APT 34

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON OILRIG/APT-34 ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

OilRig is a threat group which is suspected to have it's origin based out of Iran , which is also known as APT 34 or Twisted Kitten.

II. TARGETS

Aviation, Chemical, Education, Energy, Financial, Government, High-Tech, Hospitality, Oil and gas, Telecommunications.

III. METHODS USED

OilRig has been using W32.Disttrack is a new threat that is being used in specific targeted attacks against at least one organization in the energy sector. It is a destructive malware that corrupts files on a compromised computer and overwrites the MBR (Master Boot Record) in an effort to render a computer unusable.

In the recent attacks they set up a fake VPN Web Portal and targeted at least five Israeli IT vendors, several financial institutes, and the Israeli Post Office.

OilRig group using a tool they developed called ISMAgent in a new set of targeted attacks. The OilRig group developed ISMAgent as a variant of the ISMDoor Trojan.

IV. CAMPAIGNS

*OilRig has been linked to Shamoon attacks at the energy sector.
*Targetted attacks against the banks at Middle East
*Government organizations of Turkey , Isreal and US .
*Oilrig has also been attributed for carrying out various operations against insurance based companies in Middle East.

ATTRIBUTION

OilRig has been attributed by Fireeye and they have linked this campaign to APT34, a suspected Iranian cyber espionage threat group that believed has been active since at least 2014.
[cited from Fireeye]

AX1AL

V. IOCS

Hashes[SHA-256]

742a52084162d3789e19...
f1de7b941817438da2a4...
b142265bb4b902837d83...

47054a8d380c197a7f32
e9ccf7a3c1e24f173ae9...
e3c6f13dc3079a828386...

C2's&Format of subdomains used in DNS C2 protocol

updateorg[.]com

[00][botid]00000[base36 random number]30

[00][botid][cmdid][partid][base36 random number][48-hex-char-of-file-content]

h

VI. REFRENCES

https://unit42.paloaltonetworks.com/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=OilRig%2C%20APT%2034%2C%20Helix%20Kitten%2C%20Chrysene

https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html