An End to “Smash-and-Grab” and a Move to More Targeted Approaches

crowdstrike.com/blog/an-end-to-smash-and-grab-more-targeted-approaches/

December 20, 2017

December 20, 2017

Adam Kozy Research & Threat Intel

In late October and early November, 2017, CrowdStrike® Falcon Intelligence™ observed People’s Republic of China (PRC)-based actors conducting espionage-driven targeted attacks against at least four Western think tanks and an additional two non-governmental organizations (NGOs). This marks a significant increase in China-based activity from months prior, as the majority of observed activity in Q3 was predominantly focused on Southeast and East Asia. The previous “smash-and-grab” type of cyber operations, which typically characterized a majority of pre-2016 PRC espionage cases, appear to have ceased in favor of much more targeted intrusions focused on specific outcomes.

Previous operations targeting think tanks resembled the digital equivalents of so-called smash-and-grab robberies: the attackers indiscriminately exfiltrated data, vacuuming up whatever information was available. However, in these most recent incidents, threat actors specifically targeted the communications of foreign personnel involved in Chinese economic policy research and the Chinese economy, as well as users with noted expertise in defense, international finance, U.S.-Sino relations, cyber governance, and democratic elections.

The majority of these intrusions leveraged the *China Chopper* webshell and/or credential harvesting tools targeting the Microsoft Active Directory infrastructure such as *Mimikatz* to compromise credentials for lateral movement in victim networks. Typically, the adversary also retrieved second-stage tools from an external staging server. Actors often searched for very specific strings, such as “china”, “cyber”, “japan”, “korea”, “chinese” and “eager lion” — the latter is likely a reference to a multinational annual military exercise held in Jordan.

In at least two cases, adversaries were observed conducting email directory dumps for a full listing of departments within the victim organizations. Not only does this tactic help refine a list of targeted personnel within the organization, but access to a legitimate email server can provide a platform for conducting future spear-phishing operations. Nearly all the affected organizations likely maintain close ties to Western government officials. This makes them an attractive target for mounting further attacks against government-supporting sectors, since the intruders can masquerade as trusted sources when sending spear-phishing emails.

PANDA vs. Falcon

An interesting case study was observed by both CrowdStrike Services and the Falcon OverWatch™ managed hunting team in late October 2017, when a China-based adversary attempted to compromise the web server of a think tank. The specific target appeared to be related to an ongoing military research project. As with many of the currently observed Chinese targeted intrusions, the adversary attempted to use China Chopper for reconnaissance and lateral movement after logging in via an account compromised by spear phishing. As is prevalent among CrowdStrike customers, webshell blocking was enabled in the Falcon endpoint protection platform, which prevented the actor from using the webshell to run any commands.

The operator attempted to access the server using the China Chopper shell for four days in a row, showing particular dedication to targeting this endpoint. The actor attempted several **whoami** requests during normal Beijing business hours. On the fourth day, after repeated failures, subsequent access attempts occurred at 11 p.m. Beijing time. This after-hours attempt was likely conducted by a different operator, or possibly someone called in to troubleshoot the webshell. After a quick series of tests, the activity ceased and no attempts were made over the weekend. Except for the 11 p.m. login, the observed activity suggests that the adversary is a professional outfit with normal operating hours and assigned tasks.

On the following Monday, the actors returned, logging into the same user account and attempting a different shell, however, this attempt was also quickly staunched by CrowdStrike Services. After being forced out again, the actor appeared to switch tactics and returned via the same account to conduct a SQL injection on the web server. When the attempt failed yet again, the user signed out and a separate host began conducting a low-volume DDoS attack on the think tank’s website.

This case is notable for several reasons. First, the adversary showed a high degree of persistence and dedication to compromising the target, over the course of a week. Also, they used a different shell, failed, and then attempted to conduct a SQL attack on the server. While this may not be unusual on its own, the short timeline in which it was carried out shows the adversary's skill at adaptation. The multiple attempts to gain access also highlight the likely importance of the project and/or reveal that the adversary was under specific time constraints.

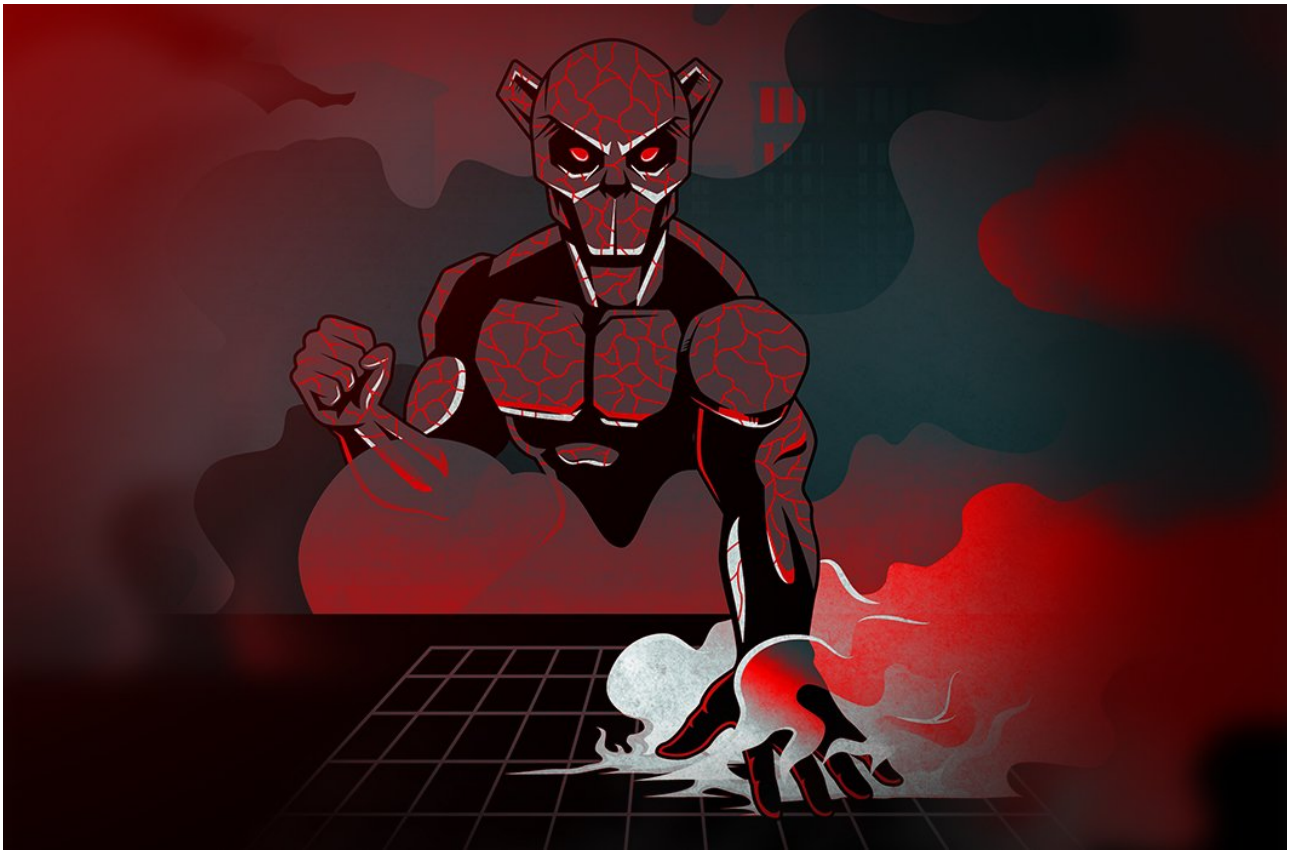
The final step of conducting a DDoS attack on the think tank's site was unusual when viewed in the context of an espionage operation. The purpose of the attack is unclear, as it did not appear to benefit the espionage objective. Given the timing and subsequent failures at gaining access to what is presumably a high-value target, this DDoS attack could have been done out of frustration.

This is believed to be the first time CrowdStrike has observed a China-based adversary engaging in a disruptive attack against what was previously (and likely, still is) an espionage target as a follow-on to normal espionage activities.

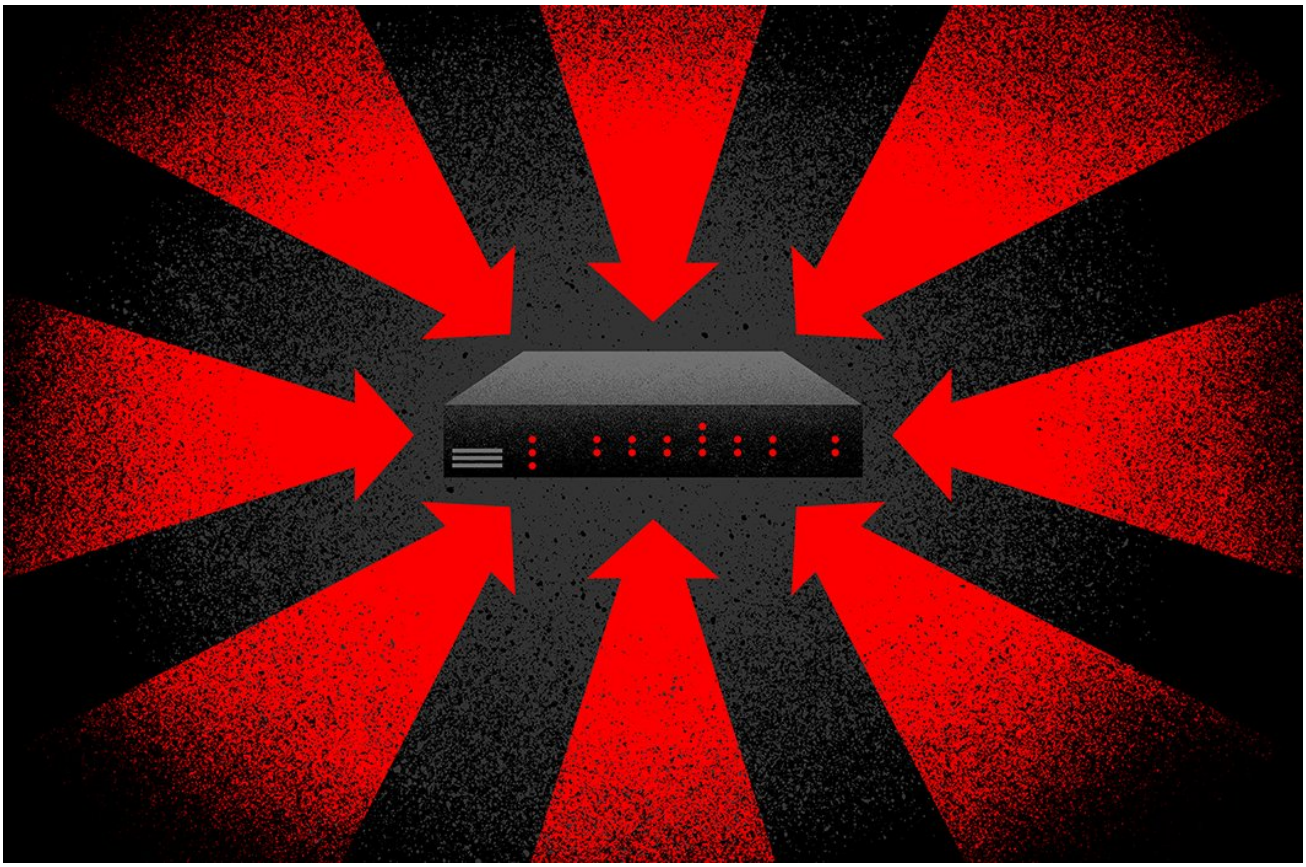
Outlook

China's renewed interest in targeting Western think tanks and NGOs is hardly surprising given President XI Jinping's call to improve China's think tanks, a response to myriad new strategic problems facing China as it seeks greater influence as a global player. The targeting of these six organizations may signal a more widespread and active campaign to collect sensitive material and enable future operations. Individuals and enterprises that maintain relationships with Western think tanks and NGOs are advised to take appropriate precautions — system security review, additional user awareness training, and ensuring comprehensive endpoint visibility are critical to identifying and preventing threats from advanced adversaries. The increase in operational tempo by Chinese associated intrusion actors that was observed during 2017 is covered in more detail in the upcoming CrowdStrike Global Threat Report 2017.

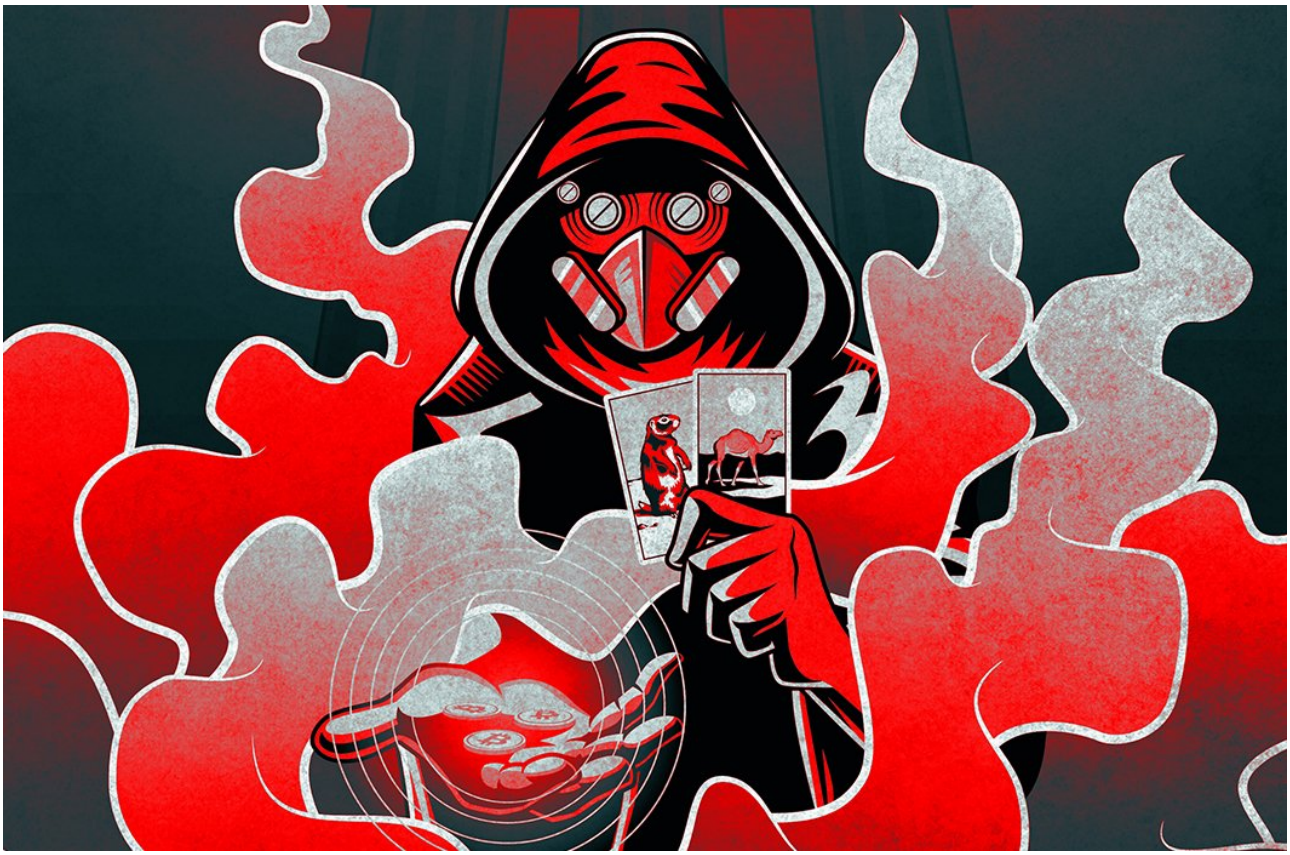
For more information on CrowdStrike's threat intelligence services, please visit https://www.crowdstrike.com/endpoint-security-products/falcon-x-threat-intelligence/.



Who is EMBER BEAR?



A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router



PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell