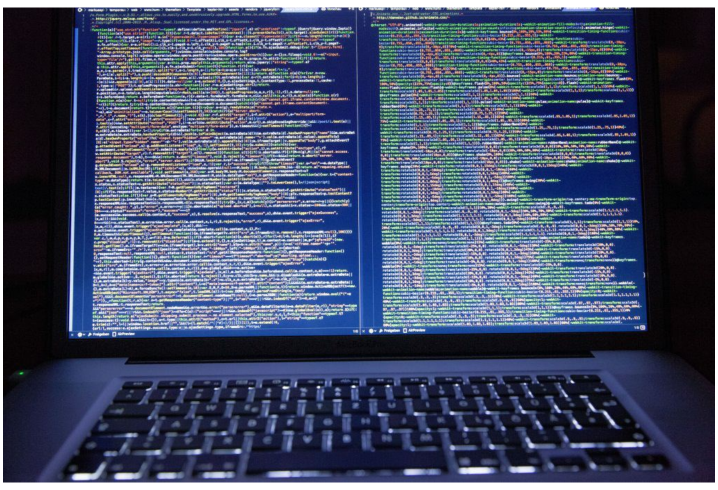
# Tibetan activists, diaspora hit by resurfacing malware in cyberespionage operation

by Luana Pascu on August 13, 2018



The Tibetan diaspora has once again fallen victim to a sophisticated malware campaign similar to one detected in 2016, reports Citizen Lab after receiving the infected files from one of the targets – a Tibetan NGO.

It appears the campaign was activated between January and March 2018 and bears a lot of similarity with another malware campaign that happened in 2016, both allegedly part of the Tropic Trooper campaign, when hackers targeted the governments of Taiwan and the Philippines.

“The Resurfaced Campaign used different exploits and payloads than the Parliamentary Campaign but shares other connections,” reads the report. “The two campaigns used similar spear phishing messages and both targeted Tibetan parliamentarians. One of the e-mail addresses used to send spear phishing messages in the Resurfaced Campaign (tibetanparliarnent[@]yahoo.com) was also used repeatedly during the Parliamentary Campaign.”

Malicious campaigns have so far targeted Tibetan activists, journalists, members of the Tibetan Parliament in exile and the Central Tibetan Administration, as part of a large-scale cyberespionage operation. Researchers believe the same hacker group could be behind all the campaigns on the Tibetan diaspora, which has been highly targeted in the past ten years.

The Tibetan activist who received the infected files was suspicious from the get-go as this wasn’t the first time such an attempt was made. Even though the email seemed legitimate, it contained a Power Point presentation and a text file.

Once analyzed by Citizen Lab, they concluded the two were indeed infected with malicious code meant to infect Windows computers. In comparison with the previous campaign which relied on targeted malware, known exploits and basic Remote Access Trojans, the 2018 campaign relied more on social engineering schemes to trick the victims into opening the corrupted files and steal credentials through phishing attempts.

“The campaign used social engineering to trick targets into opening exploit-laden PowerPoint (CVE-2017-0199) and Microsoft Rich Text Format (RTF) documents (CVE-2017-11882) attached to e-mail messages,” writes Citizen Lab. “The malware includes a PowerShell payload we call DMShell++, a backdoor known as TSSL, and a post-compromise tool we call DSNGInstaller.”

*** This is a Security Bloggers Network syndicated blog from HOTforSecurity authored by Luana Pascu. Read the original post at: https://hotforsecurity.bitdefender.com/blog/tibetan-activists-diaspora-hit-by-resurfacing-malware-in-cyberespionage-operation-20239.html

Industry News, Malware Campaign, social engineering, Tibet, Tibetan diaspora, Tropic Trooper

← Researchers Showed It’s Possible to Take Over a Network With Malicious Faxes

CISA Domain 2: Governance and Management of IT →

Most Read on the Boulevard

7 Linux Distros for Security Testing

ZeroNorth Raises $10M to Advance Risk Orchestration

Storage Is Your Data Lifecycle Weak Spot

Why Traditional Security Is Failing Us

Supply Chain Security Amid Coronavirus Fallout

Boost manufacturing security with a vendor access management strategy

What is your GCP infra worth?…about ~$700 [Bugbounty]

Upcoming Webinars »

THU 19 Securing APIs at DevOps Speed
March 19 @ 1:00 pm - 2:00 pm

MON 23 The State of Open Source Security
March 23 @ 1:00 pm - 2:00 pm

TUE 31 Protect Yourself from Cyber Attacks Through Proper Third-Party Risk Management
March 31 @ 11:00 am - 12:00 pm

APR 09 Integrate Security Early and Often For Successful DevSecOps
April 9 @ 1:00 pm - 2:00 pm

Recent Security Boulevard Chats

Cloud, DevSecOps and Network Security, All Together?

Security-as-Code with Tim Jefferson, Barracuda Networks

ASRTM with Rohit Sethi, Security Compass

Deception: Art or Science, Ofer Israeli, Illusive Networks

Tips to Secure IoT and Connected Systems w/ DigiCert

Industry Spotlight »

5 Good Reasons to Outsource Security Testing

Why Traditional Security Is Failing Us

7 Linux Distros for Security Testing

Top Stories »

Contrast Security Advances DevSecOps

Fusion Creates Online Pandemic Readiness Resource

ZeroNorth Raises $10M to Advance Risk Orchestration

Security Humor »

The Joy of Tech® ‘Your Brain Vs. Your Face’

SECURITY BOULEVARD
Home of the Security Bloggers Network

DMCA.com COMPLIANT

Join the Community

Add your blog to Security Bloggers Network

Write for Security Boulevard

Bloggers Meetup and Awards

Ask a Question

Email: info@securityboulevard.com

Useful Links

About

Media Kit

Sponsors Info

Copyright

TOS

Privacy Policy

DMCA Compliance Statement

Other Mediaops Sites

Container Journal

DevOps.com

DevOps Connect

DevOps Institute