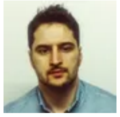
Chinese state hackers target Hong Kong Catholic Church

zdnet.com/article/chinese-state-hackers-target-hong-kong-catholic-church/

Home Innovation Security

EXCLUSIVE: Spear-phishing operation targets members of the Hong Kong Catholic Church.



Written by Catalin Cimpanu, Contributor on July 15, 2020 catholic church cross

Image: Mateus Campos Felipe

China's government hackers have targeted members of the Hong Kong Catholic Church in a series of spear-phishing operations traced back to May this year.

The attacks have come to light after reports [1, 2, 3] that some of Hong Kong's church leaders and clergy have been directly involved in supporting pro-democracy protests despite orders from the Vatican to remain neutral.

The spear-phishing campaign fits recent reports that Chinese government hacking groups focusing cyber-espionage efforts on the Hong Kong region after pro-democracy protests begun last year [1, 2].

The spear-phishing campaign

The current attacks were revealed earlier this week by a malware analyst who goes online by the pseudonym of Arkbird.

In an interview, the researcher told *ZDNet* he discovered malware samples typically associated with Chinese state groups uploaded on VirusTotal.

The malware files were ZIP and RAR archives containing Windows executable files [1, 2, 3].

According to sandbox analysis, unpacking and running the files starts a legitimate app like Microsoft Word or Adobe Reader.

The legitimate apps load a lure document, such as communications from Vatican officials or news articles from the Union of Catholic Asian News, a news portal dedicated to tracking the affairs of the Catholic church and communities across Asia.

hk-apt-lure.png

Arkbird says that alongside the legitimate apps and the lure documents, a malicious DLL file is also loaded that installs malware on the victim's computer, using a technique known as DLL-sideloading.

In a phone interview today, Fred Plan, malware analyst at Mandiant Threat Intelligence, part of US cyber-security firm FireEye, said that this particular version of the DLL-sideloading technique has been a staple of Chinese nation-state hacking groups for years.

Plan, who reviewed Arkbird's findings, said the final payload was a malware commonly known as PlugX, a remote access trojan that grants attackers control over infected hosts.

Based on previous public reporting, Arkbird attributed the malware samples to a group known as Mustang Panda, a Chinese hacking group known for its widespread use of DLL-sideloading (according to Lab52) and its targeting of religious groups, including Catholic organizations (according to Anomali).

Mandiant, who uses a more strict group-tracking system, said this particular cluster of activity around these attacks was not connected to existing clusters but confirmed its connection to Chinese cyber-espionage efforts.

Arkbird published his findings on Twitter this week after receiving the go-ahead from Italian law enforcement, where a colleague also reported the attacks.

A spokesperson for the Hong Kong Catholic Diocese did not return a request for comment sent yesterday. A spokesperson for the Rome Holy See did not want to comment.

The complicated China-Vatican relations

Relations between China and the Vatican have improved in recent years but are still on thin ice. The two broke all diplomatic ties in 1951. At the time, Beijing's fledgling communist rule begun cracking down on all religious groups with the aim of bringing local leadership structures under the Communist Party's control.

After the fallout, China began appointing its own party-approved bishops across the country, a move that split the Chinese Catholic community.

A part continued attending masses at official government-mandated churches with party-imposed bishops, while the other attended underground churches -- unrecognized by both China and the Vatican, but believed to have operated all these years with the Holy See's blessing.

Relations between the China and the Holy See eventually thawed in the 2000s, as China sought a more prominet role in international affairs, and both parties began brokering an agreement of collaboration.

The agreement, signed in September 2018, allowed the Pope to resume the Vatican's control over the Chinese Catholic Church by giving it the power to appoint bishops -- with the caveat that the bishops also had to receive a green light from by the Communist Party.

This agreement stands to be renewed in September later this year, and Hong Kong Holy See officials have used it as a reasoning point not to show public support for the protests, fearing Chinese leadership might isolate the Chinese Catholic Community again, as they did in previous decades.

Article updated to remove a link to a report about the Hong Kong Archbishop of the Anglican Church that was erroneously cited. ZDNet regrets the error.

The world's most famous and dangerous APT (state-developed) malware