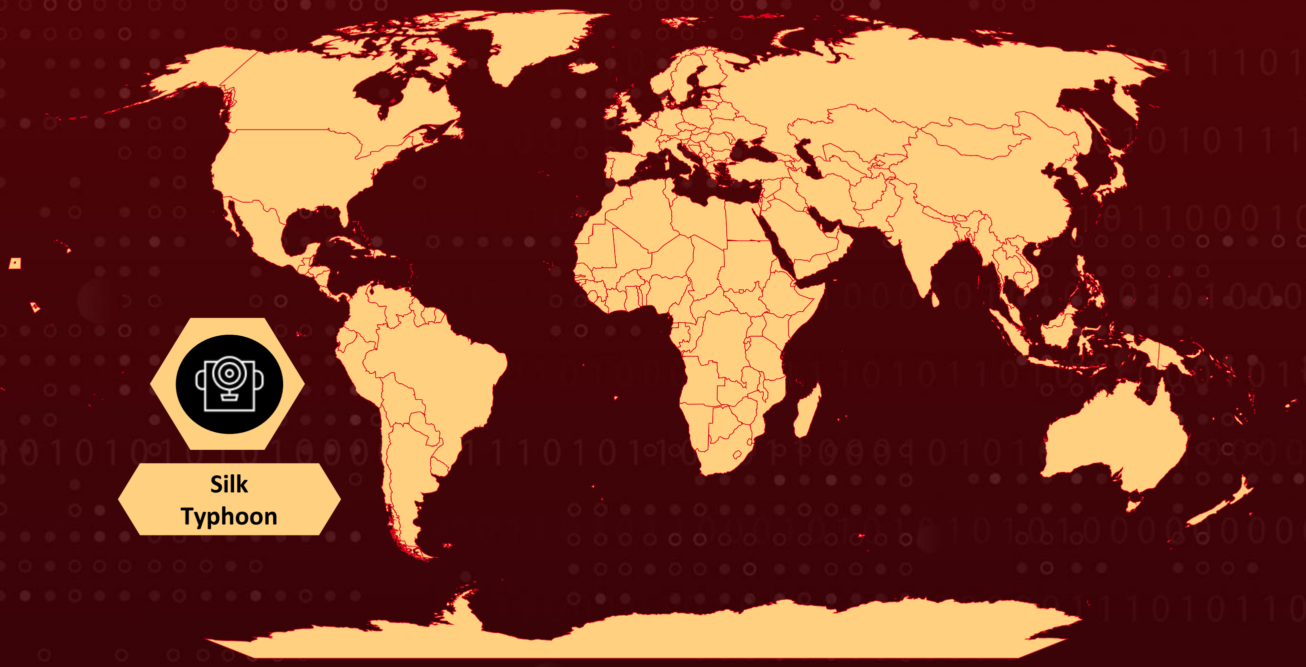
Silk Typhoon's Strategic Pivot: Exploiting IT Supply Chains for Espionage

Date of Publication	Admiralty code	TA Number
March 6, 2024	A1	TA2025067

Summary

First Seen: 2021
Targeted Countries: Worldwide
Threat Actor: Silk Typhoon (aka Hafnium, Red Dev 13, timmy, ATK233, G0125, Operation Exchange Marauder)
Targeted Industries: IT Services, Healthcare, Legal services, Higher education, Defense, Government, Non-governmental organizations (NGOs), Energy, Law firms, and Policy think tanks
Affected Platform: Windows

Actor Map



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-0282	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	✓	✓
CVE-2024-12356	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability	BeyondTrust Privileged Remote Access (PRA) and BeyondTrust Remote Support (RS)	✓	✓	✓
CVE-2024-12686	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability	BeyondTrust Privileged Remote Access (PRA) and BeyondTrust Remote Support (RS)	✓	✓	✓
CVE-2024-3400	Palo Alto Networks PAN-OS Command Injection Vulnerability	Palo Alto Networks PAN-OS	✓	✓	✓
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2021-26855	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2021-26857	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2021-26858	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2021-27065	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-44228	Log4Shell (Apache Remote Code Execution Vulnerabilities)	Apache Log4j: 2.0 - 2.14.1	✓	✓	✓

Actor Details

#1 Silk Typhoon, a sophisticated state-sponsored threat actor believed to be operating on behalf of Chinese strategic interests, now focuses on common IT solutions, such as remote management tools and cloud applications, to gain an initial foothold. By exploiting unpatched applications, they can elevate privileges and establish a presence within targeted organizations, setting the stage for further malicious activities.

#2 Once initial access is secured, Silk Typhoon abuses stolen API keys and credentials to infiltrate downstream customer networks. This involves leveraging access from compromised IT service providers, privileged access management systems, and cloud application vendors. With these keys, the attackers can perform reconnaissance, gather sensitive data, and reset default admin accounts, while also deploying web shells to maintain persistence and cover their tracks by clearing logs.

#3 In addition to API key abuse, the threat actor employs password spray attacks and password abuse techniques. They actively scour public repositories for leaked corporate credentials and use these to authenticate into corporate environments.

#4 After compromising a victim, Silk Typhoon rapidly moves laterally from on-premises networks to cloud environments. Their techniques include dumping Active Directory data, stealing passwords from key vaults, and targeting synchronization servers (such as Microsoft AADConnect/Entra Connect) to escalate privileges across both environments. By manipulating service principals and OAuth applications, they are able to exfiltrate sensitive data from services like email, OneDrive, and SharePoint via APIs such as MSGraph and Exchange Web Services.

#5 Historically active since at least 2021, Silk Typhoon's activity has shown a significant uptick since late 2024. The group has been linked to multiple CVEs over recent years, underscoring their ability to exploit vulnerabilities across diverse IT systems. Their systematic approach to infiltrating trusted networks and using advanced lateral movement techniques highlights the evolving threat landscape and the necessity for robust defensive measures.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Silk Typhoon (aka Hafnium, Red Dev 13, timmy, ATK233, G0125, Operation Exchange Marauder)	China	Worldwide	IT Services, Healthcare, Legal services, Higher education, Defense, Government, Non-governmental organizations (NGOs), Energy, Law firms, and Policy think tanks
	MOTIVE		
	Information theft and espionage		

Recommendations

Patch Management: Ensuring that all systems, especially those exposed to the internet are updated promptly with the latest security patches is essential. Regular vulnerability assessments and automated patch deployment can minimize the window of opportunity for adversaries to exploit known and zero-day vulnerabilities.

Credential Hygiene: Enforcing multi-factor authentication (MFA) and maintaining strong password policies across all accounts can help prevent unauthorized access. Regular audits and the use of behavior-based anomaly detection systems are recommended to identify compromised credentials or unusual access patterns.

Monitoring and Detection: Enhancing network visibility and monitoring can significantly improve an organization's defensive posture. Deploying advanced security monitoring tools and integrating threat intelligence feeds enable rapid detection of suspicious activities. Continuous logging and real-time analysis of network traffic, combined with periodic security audits, provide a robust mechanism to uncover potential breaches in the early stages.

Network Segmentation: Proper network segmentation limits the damage that can be done if an attacker gains access to one part of the system. By segmenting critical infrastructure from less sensitive data, organizations can better contain breaches and make lateral movement more difficult for attackers.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0007 Discovery
TA0006 Credential Access	TA0008 Lateral Movement	TA0005 Defense Evasion	TA0010 Exfiltration
TA0003 Persistence	TA0004 Privilege Escalation	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	T1110.003 Password Spraying	T1110 Brute Force
T1078 Valid Accounts	T1190 Exploit Public-Facing Application	T1586 Compromise Accounts	T1068 Exploitation for Privilege Escalation
T1027 Obfuscated Files or Information	T1555 Credentials from Password Stores	T1083 File and Directory Discovery	T1041 Exfiltration Over C2 Channel
T1505.003 Web Shell	T1505 Server Software Component	T1106 Native API	T1059 Command and Scripting Interpreter
T1574.010 Services File Permissions Weakness	T1598 Phishing for Information	T1574 Hijack Execution Flow	T1584 Compromise Infrastructure
T1195.002 Compromise Software Supply Chain	T1195 Supply Chain Compromise	T1567.002 Exfiltration to Cloud Storage	T1584.003 Virtual Private Server

Patch Links

https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US

https://www.beyondtrust.com/trust-center/security-advisories/bt24-10

https://www.beyondtrust.com/trust-center/security-advisories/bt24-11

https://security.paloaltonetworks.com/CVE-2024-3400

https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26857

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26858

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27065

https://logging.apache.org/security.html

References

https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/

https://www.microsoft.com/en-us/security/security-insider/silk-typhoon#section-master-oc2985

https://attack.mitre.org/groups/G0125/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

Contextualize
Uni5 Threat Exposure Management
Prioritize
Resolve

REPORT GENERATED ON

March 6, 2025 • 11:00 PM

More at www.hivepro.com