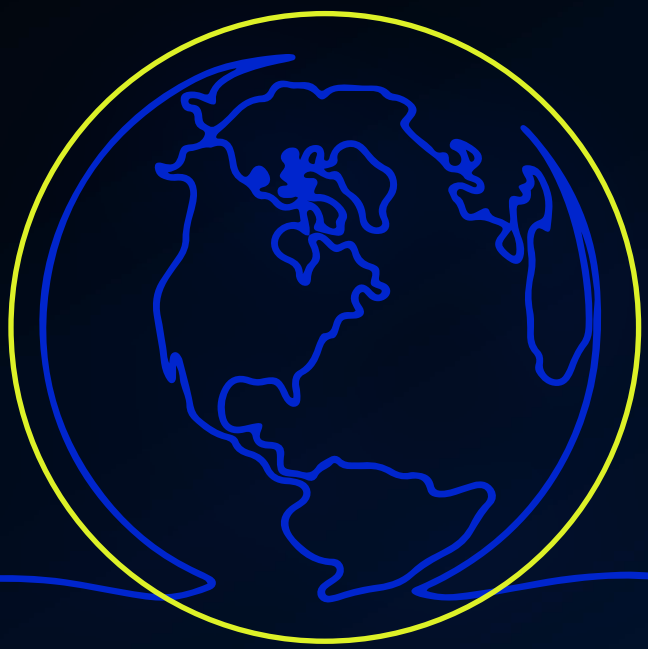
Radiflow

In the Aftermath of the Assassination: Fear of Cyber-Retaliation by Iranian Attack Groups

CIARA, THE FIRST OT-BAS PLATFORM

THE RADIFLOW CYBER-RESEARCH TEAM



IN THE AFTERMATH OF THE ASSASSINATION: FEAR OF CYBER-RETALIATION BY IRANIAN ATTACK GROUPS TARGETING OT AND IT NETWORKS

CYBER ATTACKS ARE LIKELY – AND THEY'RE NOT LIMITED TO IT NETWORKS

One of the likely consequences of the recent tension in the Middle East is retaliatory cyber attacks against US and Western interests, possibly by Iranian-nexus groups well-known to cyber-security community – APT33, Oilrig and others.

These groups are able to leverage their presence and foothold in victims' networks to carry out disruptive cyber attacks in the form of data manipulation, disk drive wiping and such; alternately, threat actors may well attack newly-identified targets.

(*See also timeline of disk-drive wiping attacks, below.*)

Other scenarios include leaking sensitive and personal data, as in the case of Iranian-attributed cyber-espionage groups such as APT39, or DDoS attacks against government institutions, financial and other national critical systems, similar to the 2013 "Operation Ababil" attacks against US financial institutions.

HACKER GROUPS (IRANIAN AND OTHER) ARE SHIFTING FROM IT TO OT

While most warnings focus on attacks against IT networks, there have been clear indications that Iranian threat actors have crossed over into OT production & automation systems, including the infamous "Shamoon" attacks against Saudi and other Gulf states infrastructures (IBM X-Force has also detected a new destructive wiper called ZeroCleare, which bears similarity to the Shamoon malware, and is suspected to have been used by another Iran-based group to target national energy and industrial Middle East.)

OT (ICS/SCADA/IIoT) networks are by and large much less protected and much more exposed to attacks than IT networks, especially networks with devices that hadn't been designed with security in mind. Left inadequately protected, OT networks are no match for a new class of sophisticated, destructive malware such as Shamoon or ZeroCleare.

At present, the types of attacks we expect to see at first from IT-hacker groups will focus on the server level (L2) rather than higher operational levels, that is more easily accessible through the IT-OT interface. That said, as hackers become more proficient we will surely see a progression toward higher network levels.

WHAT CAN YOU DO TO PROTECT YOUR OT NETWORKS

- Make sure all enterprise data is backed up, and that proper procedures have been installed to assure continued operations in the case of a disruption in OT systems.
- Enforce proper network segmentation policies to prevent attack propagation and contain potential cyber incidents. This is especially critical in the case of multinational corporations that have presence in the Middle East.
- Review protocols and procedures set in place in the case of OT network malfunction/disruption.
- Maintain network visibility into critical business processes and operations.
- Pay attention to any operational network anomalies.
- Obtain guidance from your country's national cyber security authority: DHS-CISA in the US (see their recent statement regarding possible cyber-attacks by Iranian operatives), NCSC in the UK, ANSSI in France, INCD in Israel, BSI in Germany and others.
- Keep in mind that your suppliers/contractors can be your cyber "weak link".

CONCLUSION

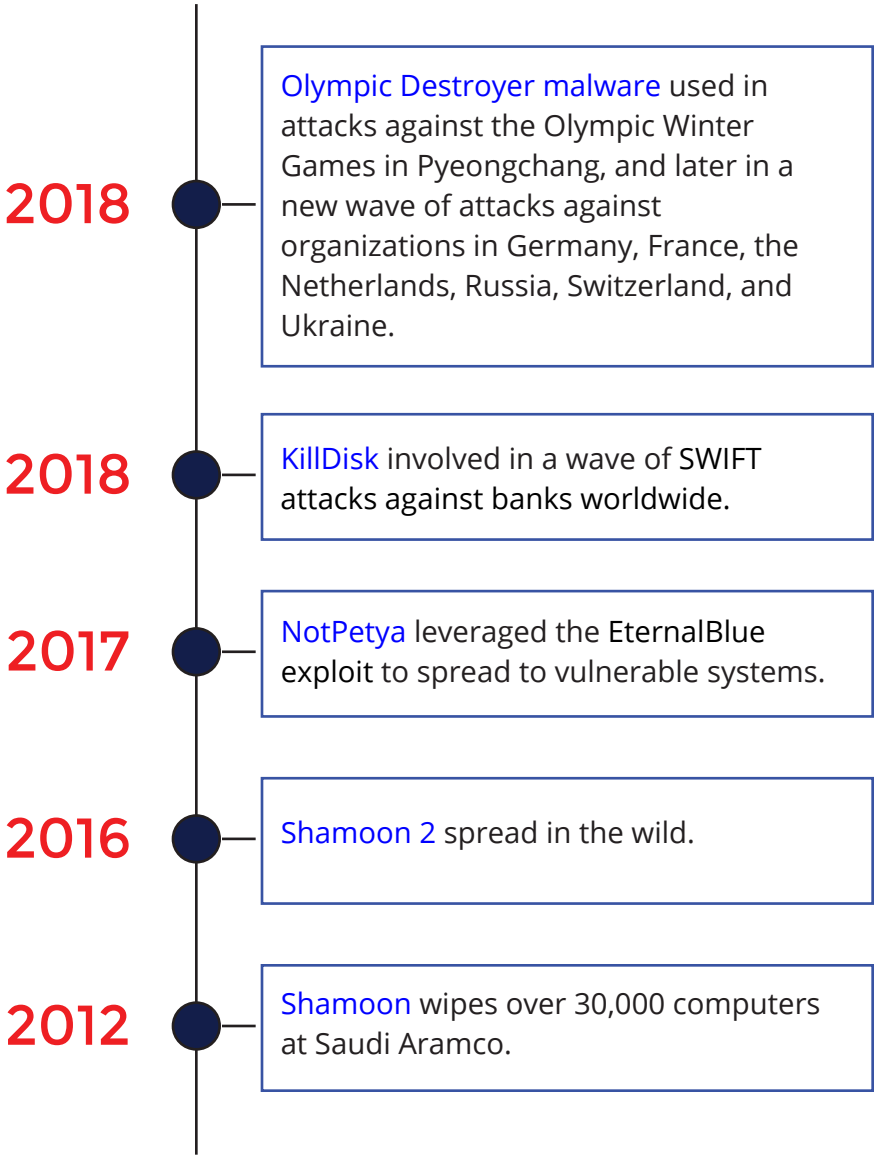
The guiding principle in the industry—that any cyber-vulnerability will be eventually exploited—has never been more relevant. Moreover, attack propagation is by nature unpredicted and your enterprise can become a victim even if attacker didn't target you specifically.

That said, highly-effective cyber-security tools are readily available. You may find that the way to go is to hire the services of an OT-specialized Managed Security Services Provider. MSSPs have established themselves as a viable alternative to in-house security departments, saving both the cost and more importantly the OT-security expertise that is extremely hard to come by. MSSPs can offer a more holistic security and network management solution, including threat intelligence, periodic risk assessment, device obsolescence management, etc.

Feel free to contact us with any concerns you may have regarding network segmentation, network visibility, secure access, risk management or any other aspect of protecting your OT environment.

Next page: timeline of disk-drive wiping attacks

TIMELINE OF DISK-DRIVE WIPING ATTACKS



KNOWN IRANIAN HACKING GROUPS

APT 33

- **Names**: APT 33, Elfin
- **Country**: Iran
- **Sponsor**: State-sponsored
- **Motivation**: Information theft, espionage and sabotage
- **Description**: APT 33 is a suspected Iranian threat group in operation since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.
- **Sectors observed**: many, particularly in the Aviation sector involved in both the defense and commercial capacities, as well as in the Energy sector with ties to Petrochemical production.
- **Countries attacked**: U.S., Saudi Arabia and South Korea.
- **Related to**: OilRig, APT 34, Helix Kitten.
- **Tools used**: AutoIt backdoor, Empire, LaZagne, Mimikatz, NanoCore, NETWIRE, PoshC2, PowerSploit, POWERTON, Pupy, Ruler, Shamoon and TURNEDUP.
- More information
- Mitre Att&Ck

APT 39

- **Names**: Chafer, APT 39
- **Country**: Iran
- **Sponsor**: State-sponsored
- **Motivation**: Information theft and espionage
- **Description**: APT 39 is an Iranian cyber-espionage group that has been active since at least 2014. They have targeted the telecommunication and travel industries to collect personal information that aligns with Iran's national priorities.
- **Observed**: Sectors: Airlines, Airports, Transportation and Logistics; Countries: USA, Turkey, Saudi Arabia, Middle East and Spain.
- **Tools used**: ASPXSpy, HTTPTunnel, MechaFlounder Mimikatz, NBTScan, Non-sucking Service Manager (NSSM), Plink, Pwdump, Remcom, Remexi, SMB hacking tools, UltraVNC and Windows Credential Editor.
- **Information**: Article 1; Article 2
- Mitre Att&Ck

OILRIG

- **Names**: OilRig, APT 34, Helix Kitten, IRN2
- **Country**: Iran
- **Motivation**: Information theft and espionage
- **Description**: OilRig is a threat group with suspected Iranian origins that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests. This group was previously tracked under two distinct groups, APT 34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity.
- **Related to**: APT 33, Elfin
- **Observed**: Sectors: Broad targeting across a variety of industries, including Financial, Government, Energy, Chemical, and Telecommunications; Countries: Israel, Kuwait, USA, Turkey, Qatar, UAE, Saudi Arabia, Qatar and Lebanon.
- **Tools used**: Shamoon, Disttrack, StoneDrill, BONDUPDATER, certutil, Helminth, ISMDoor, ISMInjector, LaZagne, Mimikatz, OopsIE, POWRUNER, QUADAGENT, RGDoor, SEASHARPEE, Systeminfo and Tasklist.
- **Information**: Article 1; Article 2

MAGIC HOUND

- **Names**: Magic Hound, APT 35, Cobalt Gypsy, Rocket Kitten, Ajax Security Team
- **Country**: Iran
- **Sponsor**: State-sponsored
- **Motivation**: Information theft and espionage
- **Description**: An Iranian-sponsored threat group operating primarily in the Middle East that dates back as early as 2014. The group behind the campaign has primarily targeted organizations in the energy, government, and technology sectors that are either based or have business interests in Saudi Arabia.
- **Observed**: Sectors: Energy, Government and Technology sectors that are either based or have business interests in Saudi Arabia; Countries: Iraq, UK, Afghanistan, Kuwait, Egypt, UAE, Turkey, Syria, Iran, Jordan, Canada, Spain, Morocco and Pakistan.
- **Tools used**: Havij, Mimikatz, Pupy and sqlmap.
- Counter operations: Microsoft slaps down 99 APT35/Charming Kitten domains (2019)
- **Information**: Article 1; Article 2
- Mitre Att&Ck