Iran: A Top Tier Cyber Threat

Steph Shample, Middle East Institute, Fellow
Washington D.C., USA
sshample@mei.edu

Timeline of Activities

2009: Green Revolution (domestic)

2010: Stuxnet response

2012: LinkedIn campaign/attacks

2015 - 2018: Ransomware (SamSam)

2018: Espionage/IP theft (Mabna Institute)

2020: US Election influence (Spearphishing, social engineering)

2020: VPN exploitation/malware

2021: Industrial Control System (ICS) targeting

2022: Cyber espionage (Muddy Water)

Cyber Bodies: MOIS, IRGC, Basij, ICA

MOIS vs. IRGC

January 12, 2022, the U.S. government publicly stated it considers TEMP.Zagros (Muddy Water) subordinate to the MOIS.

APTs and Other Cyber Groups

- Goal: Strategic espionage
- SHAPESHIFT
- DROPSHOT/Stonedrill
- Brute-force attacks
- Password spraying
- Mimikatz

- Goal: Strategic/cyber espionage
- ZEROCLEARE
- DNSPIONAGE
- PICKPOCKET
- DNS tunneling
- Powershell
- HTTP GET and POST requests
- Open SSH tunnel for remote RDP
- Mimikatz

APTs and Other Cyber Groups

- Goal: Strategic espionage
- HAVIJ
- Two-Factor Authentication Defeat
- Keylogging
- Mimikatz
- Microsoft Office vulnerability abuse

- Goal: Theft of information to support Iranian monitoring and tracking of individuals/dissidents
- SEAWEED
- CACHEMONEY
- POWBAT
- Run the front company Rana
- Vulnerable web servers
- Custom backdoors
- Mimikatz

APTs and Other Cyber Groups

Rampant Kitten

- TTPs: Use Info stealing tools, target Telegram and KeePass
    - Dharma ransomware
- Goals:
    - Espionage, financial gain
    - Target and expose/dox dissidents/Iranian minorities

Pioneer Kitten

- TTPs: Webshells, SSH tunneling, VPN exploitation
- Goals:
    - Espionage, financial gain

Static Kitten

- TTPS: Malware (PowGoop), spearphishing, powershell scripts, custom backdoors
- Goals:
    - Data theft
    - Data exfil

Iranian Malware Comparisons

	First/Last seen	Notable Specs	Notable Victims
Shamoon Version 1	2012/2016	-Uses legitimate tool “Eldos Rawdisk” -Overwrites MBR; prevents startup -”Shamoon” is a directory string found in Wiper -Replaced images -Creds preprogrammed -C2 data	Saudi Aramco (SA) RasGas (QA)
Shamoon “2.0”	2016/2018	-Deletes files, then overwrites MBR -Set attack date to the “past” for immediate activation -Encrypt data/images, vs. replacing -NO preprogrammed creds Blank C2, no entry	Saudi Arabia UAE Saipem (IT)
Zerocleare	2018	-Resembles Shamoon, but is “separate” -Uses legitimate tool “Eldos Rawdisk” -Brute force is first stage -32-bit and 64-bit version; only the latter works -inspired Dustman -use the exact same skeleton, Turla Driver Loader (TDL) -Requires two executable files for driver/payload delivery	Various MENA oil/gas companies
Dustman	2019/2022	-Likely variant of ZeroCleare -Use the exact same skeleton, Turla Driver Loader (TDL) -Designed to delete data from infected computers -Deliver all drivers and payloads in a single executable file	Bahrain’s “Bapco” (2019, Aug 2022)

Iran and Ransomware

SamSam, 2015-2018:

After gaining access to a particular network, the SamSam actors escalate privileges for administrator rights, drop malware onto the server, and run an executable file, all without victims' action or authorization. While many ransomware campaigns rely on a victim completing an action, such as opening an email or visiting a compromised website, RDP allows cyber actors to infect victims with minimal detection. Analysis of tools found on victims' networks indicated that successful cyber actors purchased several of the stolen RDP credentials from known darknet marketplaces (FBI).

Difference between SamSam and Russian variants:

The use of ransomware in global cybercrimes rose by 82% through the year (Crowdstrike). Through 2021, Iranian groups such as BlackShadow and Deus were noted among the most active Iranian ransomware actors, targeting Iran domestically as well as external targets.

Dharma, 2020-2021

Script kiddies, very unsophisticated. Used OSINT tools for operations. Delivered via RDP port spread.

Bitlocker, 2020-2022

APT35 - Bitlocker use as of January 2022, and the actors also moonlit as cyber criminals, deploying ransomware at night. Similar to SamSam.

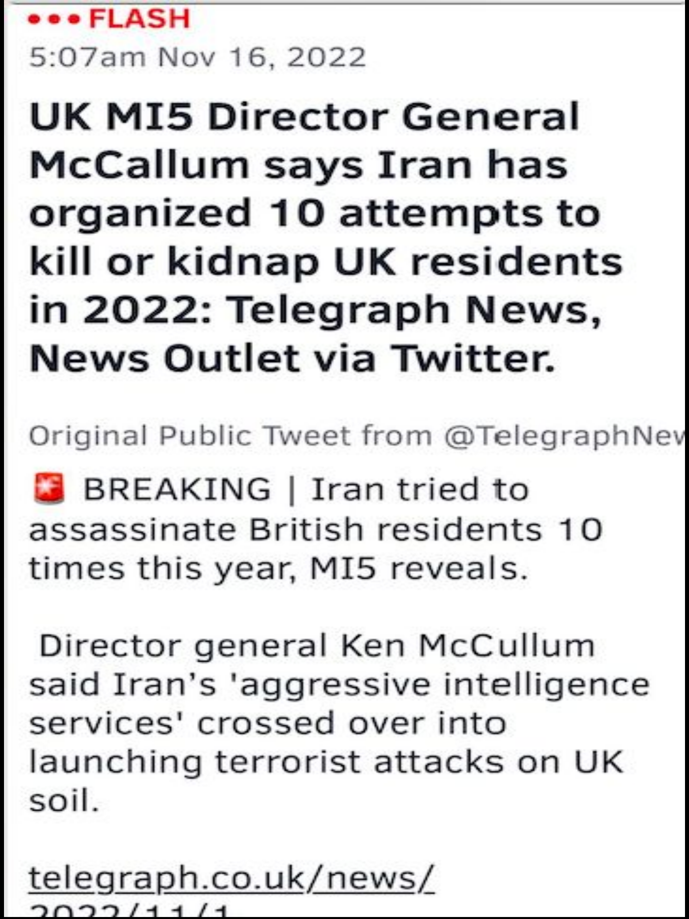
The Future

Notable Partnerships

Cryptocurrency/Crypto-mining, Front Companies

Terrorism/Fringe Group Operations

~~Oh Shit~~ Bonus Material



••• FLASH

5:07am Nov 16, 2022

UK MI5 Director General McCallum says Iran has organized 10 attempts to kill or kidnap UK residents in 2022: Telegraph News, News Outlet via Twitter.

Original Public Tweet from @TelegraphNew

🚨 BREAKING | Iran tried to assassinate British residents 10 times this year, MI5 reveals.

Director general Ken McCullum said Iran's 'aggressive intelligence services' crossed over into launching terrorist attacks on UK soil.

telegraph.co.uk/news/
2022/11/1

THANK YOU!

DANKE SCHOEN!

متشکرم

MERCI!

GRAZIE!

شكرا

GRACIAS!

For IOCs, sources, or more:

SSHAMPLE@mei.edu