1. The name advanced persistent threat was brought into the existence by the US Department of Defense to explain the cyber espionage efforts by China against American national security interests. The attack definition was limited to mean an attack on national security interests.

APT34 is an example of an advanced persistent threat believed to be Iranian that was identified by researchers at FireEye. The attack targeted companies in Middle East with attacks against financial, government, energy and chemical companies. The attackers implemented SQL injection, brute-force cracking and weak password dictionary attack.

1. Filter by the IP address

tcpdump host 192.168.0.1

Packet filter by traffic related to specific port

tcpdump port 139

tcpdump port 145

Packet filter by traffic using port range

tcpdump portrange 20-21

1. Study the MD5 hashes to identify the files that failed the integrity test by the MD5.

Examine the email to determine whether it contained a software or a malware that would conduct a spear phishing attack.

Examine the content of the two call back domains to check the parameters the call backs added and what was the exchange.

1. rule HammerToss\_malware{

meta:

description = "Encrypt data"

author = " "

reference = "hxxps://www.twitter.com/1abBob52b"

hash1 = "d3109c83e07dd5d7fe032dc80c581d08"

hash2 = "42e6da9a08802b5ce5d1f754d4567665637b47bc"

strings:

$x1 = " #101docto encryption"

$s2 = "encrypt"

condition:

(unit16(0) == 0\*5a4d and fileSize $x1) or (all of them)

}

1. Whoami & hostname & ipconfig /all & net user / domain 2 – this collects information on people currently logged in, the hostname the ip address of the host and all the users of the target system and the domains of the system.

&1 & net group "domain admins" /domain 2 – this command collects data on who the domain admins are.

>&1 & net group "Exchange Trusted Subsystem" /domain 2>&1 & net accounts /domain 2>&1 & net user 2>&1 & net localgroup administrators 2>&1 & netstat -an 2>&1 & tasklist 2>&1 & sc query 2>&1 & systeminfo 2 🡪 collects information on accounts.

The information collected from the system is used by the attacker to access privileged data and maliciously manipulate it.

1. The virus can be submitted in a password protected zip-file. This can be done by running virustotal-submit.py sample.exe.