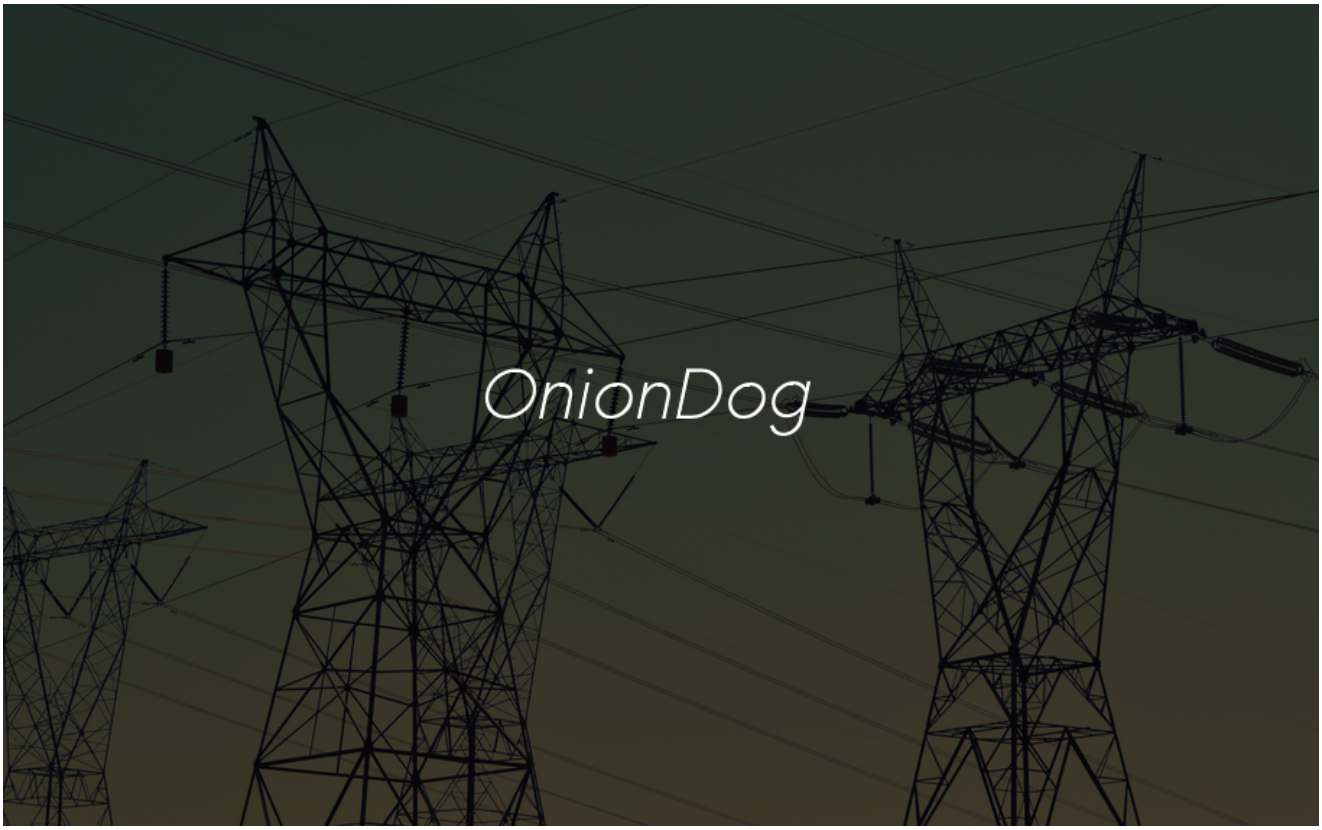
Korean Energy and Transportation Targets Attacked by OnionDog APT

news.softpedia.com/news/korean-energy-and-transportation-targets-attacked-by-oniondog-apt-501534.shtml

Catalin Cimpanu March 9, 2016



Chinese security researchers from cyber-security vendor Qihoo 360 have blown the lid on a cyber-espionage APT named OnionDog that's been targeting Korean-speaking countries since October 2013.

According to their investigation, Onion dog has been mostly active in the summer and used an arsenal of trojans and USB worms.

The trojan, which only lives on average for about 15 days, was used to exfiltrate data from targeted companies and government agencies while the USB worm was developed as a Stuxnet-like threat that can reach targets that aren't connected to the Internet.

OnionDog is mostly active during the summer

Qihoo's Helios Team was the first to come across this threat in October 2013, and the company is saying that the group truly came alive in the summer of 2014, when it hit Korean companies activating in the energy and water supply sectors.

Attacks then continued in the summer of 2015, when Qihoo saw new targets attacked, some of which were against port harbors, VTS (Vessel Traffic Systems), subways, public transportation and other transportation systems. These findings are also **consistent** with what local South Korean authorities have reported in the past months.

OnionDog malware never lived more than a month

Qihoo says that the group used 96 different types of malware, but all of it was programmed to self-delete, with no malware variant living more than 29 days.

Additionally, the researchers discovered 14 different C&C (command and control) servers attached to these campaigns, which in 2015 were moved to the Darknet, operating via the Onion City Tor2web technology.

As for their infection strategy, in the beginning, the OnionDog group used lots of spear-phishing campaigns which contained trojan-laced executables that used the icon of a popular Korean Word processing software called Hangul.

Later on, in 2015, the group switched tactics and started leveraging software vulnerabilities in the Hangul editor to download and install their malware automatically. We presented more **details on this technique** in September, and the same Hangul vulnerability seems to have been used by **the Lazarus group**, the APT suspected to have carried out the infamous Sony hack.

Even if nobody said the Lazarus group was operating from North Korea, all clues pointed toward that conclusion, and all clues point to the same conclusion for OnionDog as well.