Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage

fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html

Breadcrumb

Threat Research

Scott Henderson, Gabby Roncone, Sarah Jones, John Hultquist, Ben Read

Apr 22, 2020

3 mins read

Advanced Persistent Threats (APTs)

Threat Research

From at least January to April 2020, suspected Vietnamese actors APT32 carried out intrusion campaigns against Chinese targets that Mandiant Threat Intelligence believes was designed to collect intelligence on the COVID-19 crisis. Spear phishing messages were sent by the actor to China's Ministry of Emergency Management as well as the government of Wuhan province, where COVID-19 was first identified. While targeting of East Asia is consistent with the activity we've previously reported on APT32, this incident, and other publicly reported intrusions, are part of a global increase in cyber espionage related to the crisis, carried out by states desperately seeking solutions and nonpublic information.

Phishing Emails with Tracking Links Target Chinese Government

The first known instance of this campaign was on Jan. 6, 2020, when APT32 sent an email with an embedded tracking link (Figure 1) to China's Ministry of Emergency Management using the sender address lijianxiang1870@163[.]com and the subject 第一期办公设备招标结果报告 (translation: Report on the first quarter results of office equipment bids). The embedded link contained the victim's email address and code to report back to the actors if the email was opened.

Figure 1: Phishing email to China's Ministry of Emergency Management

Mandiant Threat Intelligence uncovered additional tracking URLs that revealed targets in China's Wuhan government and an email account also associated with the Ministry of Emergency Management.

- libjs.inquirerjs[.]com/script/<VICTIM>@wuhan.gov.cn.png
- libjs.inquirerjs[.]com/script/<VICTIM>@chinasafety.gov.cn.png
- m.topiccore[.]com/script/<VICTIM>@chinasafety.gov.cn.png
- m.topiccore[.]com/script/<VICTIM>@wuhan.gov.cn.png
- libjs.inquirerjs[.]com/script/<VICTIM>@126.com.png

The libjs.inquirerjs[.]com domain was used in December as a command and control domain for a METALJACK phishing campaign likely targeting Southeast Asian countries.

Additional METALJACK Activity Suggests Campaigns Targeting Mandarin Speakers Interested in COVID-19

APT32 likely used COVID-19-themed malicious attachments against Chinese speaking targets. While we have not uncovered the full execution chain, we uncovered a METALJACK loader displaying a Chinese-Language titled COVID-19 decoy document while launching its payload.

When the METALJACK loader, krpt.dll (MD5: d739f10933c11bd6bd9677f91893986c) is loaded, the export "_force_link_krpt" is likely called. The loader executes one of its embedded resources, a COVID-themed RTF file, displaying the content to the victim and saving the document to %TEMP%.

The decoy document (Figure 2) titled 冠状病毒实时更新：中国正在追踪来自湖北的旅行者, MD5: c5b98b77810c5619d20b71791b820529 (Translation: COVID-19 live updates: China is currently tracking all travelers coming from Hubei Province) displays a copy of a New York Times article to the victim.

Figure 2: COVID-themed decoy document

The malware also loads shellcode in an additional resource, MD5: a4808a329b071a1a37b8d03b1305b0cb, which contains the METALJACK payload. The shellcode performs a system survey to collect the victim's computer name and username and then appends those values to a URL string using libjs.inquirerjs[.]com. It then attempts to call out to the URL. If the callout is successful, the malware loads the METALJACK payload into memory.

It then uses vitlescaux[.]com for command and control.

Outlook

The COVID-19 crisis poses an intense, existential concern to governments, and the current air of distrust is amplifying uncertainties, encouraging intelligence collection on a scale that rivals armed conflict. National, state or provincial, and local governments, as well as non-

government organizations and international organizations, are being targeted, as seen in reports. Medical research has been targeted as well, according to public statements by a Deputy Assistant Director of the FBI. Until this crisis ends, we anticipate related cyber espionage will continue to intensify globally.

Indicators

Type	Indicators
Domains	m.topiccore[.]com jcdn.jsoid[.]com libjs.inquirerjs[.]com vitlescaux[.]com
Email Address	lijianxiang1870@163[.]com
Files	MD5: d739f10933c11bd6bd9677f91893986c METALJACK loader MD5: a4808a329b071a1a37b8d03b1305b0cb METALJACK Payload MD5: c5b98b77810c5619d20b71791b820529 Decoy Document (Not Malicious)

Detecting the Techniques

Platform	Signature Name
Endpoint Security	Generic.mg.d739f10933c11bd6
Network Security	Trojan.Apost.FEC2, Trojan.Apost.FEC3, fe_ml_heuristic
Email Security	Trojan.Apost.FEC2, Trojan.Apost.FEC3, fe_ml_heuristic
Helix	

Mandiant Security Validation Actions

- A150-096 - Malicious File Transfer - APT32, METALJACK, Download
- A150-119 - Protected Theater - APT32, METALJACK Execution
- A150-104 - Phishing Email - Malicious Attachment, APT32, Contact Information Lure

MITRE ATT&CK Technique Mapping

Tactic	Techniques
Initial Access	Spearphishing Attachment (T1193), Spearphising Link (T1192)
Execution	Regsvr32 (T1117), User Execution (T1204)
Defense Evasion	Regsvr32 (T1117)
Command and Control	Standard Cryptographic Protocol (T1032), Custom Command and Control Protocol (T1094)