APT-19

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON APT-19 ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

APT 19 is a threat group based out of China also goes by the name Deep Panda and Sunshop Group focused on information theft and espionage.

II. TARGETS

Targets of this threat actor/group has targeted a variety of industries,including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services

III. METHODS USED

This group uses CVE-2012-4792 vulnerability, to exploit it's citizens.
This group has also been found using Poison Ivy.

IV. CAMPAIGNS

The campaigns of this group are as follows:

Breaches of National Security Think Tanks.
Breach of the US Department of Labor website.
Breach of the US Office of Personnel Management
Breach of health insurance company Anthem
Links to Operation Kingslayer.

ATTRIBUTION

The U.S. Justice Department has charged two Chinese intelligence officers, six hackers, and two aerospace company insiders in a sweeping conspiracy to steal confidential aerospace technology from U.S. and French companies.

The threat posed by Chinese government-sponsored hacking activity is real and relentless," FBI Special Agent in Charge John Brown of San Diego said in a statement. "Today, the Federal Bureau of Investigation, with the assistance of our private sector, international and U.S. government partners, is sending a strong message to the Chinese government and other foreign governments involved in hacking activities

Deep Panda is a leading suspect in the cyberattack on the U.S. government's Office of Personnel Management (OPM), revealed in June 2015, which compromised the data of 4 million current and former federal employees.

AX1AL

V. IOCS

Hashes

ea6b2b51050fe7c07e2cf9fa232de6a602aa5eff66a2e997b25785f7cf50daa
3577845d71ae995762d4a8f43b21ada49d809f95c127b770aff00ae0b64264a3
ea67d76e9d2e9ce3a8e5f80ff9be8f17b2cd5b1212153fdf36833497d9c060c0
de33dfce8143f9f929abda910632f7536ffa809603ec027a4193d5e57880b292
b690394540cab9b7f8cc6c98fd95b4522b84d1a5203b19c4974b58829889da4c
de984eda2dc962fde75093d876ec3fe525119de841a96d90dc032bfb993dbdac
ccf87057a4ab02e53bff5828d779a6e704b040aef863f66e8f571638d7d50cd2

C2

bossas[.]org
supermanbox[.]org
microsoft-cache[.]com

IPs

121.54.168.230
218.54.139.20
210.181.184.64
42.200.18.194

VI. REFRENCES

https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/

https://www.crowdstrike.com/blog/department-labor-strategic-web-compromise/

https://gizmodo.com/u-s-indicts-chinese-hacker-spies-in-conspiracy-to-stea-1830111695