Elite cyber crime group strikes back after attack by rival APT gang

arstechnica.com/security/2015/04/elite-cyber-crime-group-strikes-back-after-attack-by-rival-apt-gang/

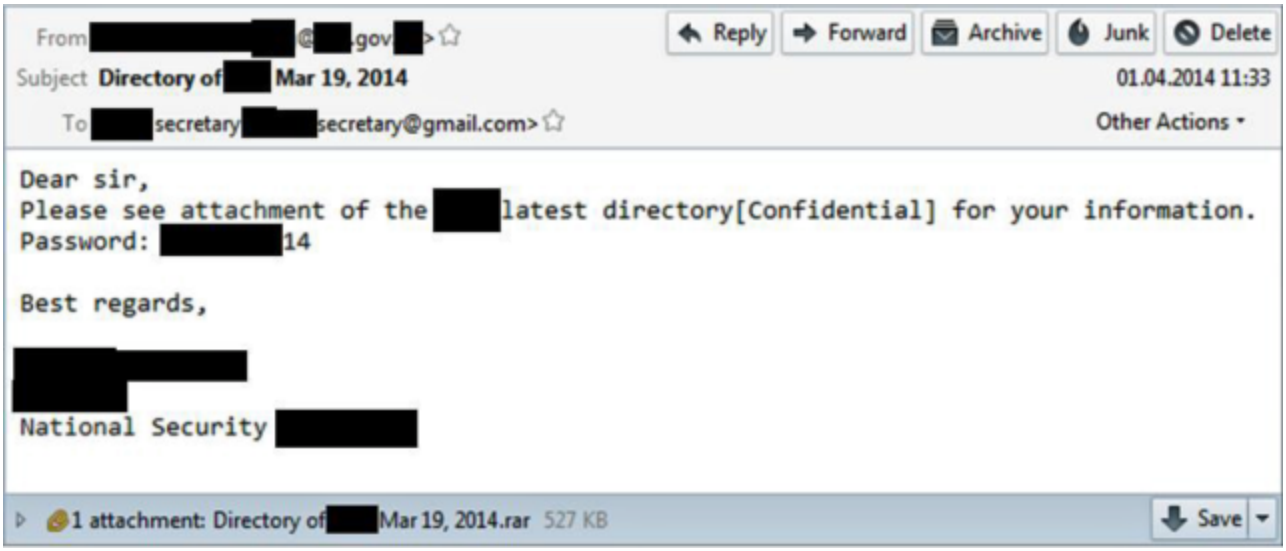
Dan Goodin

Enlarge

DeviantArt100ManoWar / MAD Magazine

One day last year, an obscure cyber espionage group sent a spear phishing e-mail. It carried the usual trappings of a spear phish sent by advanced persistent threat actors. It was short, appeared to come from an address the target knew, and attached a payload that when clicked surreptitiously installed potent malware on the reader's computer.

But there was something highly unusual about this spear phish, one that would throw the once-shadowy Hellsing group into the limelight. According to analysis from antivirus provider Kaspersky Lab, the targeted group in the spear phish wasn't a government agency or embassy as is usually the case. Instead, it was Naikon, one of Asia's largest APT gangs and a rival to Hellsing. Naikon has been active for years and is known for attacks targeting government and military leaders, diplomats, aviation authorities, and police in countries such as the Philippines, Malaysia, Cambodia, and Indonesia.



Enlarge

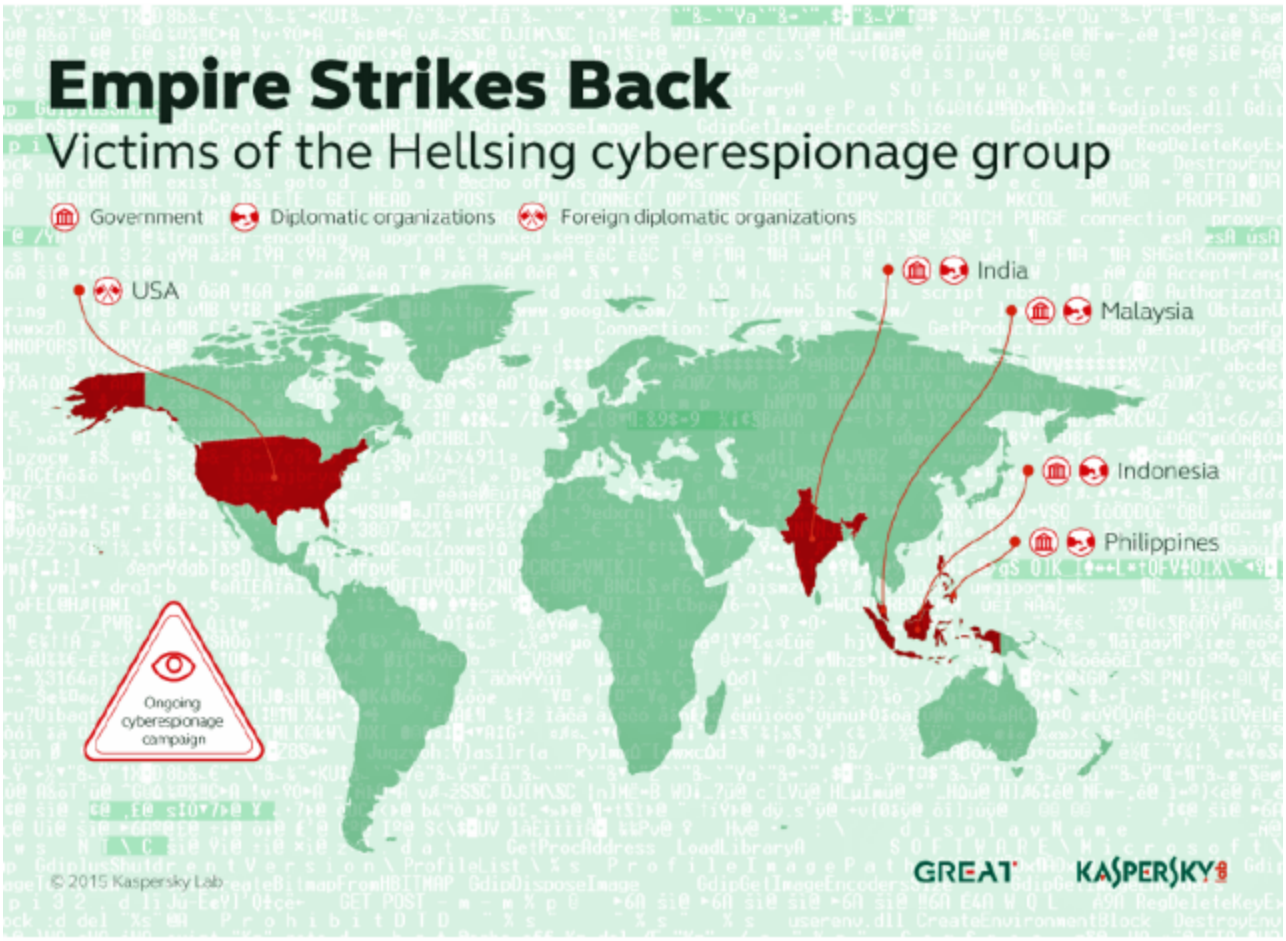
Kaspersky Lab

To be fair to Hellsing, it was Naikon that started the fight. In February, about six weeks prior to the spear phish Hellsing sent, Naikon had blasted out a spear phishing run of its own. One of the many groups that received the Naikon e-mail was Hellsing. Rather than blindly taking the bait, as is the case in so many APT-related spear phishes, Hellsing members took the time to check the legitimacy of the e-mail with the purported sender. When the sender supplied an unsatisfactory response, Hellsing members fired off their own spear phish directed at the Naikon gang. Kaspersky researchers believe the event may mark the emergence of a new trend in cyber criminal activity: APT-on-APT attacks.

"The targeting of the Naikon group by Hellsing, in some sort of a vengeful vampire-hunting-'Empire Strikes Back' style, is fascinating," Costin Raiu, director of global research and analyst team at Kaspersky Lab, said in a press release. "In the past, we've seen APT groups accidentally hitting each other while stealing address books from victims and then mass-mailing everyone on each of these lists. However, considering the targeting and origin of the attack, it seems more likely that this is an example of a deliberate APT-on-APT attack."

Watch Video At: https://youtu.be/R7n6zd4T6Bg

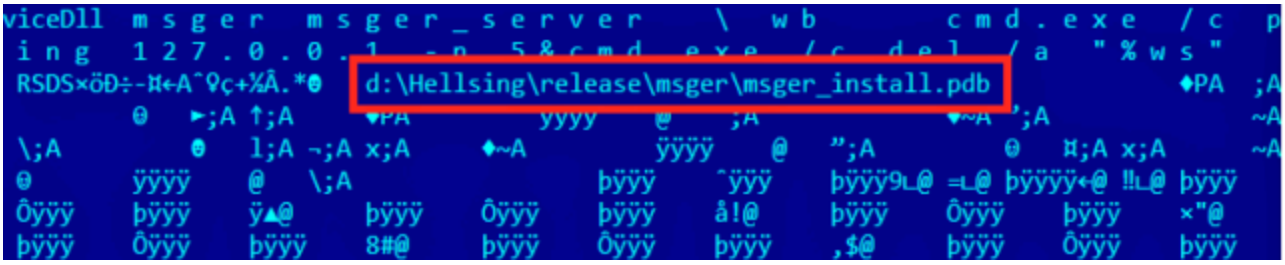
The Empire Strikes Back: welcome to the Wars of Advanced Persistent Threats. Parenthetically, a few weeks after Kaspersky Lab researchers observed Naikon targeting Hellsing came the March 8, 2014 disappearance of Malaysia Airlines Flight 370. Three days later, Naikon launched a campaign that hit most of the countries involved in the search, with booby-trapped e-mails sent to political and military leaders, diplomats, civil aviation authorities, and police. The Naikon gang, it seemed, was eager to learn whatever it could about the behind-the-scenes recovery mission for the missing flight.



Enlarge

Kaspersky Lab

Kaspersky Lab researchers said Hellsing is known to have infected only about 20 organizations, an indication of just how niche and selective the attack group is. Hellsing is also highly selective about the regions it targets, limiting them to the US, Malaysia, the Philippines, Indonesia, and India. The name Hellsing comes from the project title a developer carelessly left in some of the malicious binaries the group uses in its campaigns. It remains unknown if Hellsing succeeded in its attempt to infect Naikon.



Enlarge

Kaspersky Lab

An analysis of the command and control infrastructure shows Hellsing has ties to fellow groups known as PlayfulDragon, Mirage, and Vixen Panda. Server locations also suggest links to the APT group known as Cycldek or Goblin Panda. Kaspersky's blog post lays out a feast of other technical details about the gang.

There's a possibility Hellsing may have remained behind the scenes had they not been caught in the act of striking back at a rival APT gang. This may have been one of the first times an APT-on-APT attack has been witnessed, but it's probably not the last.