Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally

fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html

Threat Research

Scott Henderson, Steve Miller, Dan Perez, Marcin Siedlarz, Ben Wilson, Ben Read

Jul 10, 2018

9 mins read

Malware

Threat Research

Introduction

FireEye has examined a range of TEMP.Periscope activity revealing extensive interest in Cambodia's politics, with active compromises of multiple Cambodian entities related to the country's electoral system. This includes compromises of Cambodian government entities charged with overseeing the elections, as well as the targeting of opposition figures. This campaign occurs in the run up to the country's July 29, 2018, general elections. TEMP.Periscope used the same infrastructure for a range of activity against other more traditional targets, including the defense industrial base in the United States and a chemical company based in Europe. Our previous blog post focused on the group's targeting of engineering and maritime entities in the United States.

Overall, this activity indicates that the group maintains an extensive intrusion architecture and wide array of malicious tools, and targets a large victim set, which is in line with typical Chinese-based APT efforts. We expect this activity to provide the Chinese government with widespread visibility into Cambodian elections and government operations. Additionally, this group is clearly able to run several large-scale intrusions concurrently across a wide range of victim types.

Our analysis also strengthened our overall attribution of this group. We observed the toolsets we previously attributed to this group, their observed targets are in line with past group efforts and also highly similar to known Chinese APT efforts, and we identified an IP address originating in Hainan, China that was used to remotely access and administer a command and control (C2) server.

TEMP.Periscope Background

Active since at least 2013, TEMP.Periscope has primarily focused on maritime-related targets across multiple verticals, including engineering firms, shipping and transportation, manufacturing, defense, government offices, and research universities (targeting is summarized in Figure 1). The group has also targeted professional/consulting services, high-tech industry, healthcare, and media/publishing. TEMP.Periscope overlaps in targeting, as well as tactics, techniques, and procedures (TTPs), with TEMP.Jumper, a group that also overlaps significantly with public reporting by Proofpoint and F-Secure on "NanHaiShu."

Figure 1: Summary of TEMP.Periscope activity

Incident Background

FireEye analyzed files on three open indexes believed to be controlled by TEMP.Periscope, which yielded insight into the group's objectives, operational tactics, and a significant amount of technical attribution/validation. These files were "open indexed" and thus accessible to anyone on the public internet. This TEMP.Periscope activity on these servers extends from at least April 2017 to the present, with the most current operations focusing on Cambodia's government and elections.

- Two servers, chemscalere[.]com and scsnewstoday[.]com, operate as typical C2 servers and hosting sites, while the third, mlcdailynews[.]com, functions as an active SCANBOX server. The C2 servers contained both logs and malware.
- Analysis of logs from the three servers revealed:
  - Potential actor logins from an IP address located in Hainan, China that was used to remotely access and administer the servers, and interact with malware deployed at victim organizations.
  - Malware command and control check-ins from victim organizations in the education, aviation, chemical, defense, government, maritime, and technology sectors across multiple regions. FireEye has notified all of the victims that we were able to identify.
- The malware present on the servers included both new families (DADBOD, EVILTECH) and previously identified malware families (AIRBREAK, EVILTECH, HOMEFRY, MURKYTOP, HTRAN, and SCANBOX) .

Compromises of Cambodian Election Entities

Analysis of command and control logs on the servers revealed compromises of multiple Cambodian entities, primarily those relating to the upcoming July 2018 elections. In addition, a separate spear phishing email analyzed by FireEye indicates concurrent targeting of opposition figures within Cambodia by TEMP.Periscope.

Analysis indicated that the following Cambodian government organizations and individuals were compromised by TEMP.Periscope:

- National Election Commission, Ministry of the Interior, Ministry of Foreign Affairs and International Cooperation, Cambodian Senate, Ministry of Economics and Finance
- Member of Parliament representing Cambodia National Rescue Party
- Multiple Cambodians advocating human rights and democracy who have written critically of the current ruling party
- Two Cambodian diplomats serving overseas
- Multiple Cambodian media entities

TEMP.Periscope sent a spear phish with AIRBREAK malware to Monovithya Kem, Deputy Director-General, Public Affairs, Cambodia National Rescue Party (CNRP), and the daughter of (imprisoned) Cambodian opposition party leader Kem Sokha (Figure 2). The decoy document purports to come from LICADHO (a non-governmental organization [NGO] in Cambodia established in 1992 to promote human rights). This sample leveraged scsnewstoday[.]com for C2.

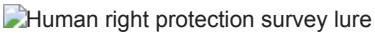

Figure 2: Human right protection survey lure

The decoy document "Interview Questions.docx" (MD5: ba1e5b539c3ae21c756c48a8b5281b7e) is tied to AIRBREAK downloaders of the same name. The questions reference the opposition Cambodian National Rescue Party, human rights, and the election (Figure 3).

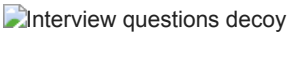

Figure 3: Interview questions decoy

Infrastructure Also Used for Operations Against Private Companies

The aforementioned malicious infrastructure was also used against private companies in Asia, Europe and North America. These companies are in a wide range of industries, including academics, aviation, chemical, maritime, and technology. A MURKYTOP sample from 2017 and data contained in a file linked to chemscalere[.]com suggest that a corporation involved in the U.S. defense

industrial base (DIB) industry, possibly related to maritime research, was compromised. Many of these compromises are in line with TEMP.Periscope's previous activity targeting maritime and defense industries. However, we also uncovered the compromise of a European chemical company with a presence in Asia, demonstrating that this group is a threat to business worldwide, particularly those with ties to Asia.

AIRBREAK Downloaders and Droppers Reveal Lure Indicators

Filenames for AIRBREAK downloaders found on the open indexed sites also suggest the ongoing targeting of interests associated with Asian geopolitics. In addition, analysis of AIRBREAK downloader sites revealed a related server that underscores TEMP.Periscope's interest in Cambodian politics.

The AIRBREAK downloaders in Table 1 redirect intended victims to the indicated sites to display a legitimate decoy document while downloading an AIRBREAK payload from one of the identified C2s. Of note, the hosting site for the legitimate documents was not compromised. An additional C2 domain, partyforumseasia[.]com, was identified as the callback for an AIRBREAK downloader referencing the Cambodian National Rescue Party.

Redirect Site (Not Malicious)	AIRBREAK Downloader	AIRBREAK C2
en.freshnewsasia.com/index.php/en/8623-2018-04-26-10-12-46.html	TOP_NEWS_Japan_to_Support_the_Election.js (3c51c89078139337c2c92e084bb0904c) [Figure 4]	chemscalere[.]com
iric.gov.kh/LICADHO/Interview-Questions.pdf	[pdf]Interview-Questions.pdf.js (e413b45a04bf5f812912772f4a14650f)	
iric.gov.kh/LICADHO/Interview-Questions.pdf	[docx]Interview-Questions.docx.js (cf027a4829c9364d40dcab3f14c1f6b7)	
unknown	Interview_Questions.docx.js (c8fdd2b2ddec970fa69272fdf5ee86cc)	scsnewstoday[.]com
atimes.com/article/philippines-draws-three-hard-new-lines-on-china/	Philippines-draws-three-hard-new-lines-on-china .js (5d6ad552f1d1b5cfe99ddb0e2bb51fd7)	mlcdailynews[.]com
facebook.com/CNR.Movement/videos/190313618267633/	CNR.Movement.mp4.js (217d40ccd91160c152e5fce0143b16ef)	Partyforumseasia[.]com

Table 1: AIRBREAK downloaders

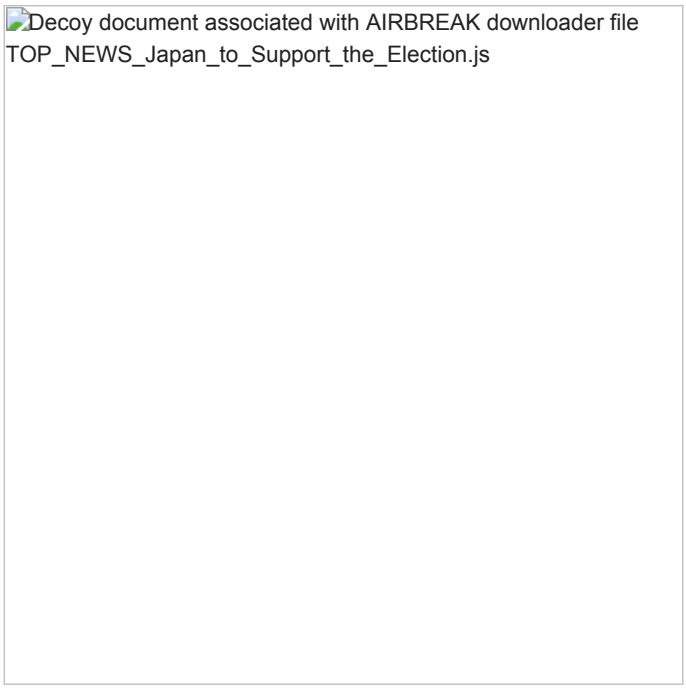

Figure 4: Decoy document associated with AIRBREAK downloader file TOP_NEWS_Japan_to_Support_the_Election.js

SCANBOX Activity Gives Hints to Future Operations

The active SCANBOX server, mlcdailynews[.]com, is hosting articles related to the current Cambodian campaign and broader operations. Articles found on the server indicate targeting of those with interests in U.S.-East Asia geopolitics, Russia and NATO affairs. Victims are likely either brought to the SCANBOX server via strategic website compromise or malicious links in targeted emails with the article presented as decoy material. The articles come from open-source reporting readily available online. Figure 5 is a SCANBOX welcome page and Table 2 is a list of the articles found on the server.

Figure 5: SCANBOX welcome page

Copied Article Topic	Article Source (Not Compromised)

Leaders confident yet nervous	Khmer Times
Mahathir_ 'We want to be friendly with China	
PM urges voters to support CPP for peace	
CPP determined to maintain Kingdom's peace and development	
Bun Chhay's wife dies at 60	
Crackdown planned on boycott callers	
Further floods coming to Kingdom	
Kem Sokha again denied bail	
PM vows to stay on as premier to quash traitors	
Iran_ Don't trust Trump	Fresh News
Kim-Trump summit_ Singapore's role	
Trump's North Korea summit may bring peace declaration - but at a cost	Reuters
U.S. pushes NATO to ready more forces to deter Russian threat	
us-nato-russia_us-pushes-nato-to-ready-more-forces-to-deter-russian-threat	
Interior Minister Sar Kheng warns of dirty tricks	Phnom Penh Post
Another player to enter market for cashless pay	
Donald Trump says he has 'absolute right' to pardon himself but he's done nothing wrong - Donald Trump's America	ABC News
China-funded national road inaugurated in Cambodia	The Cambodia Daily
Kim and Trump in first summit session in Singapore	Asia Times
U.S. to suspend military exercises with South Korea, Trump says	U.S. News
Rainsy defamed the King_ Hun Sen	BREAKING NEWS
cambodia-opposition-leader-denied-bail-again-in-treason-case	Associated Press

Table 2: SCANBOX articles copied to server

TEMP.Periscope Malware Suite

Analysis of the malware inventory contained on the three servers found a classic suite of TEMP.Periscope payloads, including the signature AIRBREAK, MURKYTOP, and HOMEFRY. In addition, FireEye's analysis identified new tools, EVILTECH and DADBOD (Table 3).

Malware	Function	Details
EVILTECH	Backdoor	• EVILTECH is a JavaScript sample that implements a simple RAT with support for uploading, downloading, and running arbitrary JavaScript. • During the infection process, EVILTECH is run on the system, which then causes a redirect and possibly the download of additional malware or connection to another attacker-controlled system.
DADBOD	Credential Theft	• DADBOD is a tool used to steal user cookies. • Analysis of this malware is still ongoing.

Table 3: New additions to the TEMP.Periscope malware suite

Data from Logs Strengthens Attribution to China

Our analysis of the servers and surrounding data in this latest campaign bolsters our previous assessment that TEMP.Periscope is likely Chinese in origin. Data from a control panel access log indicates that operators are based in China and are operating on computers with Chinese language settings.

A log on the server revealed IP addresses that had been used to log in to the software used to communicate with malware on victim machines. One of the IP addresses, 112.66.188.28, is located in Hainan, China. Other addresses belong to virtual private servers, but artifacts indicate that the computers used to log in all cases are configured with Chinese language settings.

Outlook and Implications

The activity uncovered here offers new insight into TEMP.Periscope's activity. We were previously aware of this actor's interest in maritime affairs, but this compromise gives additional indications that it will target the political system of strategically important countries. Notably, Cambodia has served as a reliable supporter of China's South China Sea position in international forums such as ASEAN and is an important partner. While Cambodia is rated as Authoritarian by the Economist's Democracy Index, the recent surprise upset of the ruling party in Malaysia may motivate China to closely monitor Cambodia's July 29 elections.

The targeting of the election commission is particularly significant, given the critical role it plays in facilitating voting. There is not yet enough information to determine why the organization was compromised – simply gathering intelligence or as part of a more complex operation. Regardless, this incident is the most recent example of aggressive nation-state intelligence collection on election processes worldwide.

We expect TEMP.Periscope to continue targeting a wide range of government and military agencies, international organizations, and private industry. However focused this group may be on maritime issues, several incidents underscore their broad reach, which has included European firms doing business in Southeast Asia and the internal affairs of littoral nations. FireEye expects TEMP.Periscope will remain a virulent threat for those operating in the area for the foreseeable future.