Onion Dog, A 3 Year Old APT Focused On the Energy and Transportation Industries in Korean-language Countries Is Exposed by 360

BEIJING, March 8, 2016 /PRNewswire/ -- The Helios Team at 360 SkyEye Labs recently revealed that a hacker group named OnionDog has been infiltrating and stealing information from the energy, transportation and other infrastructure industries of Korean-language countries through the Internet. According to big data correlation analysis, OnionDog's first activity can be traced back to October, 2013 and in the following two years it was only active between late July and early September. The self-set life cycle of a Trojan 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 countries, and it attacked network-isolated targets through a USB Worm. In addition, OnionDog also used darkweb ("Onion City") communications tools, with which it can visit the domain without the Onion browser, making its real identity hidden in the completely anonymous Tor network.

OnionDog APT targets the infrastructure industry.

OnionDog concentrated its efforts on infrastructure industries in Korean-language countries. In 2015 this organization mainly attacked harbors, VTS, subways, public transportation and other transportation systems. In 2014 it attacked many electric power and water resources corporations as well as other energy enterprises.

360's Threat Intelligence Center has found 96 groups of malicious code, 14 C&C domain names and IP related to OnionDog. It first surfaced in October 2013, and then was most active in the summers of the following years. The Trojan set its own "active state" time and the shortest was be three days and maximum twenty nine days, from compilation to the end of activity. The average life cycle is 15 days, which makes it more difficult for the victim enterprises to notice and take actions than those active for longer period of time.

Deadline	*Compilation time*	*Activate state (days)*
Sep 8th, 2015	Aug 27th, 2015	12
Aug 8th, 2015	Aug 5th, 2015	3
Aug 8th, 2015	Aug 3th, 2015	5
Aug 8th, 2015	July 23th, 2015	16
Aug 8th, 2015	July 10th, 2015	29
July 13th, 2014	July 10th, 2015	3
Aug 9th, 2014	July 18th, 2014	22
Aug 9th, 2014	July 15th, 2014	25
July 13th, 2014	July 13th, 2014	18
Oct 25, 2013	Oct 10th, 2013	15

The life cycle of Trojan malware

OnionDog's attacks are mainly carried out in the form of spear phishing emails. The early Trojan used icons and file numbers to create a fake HWP file (Hangul's file format). Later on, the Trojan used a vulnerability in an upgraded version of Hangul, which imbeds malicious code in a real HWP file. Once the file is opened, the vulnerability will be triggered to download and activate the Trojan.

Since most infrastructure industries, such as the energy industry, generally adopt intranet isolation measures, OnionDog uses the USB disk drive ferry to break the false sense of security of physical isolation. In the classic APT case of the Stuxnet virus, which broke into an Iranian nuclear power plant, the virus used an employee's USB disk to circumvent network isolation. OnionDog also used this channel and generated USB worms to infiltrate the target internal network.

"OCD-type" intensive organization

In the Malicious Code activities of OnionDog, there are strict regulations:

First, the Malicious Code has strict naming rules starting from the path of created PDB (symbol file). For example, the path for USB worm is APT-USB, and the path for spear mail file is APT-WebServer;

When the OnionDog Trojan is successfully released, it will communicate to a C&C (Trojan server), download other malware and save them in the %temp% folder and use "XXX_YYY.jpg" uniformly as the file name. These names have their special meaning and usually point to the target.

All signs show that OnionDog has strict organization and arrangement across its attack time, target, vulnerability exploration and utilization, and malicious code. At the same time, it is very cautious about covering up its tracks.

In 2014, OnionDog used many fixed IPs in South Korea as its C&C sites. Of course, this does not mean that the attacker is located in South Korea. These IPs could be used as puppets and jumping boards. By 2015, OnionDog website communications were upgraded to Onion City across the board. This is so far a relatively more advanced and covert method of network communication among APT hacker attacks.

Onion City means that the deep web searching engine uses Tor2web agent technology to visit the anonymous Tor network deeply without using the Onion Brower specifically. And OnionDog uses the Onion City to hide the Trojan-controlling server in the Tor network.

In recent years, APT attacks on infrastructure facilities and large-scale enterprises have frequently emerged. Some that attack an industrial control system, such as Stuxnet, Black Energy and so on, can have devastating results. Some attacks are for the purpose of stealing information, such as the Lazarus hacker organization jointly revealed by Kaspersky, AlienVault lab and Novetta, and OnionDog which was recently exposed by the 360 Helios team. These secret cybercrimes can cause similarly serious losses as well.

In view of OnionDog's pattern of activity, we are likely to observe a new round of attacks this summer. The relevant threat intelligence and technical analysis report will be updated by 360's Intelligence Center (https://ti.360.com).

About Helios Team

Helios Team is a senior threat research team at Qihoo 360 that is engaged in detecting and tracing APT attacks, internet security incident response, hacker industrial chain exploration and study. The team was established in December 2014. Within a year, it integrated the enormous security data at Qihoo 360 and realized the rapid correlation traceability of threat intelligence, and for the first time found and traced 10 APT organizations and hacker industrial chains. It broadened its horizon to the study of the hacker industry, filled the void of APT study domestically and has offered security threat evaluation and solutions output for many enterprises and government agencies.

SOURCE 360 SkyEye Labs

See more news releases in High Tech Security | Internet Technology | Computer Electronics | Computer Software | Surveys, Polls and Research

Custom Packages

Browse our custom packages or build your own to meet your unique communications needs.

Start today.

PR Newswire Membership

Fill out a PR Newswire membership form or contact us at (888) 776-0942.

Learn about PR Newswire services

Request more information about PR Newswire products and services or call us at (888) 776-0942.