Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

China-affiliated group Infiltrated Tibetan Websites

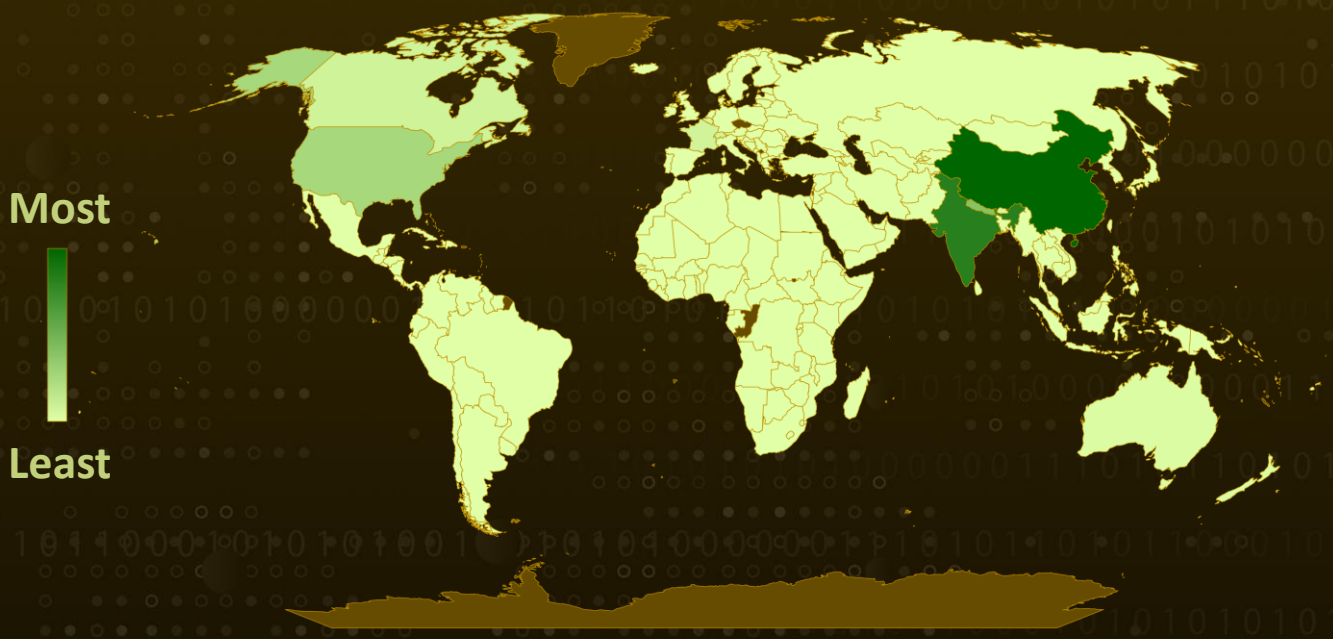
Date of Publication	Admiralty Code	TA Number
November 14, 2024	A1	TA2024431

Summary

Attack Commenced: May 2024
Threat Actor: TAG-112
Targeted Region: Worldwide (Tibetan diaspora)
Targeted Industries: Media, Education

Attack: In May 2024, the cyberespionage group TAG-112, likely a subset of Evasive Panda (TAG-102), launched a targeted attack on Tibetan-affiliated websites. Evasive Panda, a China-linked threat actor, has focused on Tibetan users since at least 2023 to gather intelligence.

Attack Regions



Attack Details

#1 In late May 2024, TAG-112 likely compromised two websites affiliated with the Tibetan community. These sites were injected with malicious JavaScript designed to mimic a TLS certificate error page and trigger a download of Cobalt Strike from infrastructure controlled by external threat actors.

#2 TAG-112 is likely a subgroup of TAG-102, also known as Evasive Panda, sharing similar intelligence objectives and primarily targeting Tibetan-focused entities. Evasive Panda, a China-linked threat actor, has conducted an extensive cyberespionage campaign against Tibetan users since at least September 2023, employing both watering hole and supply chain attacks to achieve its goals.

#3 The TAG-112 campaign's infrastructure utilized Cloudflare protection to conceal its origin. The modified websites prompted users to download a malicious executable disguised as a "security certificate" which, upon execution, loaded a Cobalt Strike payload.

#4 Both compromised sites were likely built on the Joomla Content Management System (CMS). If left unpatched or outdated, Joomla-based websites become high-priority targets for cyber threat actors. TAG-112 likely leveraged a vulnerability in these sites to introduce the malicious JavaScript.

Recommendations

Regularly Audit and Harden Web Servers and Applications: Perform regular security audits and harden web servers and applications. Disable unnecessary services, ensure that default settings are modified for secure configurations, and audit access logs frequently for suspicious activity. This reduces the attack surface and makes it more difficult for attackers to exploit vulnerabilities.

Utilize Endpoint Detection and Response (EDR) Solutions: Deploy EDR tools to monitor and analyze endpoint activities continuously. Ensure that these solutions are configured to detect suspicious behavior linked to Cobalt Strike, such as unauthorized process execution or unusual network traffic patterns. EDR tools can help detect and block malicious payloads in real time before they cause significant damage.

Automate Patch Management and Vulnerability Scanning: Implement automated patch management and vulnerability scanning solutions to ensure the timely identification, remediation, and updating of known vulnerabilities across your organization's assets. Classify assets based on their criticality and exposure to potential threats, prioritizing patching high-risk systems and other publicly accessible services. Regularly apply security patches to address vulnerabilities, focusing on assets that are commonly targeted in cyberattacks to reduce the risk of exploitation and enhance overall cybersecurity resilience.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0011** Command and Control
T1583 Acquire Infrastructure	**T1583.004** Server	**T1583.006** Web Services	**T1584** Compromise Infrastructure
T1584.004 Server	**T1189** Drive-by Compromise	**T1574** Hijack Execution Flow	**T1574.002** DLL Side-Loading
T1071 Application Layer Protocol	**T1204** User Execution	**T1204.001** Malicious Link	**T1539** Steal Web Session Cookie
T1573 Encrypted Channel	**T1057** Process Discovery	**T1105** Ingress Tool Transfer	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	tibetpost[.]net, gyudmedtantricuniversity[.]org, *[.]dnspod[.]cn, update[.]maskrisks[.]com, maskrisks[.]com, mail[.]maskrisks[.]com, checkupdate[.]maskrisks[.]com
URLs	hxxps[:]//update[.]maskrisks[.]com/?type=Chrome, hxxps[:]//update[.]maskrisks[.]com/?type=Edge, hxxp[:]//154[.]205[.]138[.]202/GetUrl/cache?time=[UNIX Timestamp], hxxp[:]//mail[.]maskrisks[.]com/[:]443/api/view[.]php, hxxp[:]//update[.]maskrisks[.]com/cache?time=[UNIX Timestamp], hxxps[:]//checkupdate[.]maskrisks[.]com/cache?time=[UNIX Timestamp], hxxp[:]//mail[.]maskrisks[.]com/:443/api/view[.]php, hxxp[:]//154[.]205[.]138[.]202/GetUrl/cache?time=[UNIXTimestamp], hxxps[:]//gyudmedtantricuniversity[.]org/templates/lt_interiordesign/js/custom[.]js, hxxps[:]//tibetpost[.]net/templates/ja_teline_v/js/gallery/jquery[.]blueimp-gallery[.]full[.]js, hxxps[:]//update[.]maskrisks[.]com/download, hxxps[:]//update[.]maskrisks[.]com/?type=Chrome, hxxp[:]//mail[.]maskrisks[.]com/api/view[.]php, hxxp[:]//154[.]205[.]138[.]202/GetUrl/cache, hxxps[:]//checkupdate[.]maskrisks[.]com/cache, hxxps[:]//update[.]maskrisks[.]com/cache
IPv4	154[.]90[.]62[.]12, 154[.]90[.]63[.]166, 154[.]205[.]138[.]202
SHA1	d4938cb5c031ec7f04d73d4e75f5db5c8a5c04ce
SHA256	d0972247c500d2a45f412f9434287161de395a35ef5b4931cba12cf513b76962, 94569f64f62eff185ba47e991dba54bdeea6d1a9e205d6bec767be6a864e4efb, 1e42cbe23055e921eff46e5e6921ff1a20bb903fca83ea1f1294394c0df3f4cd, 0e306c0836a8ee035ae739c5adfbe42bd5021e615ebaa92f52d5d86fb895651d, f1f11e52a60e5a446f1eb17bb718358def4825342acc0a41d09a051359a1eb3d,

TYPE	VALUE
SHA256	f4ded3a67480a0e2a822af1e87a727243dea16ac1a3c0513aec62bff71f06b27, 966d311dcc598922e4ab9ce5524110a8bfd2c6b6db540d180829ceb7a7253831, 1e7cb19f77206317c8828f9c3cdee76f2f0ebf7451a625641f7d22bb8c61b21b, 8d4049ef70c83a6ead26736c1330e2783bdc9708c497183317fad66b818e44cb, e190c7e097a1c38dd45d9c149e737ad9253b1cabee1cee7ef080ddf52d1b378c, 31f11b4d81f3ae25b6a01cd1038914f31d045bc4136c40a6221944ea553d6414, d0972247c500d2a45f412f9434287161de395a35ef5b4931cba12cf513b76962
File Name	RPHost.dll, update.dll

References

https://go.recordedfuture.com/hubfs/reports/cta-cn-2024-1112.pdf

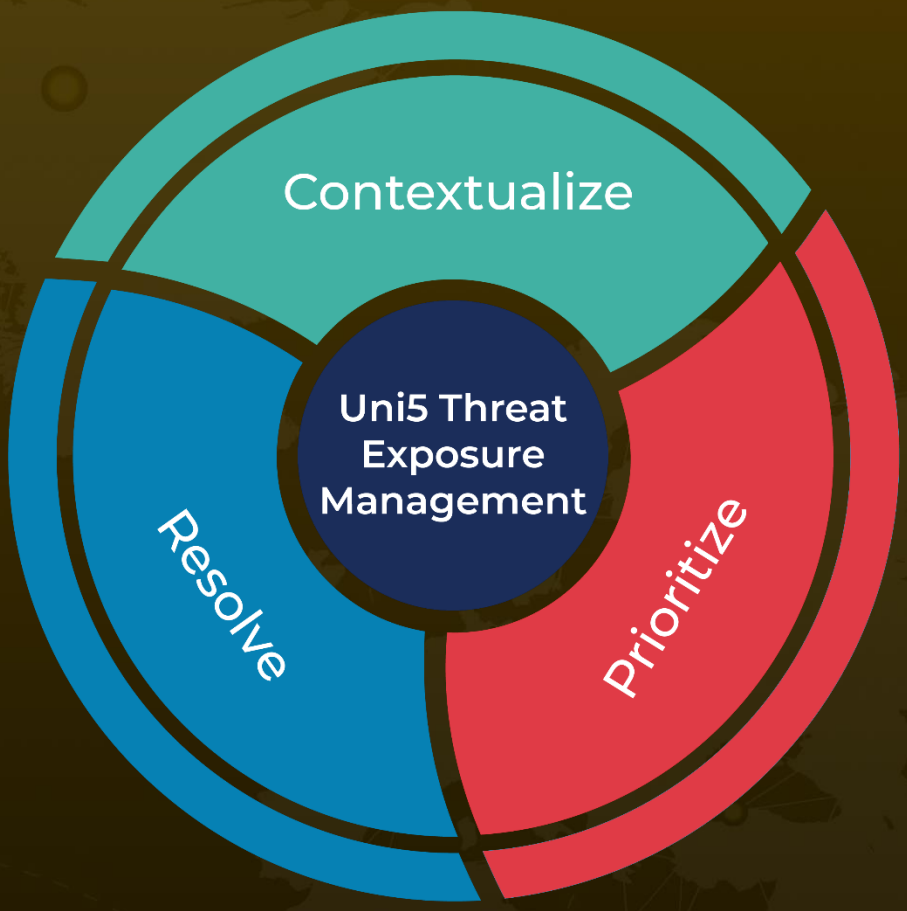
https://hivepro.com/threat-advisory/evasive-panda-china-linked-cyberespionage-targeting-tibetans/

https://hivepro.com/threat-advisory/unveiling-gambleforce-a-sql-injection-gang/

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

November 14, 2024 . 11:30 AM

More at www.hivepro.com