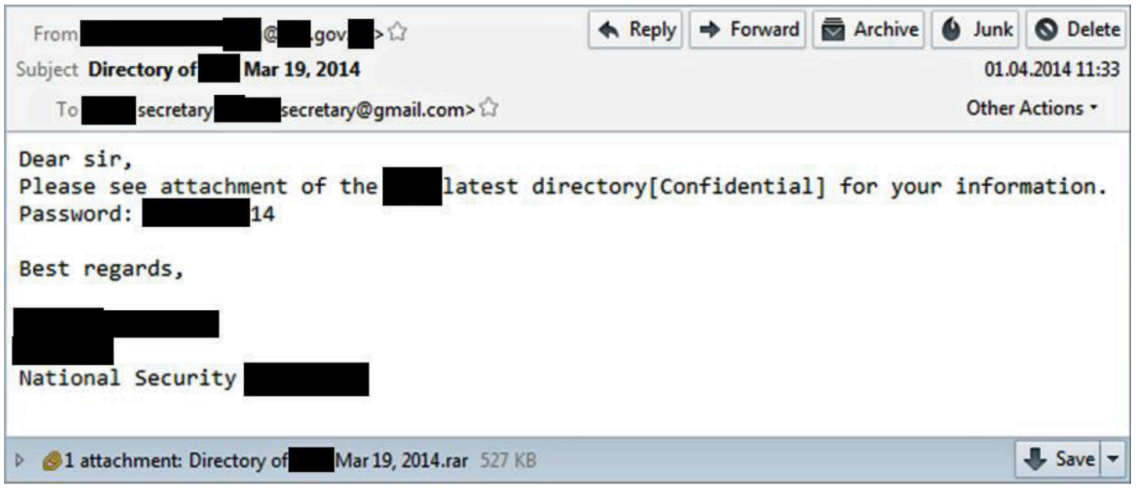
Elite cyber crime group strikes back after attack by rival APT gang

By Dan Goodin

Published: 2015-04-15 · Archived: 2026-04-05 14:21:47 UTC

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.



Credit: Kaspersky Lab

Credit: 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.”
