Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Chinese APT Masquerading as Cloud Services in Cambodia

Date of Publication	Admiralty Code	TA Number
November 9, 2023	A1	TA2023453

Summary

First appeared: September 2023
Attack Region: Cambodia
Actor Name: Chinese APT
Targeted Industry: Government, National Defense, Election Oversight, Human Rights, National Treasury and Finance, Commerce, Politics, Natural Resources, Telecommunications
Attack: Chinese APT targets Cambodian government via disguised cloud services, aiming to access sensitive data, aligning with China's regional interests. Actors adapt work hours, signaling Chinese origin, urging protective measures against state-backed cyber threats.

Attack Regions

Attack Details

#1 A Chinese Advanced Persistent Threat (APT) targeting Cambodian government organizations through disguised infrastructure posing as cloud backup services. This malicious activity, utilizing a network of servers and domains, aims to infiltrate and persistently access sensitive data from various sectors, including national defense, finance, and human rights.

#2 The Chinese APT actors utilize infrastructure with a fraudulent SSL certificate and command and control (C2) servers, employing tactics such as IP filtering and intermittent port openings to avoid detection. The malicious activity aligns with China's geopolitical strategy, particularly its interests in Cambodia, notably the Ream Naval Base project, showcasing the country's growing influence in Southeast Asia.

#3 The actor's routine activity hours coincide with both Cambodian and Chinese business hours, suggesting the actors are based in China and make efforts to blend in with local time zones. Additionally, observed activity patterns during Chinese holidays align with the Chinese government's official workdays, indicating the involvement of entities affiliated with the Chinese state.

Recommendations

- **SSL Certificate Monitoring:** Regularly monitor SSL certificates used within the organization and flag any fraudulent or suspicious certificates for immediate investigation.
- **Network Traffic Analysis:** Continuously analyze network traffic for anomalies, particularly outbound connections to suspected malicious infrastructure or IP addresses associated with threat actors.
- **Access Control and Authentication:** Strengthen access control mechanisms, enforce strong authentication methods, and regularly update passwords to prevent unauthorized access to critical systems and data.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0010 Exfiltration	TA0011 Command and Control	TA0007 Discovery
TA0040 Impact	TA0042 Resource Development	T1102 Web Service	T1046 Network Service Discovery
T1036 Masquerading	T1049 System Network Connections Discovery	T1567.002 Exfiltration to Cloud Storage	T1567 Exfiltration Over Web Service

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	143[.]110[.]189[.]141, 167[.]71[.]226[.]171, 104[.]248[.]153[.]204, 165[.]232[.]186[.]197, 172[.]105[.]34[.]34, 194[.]195[.]114[.]199
SHA1	b8cff709950cfa86665363d9553532db9922265c
Hostname	ads[.]teleryanhart[.]com, api[.]infinitycloud[.]info, connect[.]clinkvl[.]com, connect[.]infinitybackup[.]net, connect[.]infinitycloud[.]info, dfg[.]ammopak[.]site, file[.]wonderbackup[.]com, fwg[.]ammopak[.]site, jlp[.]ammopak[.]site, kwe[.]ammopak[.]site,

TYPE	VALUE
Hostname	login[.]wonderbackup[.]com, lxo[.]ammopak[.]site, mfi[.]teleryanhart[.]com, ns[.]infinitycloud[.]info, ns1[.]infinitybackup[.]net, share[.]infinitybackup[.]net, sync[.]wonderbackup[.]com, update[.]wonderbackup[.]com

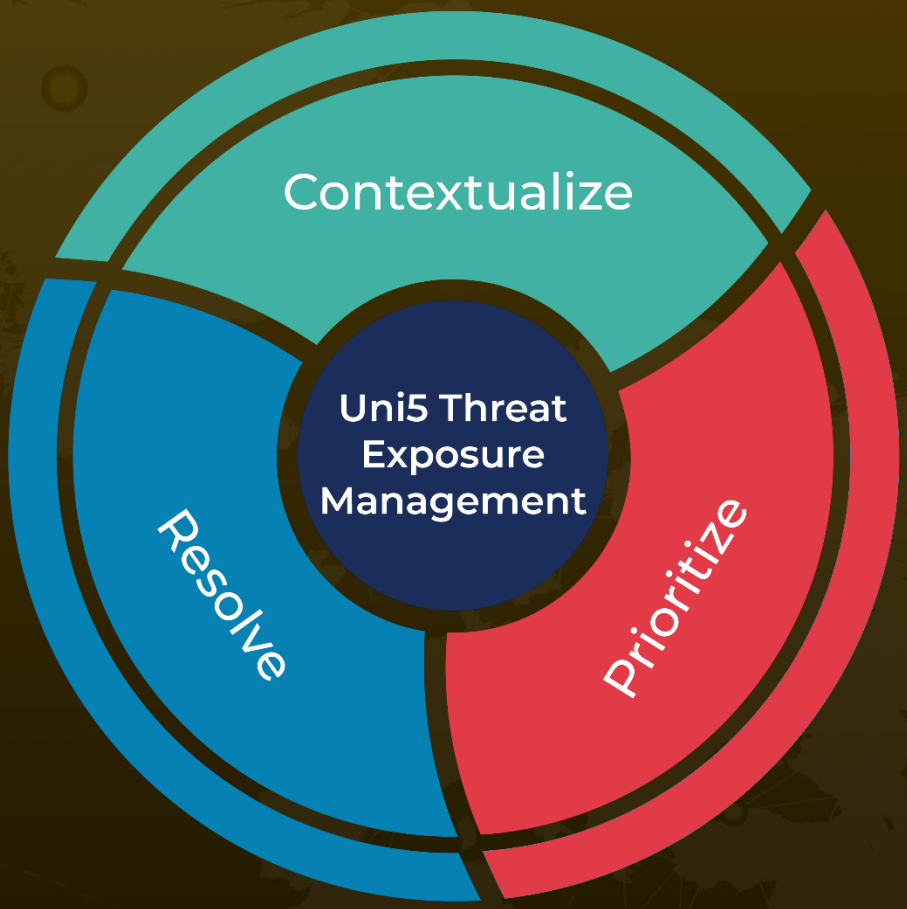
References

https://unit42.paloaltonetworks.com/chinese-apt-linked-to-cambodia-government-attacks/

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 9, 2023 • 4:30 AM

More at www.hivepro.com