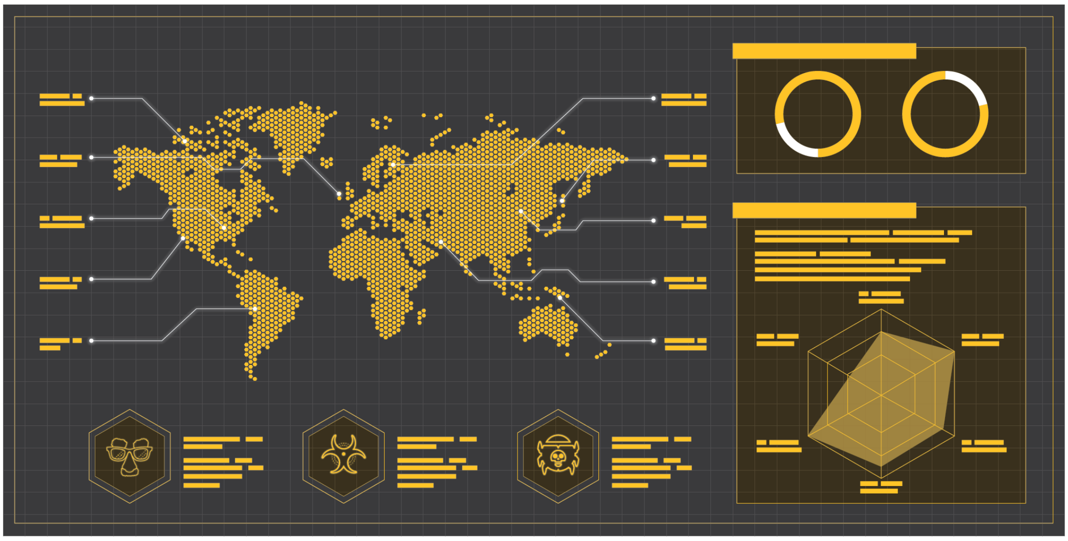
Chinese APT Targeting Cambodian Government

Unit 42 :: 11/8/2023

By Unit 42

November 7, 2023 at 9:01 PM

Category: Government



This post is also available in: 日本語 (Japanese)

Executive Summary

Unit 42 has identified malicious Chinese APT infrastructure masquerading as cloud backup services. Monitoring telemetry associated with two prominent Chinese APT groups, we observed network connections predominately originating from the country of Cambodia, including inbound connections originating from at least 24 Cambodian government organizations.

We assess with high confidence that these Cambodian government entities were targeted and remain compromised by Chinese APT actors. This assessment is due to the malicious nature and ownership of the infrastructure combined with persistent connections over a period of several months.

Cambodia and China maintain strong diplomatic and economic ties. Since Cambodia signed on to China's Belt and Road Initiative (BRI) in 2013, the relationship between these two countries has grown steadily.

In recent years, China's most notable investment has been a project to modernize Cambodia's Ream Naval Base. This project generated controversy and drew scrutiny from several Western nations due to initial attempts by both countries to conceal the project.

As the project nears completion this year, the naval base is on track to become China's first overseas outpost in Southeast Asia. As such, this project demonstrates how significant Cambodia is to China's ambitions of projecting power and expanding naval operations in the region.

Palo Alto Networks customers receive protection from this malicious infrastructure through our Next-Generation Firewall with Cloud-Delivered Security Services, including DNS Security and Advanced URL Filtering.

Related Unit 42 Topics China, APAC, APT

Table of Contents

Infrastructure Overview

Unit 42 identified infrastructure associated with the following known malicious SSL certificate:

Subject Full Name	C=US,ST=Some-State,O=Internet Widgits Pty Ltd,CN=10.200.206.100
Issuer Full Name	C=US,ST=Some-State,O=Internet Widgits Pty Ltd,CN=COM
Serial Number	15007560845348164646
SHA1 Hash	B8CFF709950CFA86665363D9553532DB9922265C
Valid From	2017-11-23
Valid To	2027-11-21

Table 1. SSL Certificate Overview.

Most recently, this certificate was used by servers on six target-facing IP addresses. Each of these servers host several subdomains associated with six domains.

Based on their names, a number of these domains appear to masquerade as cloud storage services. This disguise likely lends a sense of legitimacy to the unusual amount of traffic during times of high activity levels from the actor, such as data exfiltration from the victim network.

Figure 1 provides a visualization of the malicious infrastructure.

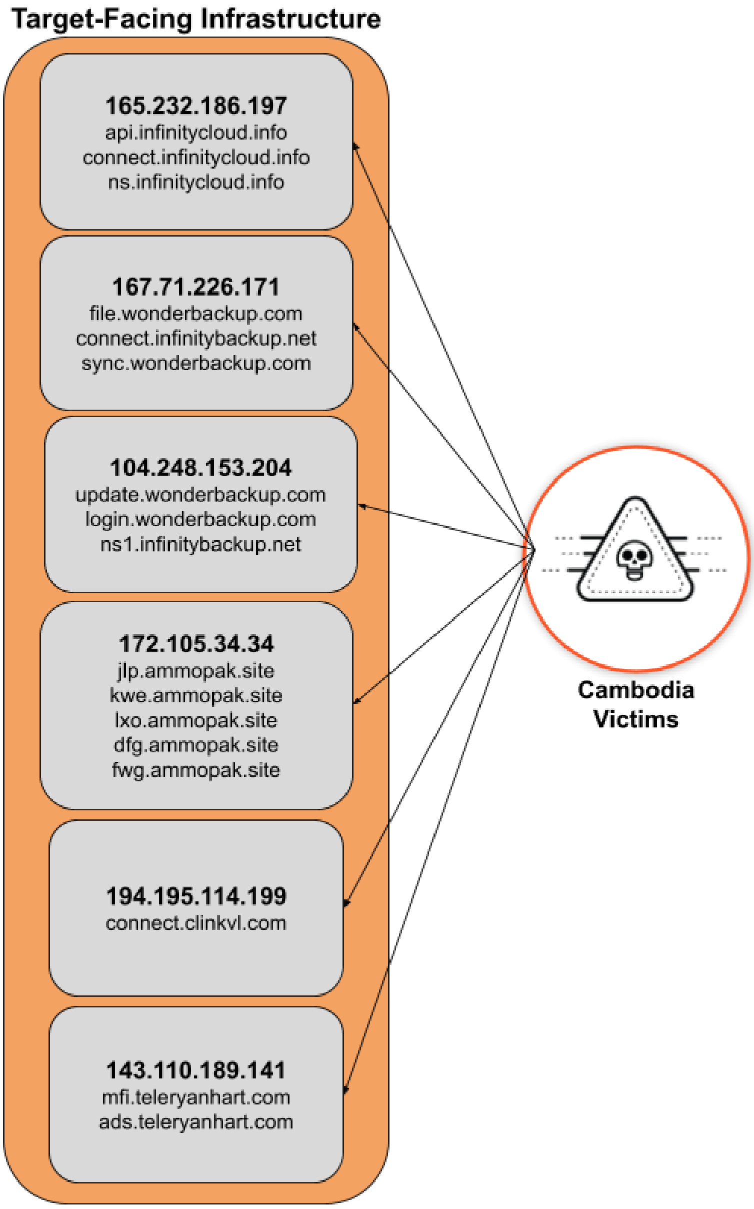


Figure 1. Infrastructure overview.

Suspected Cambodian Government Targets

We observed a total of 24 Cambodian government organizations regularly communicating with this infrastructure between September and October 2023. A number of these organizations provide critical services in the following industries:

- National defense
- Election oversight
- Human rights
- National treasury and finance
- Commerce
- Politics
- Natural resources
- Telecommunications

These targets all hold vast amounts of sensitive data, including the following:

- Financial data
- Personally identifiable information of citizens
- Classified government information

We assess that these organizations are likely the targets of long-term cyberespionage activities that have leveraged this infrastructure for persistent access to government networks of interest.

Command and Control Infrastructure

We assess with high confidence that the target-facing IP addresses are being used as command and control (C2) infrastructure by the threat actor. We believe the infrastructure is running the Cowrie honeypot on port 2222. The attackers are likely using this honeypot as a cover to deceive network defenders and researchers investigating anomalous activity.

We have also observed IP filtering on this infrastructure. Specifically, we have observed the blocking of connections from the following:

- Known Palo Alto Networks IP ranges
- Some VPS and cloud hosting providers
- IP ranges from a number of Big Tech and other cybersecurity companies

We believe this threat actor is filtering connections to the malicious infrastructure to minimize the risk of the C2s being profiled by IP scanners or identified by cybersecurity researchers.

We have also observed C2 ports open during activity times for the threat actor and closed at all other times. Again, this is likely to minimize the risk of the infrastructure being profiled by IP scanners or identified by researchers.

Table 2 outlines the known actor and target-facing ports.

IP Address	Target Port	Domain(s)
165.232.186[.]197	80, 443, 4433	api.infinitycloud[.]info connect.infinitycloud[.]info ns.infinitycloud[.]info
167.71.226[.]171	80, 81, 82, 443, 769, 4433, 8086, 8089	file.wonderbackup[.]com connect.infinitybackup[.]net share.infinitybackup[.]net sync.wonderbackup[.]com
104.248.153[.]204	82, 443	update.wonderbackup[.]com login.wonderbackup[.]com ns1.infinitybackup[.]net
143.110.189[.]141	443	mfi.teleryanhart[.]com ads.teleryanhart[.]com
172.105.34[.]34	8081, 8087, 8443, 8888	jlp.ammopak[.]site kwe.ammopak[.]site lxo.ammopak[.]site dfg.ammopak[.]site fwg.ammopak[.]site
194.195.114[.]199	8080, 8443, 9200	connect.clinkvl[.]com

Table 2. Target-facing infrastructure details.

Actor Pattern of Life

While investigating the cluster of infrastructure, we were able to determine the actor’s pattern of life. We predominantly observed the actor’s activity between 08:30 and 17:30 UTC +08:00 (China Standard Time) on weekdays (Monday to Friday). This pattern might indicate the actor is attempting to avoid detection by blending into regular Cambodian business hours which are UTC +07:00.

However, we also observed a significant change in actor activity that suggests the actor is based in China and working regular business hours in China.

This change in the actor’s pattern of life occurred between Sep. 29 and Oct. 8, 2023. Actor activity ceased on Sep. 29, with low amounts of activity through the week of Oct. 2-8, including the weekend of Oct. 7-8. We saw actor activity return to regular levels and patterns starting Oct. 9.

The dates of the actor's activity changes align with China's Golden Week, held on Sep. 29 to Oct. 6, 2023, and "Special Working Days," designated as Oct. 7-8, 2023. Special Working Days are Chinese government-mandated working days to compensate for the extended holiday.

Figure 2 shows the regular activity pattern and deviation during Golden Week, before returning to normal.

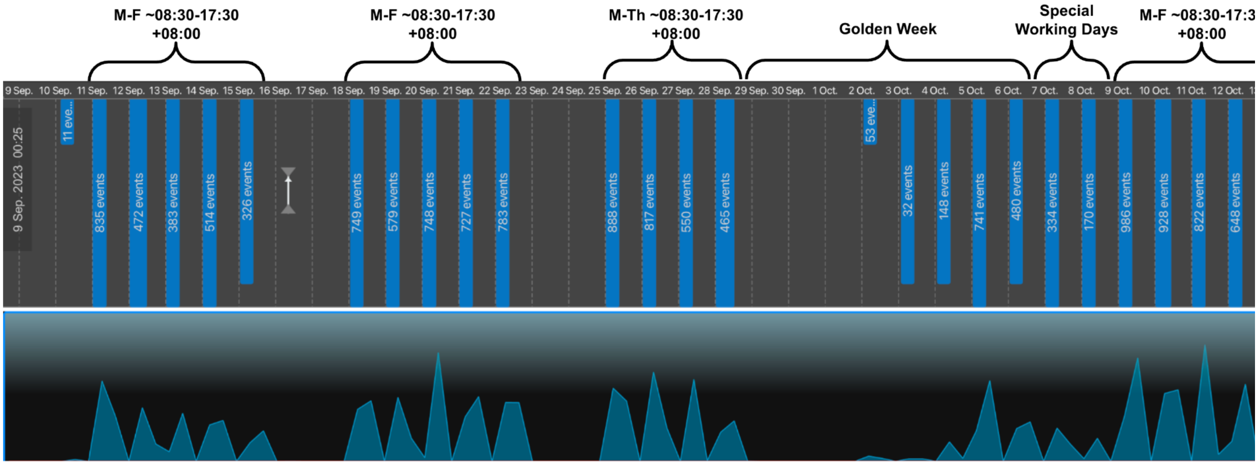


Figure 2. Actor pattern of life.

Conclusion

Unit 42 identified Chinese APT-associated activity targeting Cambodia, including over 20 Cambodian government organizations across a range of key industries. This activity is believed to be part of a long-term espionage campaign.

The observed activity aligns with geopolitical goals of the Chinese government as it seeks to leverage their strong relations with Cambodia to project their power and expand their naval operations in the region. We encourage all organizations to leverage our findings to inform the deployment of protective measures to defend against this activity.

Protection Recommendations

To defend against the threats described in this blog, Palo Alto Networks recommends organizations employ the following capabilities:

- Network Security: Delivered through a Next-Generation Firewall (NGFW) configured with machine learning enabled and cloud-delivered security services. This includes threat prevention, URL filtering, DNS security and a malware prevention engine capable of identifying and blocking malicious samples and infrastructure.
- Security Automation: Delivered through a Cortex XSOAR or XSIAM solution capable of providing SOC analysts with a comprehensive understanding of the threat derived by stitching together data obtained from endpoints, network, cloud and identity systems.
- Container Security: Delivered through the Palo Alto Networks Prisma Cloud advanced container security features for container runtime environments to ensure detection and prevention of known malicious executables. Advanced URL Filtering blocks malicious IoCs related to this operation. WildFire integration for cloud-delivered malware analysis service accurately identifies known samples as malicious.

Protections and Mitigations

Palo Alto Networks customers receive protection from the threats discussed above through the following products:

- Advanced URL Filtering blocks web requests to malicious URLs
- DNS Security effectively prevents the resolution of C2 hostnames
- Container Runtime Inspection prevents DNS requests from malicious processes

If you think you might have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730

- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Domains

- api.infinitycloud[.]info
- connect.infinitycloud[.]info
- ns.infinitycloud[.]info
- connect.infinitybackup[.]net
- ns1.infinitybackup[.]net
- share.infinitybackup[.]net
- file.wonderbackup[.]com
- login.wonderbackup[.]com
- sync.wonderbackup[.]com
- update.wonderbackup[.]com
- ads.teleryanhart[.]com
- mfi.teleryanhart[.]com
- dfg.ammopak[.]site
- fwg.ammopak[.]site
- jlp.ammopak[.]site
- kwe.ammopak[.]site
- lxo.ammopak[.]site
- connect.clinkvl[.]com

Infrastructure IP Addresses

- 165.232.186[.]197
- 167.71.226[.]171
- 104.248.153[.]204
- 143.110.189[.]141
- 172.105.34[.]34
- 194.195.114[.]199

SSL Certificate SHA-1 Fingerprint

- B8CFF709950CFA86665363D9553532DB9922265C