Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

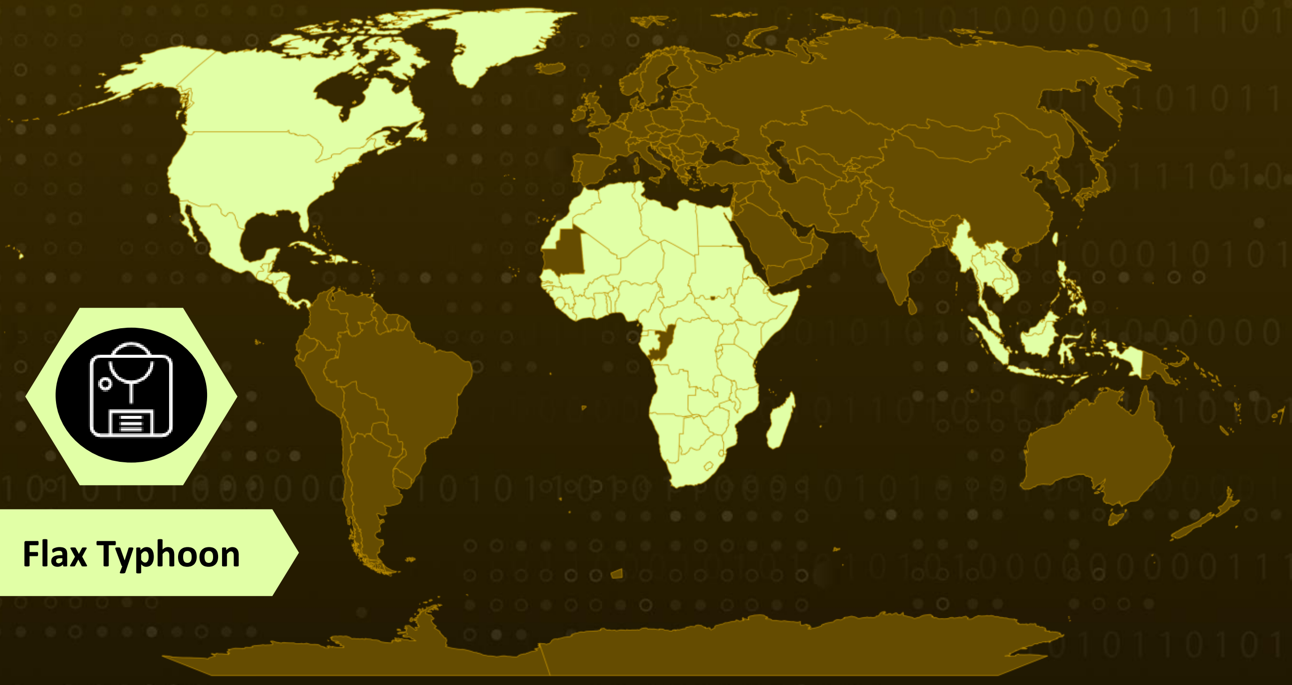
Chinese Hacking Group ‘Flax Typhoon’ Targeting Taiwan Organizations

Date of Publication	Admiralty Code	TA Number
August 28, 2023	A1	TA2023347

Summary

First Appearance: July 2021
Actor Name: Flax Typhoon
Targeted Region: Taiwan, Southeast Asia, North America and Africa
Affected Platform: Windows
Targeted Industries: Government agencies, Education, Critical Manufacturing, and Information Technology Organizations

Actor Map



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

Actor Details

#1 A Chinese nation-state activity group known as Flax Typhoon that is targeting organizations in Taiwan for espionage. Flax Typhoon gains access to Taiwanese networks using minimal malware and relies on built-in tools within the operating system for long-term access.

#2 Flax Typhoon has been active since mid-2021 and targets government agencies, education, manufacturing, and IT organizations in Taiwan, as well as other regions. The group employs various tools, including the China Chopper web shell, Metasploit, Juicy Potato privilege escalation tool, Mimikatz, and SoftEther VPN client. However, Flax Typhoon mostly relies on "living-off-the-land" techniques, utilizing legitimate tools and methods to maintain persistence and access.

#3 The attack chain involves initial access through known vulnerabilities in public-facing servers, followed by privilege escalation using tools like Juicy Potato. Flax Typhoon establishes persistence by modifying remote desktop protocol (RDP) settings and deploying a VPN connection to actor-controlled infrastructure. The group uses legitimate tools like SoftEther VPN, often renamed and operating over HTTPS, to maintain command and control.

#4 Flax Typhoon also targets credentials using Mimikatz and similar tools, aiming to obtain hashed passwords for lateral movement. While the group's behavior suggests espionage objectives.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Flax Typhoon	China	Taiwan, Southeast Asia, North America and Africa	Government agencies, Education, Critical Manufacturing, and Information Technology Organizations
	MOTIVE		
	Espionage		

Recommendations

Prioritize Vulnerability Management and Patching: Regularly update and secure public-facing servers, applications, and services to promptly address known vulnerabilities. Consistently scan and evaluate the security status of these systems to identify and fix potential weaknesses that threat groups like Flax Typhoon could exploit for initial access.

Implement Robust System Hardening: Enhance system security by adhering to best practices for hardening. Disable unnecessary services, enforce strong password policies, and limit user privileges. Implement network segmentation to restrict attacker movement. Reducing the attack surface and complicating initial access.

Monitor Actively: Implement robust monitoring for unusual behavior, focusing on credential access and system modifications. Focus on detecting unusual actions like credential access, lateral movement, and system alterations.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0001 Initial Access	TA0002 Execution	TA0011 Command and Control	TA0008 Lateral Movement
T1190 Exploit Public-Facing Application	T1505.003 Web Shell	T1505 Server Software Component	T1059 Command and Scripting Interpreter
T1546 Event Triggered Execution	T1546.008 Accessibility Features	T1105 Ingress Tool Transfer	T1543 Create or Modify System Process
T1543.003 Windows Service	T1036 Masquerading	T1036.005 Match Legitimate Name or Location	T1572 Protocol Tunneling
T1003.001 LSASS Memory	T1003 OS Credential Dumping	T1003.002 Security Account Manager	T1550.002 Pass the Hash
T1550 Use Alternate Authentication Material			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	2c95b971aa47dc4d94a3c52db74a3de11d9ba658, 5437d0195c31bf7cedc9d90b8cb0074272bc55df, 7992c0a816246b287d991c4ecf68f2d32e4bca18, cc1f0cdc131dfafd43f60ff0e6a6089cd03e92f1
IPV4	139[.]180[.]158[.]51, 45[.]195[.]149[.]224, 45[.]204[.]1[.]247, 45[.]204[.]1[.]248, 101[.]33[.]205[.]106, 134[.]122[.]188[.]20, 154[.]19[.]187[.]92, 192[.]253[.]235[.]107, 39[.]98[.]208[.]61, 45[.]88[.]192[.]118
Hostnames	vpn472462384[.]softether[.]net, vpn437972693[.]sednc[.]cn, asljkdqhkhasdq[.]softether[.]net

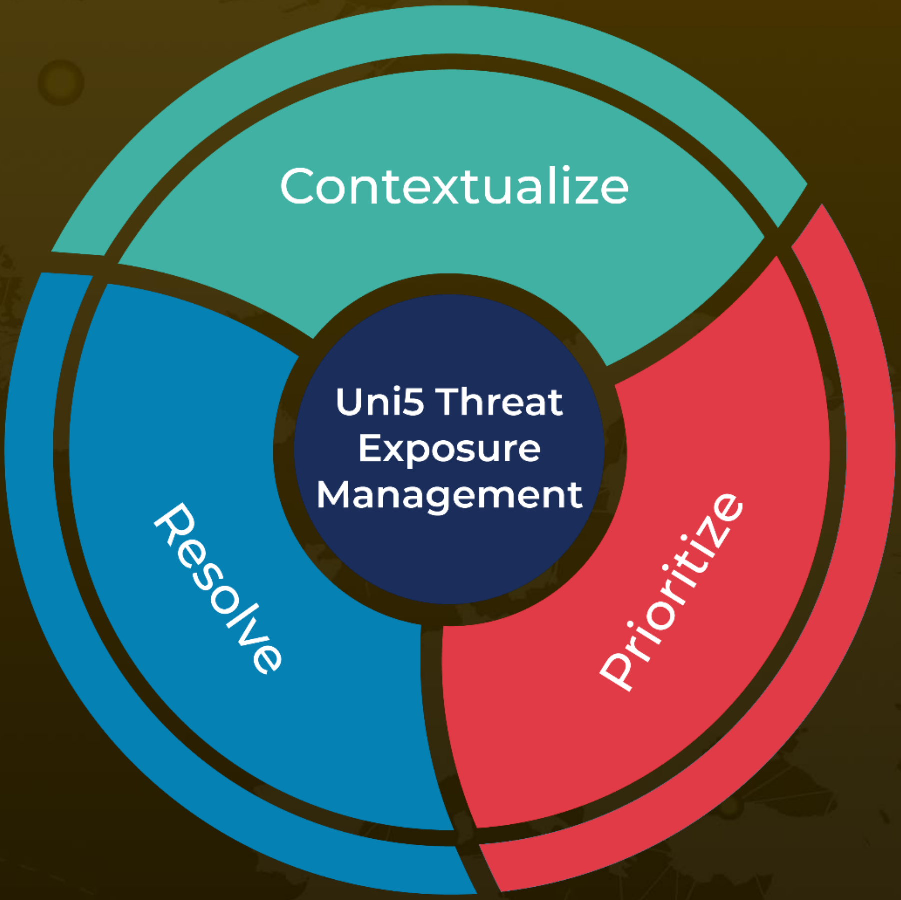
References

https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/

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.



REPORT GENERATED ON

August 28, 2023 • 6:00 AM

More at www.hivepro.com