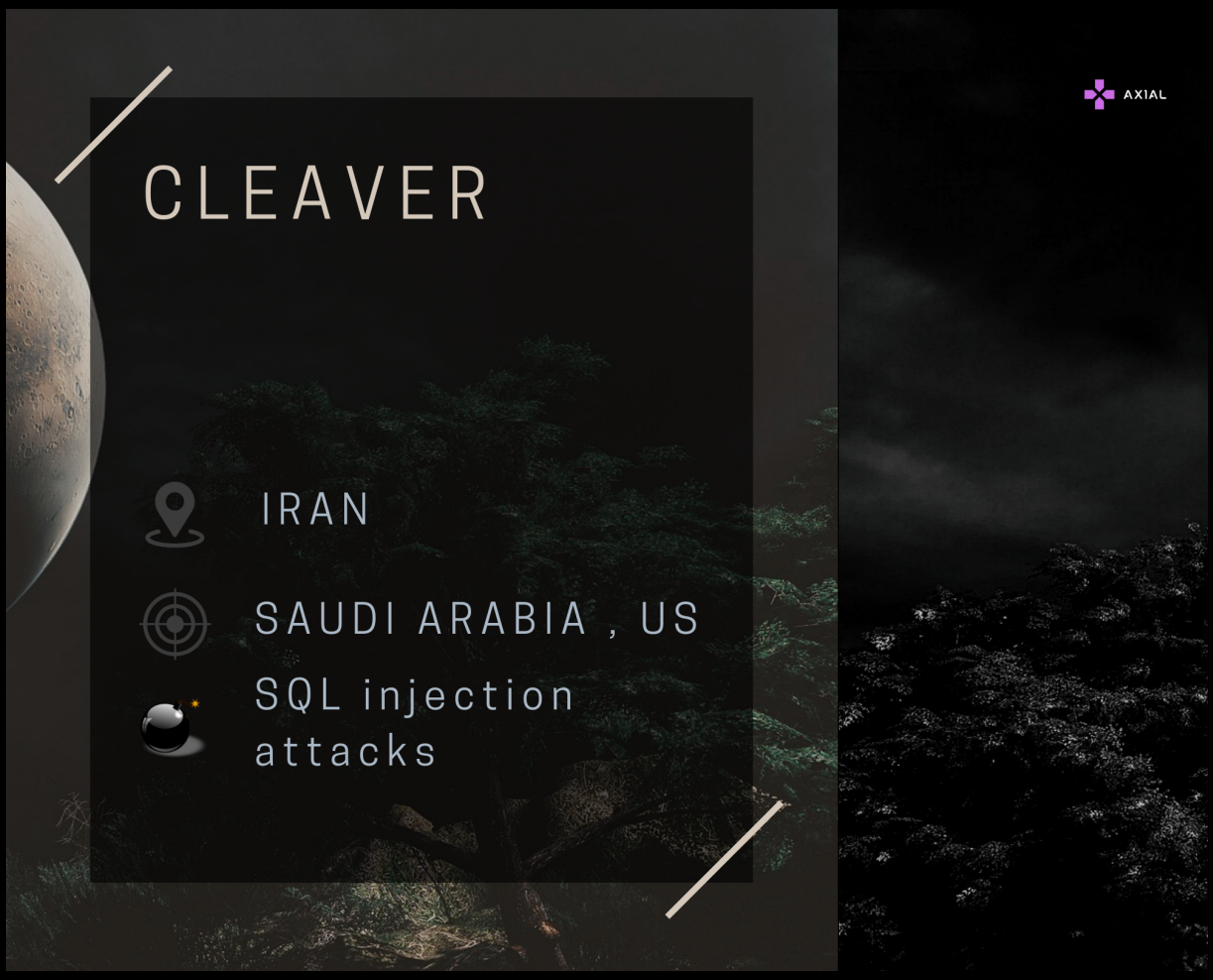
CLEAVER



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

A group of cyber actors utilizing infrastructure located in Iran have been conducting computer network exploitation activity against public and private U.S. organizations, including Cleared Defense Contractors (CDCs), academic institutions, and energy sector companies. This threat actor targets entities in the government, energy, and technology sectors that are located in or do business with Saudi Arabia.

II. TARGETS

This threat actor targets governments and private sector entities for espionage and sabotage purposes. It is believed to be responsible for compromising U.S. Navy computers at the Navy Marine Corps Intranet in San Diego, the U.S. energy company Calpine Corporation, Saudi Aramco, Pemex, Qatar Airways, and Korean Air

III. METHODS USED

The threat actors behind the Operation Cleaver uses a mix of off-the-shelf SQL injection attacks and exploits for several Microsoft vulnerabilities, including MS08-067 was also used by hackers in the popular Red October campaign.The hacker adopted TTPs similar to the ones used by other APTs operating for foreign governments, including China and Russia. The Operation Cleaver crew also have customized tools in its arsenal that have been discovered by investigators. Customized tools allow data exfiltration, syphoning of victim's credentials, network sniffing, keylogging and backdooring of targets.

IV. CAMPAIGNS

- **2014** : Security firm Cylance released a detailed report on the hacking Operation Cleaver that was run by state-sponsored hackers linked to the Iran. The Iranian hackers targeted critical infrastructure worldwide, ten of which are located in the United States.

- Experts at Cylance are cautions regarding the motivation behind the attacks on SCADA systems networks, they propend for a retaliation for Stuxnet and other campaign that hit the country. The exfiltrated data could be used by hackers to run further attacks for sabotage.

AX1AL

V. IOCS

MD5 Hashes

01606d42c64e4d15ea07d4e1fbd0c40d
0405adfc8739025ba88c746c8edebfb8
04fdf5b757764af8bc7ef88e0f8fe8c1
0512c5a8807e4fdeb662e61d81cd1645
0593352cadb2789c19c2660e02b2648b
08eabb6164b1b12307931e4f2d95f7c6
0900c3319e4c46ff9478e3e1fa9528a1
0acd8945bd162e5e7aa982cddbd8ecaa
0ad6a01a916f14fc24fa43e46813b3bb
0b2cbfa07fa9a090b35a3dfdb0ebad9d
0b80a8d2c56789b4bda9a56a53e7e2b1
0f4b526d8edf1d3d32c81a692c325733
10d019932fc43e9b39be709f8281203d
1223e93dd4a5ad0536c8232936cb35fe
144064951cceaf1bb81e8f215de76101
14a80287490f3a68d99c0f518b246fd2
17d1f25185b31044eb89a99d50d36a26
18942a44d2b5f2bbf54e2c18ac293915
18efd3f66d23c5c555e128a19de63667
19d9b37d3acf3468887a4d41bf70e9aa

C2's and Domains

88.150.214.168
microsoftactiveservices(dot)com
95.211.241.249,
88.150.214.166173.192.144.68
188.227.180.213
192.111.145.197
50.23.164.161
64.120.128.154
64.120.208.74
64.120.208.75
64.120.208.76
64.120.208.78
64.120.208.154
66.96.252.198
78.109.194.114
doosanjob(dot)com
downloadsservers(dot)com
drivercenterupdate(dot)com
easyresumecreatorpro(dot)com
googleproductupdate(dot)com
googleproductupdate(dot)net
kundenpflege.menrad(dot)de
microsoftactiveservices(dot)com
microsoftmiddleast(dot)com
microsoftonlineupdates(dot)com

TTP's

INITIAL COMPROMISE
SQL Injection
The attackers would enable xp_cmdshell:
Then connect outbound via anonymous FTP:
Spear-Phishing Campaign
PRIVILEGE ESCALATION & PIVOTING
Cached Credential Dumping

VI. References / Sources

https://github.com/lukaszbb/apt-analysis/blob/master/reports_txt/2014/Cylance_Operation_Cleaver_Report.txt
https://securityaffairs.co/wordpress/30734/intelligence/operation-cleaver-iranian-hackers.html
https://malpedia.caad.fkie.fraunhofer.de/actor/cleaver