Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:41:46 UTC

APT group: OnionDog

Names	OnionDog *(Qihoo 360)*
Country	South Korea
Motivation	Information theft and espionage
First seen	2013
Description	Seems to be a Cyber Drill that is conducted every year rather than an APT, according to findings from TrendMicro. (Qihoo 360) The Helios Team at 360 SkyEye Labs recently revealed that a hacker group named OnionDog has been infiltrating and steal energy, transportation and other infrastructure industries of Korean-language countries through the Internet. According to big data correl activity can be traced back to October, 2013 and in the following two years it was only active between late July and early September. Th attack is 15 days on average and is distinctly organizational and objective-oriented. OnionDog malware is transmitted by taking advantage of the vulnerability of the popular office software Hangul in Korean-language co isolated targets through a USB Worm. In addition, OnionDog also used darkweb ('Onion City') communications tools, with which it can Onion browser, making its real identity hidden in the completely anonymous Tor network.
Observed	Sectors: Energy, Government, Transportation, Utilities. Countries: South Korea.
Tools used	Malware on USB stick.
Information	<https://www.prnewswire.com/news-releases/onion-dog-a-3-year-old-apt-focused-on-the-energy-and-transportation-industries-in-korear exposed-by-360-300232441.html> <https://www.qianxin.com/assets/doc/apt_report/en/OPERATION%20ONIONDOG%20%E2%80%93Disclosing%20Targeted%20Attac <https://blog.trendmicro.com/trendlabs-security-intelligence/oniondog-not-targeted-attack-cyber-drill/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
