Chinese Nation-State Hackers Target U.S in Operation TradeSecret

By **Sean Michael Kerner** - April 6, 2017

The National Foreign Trade Council (NFTC) website was allegedly infiltrated by Chinese nation-state threat actors, according to a new report from Fidelis Cybersecurity. The attack against the NFTC site has been dubbed 'Operation TradeSecret' by Fidelis and is seen as an attempt to gain insight into individuals closely associated with U.S trade policy activities.

Fidelis is attributing the Operation TradeSecret attack to a group that is also known in the security research community as APT10 and Stone Panda. The same attack group has also been recently actively attacking government sites in the U.K and Japan in an attack that PWC UK and BAE Systems refers to as, Operation CloudHopper.

With Operation TradeSecret, the attackers were able to infiltrate the NFTC site and embed malware on several registration pages. The malware used is identified by Fidelis as being the Scanbox reconnaissance framework. The Scanbox malware is used by attackers to gain insight into victim's activities and information. According to Fidelis, the attack ran from February 27 to March 1 of this year. John Bambenek, Threat Systems Manager at Fidelis said that his company has informed the NFTC of the incident.

"At a high-level, this method of attack is common and has been seen against the defense industrial base and telecoms by APT10 for many years," Bambenek told *eWEEK*.

From a detection perspective, Bambenek explained that Fidelis' security tools are informed by the company's threat intelligence team, a portion of which is dedicated to nation-state adversaries.

"Those tools derive an immense amount of metadata about every session, so that we can find distinct fingerprints that point to a specific actor," Bambenek said. "We are also able to apply intelligence retroactively, so as we discover new threats we can look backwards weeks and months to see if attacks have been successful in the past."

From an attribution perspective for the new Operation TradeSecret campaign, there are a number of attributes that clearly point the finger at Chinese nation-state attackers. Bambenek commented that Scanbox is a tool exclusively seen previously being used by Chinese nation-state sponsored actors.

"The specific obfuscation and other techniques in this instance have been used in the past only by APT10," Bambenek said. "It is possible that another actor somehow got their hands on these tools and are mimicking the techniques, but it is not likely."

At this point, it's not entirely clear how the Operation TradeSecret attackers were actually able to infiltrate the NFTC site and embed the Scanbox malware. Bambenek commented that Fidelis can only speculate as to how this happened to their website. That said he noted that in general terms, there are a number of different things organizations can use to help defend themselves.

Bambenek recommends that organizations use a strong web-application firewall (WAF) to prevent against attacks on their webserver and database layer and have integrity monitoring on webpages to detect unauthorized changes. Additionally, he suggests that organizations work with their peers in the industry to share threat data, so that soft targets around government can collaboratively protect themselves against foreign intelligence services.

Sean Michael Kerner

Sean Michael Kerner is an Internet consultant, strategist, and contributor to several leading IT business web sites.