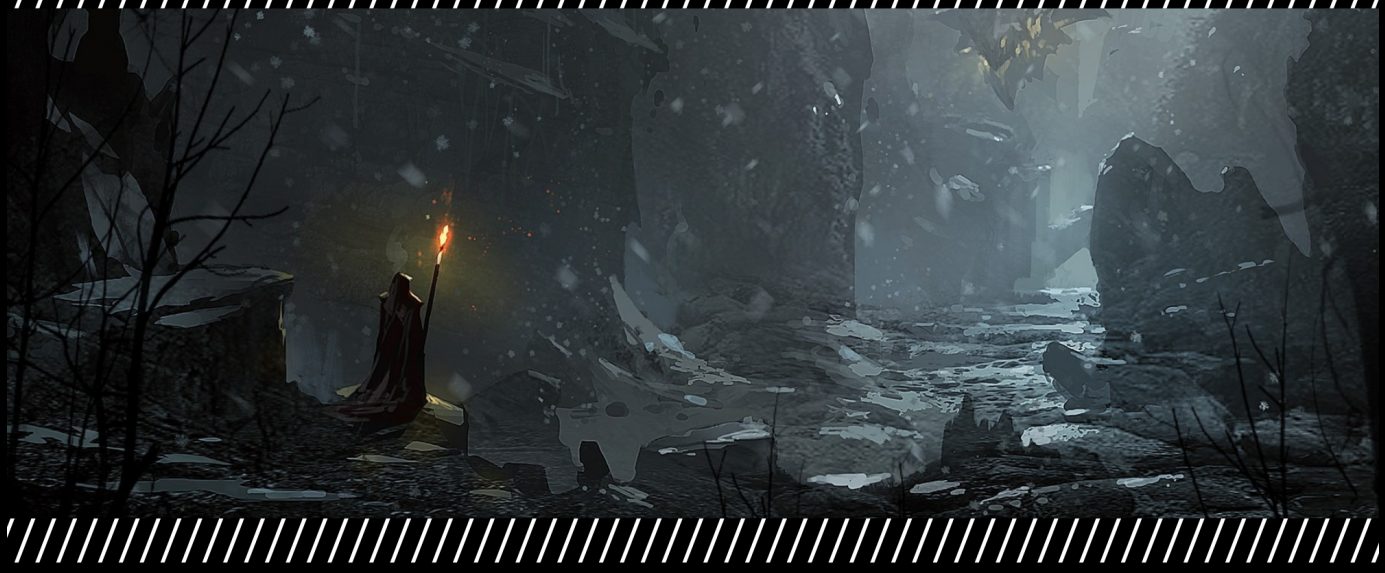
ONION DOG

AXIAL



ONION DOG

SOUTH KOREA

ENERGY, GOVERNMENT, TRANSPORTATION, UTILITIES

MALWARE ON USB STICK

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON ONION DOG ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

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.

II. TARGETS

Sectors: Energy, Government, Transportation, Utilities.

III.TOOLS USED

Malware on USB stick

IV. TECHNIQUE

OnionDog used various techniques to entice victims to open the malicious attachment. The attachments targeted a range of government agencies and utilities, such as power, water, ports, transit, and rail to lure its victims. The malware installs a back door to the compromised system, collects and forwards information about the compromised systems to the C&C server, as well as infecting any device attached to the USB drive.

AX1AL

VI. IOCS

1. dbb0878701b8512daa057c93d9653f954dde24a25306dcee014adf7ffff0bdb4
2. f8c71f34a6cfdc9e3c4a0061d5e395ffe11d9d9e77abe1a5d4b6f335d08da130
3. 7564990506f59660c1a434ce1526b2aea35a51f97b8a490353eece18ec10b910
4. 8b91cfd40529b5667bbdab970d8dba05fca0952fffba8ccbb1ad9549d204ba85
5. 1ffa34f88855991bdc9a153e01c9e18074ba52a773f4da390c4b798df6e6dc4e
6. 1e926d83c25320bcc1f9497898deac05dff096b22789f1ac1f63c46d2c1c16a7

C&C

1. korea[.]kr[.]ncsc[.]go[.]kr
2. cyber[.]ncsc[.]go[.]kr
3. drill12[.]ncsc[.]go[.]kr
4. dril113[.]ncsc[.]go[.]kr
5. drill12[.]ncsc[.]go[.]kr

VII. REFERENCES

1. https://www.prnewswire.com/news-releases/onion-dog-a-3-year-old-apt-focused-on-the-energy-and-transportation-industries-in-korean-language-countries-is-exposed-by-360-300232441.html
2. https://www.qianxin.com/assets/doc/apt_report/en/OPERATION%20ONIONDOG%20%E2%80%93Disclosing%20Targeted%20Attacks%20on%20Government.pdf
3. https://blog.trendmicro.com/trendlabs-security-intelligence/oniondog-not-targeted-attack-cyber-drill/
4. https://cybersecurity.att.com/blogs/security-essentials/oniondog-a-an-example-of-a-regional-targeted-attack
5. https://www.trendmicro.com/en_us/research/17/h/oniondog-not-targeted-attack-cyber-drill.html

AXIAL