
APT-22
AXIAL

A SURVEY ON SUCKFLY: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

APT 22 also known as Bronze Olive and Suckfly is a threat group out of china with key objectives of Information Theft and Espionage. Suckfly's interest was in targeting high-profile targets, including government and commercial organizations. These attacks occurred in several different countries, but the primary targets were individuals and organizations primarily located in India. They had stolen certificates from a South Korean mobile operator to carry out their intrusions.

II. TARGET SECTORS

Indian Government and Commercial entities in E-commerce, Entertainment, Financial, Government, Healthcare, Media, Shipping, Software development, and Video game development.

III. ENGAGEMENTS

- In 2014, multiple global targets across industries were attacked of which many organizations were of Indian Origin. Suckfly targeted one of India's largest e-commerce companies, a major Indian shipping company, one of India's largest financial organizations, and an IT firm that provides support for India's largest stock exchange.
- In late 2015, Symantec identified suspicious activity involving a hacking tool used in a malicious manner. They had discovered Suckfly conducting targeted attacks using multiple stolen certificates, as well as tools and custom malware. The group had obtained the certificates through pre-attack operations before commencing targeted attacks against a number of government and commercial organizations spread across multiple continents over a two-year period.

AX1AL

IV. METHODS USED

Suckfly used the Nidiran backdoor along with a number of other tools to infect the victim. The tools and malware used were also signed with stolen digital certificates. Data was extracted through the same backdoor.

V. IOC

C&C

1. usv0503.iqservs-jp.com
2. aux.robertstockdill.com
3. fli.fedora-dns-update.com
4. bss.pvtcdn.com
5. ssl.microsoft-security-center.com
6. ssl.2upgrades.com
7. 133.242.134.121
8. fli.fedora-dns-update.com

MD5

1. 05edd53508c55b9dd64129e944662c0d
2. 1cf5ce3e3ea310b0f7ce72a94659ff54
3. 352eede25c74775e6102a095fb49da8c
4. 3b595d3e63537da654de29dd01793059
5. 4709395fb143c212891138b98460e958
6. 50f4464d0fc20d1932a12484a1db4342
7. 96c317b0b1b14aadfb5a20a03771f85f
8. ba7b1392b799c8761349e7728c2656dd
9. de5057e579be9e3c53e50f97a9b1832b
10. e7d92039ffc2f07496fe7657d982c80f
11. e864f32151d6afd0a3491f432c2bb7a2

VI. Attributions

- The use of their custom malware known as Backdoor.Nidiran.
- The Use of stolen legitimate certificates to sign its malware.

VII. References

- https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=62e325ae-f551-4855-b9cf-28a7d52d1534&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
- https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7a60af1f-7786-446c-976b-7c71a16e9d3b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
- https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf