Rhetoric Foreshadows Cyber Activity in the South China Sea

crowdstrike.com/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/

June 1, 2015

June 1, 2015

Adam Kozy Research & Threat Intel

As the increasingly aggressive rhetoric surrounding the conflict in the South China Sea (SCS) continues to dominate both Western and Chinese media headlines, multiple outlets and normally rational China-watchers seem to be focused on predicting the next policy miscalculation on either side. The outlooks posited appear to be getting progressively hawkish as both the People's Republic of China (PRC) and U.S. officials refuse to back down from their confrontational stances, which could be a long stand-off as the first Hague tribunal deciding if China's nine-dash line is consistent with the UN Convention on the Law of the Sea (UNCLOS) does not start until July 2015. But among the slew of U.S.-Sino relations' experts dissecting every policy move, one modern yardstick of escalation seems to be mysteriously absent from the conversation: cyber reconnaissance.

How quickly everyone seems to forget – just weeks ago, cyber security was one of the foremost topics in the media. Now the attention has turned to naval strategy and political posturing, ignoring the fact that, for developed world powers, military doctrine is now inextricably linked with cyber capabilities. The world has previously witnessed the role joint cyber/kinetic warfare played in the 2008 Russo-Georgian conflict and more recently in the Russian-Ukrainian conflict, where cyber served as a means for kinetic disruption,

dissemination of disinformation, and political subversion. It would be a mistake to think that the PRC was not taking notes on the lessons learned through these modern conflicts. According to sensitive source reporting, there have been several People's Liberation Army (PLA) papers discussing such tactics and their effectiveness.

Indeed the PRC has already recently used cyber reconnaissance as a precursor to other diplomatically sensitive strategic moves in the SCS. This includes the mid-2014 GOBLIN PANDA activity against the Vietnamese government during the HYSY-981 oilrig standoff. Around the same time, the PRC's efforts to quietly quell the Umbrella Revolution in Hong Kong bore fingerprints and tradecraft attributed to multiple PANDA groups, suggesting Beijing called several known groups off of their normal targeting to address an issue of importance to the PRC government. Why should the present conflict be any different?

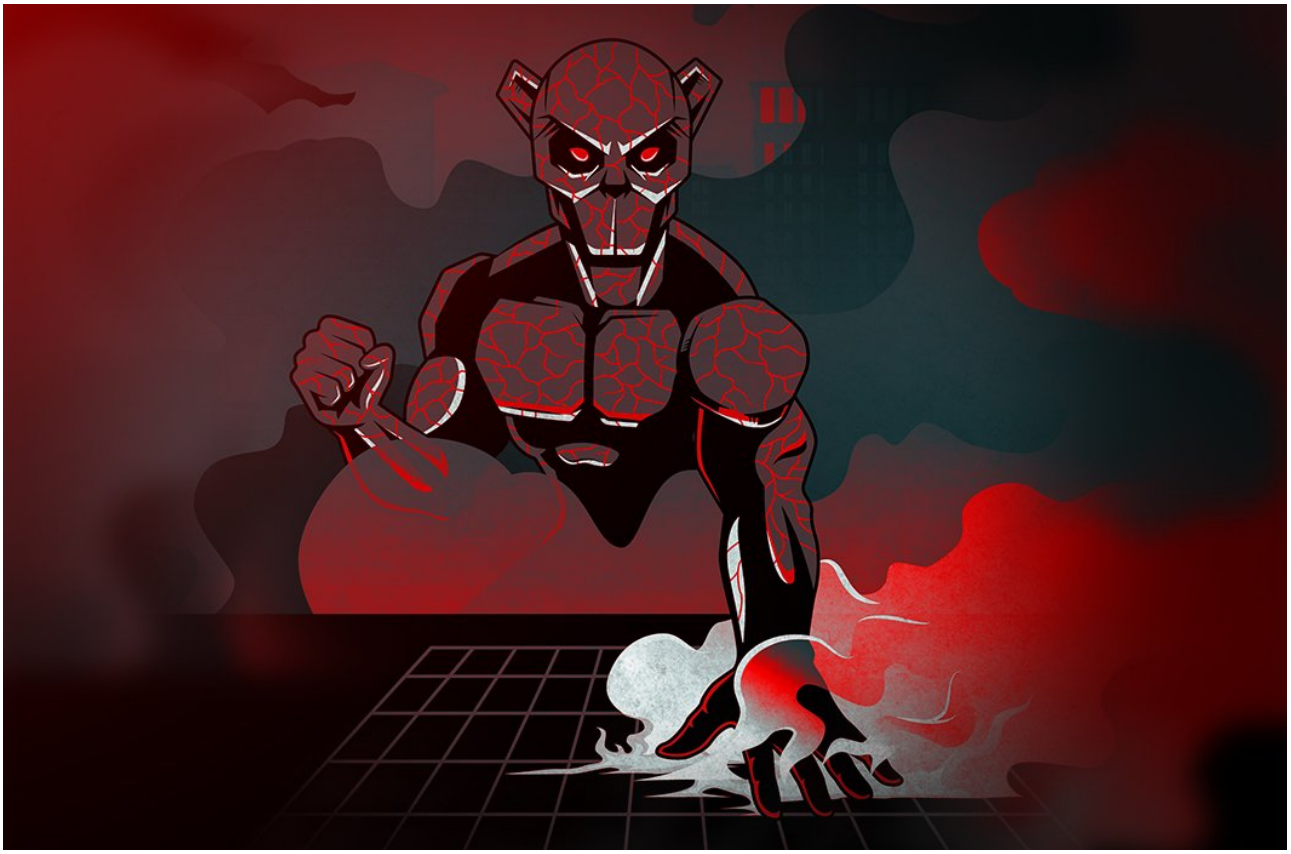
PRC-based actors such as PIRATE PANDA and LOTUS PANDA have already been observed increasing their SCS-related targeting over the past 4-6 weeks, mostly against the Philippine military. Reconnaissance and spear-phishing activity targeting U.S. and Australian military/defense forces would signify a broader, more aggressive change to China's strategy for enforcing its recent controversial SCS Air Defense Identification Zone (ADIZ) claims. No activity of this type has yet been observed, though given the fluidity of events over the past week, this is likely to change in the near future. Though China-based actors have typically not demonstrated stealthy tradecraft against Western targets, the public disclosures over the past couple years and the stakes of the present conflict may inspire slightly more awareness when targeting more advanced Western military systems.

Out of the adversaries recently observed as active in SCS-related targeting, GOBLIN PANDA's absence is particularly noteworthy given that Vietnam is the other major claimant to the Spratly Islands, where the controversial island construction is taking place. As PIRATE and LOTUS PANDA have not been overly discreet about their recent targeting, it stands to reason that GOBLIN PANDA would not have improved its capabilities enough in such a short time to be completely invisible, which suggests that GOBLIN PANDA may have either changed tactics or has some other immediate focus at present time.

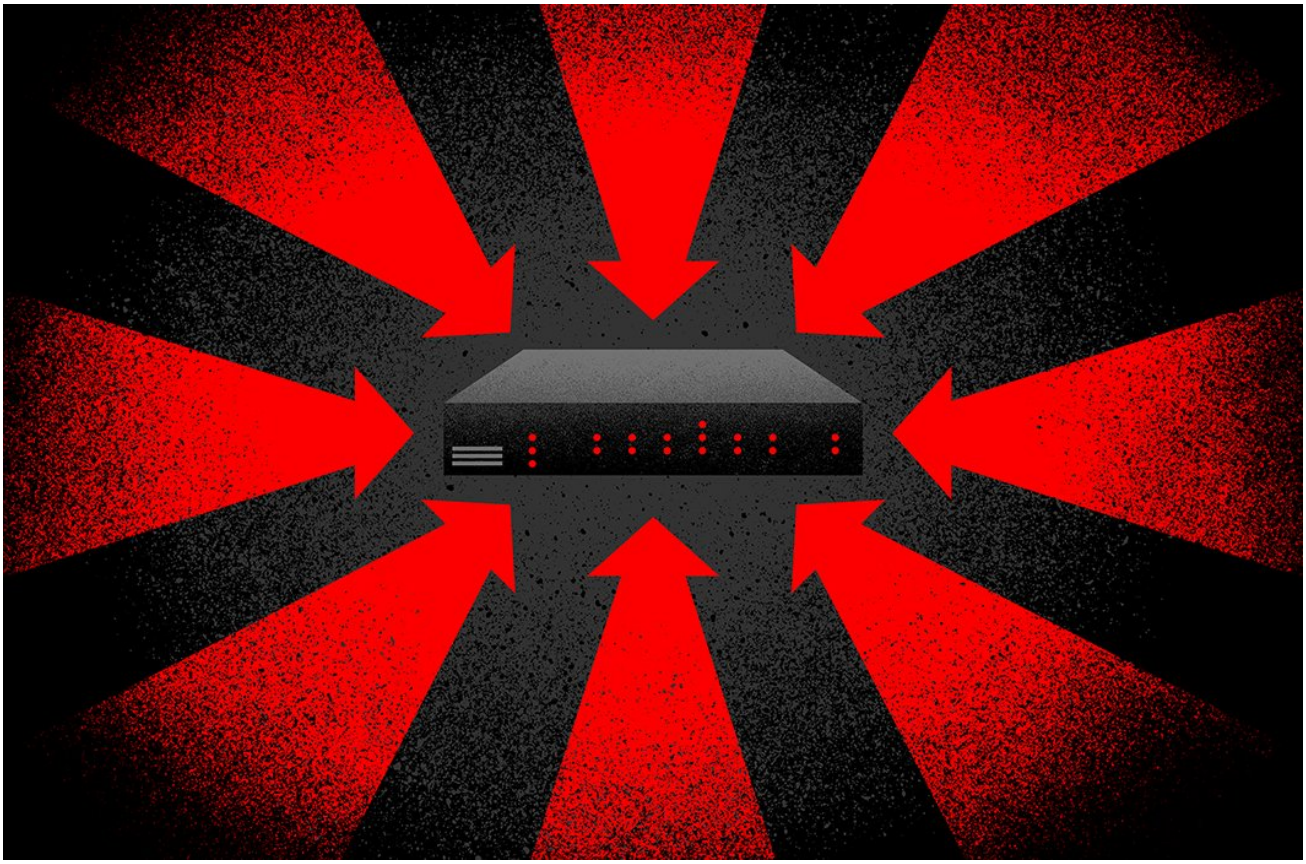
Another measure of conflict escalation via cyber means would include increased activity from China's patriotic hacker corps. These groups have typically made up the third, less sophisticated, prong of PRC cyber forces, along with specialized military units and civilian agencies like the Ministry of State Security (MSS) and Ministry of Public Security (MPS). As part of PRC militarized posturing, domestic services helping to control and regulate China's nationalistic hackers, such as the MPS, generally relax their monitoring during times of conflict. This was first observed during the brief U.S.-China hacker war after the Hainan Island incident in 2001, when China's patriotic hacker movement was at its peak. It occurred again in 2014 when the GOBLIN PANDA activity was actually preceded by attacks and defacements of Vietnamese government websites by the nationalistic 1937cn Team prior to being reigned in after their involvement in the incident was made public.

While it is always possible a severe miscalculation or military incident can cause the current situation to erupt into violent conflict, both the U.S. and China have stated that they seek a peaceful way to resolve the dispute. Both countries have measured responses for avoiding military conflict and will likely utilize them fully. Watching for changes to the cyber landscape in the SCS still presents one of the best indications of intent, as it has become a reliable precursor to armed conflict, which now depends on gaining complete information advantage over the adversary. Stay vigilant, friends.

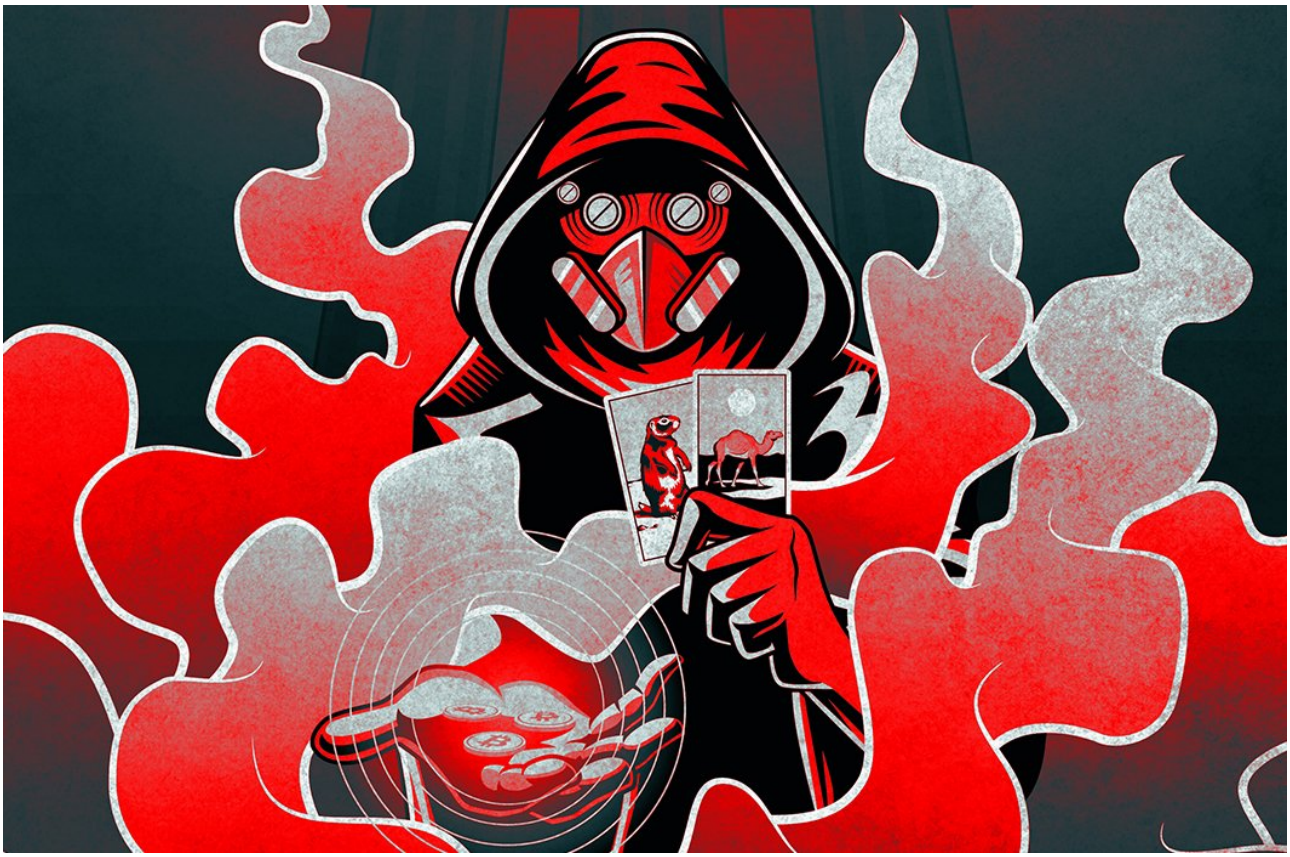
Related Content



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