Table of Contents

Executive Summary 1
Section 1: Iranian Cyber Capabilities 3
Section 2: Iranian APTs and other State Proxies 3
Section 3: Assessment of trends across all sectors and geographies 5
Section 4: Destructive Cyber Incidents 8
Section 5: Disruptive 15
Section 6: Espionage 18

Executive Summary

The following report comprises a collection and analysis of Iran's capabilities and accomplishments to date in the cyber field. Iran's cyber capabilities have been continuously improving over the course of the last five years, as state-backed groups have used digital means to supress political and protest activity within the country and project a heightened geopolitical profile amongst its neighbours and adversaries. Iran is economically weakened at present and suffering from sanctions from a number of countries. By using cyber tactics, the state is able to project substantial political profiles that outstrips their real-world economic power, thereby expanding its sphere of influence in the MENA region.

Iran plays a significant role in the development of the present cyber threat landscape. The first major cyber physical sabotage to draw mass attention on the international stage – Stuxnet – was a partnership between Western offensive coordinators to neutralise Iran's developing nuclear program. In response to the attack, Iran took steps to increase its cyber offensive capabilities to the point that it has become one of the major cyber actors operating on the global scale.

For the most part, Iran's cyber activities are conventional in nature. Linked actors regularly undertake in DDoS attacks, website defacement, phishing and spearphishing techniques, and theft of personal data or intellectual property, particularly against other MENA actors such as Israel as well as the United States. Shortly after Stuxnet, Iranian cyber teams began a prolonged series of distributed-denial-of-service (DDoS) attacks against the US financial sector, disrupting continuity at 46 major financial institutions over the course of six months. In 2017, seven hackers affiliated with various Iranian cyber groups, were indicted by the US Justice Department for the attack. These actors were also considered responsible for the presence of malware on a New York dam's SCADA systems in the same period. This indictment demonstrates the range of ambitions for many of the Iranian actors involved in its cyber campaigns, and that the US is a major target for the state. It also indicates the potential immaturity of many of the attacks, in that they can be traced and individuals can be held responsible.

All this is not to undersell the impact of Iran's capabilities, however, or to imply that the majority of its attacks are not overwhelming carried out against Middle Eastern states. Recent years have proved that its cyber attacks have the potential to cause great disruption and geopolitical tension in the region.

In 2012, for example, the infection of Saudi Aramco computer systems by the Shamoon wiper was hugely destructive and this attack has been strongly tied to Iranian cyber actors by US intelligence forces. The first Shamoon attack (there have since been several) occurred on the Islamic holiday of Lailat al Qadr, meaning that employees would be absent from offices, allowing the attack to trigger without immediate detection. This tradecraft would become something of a trend in major attacks carried out by Iranian-linked cyber groups in the years since, with multiple attacks emerging after a return to business following national religious holidays.

About the report

The following report details the most important ‘seriously disruptive’ and destructive attacks carried out by Iran in the time since Stuxnet and provides analysis of the technical trends and conclusions that open source material available on these events suggest. A set of definitions is provided, describing precisely the breadth of attacks surveyed. The report also provides a table of known Iranian cyber groups and the attacks for which they are responsible or have been linked.

In addition to these analyses and data, the report also provides a qualitative assessment of the ‘tipping point’ – the point at which Iranian cyber operations might become more drastically impactful or their key motivations change.

Section 1: **Iranian cyber capabilities**

Threat actor classification

7. State actor: agents of a nation state

6. State proxy: non-governmental actors operating in support of a nation state's policy objectives

5. Criminal: actors operating in pursuit of financial gain

4: Hacktivist: actors operating in support of political causes widely regarded as not being terrorist in nature

Intelligence requirements

1. All destructive and 'seriously disruptive' attacks conducted by or linked to Iranian actors that have been observed
2. What trends in targeting by Iranian-linked actors have been observed (i.e. geographies, sectors etc.)?
3. How have the capabilities employed by Iranian-linked actors changed over time?
4. What evidence is there of Iranian actors colluding with other actors?
5. What (non-cyber) events (geopolitical etc.) appear to have preceded significant Iranian-linked cyber campaigns and is there any correlation between events and Iranian cyber action? Relatedly, is there any correlation between non-cyber Iranian hostile action (e.g. drone strikes, terror attacks and other forms of 'hybrid warfare) and cyber actions?

Statement on Collection

All key judgements, analysis and assessments are limited by and to the sources collected

Section 2: **Iranian APTs and other State Proxies**

Table 1: APT groups, software and TTPs taken from MITRE ATT&CK

MITRE ATT&CK	APT
G0064	APTP33, Elfin
G0087	APT29, Chafer
G0058	Charming Kitten
G0003	Cleaver, ThreatGroup 2889, TG-2889
G0052	Copy Kittens
G0070	Dark Caracal (Hezbollah) (Lebanese GDGS), Operational, Timing and Strategic overlap
G0043	Group5
G0077	Leafminer
G0059	Magic Hound, Rocket Kitten, Operation Saffron Rose, Ajax Security Team, Operation Woolen-Goldfish, Newscaster, Cobalt Gypsy, APT35
G0021	Molerats, Gaza Cybergang (Palestinian), Operation, Timing and Strategic Overlap
G0069	MuddyWater, Seedworm, Temp.Zagros
G0049	OilRig, APT34, IRN2, Helix Kitten

Table 2: See annex for full individual MITRE ATT&CK Navigator profiles

PsExec S0029	RDP T1076	Mimikatz S0002	PowerShell T1086	Let's Encrypt Certs	Watering Holes	Credential H/D	DNS Redirects
Shamoon 3	SamSam S0370	ZeroCleare/ Dustman	Shamoons 1-3	DNSpionage	Leafminer G0077	Shamoons 1-3	Shamoons 1-3
ZeroCleare/ Dustman	Leafminer G0077	SamSam S0370	ZeroCleare/ Dustman	xHunt	DNSpionage	ZeroCleare/ Dustman	Leafminer G0077
SamSam S0370	xHunt	Leafminer G0077	Tortoiseshell		Tortoiseshell	Leafminer G0077	DNSpionage
Leafminer G0077	Oilrig/APT34 G0049	Magic Hound G0059	xHunt		xHunt	xHunt	xHunt
Oilrig/APT34 G0049		MuddyWater G0069	Elfin/APT33 G0064			Likely all	
Magic Hound G0059		Cleaver G0003	Copy Kitttens G0052				
Cleaver G0003		Oilrig/APT34 G0049	Jcry S0389				
		Elfin/APT33 G0064	Magic Hound G0059				
			MuddyWater G0069				
			Oilrig/APT34 G0049				

Section 3: **Assessment of trend across all sectors and geographies**

Key statement

Iranian cyber operations offer additional ways and means for national policy makers and strategists to achieve their policy goals. Cyber operations are meant to achieve real-world policy aims and are used in conjunction with more traditional instruments of national power within the context of a strategic framework. Destructive, disruptive (sabotage), and espionage cyber events generally tend to increase after prolonged escalatory statecraft between Iranian, Arab and Western countries.

Early signs

The first major indication that Iran was developing offensive cyber capabilities was a prolonged DDoS campaign that began in December 2011, intensified through September 2012 and ended around May 2013. The DDoS campaign began roughly a year following the discovery of the Stuxnet worm, and specifically targeted the US financial sector, likely in retaliation against the 2010 targeting of Iran’s nascent nuclear sector, as well as subsequent malware found in Iranian industrial control system (ICS) facilities and escalating US sanctions at the time.

The campaign used a combination of vulnerability to create Botnets and execute the DDoS attacks. A 2016 US Department of Justice indictment alleges that two teams coordinated the attacks in conjunction with Islamic Revolutionary Guard Corps (IRGC). The indictment also alleges that the DDoS teams trained IRGC officials in cyber operations.

The second major indication – the deployment of Shamoon on 15 August 2012 – represented a major step up the cyber ‘value chain.’ Shamoon was a truly destructive attack, targeting Saudi Aramco IT networks with malware capable of wiping systems of their data, ‘rendering infected systems useless.’ Shamoon overwrote the Master Boot Record (MBR), a popular tactic that has since been used by dozens of wiper strains. Shamoon also used a version of EldoS RawDisk drivers and certificates, as part of the wiper module to locate, overwrite and destroy data on the MBR and disk partitions. EldoS RawDisk has since been used in some capacity by every iteration of Iranian wiper strains since, as this report demonstrates. Later reports indicated that up to 35,000 Aramco systems were scrapped during the Shamoon wiper attack, triggering an unprecedentedly large incident response, volatility in domestic Saudi energy markets, and price increases and shortages in the global hard-drive market.

As was the case in the DDoS campaign, the timing and targeting of Shamoon aligned with increasing geopolitical tensions between Iranian, Arab, and Western states. This theme presents strongly through the majority of historical Iranian cyber activity through to the present day.

US sanctions targeting Iranian government and industry steadily intensified throughout the first half of 2012, culminating in the passage of H.R.1905 Iran Threat Reduction and Syria Human Rights Act of 2012, on 10 August 2012, five days preceding the 15 August 2012 Shamoon attack. Another key feature was the timing of the attack, which occurred during the Lailat al-Qadr holidays during the end of Ramadan. This timing was likely chosen to maximise Shamoon's ability to reap destruction while remaining undetected, limiting initial incident response due to a limited workforce capacity because of the holiday. Subsequent attacks have followed a similar methodology.

Further developments

Through 2016, there were indications that Iranian cyber capabilities were evolving and becoming more dangerous.

The next step change up the cyber 'value chain' occurred on 17 and 29 November 2016 and 23 January 2017, when a second Shamoon campaign was deployed. McAfee believes that up to 90% of Shamoon 2's code was identical to that found during the 2012 campaign. McAfee also indicated that code from previous Magic Hound and infrastructure from previous OilRig campaigns overlapped with Shamoon 2. For instance, both campaigns once again relied on EldoS Raw Disk Drivers and certificates. McAfee also indicated that Shamoon 2 incorporated workarounds for credential harvesting against Huawei VDI, which was thought to be a mitigation for wiper attacks after Shamoon 1. Palo Alto analysis confirms Magic Hound's overlap but provides greater technical detail. The major differences between Shamoon 1 and 2 is that Shamoon 2 likely achieved initial compromise from spear phishing rather than vulnerability scans. Palo Alto believes that credential theft of legitimate domain/DNS names and user and administration accounts through Active Directory (AD) were used to compromise and spread throughout networks. Palo Alto then believes that further credential theft and use of Active Directory, RDP and PsExec were used for remote access, lateral movement and execution of the wiper. Unlike Shamoon 1, Shamoon 2 was not deployed during a local holiday, but did emerge during intense competition between the Saudi Arabian and Iranian energy sectors, including several high-profile spats in OPEC.

Further Iranian campaigns through this period represented greater refinement of techniques and an increased scope in targeting for espionage. The Leafminer attack was reported on 25 July 2018, creating DNS redirects to malicious websites for credential theft, likely indicating intelligence collection or the collection of credentials for further penetration of targeted networks. Two of the DNS redirects to malicious sites indicate the collection of strategic and political intelligence. One targeted the Lebanese Internal Security Forces and possibly the Ministry of Finance. The second targeted universities in Azerbaijan that provide training in military research, development, engineering, and statecraft.

The second campaign, DNSpionage, was first reported on 27 November 2018. DNSpionage used DNS redirects to malicious but legitimate-looking government and industry websites, offered fake jobs, and then distributed malicious Word Documents to gain initial access. DNSpionage also had potential to exploit social media, such as LinkedIn. Cisco Talos Intelligence believes that DNSpionage was a RAT designed to exfiltrate data (intelligence collection) from infected systems. There were no substantial overlaps in tools or code with other previous campaigns, however the use of DNS redirects to malicious websites is also a method employed by Leafminer. Much of DNSpionage's toolkit and tradecraft would be used in later Iranian intelligence operations and disk wiper attacks.

Two of DNSpionage's DNS redirects are of particular interest. The first, targeted authorities of the UAE during the Islamic New Year holiday weekend. A further attack 11 days later followed a Sunni terrorist incident on an Iranian military parade in Ahvaz, which saw increased Iranian rhetoric against several Arab states. The second targeted Lebanon's Ministry of Finance during a contentious election year, close to the reconfirmation of Lebanon's finance minister, an AMAL member and Hezbollah ally. A second DNS redirect went on to target Lebanon's Middle East Airlines, which is the official international airline of Lebanese government officials, close to a London visit by Prime Minister Saad Hariri, a Hezbollah foe.

On 10 December 2018, Shamoon 3 was deployed, representing another evolution in Iranian capabilities. The most prominent advancement was the addition of a new wiper that erases files before Shamoon deploys to wipe the MBR. Symantec believes that erasing the files before wiping the MBR makes the attack especially destructive, as recovering wiped data becomes impossible. Symantec noted that at least three Arab-based energy sector organisations were targeted, the most prominent being Saipem, where operations were hit globally, with 300-400 servers and 100 PCs affected. The deployment of Shamoon 3 directly aligns with escalating tensions between Iranian, Arab, and Western states. The US policy of maximum pressure, increased economic and social sanctions and the 8 May 2018 US withdrawal from the JCPOA bears resemblance to the circumstances surrounding the deployment of Shamoon 1. Like its predecessor, Shamoon 3 deployment was also deployed when workforces were reduced – in this case, on the weekend.

The status quo in 2020

The third wave of Iranian cyber operations occurred through 2019. These campaigns focused on espionage, tactical intelligence for real world operations, and disruptive/destructive aims. These campaigns represent the current state of Iran's capabilities, incorporating several previously used TTPs and tools in their deployments.

The first, Karkoff, was reported by Cisco Talos on 23 April 2019, two days after the weekend and the Islamic holiday Shab e Barat.. Karkoff is an evolution of DNSpionage, with capabilities and targeting that are largely similar to DNSpionage's, such as using DNS redirects and an apparent intent to target Lebanon. Karkoff, however, can perform reconnaissance and choose specific targets, vs DNSpionage's randomised targeting. The reconnaissance phase remains the most interesting, as it allows for a full fingerprinting of a network before infection. Cisco Talos believes that this fingerprinting allows for identification of workstations, platforms, domains and operating systems. This suggests that Iranian threat actors are becoming more specific in their targeting and collection requirements. As in previous incidents, Karkoff was discovered amidst escalating tensions between Iranian, Arab and Western states, such as the 22 April 2019 US announcement to end sanction waivers to states buying Iranian oil.

The second, Tortoiseshell, was reported on 18 September 2019, though likely active from July 2018-July 2019. Tortoiseshell has the least in common with the other Iranian campaigns surveyed. Symantec believes that it is a distinct group within the Iranian campaigns, despite the use of certain similar tools and infrastructure, like OilRig's Poison Frog backdoor, which was leaked in early 2019. Tortoiseshell is thought to have been a supply chain attack, targeting Saudi ISP networks with malware and Power Shell (MSFT native tool), capable of identifying valuable customers in order to pivot to their systems and networks.

The third campaign of note, xHunt, was reported on 23 September 2019, and thought to have been active between May-June 2019. xHunt targeted Kuwaiti shipping networks, using malware, infrastructure, tools, backdoors and exploits that have been used by DNSpionage, Oilrig and ISMAgent. Like DNSpionage, xHunt used backdoor tools for DNS and HTTP tunnelling for Command and Control (C2) communications. Later itineration's of xHunt incorporated Remote Desktop Protocol (RDP) and SMB transfers to other systems and added features such as screen shots. Another itineration incorporated backdoors that could use DNS tunnelling through Power Shell, as in Tortoiseshell. The timing of xHunt aligns with escalating geopolitical tensions for Iran, particularly with regard to shipping. Occurring in tandem with the xHunt campaign were two separate kinetic attacks against shipping in the region, in the Gulf of Omen and the Strait of Hormuz, followed by months of ship seizures. As in Shamoon 1, DNSpionage and Karkoff, xHunt was launched during Islamic holidays, during month of Ramadan and Lailat al-Qadr.

Both Tortoiseshell and xHunt were later found to be conducting operations to infect systems and users through malicious websites, and this appears to be in a theme in present Iranian cyber campaigns. Tortoiseshell targeted active and transitioning US military personal and their spouses via fake job advertisements. The listings prompted the user to download a malicious application that then installed a RAT that could collect information about the system, administration rights, date, time, drivers, information on the system and more. xHunt was found to be operating a watering hole website that injected malicious HTML code into an image on a Kuwaiti website for credential harvesting. The watering hole website also used DNS redirects to other Kuwaiti organisations to maximise returns. C2 infrastructure also had backdoors for HTTP and DNS tunnelling used in the xHunt campaign. Both xHunt and DNSpionage used Let's Encrypt Certificates to make their DNS redirects look legitimate. The watering hole website is thought to have exclusively targeted Kuwaiti organisations and overlaps with the xHunt campaign, starting in June 2019, indicating that credential harvesting from the watering hole was likely used to then penetrate Kuwaiti shipping organisations.

The fourth and final wave of Iranian cyber operations to date, ZeroCleare and Dustman, represent another gradual step change up the cyber 'value chain.' ZeroCleare and Dustman are the fourth and fifth variants of Iranian disk wipers. Similar to Shamoon 2 and 3, ZeroCleare and Dustman occurred near the end of the year but did not strike during specific Islamic or national holidays. They are both thought to have targeted the energy sector in the Middle East. As in all three Shamoons, ZeroCleare and Dustman overwrote the MBR and relied on an EldoS RawDisk Driver to deliver the payload. Unlike the three Shamoons, ZeroCleare and Dustman also use a separate but 'vulnerable driver' (VBoxDrv) to deliver the unsigned EldoS RawDisk Drivers as a workaround against Windows Driver Signature Enforcement (DSE), evading wiper mitigations.

Key judgements

- Every single campaign has overwhelmingly targeted Middle Eastern entities
    - Campaign targeting is organised and centrally directed
    - Requirements are organised around specific tasks and goals. For instance:
        - The Shamoon , ZeroCleare and Dustman campaigns are covert sabotage operations intended to create severe disruption or destruction in the Middle Eastern energy sector and global energy markets
        - Espionage campaigns are planned and directed around a hierarchy and division of requirements into:
            - Short term or tactical (xHunt targeting ships),
            - Mid-term or operational (Tortoiseshell ISPs)
            - Long-term or geostrategic (DNSpionage and Leafminer political/geo-strategic/future targeting)
        - Espionage campaigns can be re-tasked in a reactionary way to be tailored to real time developments. For instance:
            - Tortoiseshell was initially tasked with supply chain attacks against Saudi ISPs. Shortly after the 14 September Abqaiq attack, Cisco Talos Intelligence discovered a watering hole website masquerading as a website looking to connect US service members with employment in the private sector.
            - DNSpionage's second targeting of the UAE occurred on 24 September 2018, two days after the Ahvaz terrorist attack in Iran. Iran blamed terrorists aligned with 'a Gulf state'.
        - Disruptive campaigns tend to have a wider scope of targeting. For instance:
            - Both the 2011-2013 DDoS campaign and the SamSam ransomware strain targeted predominantly US critical national infrastructure (CNI), such as the financial, government, and healthcare sectors.
            - General defacement campaigns, such as the one preceding the assassination of General Soleimani, are numerous and random. They are most likely used for minor disruption, propaganda, and harassment purposes.

        - Disruptive attacks generally yield the least results but are easiest to deny.
- Several campaigns have targeted organisations during or near Islamic or national holidays, and/or on weekends. For instance:
    - Shamoon 1, DNSpionage/Karkoff and xHunt all occurred around Islamic holidays.
    - Shamoon 3 and Dustman occurred on the weekend (Sundays)
- Different groups with different tasks can be used to create synergy, indicating an entire government approach to long-term strategic planning and direction. For instance:
    - Shamoon 1 (destructive) and the 2011-2013 DDoS (disruptive) campaigns overlapped, targeting both Saudi energy infrastructure and the US financial system
        - The campaigns were likely attributable to escalating scrutiny and sanctions placed on Iran due to their nuclearisation program
        - The xHunt campaign targeted Kuwaiti shipping networks for tactical intelligence during an escalating geopolitical crisis in the Gulf. The Iranians were threatening to target shipping in the Strait of Hormuz and the Gulf to disrupt global markets, which is part of Iran's naval doctrine. The campaign overlaps with several ship seizures in the region, showing how cyber intelligence can have kinetic effects.
- Iranian espionage and CNA operations are well disciplined and are not connected to singular events.
    - Campaigns have followed prolonged periods of escalatory behaviour between Iranian, Arab and Western states, especially in relation to traditional forms of statecraft such as sanctions and geo-economics, as much as they are a response to adversarial CNA operations. For instance:
        - Shamoon 1, 2 and 3, ZeroCleare and Dustman and the 2011-2013 DDoS, DNSpionage , Leafminer, Tortoiseshell and the xHunt campaigns all were components of long-term strategic thinking and were discovered during increased scrutiny of Iran, economic and political sanctions and increased economic and political regional competition.

The tipping point

Iranian cyber operations are already being used to great effect for sabotage and as a force multiplier throughout the Middle East. A cyber attack/contagion that either deliberately or accidently targets core military infrastructure, like nuclear command, control, and communications (C3) networks, can lead to a conventional escalation spiral. A cyber attack/contagion that deliberately or accidently causes large civilian loss of life would result in a similar conventional escalation.

Section 4: **Destructive Cyber Incidents**

Threat actor classification

(7) State actor: agents of a nation state

Possibly APT33/Elfin, Possibly APT34/Oilrig

Assessment

There have been few physically destructive cyber attacks to date. The only industry acknowledged physically destructive cyber incident, Stuxnet, occurred a decade ago. Other cyber incidents, such as Russia's CRASHOVERRIDE in 2016 and TRITON/TRISIS in 2017, were specifically designed to trigger physical destruction but were used for either R&D or signalling, or else failed due to design flaws.

Per CRS and Pool Re definitions, a destructive cyber attack requires an element of physical damage. However, it has become commonplace within the cyber security industry to categorise certain non-physically destructive cyber incidents as destructive, such as disk wipers.

Iranian use of disk wipers has been limited to a few clustered incidents. Iranian disk wiping campaigns that have been reported have reduced in reported impact but are technically capable of achieving substantially greater disruption and damage. Media coverage of Iranian disk wiping incidents are high profile, global, and are often sensationalised. The past year has seen a degradation of sourcing and vetting within the traditional media's coverage of cyber, such as in this much maligned Bloomberg article on Dustman, and conflation of events based on limited sourcing and technical indicators is likely to further erode the trust in mainstream cyber journalism. Iranian use of disk wipers are not connected to singular events. Rather, disk wiping campaigns have followed prolonged periods of escalatory behaviour between Iranian, Arab, and Western states. Likewise, Iranian disk wipers seem to be deployed in retaliation to traditional forms of statecraft such as sanctions and geo-economics as much as they are a response to adversarial CNA operations. Finally, Iranian disk wiping campaigns are designed to reside below the threshold of traditional warfare, limiting potential escalation and reciprocity from adversaries while demonstrating Iranian capabilities.

There have been four reported Iranian wiper campaigns to date:

1. 15 August 2012 Shamoon 1
2. 17 & 29 November 2016 and 23 January 2017 Shamoon 2
3. 10 December 2018 Shamoon 3
4. September & 29 December 2019 ZeroCleare & Dustman

Shamoon 1: 15 August 2012 (Elfin/Apt33)

On 15 August 2012, Saudi Aramco began to experience severe disruption to 'three quarters' of their servers and workstations. The disruption was identified as malware designed to wipe data on servers, workstations and PCs in order to disrupt operations and cost the target substantial amounts of money. The wiper only affected corporate networks. Later reports estimated that up to 35,000 PCs were damaged.

By October 2012, the attack, dubbed Shamoon, was being publicly attributed to Iran, due to increasing geopolitical tensions and the image of a burning American flag that replaced wiped data. Subsequent analysis, such as from this blog, indicates that a string within Shamoon contained the phrase 'ArabianGulf,' which could be construed as a taunt over the naming conventions of the Arabian/Persian Gulf, a long-term contention between Iran and Arab countries. The blog also mentions that reconnaissance and targeting information were posted on websites such as Pastebin.com by actors claiming credit for Shamoon. The initial message, posted by the 'Cutting Sword of Justice,' excoriated the Saudi monarchy. Shamoon was launched during Ramadan, specifically on the night before Lailat al-Qadr, an important Islamic holiday. It is likely that this date was chosen because it would maximise the likelihood of Shamoon's success, an important piece of targeting tradecraft that appears repeatedly throughout Iranian cyber operations. The posting of legitimate reconnaissance and targeting information on public websites by unknown 'hacktivist' groups is also an important piece of tradecraft, as the act causes doubt about government attribution and acts as disinformation. Initial reporting indicated that security researchers believed Shamoon was deployed by insider threats, which was subsequently disproved, as the wiper, like Stuxnet, was eventually found to be self-replicating and delivered by a phishing email.

Security researchers were quick to highlight that Shamoon 1 followed the discovery of Stuxnet in 2010 and FLAME(R), another malware that targeted Iranian ICS facilities in the spring of 2012. Another malware, Duqu, which was based on Stuxnet and was considered a precursor to offensive CNA, was discovered late 2011. During the lead up to the deployment of Shamoon 1, Iran was under intense scrutiny, facing escalating economic and political sanctions due to their nuclear program. US sanctions were numerous and particularly biting. On 31 July 2012, President Obama signed an executive order strengthening previously enacted sanctions. And on 10 August 2012, five days before the detonation of Shamoon 1, the US Congress passed HR 1905, the Iran Threat Reduction and Syria Human Rights Act, further pressurising Iranian policy makers.

Researchers were quick to point out Shamoon as a possible retaliatory strike by Iran due to cyber interference. However, Iranian strategists likely deployed Shamoon due to a combination of cyber and traditional diplomatic pressure, especially the last two rounds of US sanctions. Deployment of Shamoon to counter a US whole of government approach, i.e. projecting every instrument of national power to degrade Iranian capabilities, makes strategic sense. Plausible deniability and limiting countervalue US targets would minimise the chances of a major US escalation while demonstrating Iranian capabilities.

Shamoon, dubbed W32.Disttrack, remained relatively unchanged between its first and second variants. Shamoon was designed to wipe data on systems by overwriting the Master Boot Record (MBR) and replacing file images with a burning American flag. Both variants contained a 32-bit and 64-bit versions. McAfee claims that the 64-bit version malfunctioned in Shamoon 1. Early variants of Shamoon had three basic stages:

- A 'dropper' named 'NtsSrv' that determined which version was dropped and then laterally spread throughout networks
- A 'wiper' that deployed an Eldos driver to avoid APIs and overwrite the disk. Eldos drivers have been used repeatedly throughout Iranian campaigns, especially in their most recent wiper deployments
- A 'reporter' that provided the ability for c2 communications and monitoring function to verify success of Shamoon

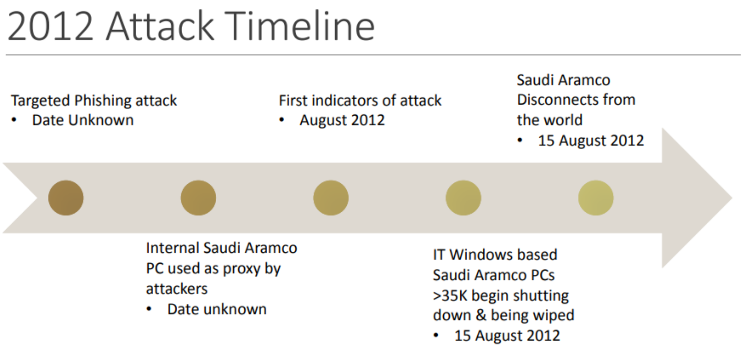
2012 Attack Timeline
Targeted Phishing attack
• Date Unknown
First indicators of attack
• August 2012
Saudi Aramco Disconnects from the world
• 15 August 2012
Internal Saudi Aramco PC used as proxy by attackers
• Date unknown
IT Windows based Saudi Aramco PCs >35K begin shutting down & being wiped
• 15 August 2012

Figure 1: Chris Kubecka Initial IR

Shamoon 2: 17 & 29 November 2016 and 23 January 2017

(Shamoon 2 intelligence from Palo Alto, Palo Alto, McAfee, Security Intelligence)

Shamoon 2 was deployed less than one year after diplomatic negotiations eased tensions on Iran, primarily relief from economic sanctions due to the JCPOA. Unlike Shamoon 1, Shamoon 2 did not target Arab facilities during a holiday. However, Shamoon 2 was deployed during intense competition between the Saudi Arabian and Iranian energy sectors, including several high-profile spats in OPEC.

Shamoon 2 was a staggered campaign, with McAfee detailing 3 separate attack waves:

- **'Attack Wave 1:** Wiped systems on November 17, 2016, at 20:45 Saudi time.
- **Attack Wave 2:** Wiped systems on November 29, 2016, at 01:30 Saudi time.
- **Attack Wave 3:** Began January 23, 2017, and ongoing, with similar samples and methods and TTPs as in Waves 1 and 2'

Although Shamoon 1 and 2 were similar, slight changes did occur, and these made the attack technically capable of greater damage than Shamoon 1:

- The attack had a workaround against Virtual Desktop Interfaces (VDI) which are usually deployed to counter wiper attacks. Used credential harvesting, especially against Huawei VDI to counter VDI's and make the attack more destructive
- Used legit domain names, user and admin account credentials to laterally move and propagate throughout networks (at least 16 had Disttrack hardcoded)
- 29 November 2016 incident commenced at 1:30 am local Saudi time
- Both 2012 and 2016/17 campaigns saw the wiper 'setting systems to a random date between August 1-20, 2012' to use a temp license key from Eldos driver
- ELDos RawDisk drivers have been used in all Iranian wiper cases
- Saudi Aramco was attacked in 2012, sources say several industrial, energy and government institutions were attacked in 2016/17, but details remain sketchy
- McAfee claimed in April 2017 that 15+ Saudi targets were hit in three attack waves
- Attackers had capability to exfiltrate data and conduct recon to further spread attack
- Use of DNS tunnelling and PowerShell scripts
- Indications of both Oilrig/APT34 and Rocket Kittens, believes that multiple groups may have collaborated

McAfee Event Flows:

'**Step 1.** Once a target is identified, the attackers send spear-phishing emails to individuals working within the organization. The recipients of these messages are chosen carefully, with the assumption that they will enable network access to the most sensitive information and systems in the organization.

Step 2. The email recipient is lured into clicking on a link within the email or opening a Microsoft Office file embedded with macros that allow the attackers to create backdoor access to the organizations.

Step 3. The attackers conduct reconnaissance across the network to identify valuable information and critical systems.

Step 4. Once the reconnaissance is complete, the attackers weaponize the attack and wipe the hard drives of the master boot records (MBRs). In the 2016 to present case, the attackers launched multiple simultaneous waves of attacks.'

Shamoon 3: 10 December 2018

On 10 December 2018, Shamoon 3 was reported to have attacked Saipem, an Italian-based energy sector engineering, drilling and construction company. Saipem's connection to several Gulf businesses makes it a strategic target for offensive CNA operations, particularly if disruption and or pivoting to target networks (supply chain attack) are the operational goals. The intervening years between Shamoon 2 and Shamoon 3 saw a deterioration of U.S./Iranian relations, due to the Trump Administration's policy of maximum pressure and repudiation of the JCPOA. Like Shamoon 2, Shamoon 3 did not target Arab countries during a significant Islamic or national holiday, though 10 December was a Sunday. However, the targeting dates of both Shamoon 2 and Shamoon 3 occurred towards the end of the year, 17 & 29 November 2016 and 23 January 2017 and 10 December 2018**.**

Relations in intervening years

- February 2017, Trump administration begins to reimpose sanctions that were relaxed during JCPOA
- 4 June 2017, Saudi Arabia, GCC, Qatar, Iran and Turkey dispute
- Several other sanctions follow
- The most interesting being the 14 September 2017 sanctioning of 11 entities with ties to the IRGC, technological innovation/R&D and cyber operations

- 13 October 2017 President Trump escalates rhetoric, including calling out proxy support, increased sanctions on the IRGC and a renegotiation/scrapping of the JCPOA
- First week of November saw Lebanese/Saudi PM Hariri resignation scandal
- 6 November 2017 rhetoric between Saudi Arabia and Iran escalates, including Saudi's blaming Iran and Hezbollah for Houthi missile strikes. Says Lebanon is declaring war. Iran blames Saudi's for suffering in Yemen etc.
- 18 May 2018, US officially withdraws from JCPOA

Relations immediately preceding the attack

Iran began to feel pressurised in December 2018, reacting with jingoistic behaviour meant to signal Iranian resolve and demonstrate Iranian capabilities:

- 4 December 2018, Iran begins testing MRBMs
- 4 December 2018, Rouhani escalates rhetoric, threating to disrupt SLOCs in Strait of Hormuz and moans about sanctions
- 6 December 2018, UNSC report
- Concerns over several missiles/drones launched at/in Saudi Arabia & Syria, particularly technology/weaponry transfers
- Flight tests (23 November) and MRBM launches (4 December)

Shamoon 3 added additional capabilities, such as the ability to wipe files and overwrite the MBR, as well as the use of PSExec, a legitimate program to execute commands, making Shamoon 3 technically capable of more disruption/damage then Shamoon 1 or 2.

- Saudi Arabia, UAE, and Italian oil services firm Saipem are hit
    - Up to 3-400 servers and 100 PCs affected
    - Attack originated in India and spread to Saipem networks in the Middle East, Aberdeen and Italy
- An additional wiper component, Trojan.Filerase, is now part of the malware
- Trojan.Filerase overwrites files on infected systems, amplifying the destructiveness of an attack by making files on a system unrecoverable
- The new variant conducts reconnaissance and compiles a target list of systems, distributes via OCLC.exe, and then passes to a second executable, Spreader.exe, which distributes Trojan.Filerase to systems on the initial targeting list
- Symantec witnessed PSExec being used to execute Shamoon, indicating prior recon including credential harvesting. PSExec has been used throughout the kill chain in several APT campaigns and has become increasingly popular in ransomware
- Symantec believes proximity to other attacks and targets connects Elfin/APT33 with Shamoon, but is unable to confirm the attribution

ZeroCleare & Dustman (Oilrig/Apt34)

ZeroCleare and Dustman are the fourth disk wiper campaigns to be attributed to Iran. Like the previous three Shamoon campaigns, ZeroCleare and Dustman appeared during the tail-end of prolonged escalatory behaviour between Iran, Arab, and Western states. By early December 2019, the US strategy of maximum pressure had eroded Iran's GDP by at least 14% in the previous two years, surpassing 2012 levels. Social unrest in Iran also increased to an intensity not seen since the 2011 Arab Spring protests. Like Shamoon 2 and 3, ZeroCleare and Dustman occurred near the end of the year but did not occur on specific Islamic or national holidays. Another similarity is that the 32-bit version of ZeroCleare failed. During the 2012 Shamoon 1 attack, the reverse was true, with the 64-bit version malfunctioning. As in all three Shamoon attacks, ZeroCleare and Dustman overwrote the MBR and relied on an EldoS RawDisk Driver to deliver the payload.

A note on strategic intelligence

- The Dragos report conflates strategic intelligence with operational and technical intelligence
- They state that targeting BAPCO, a Bahraini asset, is only tenuously linked to Iran's strategic interests and that there is no hard evidence. While technical indicators support their claim, grey/hybrid operations have underpinned Iranian long-term strategic interests throughout the region since at least 2014, if not the last two decades
    - This proved especially true through the last year, during which several states industrial and energy infrastructure has been targeted in espionage, sabotage and kinetic attacks. Bahrain is dependent on the Strait of Hormuz, is part of the GCC, is the home of the US Fifth Fleet, and has a Shia majority which has focused on social unrest in the past few years. If the Iranians wish to destabilize global energy prices, strike at US or Saudi allies, create fissures in the Saudi, US GCC alliance or demonstrate capabilities to reintroduce deterrence or use as leverage in future diplomatic negotiations, then Bahrain is most certainly a strategic target

Relations around the attack

- ZeroCleare alert overlaps in the heat of Gulf Crisis (September 2019)
    - Abqaiq, Tanker Seizures (See xHunt), US cyber retaliation, Red Sea strikes
- Region wise, 29 December (date of Dustman) saw an escalation in Iraq and Syria, with US conducting airstrikes against Kaitab Hezbollah, an Iranian proxy (the time of detonation is unclear, but the 'urgency' of Dustman's deployment is interesting if it overlaps with the beginning of US airstrikes)
- 22 June 2019 DHS director warns of Iranian cyber escalation, especially targeted wiper attacks
- 6 January 2020 DHS CISA/US-CERT warns of potential retaliatory cyber behaviour by Iran after Soleimani strike, including DDoS, wipers and potential force multiplier for a kinetic attack

Technical details

- ZeroCleare technical report released January 2020 (Disk Wiper) (Oilrig/APT34)
- Blog first released 4 December 2019
- First alert released on September 2019
- The technical report and blog indicate a mid-2018 campaign start date
- Initial access was likely accomplished in autumn of 2018
    - Speculative thinking/questions: initial access occurred mid-2018, Shamoon 3 occurred at the end of 2018. Is there unreleased information showing infrastructure overlap? Was Shamoon 3 recon and targeting used to deploy ZeroCleare? Were Shamoon 3 footholds in target networks utilised to deploy ZeroCleare?
- ZDNet believes that ZeroCleare was first seen in the wild in September 2019
- The technical paper and blog indicate that one IP address overlaps with another Iranian campaign from a likely different Iranian threat actor (193.111.152[.]13)
- The technical paper and blog indicate that an adjacent IP address linked to xHunt was used several months before the xHunt campaign (194.187.249[.]102) to ZeroCleare (194.187.249[.]103)
- MISP does not have either IP address. Few AV companies on VT mark the IPs as malicious at time of reporting
- The technical paper and the blog indicate that Turla had access to Oilrig tools and infrastructure during the campaign period
- IBM describes the campaign as targeting the Middle Eastern energy & industrial sector with destructive disk wiping attacks
- Has similarities with Shamoon in targeting and TTPs. Such as:

        - Overwriting Master Boot Record (MBR) & Disk Partitions
        - Using EldoS RawDisk Driver to deliver payload
    - ZeroCleare was designed for both 64-bit and 32-bit systems
        - The 32-bit version failed
    - Infection Flow (IBM)
        - Soy.exe (modified Turla Driver)
        - Saddrv.sys (vulnerable signed VirtualBox Driver) delivered by soy.exe
        - Unsigned EldoS RawDisk Driver (64-bit) delivered by saddrv.sys to get around Windows Driver Signature Enforcement (DSE)
        - Clientupdate.exe (ZeroCleare Wiper Payload) delivered by EldoS
    - PowerShell used to spread to domain controllers and Active Directory, then identified systems and created target lists to execute ZeroCleare
    - EldoS Raw Disk had a legitimate license key
    - Initial compromise and destructive phase consisted of brute forcing passwords in order to network accounts
        - Mimikatz
        - TwoFace/SEASHARPEE
        - Teamviewer
    - Overlap of tools with Oilrig/APT34 and the China Chopper web shells
    - IBM believes TTPs and IOCs also overlap with xHunt and Oilrig's Tortoiseshell campaign
    - Timeline of the campaign is undefined and too long to make judgements on geopolitical triggers or motivations. However, several geopolitical events throughout the region and timeline present in other campaigns overlap with ZeroCleare's targeting and strategic direction

- **Dustman 29 December 2019 (Sunday) detonation date (Disk Wiper) (ZeroCleare Variant)**
    - New variation of ZeroCleare disk wiper analysed by Saudi National Cyber Security Centre (NCSC), National Cybersecurity Authority (NCA)
    - NCA describes 'urgency' in perpetrating the attack, due to several OPSEC failures
    - Relies on EldoS RawDisk to bypass as in ZeroCleare
    - Kill Chain (NCA)
        - 'Initial Access, remote execution vulnerabilities in VPN appliance
        - Lateral Movement: Credential Harvesting and anti-virus management console service account
        - Weaponisation: compiling threat actor infrastructure minutes before an attack, anomaly
        - Instalment: copying malware through PsExec
        - Execution: executing set of commands through anti-virus management control to distribute malware to networked machines through PsExec, which executed and dropped three files, the two drivers and wiper
        - Covering Tracks: logging into VPN and deleted recent access logs, used a legit file deletion tool '
    - Differences with ZeroCleare
        - NCA believes Dustman is a new variant that is optimised
        - Dustman.exe is not the wiper, but drops the needed file on execution
        - All drivers, loaders and destructive capabilities are delivered with a single executable function; two were used in ZeroCleare
        - Dustman overwrites the volume, ZeroCleare wipes the volume by overwriting it with junk files
        - Dustman wiper file named agent.exe

- 28 January Bloomberg article released detailing an early January ransomware wiper that targeted the ICS systems of the Bahrain Petroleum Company (BAPCO). Bloomberg claimed, with limited details, that 'Snake,' the ransomware/wiper, attacked ICS processes, especially GE products
    - This article conflates Snake/Ekans with Dustman and was single sourced by Israeli cyber security firm Otorio
    - Otorio is a relatively new cybersecurity company, helmed and staffed by former senior IDF officers
    - Otorio's blog, which presumably was foundational to the Bloomberg article, also lack's details and relies on initial information from @VK_Intel and @MalwareHunterTeam. The most interesting part of Otorio's blog is that the 'Snake' ransomware is an evolution of the MegaCortex ransomware strain, which can be located as incident 05/02/050/05/2019 in the Centre's database
- @Vk_Intel and @MalwareHunterTeam reported on a possible Dustman/Snake overlap in BAPCO on 09/01/2020
- By 01/28/2020 @VK_Intel & @MalwareHunterTeam had reassessed their initial assumptions and concluded that the Bloomberg article & Otorio's conclusions were wrong, and that Snake/Ekans ransomware and Dustman are separate entities
    - For detailed information on Snake ransomware SentinelLabs blog, VK_Intels company, has a good write-up (23/01/2020)
- Joe Slowick of Dragos also called into question the integrity of Bloomberg's and Otorio's reporting
- Slowick acknowledges impact on ICS, but insists that actual effects remain minimal
- Slowick also discounts the linking to Dustman and Iran, and maintains that Snake/Ekans is not a wiper, but a traditional ransomware
- Dragos goes into more detail about how Snake/Ekans are not related to Dustman (no tech/infrastructure overlap). The report is very good source of information but questions the sourcing, saying that the Saudi NCA, not Bahraini authorities reported on the incident, making it more likely that initial Dustman detonation was in Saudi Arabia, not Bahrain
- The report later goes on to say that either BAPCO experienced 'a prior' ransomware breach before being infected with Dustman or that various news sources are conflating Saudi reporting of Dustman with the BAPCO incident
- Conflation was initial assessment, as evidenced by a quick Google Search

Section 5: **Disruptive**

Threat actor classification

(6) State proxy: non-governmental actors operating in support of a nation state's policy objectives

(5) Criminal: actors operating in pursuit of financial gain

(4) Hacktivist: actors operating in support of political causes widely regarded as not being terrorist in nature

Assessment

Like Iranian disk wiper campaigns, disruptive Iranian cyber campaigns tend to be clustered around prolonged escalatory behaviour between Iran, Arab, and Western states. Disruptive attacks can be used as a force multiplier, such as the overlap of the deployment of Shamoon 1 and the second intense wave of targeted DDoS attacks in September 2012. When used alone, disruptive attacks are the least valuable of Iranian cyber capabilities, as more can be gained from deploying destructive and espionage malware. Disruptive attacks can also be used as cover for espionage operations.

24 March 2016 DOJ IRGC DDoS Indictment

On 24 March 2016, the US Department of Justice (DOJ) indicted several Iranian hacktivists for a prolific DDoS campaign that began in December 2011 and ceased in May 2013. At one point, the actors attempted to hack a US-dam's SCADA system. The campaign targeted dozens of US financial institutions across 176 days of attacks. The cost to US financial institutions in down-time, rebuilding, and mitigation efforts reached 'tens of millions of dollars.'

The threat actors behind the DDoS campaign are thought to have been proxies for and provided training to, the IRGC. The timing of the DDoS campaign aligns with prolonged escalatory behaviour between Iran, Arab, and Western states. The DDoS campaign began less than one year after the discovery of Stuxnet, less than one month after the discovery of the Stuxnet based Duqu, and intensified in September 2012 after the imposition of several US sanctions and the deployment of Shamoon 1. The targeting of US financial institutions, particularly after the imposition of sanctions, can be viewed as tactical retaliation. When combined with the Shamoon 1 attack on Aramco, whose energy production is another vital component of global markets, the two attacks become synergistic. Synergy between the DDoS campaign and Shamoon 1 indicates long-term strategic thinking that would require planning and direction by a central authority, such as a clandestine intelligence agency.

The targeting of critical national infrastructure exceeds most hacktivist goals and represents a major escalatory action. Likewise, targeting critical national infrastructure, in this case a dam, which is a countervalue target, further corroborates planning and direction from a central authority. The demonstration of capabilities that could lead to cyber physical destruction can be considered an important signal if the aggressor state wishes to introduce a new deterrent.

Relations around the attack

- 13 November 2011: Iran discovers Duqu, a variant of Stuxnet that is used to commit recon on ICS networks
- 8 December 2011: Iran releases footage of a recently 'hijacked' RQ-170 Sentinel Stealth drone
- 2012 saw at least 4 EO imposing sanctions on Iran, in addition to regular legislation (see Shamoon)
- 6 February 2012: saw sanctions against Iranian Central Banks
- April 2012: unclassified report on Iranian Missile testing and capabilities, including using space platforms as R&D for greater missile development
- 10 August 2012: H.R.1905 Iran Threat Reduction and Syria Human Rights Act of 2012 passed
- May 2013: Iranian elections see Ahmadinejad bowing out
- May 2013, DDoS campaign ends (de-escalation)
- 14-15 June 2013: Hassan Rouhani, a reformer, is elected as Iran's President

Technical details

- Two separate Iranian entities were indicted for long-term widespread targeted DDoS attacks against the financial sector and SCADA operations in the US. Both entities are alleged to have been directed by the Iranian government, particularly the IRGC and both sporadically targeted financial institutions from December 2011 to September 2012.

    From September 2012 to at least May 2013, the teams followed a pattern of targeting US entities between Tuesday and Thursday during US business hours. The attacks reached a height of 140GB per second
- 46 major US financial institutions were targeted in at least 176 days of attack, leading to tens of millions in lost revenue and mitigation expenses
- ITSec Team was active between December 2011 up to December 2012 and scanned the Internet for vulnerable website content management software, obtained access, obtained remote access and installed malware capable of committing 'remote script' DDoS attacks, creating a botnet. They then leased servers to act as Command & Control C2 and monitor attacks

- Mersad was a collective composed of Sun Army and Ashiyane Digital Security Team (ADST), active from at least September 2012 to May 2013. During this time, Mersad executed 150 days of DDoS attacks against 24 US financial institutions and also claimed to have penetrated NASA on 12 February 2012. It is believed that the group provided training to Iranian intelligence officers and built a botnet with servers based in the US, UK, and Israel. Mersad is also alleged to have perpetrated penetrations against Bowman Dam in New York, in which they attempted to control water levels and temp and gate controls (SCADA)

SamSam December 2015- July 2018 SamSam, SamSam indictment

The SamSam ransomware campaign was active from January 2016 to July 2018. Cyber crime is usually profit motivated, yet several unique circumstances elevate the SamSam campaign beyond traditional cyber crime. First, SamSam was highly successful, accruing just under $6m in criminal proceeds. Second, SamSam was one of the first ransomware campaigns to target critical national infrastructure, which accounted for 50% of the group's targeting profiles, as illustrated by a US indictment. Third, the indictment indicates that the SamSam perpetrators were of Iranian origins, carried out their ransomware campaign from Iranian territory and converted their ransom into Rial with Iranian-based Bitcoin exchanges. Finally, SamSam used legitimate tools such as PsExec, Remote Desktop Protocol (RDP) and Mimikatz, which Iranian APTs have leveraged in Shamoon, ZeroCleare & Dustman, DNSpionage, Leafminer and xHunt.

Although no direct connection between SamSam and the Iranian state exists, SamSam was likely allowed to persist in their criminal activity because their interests aligned with the state. A non-state actor targeting adversaries CNI with disruption and monetary loss is a cheap and deniable way to harass and degrade an rival's capabilities. Likewise, SamSam could be used as a cover for future Iranian espionage operations. Deploying SamSam after exfiltration or pre-discovery of malware can frustrate attribution, recovery, and mitigation attempts, and blur post-attack analysis regarding threat actor intent. SamSam can also be leveraged as a force multiplier in future Iranian escalation, as evidenced in the 2016 IRGC DDoS indictments. The conversion of profits into Rial on Iranian-based Bitcoin exchanges also helps substantiate the Centre's hypothesis in Threat Assessment Q3-Q4 2019 that adversarial nation states, not insurgents, are best positioned to exploit cybercriminal proceeds in Bitcoin.

4 January 2020 Defacement campaign

Iranian defacement campaigns have been prolific for years. Defacements are often random-seeming and pick obscure websites due to their lack of security. Iranian defacements usually occur for ideological reasons, especially after major events; the latest defacement campaign occurred days after the assassination of General Qassem Soleimani, leader of the IRGC-QF. Defacements are hard to attribute directly to states and sometimes defacers are not even ideologically aligned with the messages they are purporting to support.

- 3 January 2020: General Qassem Soleimani, leader of IRGC-QF and main influence behind regional insurgency movements, militias, terrorist organisations, and Iranian hybrid strategy, is killed in Iraq by US airstrike
- 4/5 January 2020: Iranian 'hacktivists' begin defacement campaign targeting US government and municipal websites, beginning with Federal Depository Library Program
- 7 January 2020: Texas state agency websites face up to 10,000 attempted compromises per minute, believed to be originating from Iran
- Vice Media claims that the defacers mentioned Ashiyane, likely referring to Ashiyane Digital Security Team (ADST)
    - ADST part of the IRGC directed Mersad that participated in a prolific DDoS campaign from 2011-2013 (after Stuxnet & sanctions) or the security forum of the same name
    - CISA and FBI Alerts

Section 6: **Espionage**

Threat actor classification

(7) State actor: agents of a nation state

Assessment

Most Iranian cyber operations deal with espionage, which usually are neither destructive nor disruptive. At times, espionage operations are designed as a force multiplier for kinetic attacks or diplomatic leverage, such as during the targeting of Kuwaiti shipping during the xHunt campaign or DNSpionage targeting of Lebanon's Ministry of Finance, likely for political leverage, in 2018. As in destructive and disruptive attacks, Iranian espionage operations are not connected to singular events. However, like most espionage organisations, there is a clear hierarchy and division of requirements into short term or tactical (xHunt targeting ships), mid-term or operational (Tortoiseshell) and long-term or geostrategic (DNSpionage and Leafminer) collection. Although Iranian espionage operations are wide ranging, Arabic states are predominantly targeted, as evidenced in every single major espionage operation surveyed. Iranian espionage operations often have overlaps or near overlaps in infrastructure, TTP use and targeting, despite the presence of several distinct groups. A good example is the use of DNS tunnelling and redirects in DNSpionage and xHunt. Another example is the use of watering hole websites, especially for credential harvesting, like in Leafminer, Tortoiseshell and xHunt. Duplicate efforts suggest a high level of coordination. More likely, these groups are in fact different units within the same agency that have been tasked with slightly different objectives. Iranian espionage groups often begin with distinct targeting and collection requirements which eventually widen. For instance, Tortoiseshell was initially tasked with supply chain attacks against Saudi ISPs. Shortly after the 14 September Abqaiq attack, Cisco Talos Intelligence discovered a watering hole website masquerading as a website looking to connect US service members with employment in the private sector. It is likely that Tortoiseshell was re-tasked after the Abqaiq attack to collect on US personnel, perhaps in order to gain a better picture of US military postures.

Technical and geopolitical details, timeline specific

- **Leafminer 25 July 2018 (1st observation early 2017)**
    - Lebanon, Saudi Arabia, Azerbaijan
        - 44 systems, with at least 809 targets, throughout Middle East, Egypt, Israel, Palestine, Lebanon, Saudi Arabia, UAE, Kuwait, Bahrain, Qatar, Afghanistan
        - Observed between early 2017 and July 2018
        - Does not mention specific targeting but mentioned three non-time specific DNS redirects functioning as water holing sits in Lebanon, Saudi Arabia and Azerbaijan. It is impossible to know what exactly page/organisation was redirected with URL lookups. Financial, Government, Petrochemical and shipping made up most targets
    - Lebanon
        - One of the watering hole websites redirected to what Symantec describes as an intelligence agency
        - Virus Total lookup of the domain (TLD) (gov.lb) comes back with a number of hits, the top two being Lebanon's Internal Security Forces (ISF) and the Ministry of Finance (MOF) public-facing websites. Both have portals for sign-ins, perfect for credential harvesting. Note the 6 November DNSpionage MoF targeting
    - Saudi Arabia
        - Saudi Arabia is less interesting, several health portals appear on Virus Total under the domain (TLD) (org.sa). Most have sign-in pages
    - Azerbaijan

        - Azerbaijani lookups on Virus Total indicate that the watering hole site belonged to a university. Two of the most prominent universities at the top of the search are Azerbaijan Technical University (AzTU) and a login page for ADA University
        - AzTU Special Processes and Technology provides technical military design and studies degree programs. Much of the rest of AzTU appears engineering-focused
        - The ADA (Diplomatic university in Azerbaijan) operates a student/staff login page, which may be used for credential harvesting
    - Watering hole websites
        - Compromised webservers
        - SMB Hashes exfiltrated (Credential Harvesting)
        - SMB credentials brute forced offline
    - Remote attacks
        - Malware Backdoor.Sogru
            - Remote access
        - Malware Trojan.Imecab
            - Persistent remote access
            - Guester.exe
            - Achieve persistence and ensure guest account remains available
        - Reflective loader DLLs
            - Used as payloads for shellcode
            - RDP
            - Fuzzbunch
        - Several off the shelf tools (LOTL) used for brute force, lateral movement and exfiltration (much more in total)
            - Mimikatz
            - THC Hydra
            - Sysinternals PsExec
            - Total SMB Bruteforcer
            - MailSniper
        - Custom Mimikatz OrangeTeghal
    - Scanned for Heartbleed (CVE-2014-0160)

- **DNSpionage (OilRig Overlap) (Leak) 27 November 2018**
    - United Arab Emirates
        - UAE law enforcement and telecommunication regulatory authority targeted
        - First observed 13 and 15 September 2018, Thursday and Saturday Islamic New Year long weekend
        - Second observation on 24 September 2018, two days after terrorist attack in Ahvaz, Khuzestan province. The next few days saw increased Iranian rhetoric, including videos threatening missile strikes on UAE and Saudi Arabia
    - Lebanon
        - Lebanon’s Ministry of Finance targeted on 6 November 2018
        - Highly contentious Lebanon’s elections were held in spring 2018. Hezbollah made significant gains and demanded better ministerial representation, deadlocking the government. By 19 December Ali Hassan Khalil was reconfirmed as finance minister in Lebanon. Khalil is an influential member of AMAL, a Shia political party aligned with both Iran and Hezbollah.
        - Second redirect on 14 November 2018 targeted Lebanon’s Middle East Airlines (MEA). MEA is the official airline of the president and presumably other government officials for international trips. On 12 December 2018, Prime Minister Saad Hariri was

present at the Lebanese Embassy in London, giving a talk on trade. The talks included an announcement of a $300m contract between MEA and Rolls Royce. Hariri is aligned with Saudis and was held in SA on a November visit in 2017, extracting a fake resignation for sharing government power with Hezbollah and meeting with Iranian officials.

  - DNS Exfiltration & redirection
  - Phishing websites distributing fake jobs
  - Malicious Office docs (Macros)
  - DNS & HTTP for communication
  - Let's Encrypt Certificates for DNS redirect websites
  - Email, social media, such as LinkedIn
  - Malware was a remote administration tool for exfiltration over DNS (JSON Files)

- **Karkoff, reported 23 April 2019 (DNSpionage evolution)**
  - First seen in April 2019. Timeline remains undefined
  - 21 April 2019 was Shab-e -Barat, an Islamic holiday that fell on the weekend
  - 22 April 2019 saw Trump administration announce end of oil exemptions on US sanctions for China, India, Japan, South Korea and Turkey
  - C2 server mimicked GitHub, alludes to DNSpionage previously mimicking Wikipedia, can fingerprint and perform other recon activities via WMIC and identifies user and computer name, OS, and platform
  - Karkoff can perform remote code execution via the C2, but isnot well obfuscated
  - During the leaks, it was discovered that some overlap exists between DNSpionage campaigns and OilRig

- **Tortoiseshell (OilRig tools but distinct) 18 September 2019 (See Q3-Q4 2020)**
  - Active from July 2018, last observation in July 2019
  - 11 organisations targeted, the majority of which were in Saudi Arabia. Two organisations saw the group achieve domain admin-level status with several hundred computers infected with malware.
  - Symantec believes that the ultimate goal of the campaign is to infect ISPs in order to commit supply chain attacks
  - Initial infection is unknown, possible webserver compromise
    - Webshell for webserver d9ac9c950e5495c9005b04843a40f01fa49d5fd49226cb5b03a055232ffc36f3
  - The malware gathers information about infected machines and runs even when a user logs in, meaning it likely gains domain-admin abilities and access to all networked machines
    - IP configuration
    - Running applications
    - System information
    - Network connectivity
    - Firefox data
  - Backdoor.Syskit
    - Backdoor and exe
    - -install
    - Reads config file
    - Writes base64 AES Encrypted
  - HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\policies\system\Enablevmd
    - Writes base64 to send C&C info

- HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\policies\system\Sendvmd
    - Send info to the C&C
- Backdoor
    - Kill_me (dllhostservice and deletes)
    - Upload (downloads from C&C URL)
    - Unzip (powershell to unzip files on specified location)
- Tools
    - Public
    - Infostealer/Sha.exe/Sha432.exe
    - Infostealer/stereoversioncontrol.exe
    - Get-logon-history.ps1
    - Poison Frog Oilrig tool also discovered, likely different threat actor
- On 24 September 2019, Cisco Talos discovers a watering hole website (hxxp://hiremilitaryheroes.com) where Tortoiseshell is observed setting up watering hole websites. The site prompts users to download an app that then uses same backdoors & tools and also installs a Remote Administrative Tool/Access Trojan (RAT)
        - IvizTech
        - Allows C2 to install modular malware
        - Uses same process as backdoor
    - Collects similar info such as
        - Date, time and drivers
        - Information on system
        - Patch level
        - Number of processors
        - Network configuration
        - Hard & firmware
        - Domain controller
        - Name of admin, account
- Cisco Talos believes that the site is meant to mimic hiringourhereos.org which is a site dedicated to finding veterans as well transitioning service members and active service member spouses employment.
- The campaign was described as recently discovered and was publicly released ten days after the Abqaiq attack (14/09/2019).
- The campaign targeted retired and transitioning service members and active service member spouses. This is important because intelligence agencies can use information about employment shifts, especially transitioning and active service member spouses to estimate likely troop and force structures/postures in a region.
    - On 16 September 2019 the Trump administration first officially attributed the attack to Iran
    - By 20 September the Pentagon had shifted 'a moderate number' of service members to Saudi Arabia
    - This number expanded to the low 3000s by 11 October 2019 to several air wings and missile batteries, including THAAD
    - On 20 September 2019 the US Department of the Treasury designated the Central Bank of Iran (CBI) and other Iranian financial institutions as facilitating terrorism, triggering sanctions under EO 13324. The sanctions extend to any domestic or foreign institution who facilitates business/transactions with the designated entities.
    - Several sanctions have been enacted, most can be found in this recent Congressional Research Services white paper and this Department of the Treasury

webpage. Sanctions have intensified after the 14 September 2019 Abqaiq attack. Especially those targeting Iranian oil export waivers and Iranian shipping networks

- For instance, on 4 September 2019, the US Department of Treasury expanded sanctions to several Iranian foreign and domestic shipping, port and bunkering facilities
- On 25 September 2019 several Chinese shipping firms, including COSCO, were sanctioned for transporting Iranian oil

- **XHunt 23 September 2019 first reporting**
    - Timeline of May-June 2019 with a secondary (pre) campaign 'mid-to-late 2018', with infrastructure overlap or similarities dating back to 2017
    - On 19 May 2019, the first Kuwaiti transportation and shipping industry is targeted
        - Sakabota and Hisoka, ISMAgent, Oilrig, MISP confirms DNSpionage (Palo Alto does not)
    - Backdoor tools used for HTTP and DNS tunnelling for C2 comms
    - Outdated method uses Exchange Web Services (EWS) and stolen credentials for C2 comms
        - Sakabota
        - Hisoka
        - Netero
        - Killua
    - Additional tools allow for backdoors to commit post exploitation activity
    - Uses Base64 for C2 communications and payloads
    - A second Kuwaiti organisation is targeted between 18-30 June 2019. The malware:
        - Scans for open ports, up and download files, take screenshots, find other networked systems, run commands and create RDP sessions.
        - Removes threat actor behaviour and obfuscates artefacts if a legitimate user logs in
        - Transfers tools to other systems via SMB
        - On June 30, both Hisoka and Killua use a third-party help desk to copy files to an additional system
    - On 10 October 2019, Unit42 discovers a second C2/domain activity distributing CASHY200, a PowerShell based backdoor
        - Activity began in September 2019
        - Similar activity has been found showing evidence of targeting Kuwaiti government organisations since spring 2018
    - On 4 December 2019, Unit42 released an xHunt 'Cheat Sheet' with tools, infrastructure and IOCs, likely developed for operators, describing the 'examples of commands needed for persistence, network reconnaissance, pivoting, credential dumping, general system and network data gathering, as well as data exfiltration and commands to configure the system to allow remote desktop protocol (RDP) sessions.'
    - Another Kuwaiti watering hole was reported on 27 January 2020, but was likely testing up to one year before operational use
        - Likely active between June and December 2019, the website injected HTML code into webpage likely to harvest credentials, targeting Kuwaiti shipping corporations
        - This data was then likely used to infiltrate other websites/organisations with legitimate credentials in order to install backdoors, RATs etc.
        - The webpage used DNS redirects which Palo Alto believes substantiates credential harvesting and hosted images on Hisoka C2 infrastructure
        - Passively harvested credentials through NTLM hashes

- One technique of capturing NTLM hashes includes using SMB protocol, the same protocol that WannaCry/NotPetya and NSA tools use (false positive theories)
- Used DNS redirects to target other Kuwaiti government and industry websites
  - DNS redirects overlap with Oilrig and other Iranian associated infrastructure
  - Palo Alto confirms that some of the DNS redirect infrastructure overlapped with DNSpionage, which MISP confirmed before Palo Alto
  - Used Let’s Encrypt certificates
- First targeting began on 19 May 2019, exactly one week after four fuel vessels were targeted in sabotage operations in the Gulf of Omen near Fujairah
- Second targeting occurred roughly one month later, 18-30 June, almost one week after two vessels were targeted with probable limpet mines
- May/June 2019 featured the advents of Ramadan (6 May -4 June) and Laylat al-Qadr (31 May) and also similar timing of the 2012 Shamoon attack
- Starting in July, Iran began seizing energy sector vessels traversing chokepoints throughout the region
  - 4 July 2019, the UK seized Iranian energy sector vessel near Gibraltar
  - On 19 July 2019, Iran seized the British tanker Stena Impero in the Strait of Hormuz in Omani territorial waters. The British-managed Liberian-flagged Mesdar was boarded and later released
  - On 31 July 2019, IRGC seizes Iraqi energy sector vessel in the Persian Gulf, alleging smuggling, confiscating and redistributing the fuel
  - On 7 and 16 September 2019, IRGC seized two vessels in the energy sector in the Strait of Hormuz, alleging fuel smuggling to the UAE
    - The seizures occurred days before and after the Abqaiq attack (14 Sept 2019)
  - On 31 December 2019 IRGC seized an unnamed energy sector vessel in the Persian Gulf, alleging smuggling, arresting 16 Malaysian crew members, and confiscating and redistributing the fuel