VISA Visa Threat Intelligence
powered by FireEye

Suspected Chinese State Sponsored Actors, Known as Hammer Panda, Linked to Targeting of Financial Industry

By Visa | Posted At: 05/19/17 3:00 AM PDT

https://apps.fireeye.com/visa-vti/briefings/B-5W48DTP

This confidential report is provided to you in accordance with the Terms and Conditions of this service. Except as clearly provided in the Terms and Conditions, any use or disclosure of this report or any information contained herein is strictly prohibited. This report is Visa Confidential information and only meant for distribution to authorized recipients of this Service. If you are not authorized to use this Service, you should return or destroy this report.

Executive Summary:

- On 28 April 2017, VTI observed spear-phishing attempts from the Chinese attributed, espionage group known as Hammer Panda (also known as TEMP.Zhenbao, NetTraveler, and Hammerhead.)

- VTI notes Hammer Panda actors targeted financial analysts focusing in telecommunications, all working actively in Russian and Commonwealth of Independent State geographical areas.

- Hammer Panda activity was observed utilizing the very recently published Microsoft Office vulnerability (CVE-2017-0199) to deliver the ZeroT Trojan and later download a customized variant of the PlugX Trojan which shows an increase in capability from previous activity.

Background:

On 27 April 2017, VTI sources reported on the targeting of financial sector entities on 20 April 2017 by actors attributed to the Chinese nation-state backed espionage group known as Hammer Panda (also known as TEMP. Zhenbao, NetTraveler, and Hammerhead). Hammer Panda attributed actors have long been observed targeting entities working in Central and Eastern Europe as well as Mongolia and other geographic locations when those entities' interests align with the Chinese government. The malware campaign utilized highly targeted spear phishing emails appearing to originate from the Spanish Embassy in Khazakhstan (**embajada@kazesp[.]org**). The phishing email were sent to and targeted analysts focused on the telecommunications industry in Russia and the surrounding regions.

Analyst View:

In the most recent campaign attributed to Hammer Panda, actors delivered a single phishing email which carried the blank Microsoft Word attachment “0721.doc”. The phishing email attachment attempted to take advantage of a Microsoft Office vulnerability that was disclosed just days prior. VTI notes that execution of the attached malicious document would launch a Hammer Panda specific Trojan known as ZeroT. Once successfully implanted, the ZeroT Trojan would then deploy the PlugX Trojan which is heavily utilized by Chinese APT actors as well as eCrime elements.

- The “0721.doc” attachment once executed will attempt to download “power.rtf” from 112.93.52[.]215, which is actually a HTML Application (HTA) file that is utilized in Microsoft Windows as an executable. “power.rtf” would then call out to the domain previously attributed to Hammer Panda in order to download and execute a powershell script “power.ps1”.

- The aforementioned powershell script then launches a newly modified version of the Hammer Panda specific ZeroT Trojan. Once communication is established, the malware then retrieves stage 2 payloads, which attempt to obfuscate their purpose by appearing as Bitmap (BMP) images. This BMP images utilized Least Significant Bit (LSB) Steganography to hide the malicious payloads. Launching these files will appear as normal images to the targeted individual.

- Once infected with the ZeroT Trojan, the victim machine downloads and beacons out to the attributed Hammer Panda domains: (1) firesyst[.]net, (2) icekkk[.]net, and (3) icefirebest[.]com.

VTI notes that the domains attributed to this campaign follow very similar past infrastructure utilized by Hammer Panda attributed actors. While the use of firesyst[.]net resolves to the IP address 43.249.8[.]116, the other C2 channels resolve to 103.43.17[.]88. VTI investigation determined that the latter IP address has been used in attacks involving the ZeroT Trojan and the other domains which all resolve to the 103.43.17[.]88 IP address: (1) www.tassnews[.]net, (2) www.interfaxru[.]com, (3) www.riaru[.]net, (4) www.info-spb[.]com, and (5) www.mogoogle[.]com. In addition to utilizing the same IP address, all of the above domains were set up with the same registrar: *"Shanghai Meicheng Technology Information Development Co., Ltd"* which further attributes the activity to a single actor group. VTI has created several holistic network detection signatures to identify the Hammer Panda network traffic. VTI is actively working with Sensor Tuning and Enrichment (ST&E) to deploy the custom IDS signatures to detect any malicious activity related to the actors going forward.

Indicators (11)

FQDNs (8)

firesyst.net

icekkk.net

icefirebest.com

www.tassnews.net

www.interfaxru.com

www.riaru.net

www.info-spb.com

www.mogoogle.com

IPs (2)

43.249.8.116

103.43.17.88

Emails (1)

spoofed from embajada@kazesp[.]org