EC-Council CISO MAG IS EVOLVING
As a response to our community and to ensure timely and relevant content, CISO Mag's digital edition will be replaced with the new EC-Council Cybersecurity Exchange. Stay tuned for new, free online content, coming soon via Cybersecurity Exchange!

FREE Certified Ethical Hacker CEH + FREE Specialization Course Wireless Ethical Hacking WAHS = Build the Ultimate Career in Ethical Hacking
SIGN UP FOR THE DUAL PROGRAM AT NO ADDITIONAL COST!
Valid until December 31, 2021 * Terms & Conditions Apply

GOVERNANCE NEWS THREATS

Vietnam's APT32 Group Uses COVID-19 to Target Chinese Health Authorities

By CISOMAG - April 27, 2020

SHARE Facebook Twitter G+

According to a report from Fireeye, the Vietnamese threat group APT32 is suspected to have carried out a series of attacks aimed at the Wuhan province government and China's Ministry of Emergency Management to collect intelligence on the COVID-19 crisis. The researchers noted that the attackers targeted multiple users through a spear-phishing campaign run from at least January in April 2020.

> *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.*
>
> *– Fireeye*

Brief History of APT32

APT32 aka OceanLotus or APT-C-00, is suspected to be backed by the Vietnamese government. APT32 is popularly known to carry out cyber espionage campaigns against companies and countries doing business, manufacturing, or preparing to invest in Vietnam. The threat actors leverage a phishing mail to initiate an attack that contains ActiveMime files. They make use of social engineering as a bait to lure the victim into enabling the macros. Once executed, the initialized file downloads multiple malicious payloads like Soundbite, Windshield, Phoreal, Beacon, and Komprogo from a remote server.

Phishing Emails with Tracking Links

The first phishing attack was traced to January 6, 2020, when APT32 sent an email to China's Ministry of Emergency Management using the sender address as 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 email's content had an embedded link that sent the victim's email address and codes back to the threat actors indicating them that the email was opened.

Figure: Phishing email to China's Ministry of Emergency Management (Image Source: Fireeye)

Researchers also found that the libjs.inquirerjs[.]com domain was being used since December as a C2 domain for a METALJACK phishing campaign to target Southeast Asian countries. APT32 likely used COVID-19-themed malicious attachments in Chinese-Language as a decoy to drop a METALJACK payload.

Threat Summary	
Threat Group	APT32
Threat type	Spear-phishing, phishing
Payload Name	METALJACK
Target Audience	South-east Asia, Chinese speaking
Campaign Active Since	From at least January 2020
Domain Indicators	- m.topiccore[.]com - jcdn.jsoid[.]com - libjs.inquirerjs[.]com - vitlescaux[.]com
Email Address Used	lijianxiang1870@163[.]com
Malicious File Names	MD5: d739f10933c11bd6bd9677f91893986c – METALJACK loader MD5: a4808a329b071a1a37b8d03b1305b0cb – METALJACK Payload MD5: c5b98b77810c5619d20b71791b820529 – Decoy Document (Not Malicious)
Damages caused	Intellectual and confidential COVID-19 related state and government data can be compromised. Additional trojans and malware infections can be installed to exfiltrate data in future.

Researchers added that, "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. Until this crisis ends, we anticipate related cyber espionage will continue to intensify globally."

TAGS ADVANCED PERSISTENT THREAT APT32 APT32 GROUP CHINA CHINA MINISTRY OF EMERGENCY MANAGEMENT COVID-19 THREAT GROUP VIETNAM WUHAN

SHARE Facebook Twitter G+

Previous article
South Korean and US Payment Card Records Valued at $2 Mn up for Sale on Dark Web

Next article
Hackers Illicitly Access 160,000 Nintendo Accounts

CISOMAG
https://cisomag.eccouncil.org/

RELATED ARTICLES MORE FROM AUTHOR

News
FBI Issues a Lookout for SIM Swapping Attacks

News
How Remote Work Increase Digital Anxiety

News
Ransomware: To Pay or Not to Pay?

Active Directory Protection Like You've Never Seen Before!
• Continuous Exposure Visibility
• Live Attack Detection
• Conceal AD Objects
• Remediation Recommendations
Attivo NETWORKS LEARN MORE

Latest Issue Is Out!

SUBSCRIBE NOW

EC-Council
Boost Your Cybersecurity Career
Be a Leader.
Be a C|CISO.
Learn more

EC-Council
Are You A Red Team Engineer
WEB APPLICATION HACKING & SECURITY
THIS SKILL IS FOR YOU
Learn More

FOLLOW US FOR MORE UPDATES

CISO MAG
EDITORIAL CALENDAR 2021
DOWNLOAD NOW

Subscribe Now to receive Free Newsletter
Full Name*
Email*
Captcha*
Nggf7b
Refresh
By signing up, you agree to EC-Council's CISO MAG using your data, in accordance with our Privacy Policy & Terms of Use. We use your data to personalize and improve your experience as a member and to provide the services you request from us. You can change your preferences or unsubscribe at any time by editing your profile on your Member Dashboard or by clicking here*
Subscribe

CYBER SHOTS
Quick, punchy updates on Cyber trends, news and links to free resources. Only via Telegram and Signal. Join the groups now!
Click Here Click Here

MOST POPULAR

45% companies don't have cybersecurity leader: Study
CISOMAG - December 11, 2017

Nearly half of companies have suffered a data breach in the past year: Survey
November 15, 2017

Mobile messaging apps new hideout of Dark Web activities: Study
October 27, 2017

NSA hacking code lifted from a personal computer in U.S.: Kaspersky
October 30, 2017

Instagram data breach! 49 million users' sensitive data exposed online
May 23, 2019

RECENT POSTS

FBI Issues a Lookout for SIM Swapping Attacks
February 15, 2022

How Remote Work Increase Digital Anxiety
February 9, 2022

How to Update Web Browsers for Secure Browsing
February 8, 2022

We'll See More Data Exfiltration and Data Leak Threats
February 7, 2022

A Beginner's Guide to Forensics as a Service (FaaS)
February 4, 2022

We Care
Ensuring that you get the best experience is our only purpose for using cookies. If you wish to continue, please accept. You are welcome to provide a controlled consent by visiting the cookie settings. For any further queries or information, please see our privacy policy.
Do not sell my personal information.
Cookie Settings Accept