BLACK TECH

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. ABOUT

BlackTech is a cyber espionage group operating against targets in East Asia, particularly Taiwan, and occasionally, Japan and Hong Kong. Based on the mutexes and domain names of some of their C&C servers, BlackTech's campaigns are likely designed to steal their target's technology. They also goes by names Circuit Panda (CrowdStrike), Radio Panda (CrowdStrike), Palmerworm (Symantec), T-APT-03 (Tencent).

II. TARGET SECTORS

Black Tech Targeted Various Industries and Organizations Including: Construction, Financial, Government, Healthcare, Media, Technology.The media, electronics, and finance companies were all based in Taiwan, the engineering company was based in Japan, and the construction company in China. It is evident Palmerworm has a strong interest in companies in this region of East Asia.

Palmerworm activity was first spotted in this campaign in August 2019, when activity was seen on the network of a Taiwanese media company and a construction company in China. The group remained active on the network of the media company for a year, with activity on some machines there seen as recently as August 2020.

III. ENGAGEMENTS

- 2012 : Operation "PLEAD"PLEAD is an information theft campaign with a penchant for confidential documents. Active since 2012, it has so far targeted Taiwanese government agencies and private organizations.
- In 2017 security vendor Trend Micro tied three separate and long-running cyber espionage campaigns to Palmerworm/Blacktech. One of them was a data theft campaign focused on the theft of confidential data from private-sector and government organizations in Taiwan
- In 2018 ESET researchers have discovered a new malware campaign misusing stolen digital certificates.We spotted this malware campaign when our systems marked several files as suspicious. Interestingly, the flagged files were digitally signed using a valid D-Link Corporation code-signing certificate. The exact same certificate had been used to sign non-malicious D-Link software; therefore, the certificate was likely stolen.
- At the end of April 2019, ESET researchers utilizing ESET telemetry observed multiple attempts to deploy Plead malware in an unusual way. Specifically, the Plead backdoor was created and executed by a legitimate process named AsusWSPanel.exe. This process belongs to the Windows client for a cloud storage service called ASUS WebStorage.

AX1AL

IV. METHODS USED

- BlackTech has exploited a buffer overflow vulnerability in Microsoft Internet Information Services (IIS) 6.0, CVE-2017-7269, in order to establish a new HTTP or command and control (C2) server.
- BlackTech has exploited multiple vulnerabilities for execution, including Microsoft Office vulnerabilities CVE-2012-0158, CVE-2014-6352, CVE-2017-0199, and Adobe Flash CVE-2015-5119.
- BlackTech has used right-to-left-override to obfuscate the filenames of malicious e-mail attachments.
- BlackTech has used spearphishing e-mails with links to cloud services to deliver malware.
- BlackTech has used spearphishing e-mails with malicious documents to deliver malware.

V. IOC

C&C

1. asiainfo.hpcloudnews.com
2. loop.microsoftmse.com

IP Addresses

1. 103.40.112.228
2. 172.104.92.110
3. 45.76.218.116
4. 45.77.181.203

SHA-256

1. 28ca0c218e14041b9f32a0b9a17d6ee5804e4ff52e9ef228a1f0f8b00ba24c11
2. 3277e3f370319f667170fc7333fc5e081a0a87cb85b928219b3b3caf7f1e549c
3. 35bd3c96abbf9e4da9f7a4433d72f90bfe230e3e897a7aaf6f3d54e9ff66a05a
4. 485d5af4ad86e9241abd824df7b3f7d658b1b77c7dcc3c9b74bfe1ddc074c87d
5. 4c05ee584530fd9622b9e3be555c9132fad961848ea215ecb0dd9430df7e4ed8
6. 50ba9a2235b9b67e16e6bd26ae042a958d065eb2c5273f07eee20ec86c58a653
7. 5818bfe75d73a92eb775fae3b876086a9e70e1e677b7c162b49fb8c1cc996788
8. 5a35672f293f8f586fa9cfac0b09c2c52a85d4e8bc77b1ed4d7c16c58fe97a81
9. 69d60562a8d69500e8cb47a48293894385743716e2214fd4e81682ab6ed1c46b
10. 6d40c289a154142cdd5298e345bcea30b13f26b9eddfe2d9634e71e1fb935fbe

VI. References

- https://malpedia.caad.fkie.fraunhofer.de/actor/blacktech
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt
- https://attack.mitre.org/groups/G0098/
- https://securityaffairs.co/wordpress/74317/malware/blacktech-apt-stolen-certificates.html
- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=BlackTech%2C%20Circuit%20Panda%2C%20Radio%20Panda&n=1