Occupy Central: The Umbrella Revolution and Chinese Intelligence

crowdstrike.com/blog/occupy-central-the-umbrella-revolution-and-chinese-intelligence/

October 2, 2014

October 2, 2014

Adam Kozy Research & Threat Intel

First observed in late 2013, the People's Republic of China (PRC) has steadily increased the use of its intelligence services and cyber operations in Hong Kong as part of a response to the growing protests supporting universal suffrage and democracy headed by Occupy Central (和平占中). The Hong Kong protests fueled fears in the Chinese Communist Party (CCP), which perceives them as a threat to its one-party rule in mainland China. This perceived threat likely prompted the flurry of malicious cyber activity taken against various organizations and citizens operating in support of the protests within Hong Kong.

Make no mistake, the CCP, which made public protests illegal following the brutal Tiananmen Square crackdown in 1989, likely sees the situation in Hong Kong as one of the biggest threats it has faced in recent history, as the protests have the potential to inspire mainland Chinese to take similar action against perceived injustices. The observed multi-

pronged approach Beijing has taken to collect information on the protests, disrupt communications between protestors, and block media coverage of the events in the PRC demonstrates how seriously the CCP regards the unfolding events.

The methods used have been a smattering of cyber tactics and HUMINT (on the ground) methods to collect information about leaders of the Occupy Central Movement, locations of its supporters, and to gain an overall picture of Hong Kong citizens' perception of the protests. This began with strategic web compromises of key websites associated with Occupy Central in late 2013, followed by extensive HUMINT activities carried out by suspected Ministry of State Security (MSS) officers likely designed to elicit information from influential figures in Hong Kong and pressure them to support Beijing's stance in exchange for gifts.

Following a PRC white paper stating that candidates for Hong Kong's Chief Executive "must love China", the Occupy Central movement organized an online referendum, which drew over 780,000 votes. At the height of voting, a massive DDoS attack attempted to take down the voting platform, Popvote, via a variety increasingly persistent Layer 3 and 4 network attacks, as well as more advanced Layer 7 attacks. Although the attack traffic came from everywhere BUT China, the recent appearance of a new Chinese DDoS tool and observed China-based targeted intrusion activity connected to the attacks indicates some sloppy cover-ups from what was likely PRC involvement. CrowdStrike Intelligence customers have access to additional reporting on this subject.

More recently, in late September, Android mobile malware disguised as an Occupy Central support application was actually designed to target Hong Kong users associated with the movement. The malware collected call information and texts of the users, and also mapped their GPS locations. One of the Command-and-Control (C2) servers for this malware connected back to a user with ties to legacy Chinese hackers and the current Chinese hacking underground. Another malware variant targeting users of the iOS mobile platform was recently discovered that is believed to serve a similar purpose.

In addition, a decoy document using Occupy Central as a lure was discovered around the same time and shares a callback with previously observed SABRE PANDA activity, which is believed to have a mandate of targeting dissidents and perceived threats to CCP rule. Additional targeted intrusion activity likely targeting organizations related to this pro-democracy movement have also been identified. CrowdStrike Intelligence customers have access to additional reporting on this subject.

Despite the attempted sabotage and information collection operations, Occupy Central has continued to gain momentum over the past week, receiving an unexpected boon in the form of student protests beginning Friday, 26 September 2014, which lasted through the weekend. Occupy Central had originally stated its mass protests would coincide with the

public holiday China National Day, beginning on Wednesday, 1 October, however, student-led protests and the storming of Hong Kong government buildings prompted the group to take action earlier than anticipated.

Many of the protestors are aware of the surveillance activities taking place and have resorted to peer-to-peer messaging services such as Firechat, which uses either Bluetooth or Apple's Multipeer Connectivity feature to exchange messages to other users within 200 feet. Although the messages are public and not encrypted, they allow protestors to communicate even without Internet connectivity. It is almost certain that MSS officers are in place to intercept some of these messages, although the sheer numbers associated with the protests likely make full coverage difficult.

The conglomeration of student and Occupy Central protestors, currently christened the Umbrella Revolution for their use of umbrellas to block tear gas canisters fired by Hong Kong Police, demanded the resignation of current Chief Executive LEUNG Chun-ying (梁振英), which LEUNG declined to do. In response, the protestors have occupied more government buildings.

For now, LEUNG and the Hong Kong government appear content with playing the waiting game in order to outlast the protestors (weeks if necessary), as they see defying Beijing's wishes as an infeasible option. However, increasingly assertive activity by the Umbrella Revolution will likely push this timeline up significantly. Keeping Central shut down for weeks would be detrimental to Hong Kong's economy and much of the world's financial health given Hong Kong's status as the world's third most important financial center. Considering that the protestors have been extremely peaceful thus far, LEUNG has refrained from mobilizing more riot police, realizing that the first use of riot police and tear gas against protestors only spurred more Hong Kongers to join the Umbrella Revolution.

For its part, Beijing has been fairly reserved in its overt response, with the mainland media and CCP mouthpieces sticking to the rhetoric that the protests are illegal and organized by "radicals". But Beijing is in a precarious position – on the one hand, it absolutely cannot acquiesce to the protestors demands and give up its control over the current electoral process in Hong Kong, but the CCP is also feeling the pressure as it desperately tries to keep news of the democratic protests away from curious mainlanders via its censorship juggernaut, relying instead on the Hong Kong government to handle the situation for the moment. Although it is projecting an image of calm, measured responses to the unfolding events, the balancing act may not be sustainable for much longer.

Support for the Umbrella Revolution has spread to Taiwan and Macau, confirming the CCP's fears that the movement could carry enough potency to eventually infiltrate the mainland. In addition to massive amounts of censorship, the Chinese Ministry of Public Security (MPS) has already rounded up the mainland political activists supporting the movement.

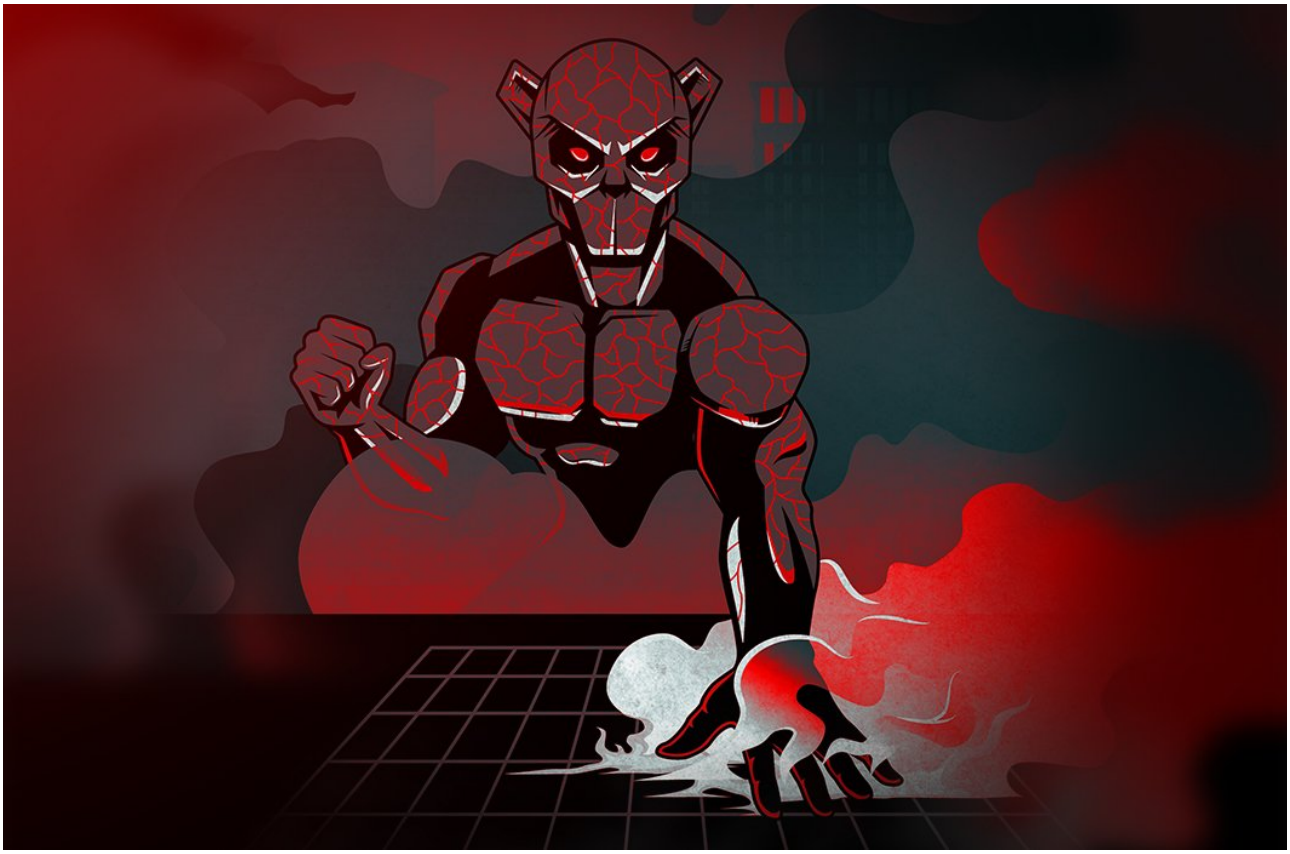
The movements of the PRC's intelligence services and cyber forces show that the CCP is anything but calm about the protests, and they are engaged in ongoing operations to discredit the movement and collect information about its supporters. Sending the Chinese People's Liberation Army (PLA) soldiers into Central is a last-resort option for Beijing, as the international backlash would be swift without proper predication.

The collection efforts underway may be staging for forthcoming disinformation campaigns designed to show the leaders of the Umbrella Revolution as radicals capable of violence. Given that the protestors have been remarkably peaceful, the goal may be to initiate a catalyst of sort to spark violence. This would become predication for further PRC involvement, echoing the ongoing situation in Ukraine, where Russian "peacekeeping operations" have become a frequent mantra. Already there are almost laughable attempts by both the PRC and Russia to credit the protests as being elaborate operations carried out by American and British intelligence services.

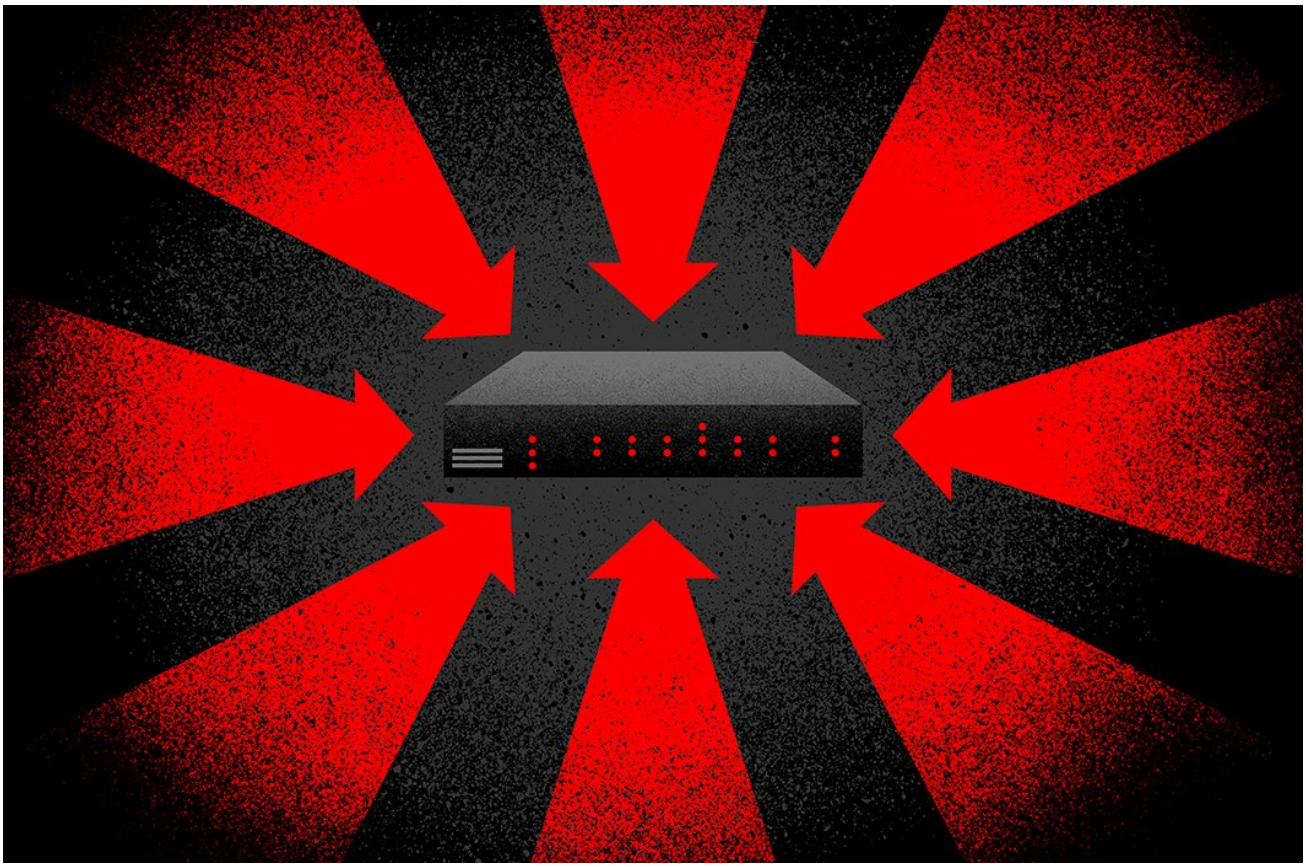
As the Umbrella Revolution continues, expect more cyber activity from China-based adversaries and their proxies to occur in the background until the standoff reaches a climax, after which there may be entirely different sets of activity with more damaging consequences.

CrowdStrike Intelligence provides customers with actionable threat intelligence about adversaries, including but not limited to those mentioned in this post. For further information and technical indicators on observed activity surrounding the protests in Hong Kong, please contact intelligence@crowdstrike.com and inquire about Falcon Intelligence, our Cyber Threat Intelligence subscription.

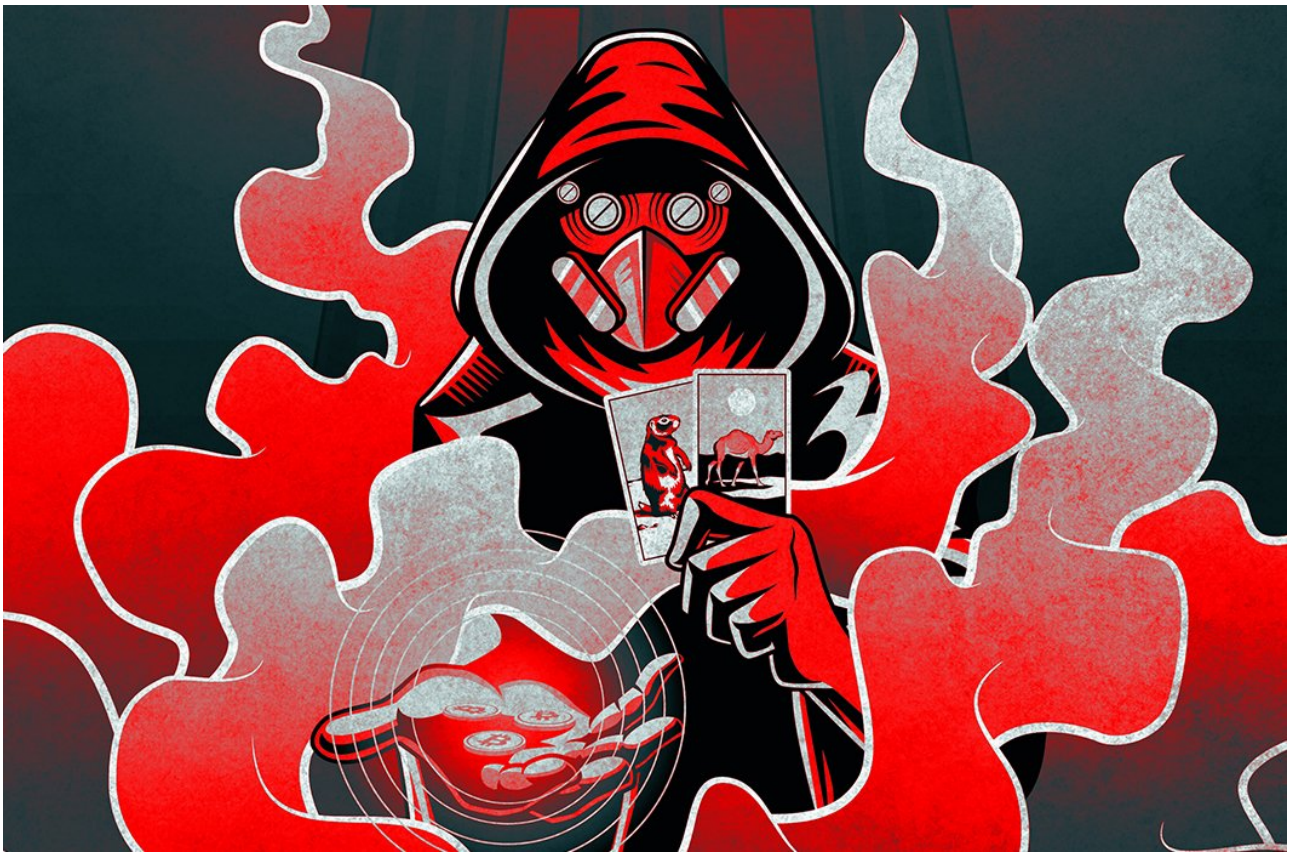
Related Content



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