Report

Iranian Cyber-activities in the Context of Regional Rivalries and International Tensions

Author(s):
Baezner, Marie

Publication Date:
2019-05

Permanent Link:
https://doi.org/10.3929/ethz-b-000344841 →

CSS CYBER DEFENSE PROJECT

Hotspot Analysis:

Iranian cyber-activities in the context of regional rivalries and international tensions

Zürich, May 2019

Version 1

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zurich

ETH zürich

Authors: Marie Baezner

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css.info@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group Myriam Dunn Cavelty, Deputy Head for Research and Teaching, Andreas Wenger, Director of the CSS

Please cite as: Baezner, Marie (2019): Hotspot Analysis: Iranian cyber-activities in context of regional rivalries and international tensions, May 2019, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

Executive Summary

Targets:	Multiple industries, government institutions, Non-Governmental Organizations (NGOs)[1] in Western and Middle Eastern states and Iranian dissidents in Iran and abroad.
Tools:	Distributed Denial of Service[2] (DDoS), fake personas on social media for spear phishing and malware.
Effects:	Surveillance of Iranian opposition, economic costs due to destructive cyberattacks and DDoS attacks, low sophistication but efficient enough cyberattacks, Stuxnet as wakeup call for the international community, cyber-operations as asymmetrical warfare technique, proxy wars transposed to cyberspace, decrease of malicious cyber-activities after the signature of the Joint Comprehensive Plan Of Action (JCPOA) and Iranian actors conducting influence campaigns.
Timeframe:	From mid-2000s and still ongoing.

Iran is an important actor in the Middle East. The country stands out from its neighbors because of its history, economy and religion. Due to these differences, Iran's neighbors and parts of the international community see the Islamic Republic as a regional rival generating tensions in the region. With regard to cybersecurity, Iran is also an interesting actor, both as a target and as a threat actor. As a target, Iran discovered Stuxnet in its nuclear facility at Natanz in 2010 and is regularly targeted by the US and Israel. As a threat actor, Iranian Advanced Persistent Threats (APTs) regularly involve destructive and cyberespionage campaigns, including a recent online influence campaign in the US.

This Hotspot Analysis examines cyber-activities in relation to Iran within the context of regional rivalry and international tensions. The objective of this report is to understand the dynamics of these cyberspace activities in such complex settings.

Description

Due to regional rivalry and international tensions, Iran has engaged in multiple and diverse cyber-activities. While a majority of sources report on APTs that are nebulous and flexible entities with likely ties to the Iranian authorities, a minority also reports on actors targeting Iran. The majority of Iranian cyber-activities consists of espionage targeting various industries, government institutions, NGOs and Iranian dissidents. The goal of these campaigns is to gather information relevant to Iranian authorities. While other cyberattacks have had destructive characteristics in that they wiped hard-disk contents and rendered computers useless. Iranian APTs have used a mix of freely available, commercial and custom-made malware to compromise their targets and steal relevant information. Iranian patriotic hackers have also played a significant role in cyberspace, but their actions have been primarily limited to DDoS attacks. However, Stuxnet and Flame are evidence that the US and Israel have targeted the Islamic Republic.

Effects

The social effects of cyber-activities in Iran consist of control over internet content and the surveillance of opposition figures as part of governmental control over the information sphere. Iranian authorities strictly regulate websites that are accessible on Iranian territory by censoring websites judged to be contrary to Islamic values. Opposition figures' activities are also closely monitored on the internet.

Economic effects comprise the economic costs of the various cyberattacks attributed to Iranian APTs and patriotic hackers. Companies in the Middle East have had to replace damaged computers after destructive attacks, and US banks have had to bear the financial costs of DDoS attacks.

One technology effect concerns the low sophistication of Iranian APTs' cyberattacks, which has not prevented them from achieving their strategic goals. Another technological effect consists of the fact that Stuxnet constituted a turning point in cybersecurity in terms of awareness of cyber capabilities.

There were multiple effects of Iranian-related cyber-activities on the international level. First, Iranian authorities consider cyber-operations as tools for asymmetrical warfare. The Iranian government is aware that it cannot compete with the US or US allies in military terms, but cyber-operations give Iran the opportunity to harass its adversaries with limited risks of retaliation because of low barriers of entry and relative anonymity. Second, Iran fights proxy wars against its regional rivals in both the physical world and in cyberspace. Third, the number of malicious cyber-activities between the US and Iran diminished after the JCPOA was signed and increased again once the US withdrew from the agreement. This confirms that state-sponsored cyber-activities are related to events in the physical realm. Finally, Iranian APTs have been involved in online influence campaigns in the US mid-term elections to influence political opinion in favor of Iranian interests.

Policy Consequences

Policy recommendations focus on improving cybersecurity, sharing information on Iranian APTs, raising awareness of influence campaigns and monitoring US-Iran relations.

[1] Abbreviations are listed in Section 10.

[2] Technical terms are explained in a glossary in Section 9.

1 Introduction

Iran is a significant actor in the Middle East and also in cyberspace. Because of its history, economy, religion and political ambitions, Iran cannot be ignored as a regional power and is considered as a threat by its neighbors. While access to certain internet content is strictly controlled inside Iran, Iranian Advanced Persistent Threats (APTs)[3] have become infamous for targeting energy companies in neighboring countries with destructive malware[4] and cyberespionage campaigns. However, Iran is also known for being the target of highly sophisticated cyberattacks, the most famous being Stuxnet, which was jointly developed by the US and Israel.

This Hotspot Analysis analyzes cyber-activities in relation to Iran in the context of its regional rivalry with its neighbors and its relationship with the US, which has come under renewed strain. In this context, cyberattacks are instruments that states can deploy in case of tensions, whether to defuse heightened tension (e.g. Stuxnet), to harass, to spy on rivals and dissidents or as a warfare technique. Cyber-activities also enable weaker states to cause damage to more powerful states in asymmetrical warfare. The objective of this Hotspot Analysis is to better understand the dynamics of cyber-activities in regional rivalries and broader international tensions related to Iran.

Iranian-related cyber-activities are primarily focused on spear phishing and credential theft with occasional destructive attacks. These cyberattacks, which are relatively low-level, are rooted in the regional rivalry between Iran and its neighbors and in the tensions with the US. Additionally, while current open-source research suggests that Iranian threat actors are highly active, it is in reality more likely that Iranian systems are regularly targeted by Western states. Information on these latter cyberattacks is unfortunately very limited.

This Hotspot Analysis is organized in four sections. Section 2 gives an account of the historical and international context of Iranian cyber-activities and cyberattacks against Iran. The goal of the chronology in this section is to place cyber-activities relating to Iran within their political and historical setting.

Section 3 describes first some of the multiple actors involved in cyber-activities related to Iran. This section only examines the main APTs from Iran, the main Iranian patriotic hackers, and actors in the US and Israel. It details targets of cyber-activities related to Iran and shows that Iranian APTs have targeted Iranian opposition groups both in Iran and abroad, while also carrying out cyberespionage and destructive campaigns against companies in multiple states in the Middle East. Iranian APTs also conducted cyberespionage campaigns against industries, government institutions and Non-Governmental Organizations (NGOs) in Western states and in the Middle East. Finally, the section looks at tools and techniques used in the Iranian context. This section demonstrates that Iranian patriotic hackers used Distributed Denial of Service (DDoS) attacks, that Iranian APTs created fake personas on social media for spear phishing campaigns and used a mix of freely available, commercial and custom-made malware in their cyberattacks, and that Western actors used sophisticated malware against Iranian targets.

Section 4 examines the effects of cyber-activities at the national and international levels. The first subsection analyzes the effects of Iranian authorities' control over internet content and online surveillance of dissidents. The second subsection details the economic effects of destructive cyberattacks on energy companies and the economic effects of DDoS attacks. The third subsection examines the fact that Iranian APTs are not technically sophisticated but still manage to achieve their strategic goals. This subsection also looks at how the discovery of Stuxnet was a wakeup call for the international community. The final subsection looks at the effects of cyber-activities related to Iran on international relations. First, Iran considers cyberspace as a space for asymmetrical warfare against its regional rivals and its more powerful adversaries. Second, proxy wars between Iran and its regional rivals unfold primarily in the physical realm but are also transposed to cyberspace. Third, after the Joint Comprehensive Plan Of Action (JCPOA) between Iran, the US, China, France, Germany, Russia and the UK was signed in 2015, malicious cyber-activities between the US and Iran seemed to diminish but restarted after the US withdrawal. This change in malicious activities shows that cyber-activities evolve together with the development of relations between the two states. Fourth, Iranian APTs started to conduct online influence campaigns targeting US citizens. They copied Russian tactics and tried to influence political opinion in favor of Iranian interests.

Finally, Section 5 contributes some generic policy recommendations for mitigating the risks of being impacted by cyberattacks from the Iranian context. This section recommends that cybersecurity be improved, information about Iranian APTs be shared, awareness about Iranian influence campaigns be raised and US-Iran relations be monitored.

This Hotspot Analysis will be updated as new information concerning cyber-activities relating to Iran is published. The goal is to keep the Hotspot Analysis as accurate as possible. This report will also be integrated in a broader study comparing multiple Hotspot Analyses.

[3] Abbreviations are listed in Section 10.

[4] Technical terms are explained in a glossary in Section 9.

2 Background and chronology

Iran as a regional power plays a significant role in the Middle East. The Islamic Republic has geostrategic importance because of its proximity to the Strait of Hormuz, and its history, religion, culture and language differentiate it from the other countries in the Middle East and more specifically from Saudi Arabia, its regional rival. Iran supports Shia communities and organizations in the Middle East like Hezbollah in Lebanon and Shia opposition groups in Bahrain as well as regimes like the Syrian Alawites. US-Iran relations deteriorated after the Islamic revolution in 1979 and continued to worsen with Iran's development of a civilian and military nuclear program. Relations between Saudi Arabia and Iran remain strained, and the tensions between the two states increased after the JCPOA was signed (Mabon, 2018).

Iran was connected to the internet in 1992. The cyber realm was quickly integrated into the Iranian government's set of tools for surveilling dissidents both domestically and internationally. Iranian patriotic hackers also used cyberspace to promote the government's ideology and patriotic views. However, the discovery of the malware Stuxnet in Iranian nuclear facilities acted as a wakeup call and drove Iranian authorities to develop cyber capabilities for more sophisticated cyberattacks than website defacement and DDoS attacks.

The following chronology outlines the historical context of events affecting the relations between Iran, Saudi Arabia and the US, and these countries' main cyber-activities.

Rows colored in gray refer to cyber-related incidents.[5]

Date	Event
08.1953	British and US intelligence services organize a covert operation for a coup that overthrows Iran's Prime Minister Mossadeq and marks the return of the Shah.
09.1978	Iran's population starts to riot, strike and demonstrate after the Shah passes policies that disempower the clergy. The Shah imposes martial law to regain control.
01.1979	The Shah and his family flee Iran.
02.1979	Ayatollah Ruhollah Khomeini, the opposition clerical leader in exile, returns to Iran.
04.1979	After a referendum, Iran becomes the Islamic Republic of Iran and the Ayatollah Khomeini becomes its Supreme Leader.
11.1979	Islamic militants take 52 employees of the US embassy in Tehran hostage.
22.09.1980	The war between Iran and Iraq starts.
01.1981	The US embassy hostages are released.
07.1988	USS Vincennes mistakenly shoots down an Iranian airplane.
07.1988	The United Nations (UN) obtain a ceasefire agreement between Iran and Iraq.
09.1990	Iran and Iraq resume diplomatic ties.
1995	The US imposes economic sanctions on Iran for sponsorship of terrorism and the development of nuclear weapons (BBC News, 2018).
2000	The Iranian Cyber Army (ICA) conducts its first patriotic hacking activities (Cylance, 2014).
2001	Less than ten years after the first internet connection in Iran, the government starts its online surveillance program (Anderson and Sadjadpour, 2018).
29.01.2002	In his State of the Union address, US President George W. Bush includes Iran in the "axis of evil" along with the Democratic Republic of North Korea (DPRK) and Iraq for seeking to develop nuclear weapons (The Economist, 2002).
08.2002	The Iranian dissident group Mojahedin-e-Khalq[6] (MeK) discloses that the Iranian government is enriching uranium in the nuclear facility of Natanz (Anderson and Sadjadpour, 2018).
09.2002	Russian technicians start the construction of the first Iranian nuclear reactor in the nuclear facility of Bushehr against US objections.
02.2003	The Iranian government admits that it is enriching uranium in the Natanz facility. The International Atomic Energy Agency (IAEA) is allowed to visit the facility for the first time and continues to visit it on a regular basis (Davenport, 2016).

[5] A more detailed list of cyber-activities related to Iran can be found in Annex 1.

[6] MeK is also known as the People's Mojahedin Organization of Iran (PMOI).

11.2003	The Iranian government accepts stricter UN inspections of its nuclear facilities and announces the suspension of its nuclear program. The IAEA reports it has not found any evidence of Iran developing nuclear weapons.
04.2003	The IAEA reprimands Iran for not cooperating fully in inspections of nuclear facilities (BBC News, 2018).
2005	The blog of a former Iranian Vice-President is defaced by Iranian hackers associated with the Iranian government (Anderson and Sadjadpour, 2018).
05.06.2005	Mahmoud Ahmadinejad, Tehran's ultra-conservative mayor, wins the presidential elections.
08.2005	The Iranian government admits that it has resumed its nuclear program and asserts that it is intended for peaceful use. The IAEA reports no evidence of violation of the Non-Proliferation Treaty (BBC News, 2018).
2006	US President George W. Bush starts the development of Operation Olympic Games, which includes Stuxnet (Sanger, 2012).
08.2006	Iran fails to meet the UN Security Council's deadline for halting its nuclear development (BBC News, 2018).
09.2007	Israel conducts an airstrike on a Syrian nuclear site in the Deir ez-Zor region and uses cyberattacks to disable Syrian radars (Associated Press, 2011).
10.2007	The US imposes new sanctions on Iran (BBC News, 2018).
09.2008	Iranian patriotic hackers engage in defacement campaigns against Emirati websites after Emirati actors defaced the website of the Grand Ayatollah al-Sistani (Anderson and Sadjadpour, 2018).
09.2008	The UN Security Council unanimously accepts a new resolution demanding that Iran stop its nuclear program.
2009	Iranian authorities block Facebook and Twitter on their territory (Crowdstrike, 2018).
12.06.2009	Mahmoud Ahmadinejad is reelected, but his rival candidate challenges the election result. Opposition supporters subsequently launch the Green Movement and demonstrate in the streets. During the demonstrations, at least 30 people are killed and more than 1,000 arrested (BBC News, 2018).
12.2009	ICA disables Twitter's website in retaliation for the Green Movement.
2010	The Basij paramilitary force creates the Basij Cyber Council for conducting influence campaigns and controlling media online (Denning, 2017).
12.01.2010	An Iranian nuclear scientist is assassinated, allegedly by US and Israel intelligence services.
03.2010	The Iranian government takes credit for taking down human rights activists' websites (Anderson and Sadjadpour, 2018).
06.2010	Iranian scientists send a computer that keeps rebooting itself to VirusBlockAda, a Belarussian antivirus company. The company discovers Stuxnet on the computer, a highly sophisticated piece of malware later attributed to the US and Israel (Zetter, 2011a).
06.2010	The UN Security Council imposes a new round of sanctions on Iran because of its nuclear program (BBC News, 2018).
08.2010	The Iranian power plant of Bushehr delays the launch of its nuclear energy section due to unspecified problems, according to Iranian officials. Others suspect the plant to have been infected by Stuxnet (Collins and McCombie, 2012).
09.2010	Iranian officials admit that some personal computers of Bushehr employees have been infected by a computer virus.
11.2010	Iran completely stops its uranium enrichment at the nuclear plant of Natanz (Farwell and Rohozinski, 2011).
29.11.2010	An Iranian nuclear scientist is killed and another wounded in two different attacks allegedly organized by the US and Israeli intelligence services.

2011	The Green Movement officially ends its protests against the Iranian government in view of ongoing repression.
2011	IAEA inspectors involved in Iran accuse the Iranian government of tampering with and surveilling their electronic devices (Anderson and Sadjadpour, 2018).
2011	After repressing demonstrations, Syria falls into a civil war in which Iran is said to be a proxy actor (Fisher and Keller, 2011).
23.07.2011	Another Iranian nuclear scientist is shot dead in a targeted attack, allegedly organized by the US and Israeli intelligence services (BBC News, 2011).
09.2011	The Iranian government announces that the Bushehr nuclear plant has been connected to the Iranian electric grid (BBC News, 2018).
09.2011	Iranian hackers working for the Iranian government breach DigiNotar, a Dutch digital certificate authority. This hack enables the Iranian government to access specific certificates for spying on Gmail accounts (Anderson and Sadjadpour, 2018).
11.01.2012	Another Iranian nuclear scientist is assassinated in a bomb attack, allegedly organized by the US and Israeli intelligence services (Dehghan, 2012).
02.2012	Iranian authorities block access to Gmail, Google and Yahoo websites on their territory until October 2012 (Crowdstrike, 2018).
02.2012	US President Obama imposes new sanctions on Iran, including the exclusion of Iran from the SWIFT money transfer system (Gundert et al., 2018).
03.2012	Iranian authorities create the Supreme Council of Virtual Space to manage internet policy and regulation and develop an Iranian national internet (Crowdstrike, 2018).
04.2012	The Iranian Oil Ministry discovers a cyberespionage campaign in its network using the malware Flame (Anderson and Sadjadpour, 2018).
06.2012	An article in the New York Times confirms that Stuxnet was developed by the US as part of Operation Olympic Games (Sanger, 2012).
15.08.2012	Saudi Aramco, the Saudi national oil company, is targeted by cyberattacks with the Shamoon malware, wiping the contents of 30,000 computers. A group named Cutting Swords of Justice claims responsibility for the attack.
30.08.2012	The Shamoon malware hits the Qatari RasGas (Cylance, 2014).
09.2012	The IAEA reports that Iran is ramping up its nuclear production and obstructing the inspection of a military site (BBC News, 2018).
09.2012	Iran and the DPRK sign a technology cooperation treaty about sharing technology, including cyber technologies.
09.2012	A series of DDoS attacks called Operation Ababil targets US banks' websites through to January 2013. An Iranian group called Izz ad-Din al-Qassam claims responsibility for the attacks, while Iranian officials deny any involvement (Cylance, 2014; Perlroth and Hardy, 2013).
06.2013	Hassan Rouhani wins the presidential election (BBC News, 2018).
09.2013	The US Navy discovers that Iranian hackers got access to unclassified Navy computers (Cylance, 2014).
11.2013	The US, China, Russia, the UK, France, Germany and Iran start nuclear negotiations (Anderson and Sadjadpour, 2018).
01.2014	Iranian authorities announce that China will help Iran with the development of an Iranian national internet (Crowdstrike, 2018).
02.2014	Sands Las Vegas Corporation is targeted by a cyberattack that steals customers' information and probably also destroyed data. The attack is attributed to Iran and is said to be in retaliation for a statement by the company's CEO regarding a US nuclear attack on Iran (Pagliery, 2015a).
30.06.2015	The Iranian authorities present their sixth Five-Year plan, which includes some points focusing on developing cyber capabilities and infrastructures (Crowdstrike, 2018).
14.07.2015	Iran, the US, Russia, the UK, France and Germany sign the JCPOA. Iran agrees to reduce and limit its nuclear activities in exchange for the lifting of international economic sanctions.

01.2016	Relations between Iran and Saudi Arabia deteriorate after Saudi Arabia executes a leading Shia cleric and protesters in Iran set the Saudi embassy on fire. Saudi Arabia subsequently closes its embassy in Tehran.
16.01.2016	The UN declare that they are satisfied with Iranian progress in fulfilling the JCPOA and lift international economic sanctions (BBC News, 2018).
24.03.2016	The US Department of Justice indicts seven Iranians for their involvement in Operation Ababil (Anderson and Sadjadpour, 2018).
11.2016	The Shamoon malware returns in a new variant, Shamoon 2.0, which targets the Saudi transportation sector in two waves in November 2016 and January 2017 (GReAT, 2017; "Shamoon 2.0," 2016).
06.2017	The Islamic State in Iraq and Syria (ISIS)[7] claims responsibility for a coordinated attack on the Iranian parliament and the shrine of Ayatollah Khomeini that kills several people (BBC News, 2018).
03.2018	The US Department of Justice indicts nine Iranians involved in the Mabna Institute group, a group of hackers stealing academic credentials to access academic publications (Hassold, 2018).
08.05.2018	US President Trump announces that the US is withdrawing from the JCPOA. In response, Iran announces that it will increase its uranium enrichment capacities (BBC News, 2018).
05.2018	Cybersecurity experts notice an increase in Iranian hacking activities against US targets.
08.2018	Facebook announces the discovery of Russian and Iranian disinformation campaigns aimed at users in the US, Latin America and the Middle East.
10.2018	The head of the Iranian civil defense agency announces that new Stuxnet malware has been neutralized in Iranian networks (Center for Strategic and International Studies, 2018).
11.2018	The US Department of Justice indicts two Iranian individuals involved in the ransomware that targeted the city of Atlanta in March 2018.
04.11.2018	The US reinstates economic sanctions against Iran (Certfa Lab, 2018).
13.02.2019	The US Department of Justice indicts a former US Air Force intelligence officer and four Iranian nationals. The former officer is charged with espionage on the account of Iran, while the four Iranians are charged with cyber-operations against their former colleagues (Department of Justice, 2019).

[7] ISIS is also known as the Islamic State of Iraq and the Levant, the Islamic State and Daesh.

3 Description

This section describes the multiple actors involved in cyber-activities in relation to Iran, their targets, tools and techniques.

3.1 Attribution and actors

While state-actors have come to publicly attribute cyberattacks more commonly, and attributions of this kind are becoming more important, they remain a challenge. To be credible, attribution must be based on both technical evidence and on the "*cui bono*" (to whose benefit) logic. However, even well-evidenced attribution can be wrong, as perpetrators cannot be identified with absolute certainty and have been known to use techniques, tactics and procedures associated with other actors to confuse investigators by posing as different threat actors.

Moreover, this Hotspot Analysis is based on publicly available sources primarily in English such as academic journal articles, media and cybersecurity firms' reports. Most cybersecurity companies that publish reports on APTs and malware for marketing purposes are based in Western countries and tend to focus on non-Western threat actors. These reports therefore create a bias in the general overview of the cyberthreat landscape by overrepresenting non-Western threats. Given the current state of open-source research, this Hotspot Analysis can only be based on such reports. Readers must therefore keep in mind that the apparent imbalance between Iranian and other threat actors most likely does not reflect reality, and other actors, in this case primarily the US and its allies, are just as active as Iranian threat actors but are not addressed in cybersecurity reports.

There are numerous actors with links to Iran engaged in cyber-activities. They have been divided into four groups in this analysis. The first group is Iranian APTs and contains the greatest number of actors. The second group comprises Iranian patriotic hackers, who have been predominantly involved in website defacement campaigns. The third group consists of Western actors such as the ones behind Stuxnet and other sophisticated malware which targeted Iran. The fourth group consists of actors that do not fit into the other categories but are involved in cyber-activities relating to Iran.

Iranian APTs

Iranian APTs are numerous and difficult to figure out. The Iranian government and IRGC use these groups as proxies to obfuscate their involvement in cyber-operations. The structure of these APTs is difficult to grasp because some seem to be connected to each other (e.g. as they use the same malware or command and control infrastructure (C&C)) but at the same time appear to be clearly separate entities. Anderson and Sadjadpour (2018) explain that Iranian APTs are fluid entities that usually disappear once a cybersecurity company reports on them. Disclosed APT groups are dissolved, and their members are reallocated to other groups. These movements within and across APTs would explain both the similarities and differences among these entities. Gundert et al. (2018) report that the Iranian government and IRGC struggled to find personnel for cyber-operations that had not only the right technical skills, but were also aligned with the government in terms of ideology and religion. The Iranian government and IRGC therefore recruited loyal managers in charge of assigning tasks to contractors.

Gundert et al. (2018) report that more than 50 contractors conducted cyber-operations for the Iranian authorities. Most of the time, these organizations competed against one another for contracts, but they were at times also asked to collaborate on certain operations, with one contractor developing malware while another ran the operation. According to Gundert et al. (2018), these contractors were only paid once the objective of the operation was achieved. The use of contractors also explains the nebulosity of the Iranian APT landscape. In addition, academic institutions, such as Shahid Beheshti University and Imam Hossein University, also act as contractors for cyber-operations. Some of these institutions have been identified in various cyberattacks (Gundert et al., 2018).

However, the use of contractors presented disadvantages for Iranian authorities. Such groups tended to be less loyal to the government's ideology and were more difficult to control than loyalists (Gundert et al., 2018). It is therefore possible that some of these contracted groups got involved in cybercrime without the knowledge of the authorities and accidentally linked the Iranian government to their activities.

Due to the large number of Iranian APTs, only a sample is described in this subsection[8]. The five selected APTs were chosen because they present the most interesting behavior, technique and activities.

Helix Kitten

Cybersecurity experts believe that Helix Kitten[9] has been one of the most active Iranian APTs in recent years. Cybersecurity firms estimate that the group has been active at least since 2015. The group specializes in cyberespionage campaigns aligned with Iranian government interests, making it likely that Helix Kitten acts for Iranian authorities. Contrary to other Iranian

[8] A more detailed list of the Iranian APTs is provided in Annex 2 in Section 7.

[9] Helix Kitten is also known as APT34, OilRig, Crambus, Helminth, Clayslide, IRN2, Cobalt Gypsy and Twisted Kitten.

groups, Helix Kitten does not conduct cyberespionage on Iranian domestic targets. The group's primary targets are situated in the Middle East, but Helix Kitten has also targeted entities in Africa and in the US (Mandiant, 2018). The group uses primarily spear phishing messages to deliver their malware and tools. Like other Iranian APTs, Helix Kitten creates fake personas on social media to build trust among their spear phishing targets (Brewster, 2017a). The group is also known to reuse stolen data from previous campaigns in other campaigns (Mandiant, 2018). Helix Kitten stole a digital certificate from a US software company to digitally sign one of their malicious tools to get their victims' trust and avoid detection (Brewster, 2017b). While cybersecurity experts consider Helix Kitten's delivery technique to be rather basic, they admit that the group's tools were more sophisticated than those of other Iranian hacker groups (Lee and Falcone, 2018). Helix Kitten is also known to regularly and incrementally modify their tools to avoid detection. They have used tools leaked from the US National Security Agency (NSA) in addition to their own custom-made malware (O'Neill, 2018a, 2018b). ClearSky Cyber Security (2017), an Israeli cybersecurity firm, noticed an overlap in C&C and Internet Protocol (IP) addresses between Helix Kitten and Chafer, another Iranian APT group. Researchers from FireEye Inc, a US cybersecurity firm, also noticed that Helix Kitten used the same infection methods, and backdoor, and targeted the same sectors as APT39. However, the US cybersecurity firm stated that the two groups were most likely two different entities which possibly shared infrastructure or worked together (Hawley et al., 2019).

Flying Kitten

Flying Kitten[10] is an Iranian APT that likely started its activities around 2009-2010 as a patriotic hacking group under the name of AjaxTM. The group initially specialized in website defacement to demonstrate their hacking skills. Starting in 2012, the group got increasingly involved in politicized hacking and refocused on cyberespionage in late 2013 / early 2014. Flying Kitten's technical skills are not highly sophisticated, but the group uses its own custom-made malware and manages to bundle its malware with legitimate anti-censorship tools (Villeneuve et al., 2014). Flying Kitten primarily targeted Iranian individuals and defense contractors for cyberespionage. The group most likely dissolved after researchers from FireEye Inc. reported on it in 2014. Anderson and Sadjadpour (2018) point out that Flying Kitten and Rocket Kitten shared some similarities in terms of tactics, techniques and procedures, suggesting possible ties between the two groups. In addition, Flying Kitten targeted the same Kurdish organizations as Infy[11], another Iranian APT (Anderson and Sadjadpour, 2018). ClearSky Cyber Security stated that Flying Kitten could also be Charming Kitten (ClearSky Cyber Security, 2017). However, it remains unclear whether there are in fact direct links between Flying Kitten and the Iranian government. Anderson and Sadjadpour (2018) claim that this APT group has a direct relationship with the Iranian authorities, while Villeneuve et al. (2014) state that there is no evidence of such relationship.

Rocket Kitten

Rocket Kitten is an Iranian APT group that has been widely documented and is most likely state-sponsored. The group is said to have been active at least since 2011 but increased its activities in 2014 and 2015. Rocket Kitten conducts cyberespionage on individuals working in academic institutions, defense industries, government agencies, and media outside Iran. The group is not technically advanced, as its spear phishing emails are simply designed, and its malware is either repurposed off-the-shelf and / or commercial software or likely purchased from developers. However, Rocket Kitten compensates its lack of sophistication through persistence. The group is said to send spear phishing emails several times to the same victims and sometimes to even contact them by phone to gain their trust and encourage them to click on malicious links or download malicious attachments in emails (Anderson and Sadjadpour, 2018; Check Point Software Technologies, 2015; Pernet and Sela, 2015). Pernet and Sela (2015) state that the group is agile and tries to avoid detection by continuously updating its malware with new layers of encryption. Based on their observation of the online behavior of Rocket Kitten's members, Pernet and Lu (2015) report that the group's members are likely in contact with cybercriminals or conduct cybercrime activities in their spare time. While Rocket Kitten seems to be a rather distinct group, overlaps with other groups blur this specific distinction. The group shares C&C, malware source code and possibly members with Flying Kitten[12] (Guarnieri and Anderson, 2017a), but there are also similarities with Charming Kitten in terms of infrastructure, tools, targets and modus operandi (ClearSky Cyber Security, 2017). Researchers at ClearSky Cyber Security (2017) have also suggested that Rocket Kitten potentially shares ties with APT33.[13]

[10] Flying Kitten is also known as the Ajax Security Team.

[11] Infy is also known as Prince of Persia.

[12] Following Flying Kitten's disbandment after the FireEye report in May 2014, some of its members likely joined Rocket Kitten (Guarnieri and Anderson, 2017a).

[13] APT33 is also known as Magic Hound.

Charming Kitten

Charming Kitten[14] is an Iranian APT that has been active since at least 2014. The group is focused on long-term cyberespionage and specializes in developing complex networks of fake personas on social media and fake websites. Charming Kitten uses a mix of open-source and custom-made tools to infiltrate its targets' networks. The group's tools are described as not particularly sophisticated, but the group is persistent. Mandiant (2018), a cybersecurity firm that is now part of FireEye inc., claimed that Charming Kitten is well-resourced and most likely sponsored by the Iranian government, because developing and maintaining such complex networks of fake personas and websites requires significant resources. While the group is not considered technically sophisticated, it has shown some technical flexibility by developing malware for mobile phones and Mac computers (Guarnieri and Anderson, 2017b; iSightPartners, 2014). ClearSky Cyber Security (2017) states that Charming Kitten's infrastructure and modus operandi overlap with Rocket Kitten's. Furthermore, the group may have connections to APT33, the Iran Cyber Security Group (a patriotic hacker group) and Flying Kitten (Guarnieri and Anderson, 2017b; Lee and Falcone, 2017).

Shamoon Group

The Shamoon Group[15] is the actor that claimed responsibility for the Shamoon attack[16] on Saudi Aramco and RasGas in Qatar in 2012. Little is known about this group except that it performs occasional large-scale destructive cyberattacks. These attacks attract a lot of attention, and the group then disappears until the next wave of cyberattacks. Since 2012, the group has conducted and launched three waves of cyberattacks using Shamoon, each time modifying the malware to avoid detection.[17] The Shamoon Group targeted Saudi Arabian and Qatari energy companies in the first two waves but directed its latest wave of attack in 2018 at Saipem, an Italian oil and gas contractor and customer of Saudi Aramco. It remains unclear how the group managed to implant its wiper in their victims' networks, but it is possible that other Iranian actors stole targets' credentials and gave them to the Shamoon Group for their operations (Hay Newman, 2018). Some cybersecurity experts claim that the Shamoon Group could be APT33 or at least be connected to it (Ackerman et al., 2018).

Iranian patriotic hackers

The patriotic hacking ecosystem in Iran is as complicated as its APTs counterpart. There are many groups which officially act independently from the Iranian authorities, but the Iranian government has also openly encouraged these groups to launch cyberattacks against enemies of Iran (Denning, 2017). Some of these patriotic hackers appeared in the early 2000s and evolved over time, and some groups have disbanded while others remained. Cybersecurity experts have not considered these Iranian patriotic hackers to be technically sophisticated. This section depicts the two best-known groups[18]. Other states (e.g. Saudi Arabia, Yemen, Bahrain, Qatar) also have patriotic hackers who got involved in tit-for-tat defacement campaigns with Iranian patriotic hackers, but these activities are minor in comparison to cyberespionage and destructive cyberattacks. Therefore, these minor defacement campaigns will not be discussed in detail in this Hotspot Analysis.

The Iranian Cyber Army

The Iranian Cyber Army (ICA) is believed to have been created in the late 2000s and was active during the demonstrations of the Green Movement (Lukich, 2011). The ICA is known for defacing the websites of Twitter in 2009, of Baidu in 2010 and of Voice of America in 2011 (Denning, 2017). While the defacements attracted a lot of attention, they were not technically sophisticated and only caused relatively minor disturbance. The group also targets Iranian opposition websites and is believed to act for the IRGC (Denning, 2017; Gundert et al., 2018). ICA seems to share certain techniques, tools and procedures with some Iranian APTs. It is likely that some members of this patriotic hacking group later joined cybersecurity contractors hired by Iranian authorities or cybersecurity units within the Iranian government. Villeneuve et al (2014) state that it is not uncommon for patriotic hackers to evolve to cyberespionage after a phase of politicization.

The Cyber Fighters of Izz ad-Din al-Qassam

The Cyber Fighters of Izz ad-Din al-Qassam[19] is a group of patriotic hackers responsible for Operation Ababil. As part of this operation, the group launched massive DDoS attacks on websites of major US banks between 2012 and 2013. Operation Ababil was believed

[14] Charming Kitten is also known as Newsbeef APT, Newscaster and APT35.

[15] The Shamoon Group is also known as the Cutting Sword of Justice.

[16] The Shamoon attack will be developed in detail in section 3.3.

[17] However, it remains unclear if the same group is behind all the waves of Shamoon attacks or if it is a different group each time.

[18] A more detailed list of patriotic hacker groups can be found in Annex 2 in Section 7.

[19] The group is also tied to a cyber-operations contractor, the Nasr Institute, a contractor who was also involved in Operation Ababil and has most likely links to an Iranian APT called APT33 (Brewster, 2017c).

to have been launched in retaliation for new economic sanctions that the US imposed on Iran. The US intelligence community attributed Operation Ababil to the Quds Force, a special unit of the IRGC, but Iranian authorities denied any involvement (Nakashima, 2012; Perlroth and Hardy, 2013). While DDoS attacks were not technically sophisticated, the operation was described as one of the largest attacks at the time. However, US banks adapted their cyberdefense quickly, and the latest waves of attacks had limited effects on their websites (Anderson and Sadjadpour, 2018). In 2016, the US Department of Justice indicted seven Iranian hackers for Operation Ababil and the hack of a New York dam (Volz and Finkle, 2016).

Western actors

The high number of reports on Iranian actors in cyberspace creates a bias and obfuscates the fact that Western states regularly target Iranian networks. The US and Israel are on top of the list and are represented in this Hotspot Analysis. However, other states like France have also been reported to have infiltrated Iranian systems (Paganini, 2015).

USA

The most famous US cyber-operation against Iran was Olympic Games, which formed part of a larger campaign called Nitro Zeus. In Operation Olympic Games, the US developed several malware items, among them Stuxnet, which was discovered in 2010. The operation started in 2006 under US President George W. Bush and continued under US President Obama. The NSA worked on the operation together with the Central Intelligence Agency (CIA) and the help of Israeli intelligence. In preparation for Stuxnet, the US placed implants in Iranian computer networks. Flame, another well-known malware discovered in Iranian networks in 2012, was most likely one of these implants (Bamford and Weaver, 2013). Nitro Zeus formed part of Operation Olympic Games and continued in parallel to the nuclear negotiations when they started in 2013. Nitro Zeus prepared a contingency plan in case the negotiations failed. It planned for an offensive cyber-operation attacking Iranian networks with the aim to disable computers in the nuclear facility of Fordo, but also Iranian air defense, communications and power grids in the event of kinetic attacks (Sanger and Mazzetti, 2016).

Unit 8200

Unit 8200 is an Israel Defense Force (IDF) unit specialized in signal intelligence, cyber-operations and technological research and development. The unit is carefully shrouded in secrecy, and information about Unit 8200 is scarce. Its size is estimated to be 5,000 active members, but former active members remain reservists and continue to serve in the unit for three weeks every year (Behar, 2016). It is believed that Unit 8200 collected intelligence and hacked Syrian radars during Operation Orchard, which destroyed Syrian nuclear facilities in 2007. Also, Unit 8200 is believed to have collaborated with the CIA in the development and testing of Stuxnet (Behar, 2016; De Falco, 2012; Halliday, 2010). Iranian APTs regularly target Israel's institutions, but it can be assumed that the IDF unit 8200 also conducts regularly cyber-operations against Iranian targets.

3.2 Targets

Both Iranian APTs and patriotic hackers, and other states' APTs and patriotic hackers have conducted cyberattacks on a large variety of targets. In this Hotspot Analysis, these targets are divided into the following three categories: Iranian domestic targets, targets in the Middle East and other types of targets.

Iranian domestic targets

The majority of Iranian APTs target individuals and groups inside Iran. These domestic targets are primarily dissident, opposition and specific ethnic groups. Iranian APTs target these groups mainly for surveillance, blackmail or to use compromised accounts to target other victims. The goal of such surveillance is to keep control over these groups and to gather information on their structure and members. Sometimes Iranian security agencies use such surveillance to arrest dissident groups' members. Moreover, Iranian patriotic hackers target these groups' websites with defacement attacks that advertise pro-Iranian government messages. Cyberspace is only another sphere in which the Iranian security apparatus operates, while it also monitors the opposition in other forms of communications.

Anderson and Sadjadpour (2018) report that the various departments and ministries within the Iranian government spy on each other. They state that the IRGC has sent spear phishing emails to Iranian diplomats and monitored them. This type of practice shows the level of distrust among Iranian state institutions.

Middle East

Iranian APTs and patriotic hackers regularly target entities and government agencies in neighboring countries and more especially Saudi Arabia (e.g. Shamoon attacks). Targeting these types of targets makes sense for Iran, as it seeks to gather information on rivals' civilian and military activities. It is even more important for Iran to monitor Saudi Arabia, as both states are involved in proxy wars in Yemen and Syria.

Moreover, Saudi Arabia represents an easier target than the US for Iran, because the Saudi Arabian cybersecurity apparatus is less well developed. Therefore, Iran focuses the majority of its cyberattacks on Saudi Arabia. This can be seen as indirect retaliation for US actions (Anderson and Sadjadpour, 2018).

Cyberattacks in the Middle East target a wide range of entities. Iranian APTs tend to focus on strategically relevant targets such as aerospace, energy (primarily oil and gas), telecommunications and technology companies. In addition, APTs also target government agencies such as ministries of defense and foreign affairs.

Other targets

This category comprises all targets of cyberattacks related to Iran. Iranian APTs have targeted US NGOs, academics, media outlets, aerospace and technology firms and the Iranian diaspora around the world. In some cases, APTs stole data for reuse in other attacks, like the above-mentioned digital certificate, whereas in other cases they spied for political motives, to find compromising information or to look for information about data which targets could have on Iran.

3.3 Tools and techniques

There are various types of cybertools used in the context of Iranian cyber-activities. These range from highly sophisticated and specialized tools to publicly available tools. Iranian APTs tend to use a mix of publicly available, commercial and custom-made tools. Apart from Helix Kitten's tools, other Iranian APTs' custom-made tools tend to be rather unsophisticated. However, cybersecurity experts consider Iranian APTs' social engineering techniques to be advanced and complex.

Distributed Denial of Service (DDoS) attacks

Iranian patriotic hackers conducted DDoS attacks against various targets in the context of cyber-activities in Iran. The goal of DDoS attacks is to render the targeted website inaccessible by overloading it with internet traffic to disrupt and cause financial losses for the victims. Patriotic hackers involved in Operation Ababil against US banks used a malware that created botnets from networks of computers in data centers to reroute traffic to targeted websites (Perlroth and Hardy, 2013). Iranian actors also used DDoS attacks against targets in the Middle East. While these attacks usually attract a lot of attention, they have not been particularly sophisticated (Anderson and Sadjadpour, 2018).

Fake personas, social engineering and spear phishing

Many Iranian APTs use fake personas and websites to gain their victims' trust and lure them more easily toward spear phishing emails or websites containing malicious links. Charming Kitten has created more than 2,000 accounts on social media to support fake personas' networks and to make these accounts look more legitimate to their targets (iSightPartners, 2014). Some groups have even been known to call their victims to convince them to download malicious attachments or click on malicious links. While cybersecurity experts have underlined the lack of sophistication of Iranian APTs' tools and malware, they believe that Iranian APTs must be spending more resources on social engineering (Mandiant, 2018).

Iranian APTs use spear phishing as the primary delivery method for their malware. They usually send emails with an attachment containing a malicious macro that then downloads malware onto the target's computer. Alternatively, they send emails with a link to a cloud service, where the target is asked to download a file with a malicious macro, or to a fake login page to steal credentials. Iranian APTs are described as persistent and sometimes send several spear phishing emails to the same target to ensure that they will fall into their trap (ClearSky Cyber Security, 2015).

Malware

The range of malware found in the context of geopolitical tensions with Iran is large, from off-the-shelf, publicly available tools to highly sophisticated and highly target-specific malware and every option in between.

Iranian APTs' malware

Apart from some specific malware, cybersecurity experts have described most of the Iranian APTs' malware as unsophisticated. Indeed, Iranian APTs directly reuse publicly available malware, repurpose it, or copy code from other malware or open-source projects (e.g. Rocket Kitten repurposed commercial software for penetration-testing Core Impact Pro into the Ghole malware (Pernet and Sela, 2015)). Some Iranian APTs are more technically sophisticated and develop their own custom-made malware and modify it regularly to avoid detection (Lee and Falcone, 2018). The majority of Iranian APTs' malware is designed for espionage and credentials theft, but some also has destructive capabilities (e.g. Shamoon) (Hay Newman, 2018). Iranian APTs' lack of technical sophistication is most likely due to a lack of resources and expertise (Anderson and Sadjadpour, 2018). However, this lack of resources and maturity does not prevent Iranian APTs from achieving their goals.

Western malware

Malware from Western states, and more specifically malware developed by the US and Israel, is more sophisticated than Iranian malware. Its level of sophistication requires significant resources and knowledge about targets and their networks. Three of these very sophisticated malware products have been found in Iranian networks.

Stuxnet

Stuxnet[20], a very specialized piece of malware, was part of Operation Olympic Games already referred to above. It was designed to target Supervisory Control And Data Acquisition (SCADA) systems in the Iranian nuclear facility at Natanz. The malware disrupted the function of centrifuges to damage them beyond repair. This malware, which was discovered on an Iranian computer in June 2010, was developed by the US in partnership with Israel (De Falco, 2012; Zetter, 2011a).

Flame

Flame is an espionage malware discovered in May 2012 on computers of the Iranian Oil Ministry. Flame is a very complex malware designed to spy and steal documents. It can scan for specific documents, turn on the microphone and register conversations, scan for Bluetooth-enabled devices in the vicinity, and take screenshots. Flame shares two similarities with Stuxnet: an export function and the ability to spread via USB drives using the same vulnerabilities as Stuxnet. It is believed that Flame has infected more than 1,000 computers around the world, but was not specifically developed to target Iran (Zetter, 2012).

Duqu

Duqu is a trojan designed to perform reconnaissance on Industrial Control Systems (ICS). It was discovered on computers in Iran and Europe in 2011 but does not specifically target Iran. The malware contains a keylogger and is programmed to erase itself after 36 days on a system (Zetter, 2011b). Symantec and Kaspersky Lab stated that Duqu is very similar to Stuxnet and may have been developed by the same authors. However, Dell and Bitdefender disagreed on that statement. They argued that, just because both have similar features, it does not mean that they share the same source code (Brodkin, 2011). Carr (2016) argued that the author of Duqu could be Unit 8200.

[20] Stuxnet has been widely documented and will not be described in details in this Hotspot Analysis, for further information on Stuxnet, please see: Baezner, Marie; Robin, Patrice (2017): Hotspot Analysis: Stuxnet, October 2017, Center for Security Studies (CSS), ETH Zürich.

4 Effects

This section analyzes the effects of cyber-activities related to Iran. It examines the impact of online surveillance on Iranian society, the economic costs of destructive and DDoS attacks, and technological implications. Furthermore, this section looks at the effects of cyber-activities related to Iran on tensions between the US and Iran, on regional tensions, and on the Iranian nuclear agreement.

4.1 Social effects

At the social level, Iranian-related cyber-activities are focused on controlling internet content and domestic surveillance. Since the mid-2000s, Iranian authorities have increased censorship to decrease risks of Western influence. The Iranian government is worried that Western media might influence its people, an act that Iranian authorities consider to be part of cyber warfare (Anderson and Sadjadpour, 2018). The Iranian government established a Supreme Council of Virtual Space in 2012 to decide which internet websites should be blocked and to regulate policies regarding the internet. Websites (e.g. Facebook, Twitter and YouTube) judged to be blasphemous or violating Islamic values are blocked to the Iranian population (BBC News, 2012). This censorship also extends to opposition movements to prevent them from promoting their opinions and influencing the Iranian people. Censorship is also combined with disinformation campaigns aimed at discrediting opposition members (Crowdstrike, 2018). However, Iranian users often employ Virtual Private Networks (VPNs) and censorship circumvention tools to access blocked websites. As a result, authorities established the Iranian Cyber Police (FATA) in 2011 to both control internet usage and investigate cybercrime (Siboni and Kronenfeld, 2012). This police force uses software (e.g. Black Spider) to investigate accounts on Western social media and messaging applications. This internet monitoring has led to some arrests of individuals criticizing the government online or posting content judged contrary to Islamic values (Crowdstrike, 2016). In addition, all Iranian APTs, except Helix Kitten, target Iranian individuals with ties to opposition movements and minorities inside and outside Iran to gather information on them that then leads to arrests (Anderson and Sadjadpour, 2018).

Moreover, the Iranian government has dedicated some points of its sixth Five-Year Plan (2016-2021) to developing and improving cyber capabilities and infrastructures. Among these is the intensified

development of local online social networks and other platforms to create local solutions and offer alternatives to Western websites. In 2006, Iranian authorities launched a project to build their own national intranet, which would be easier to control and more difficult to infiltrate but also more arduous to implement and impractical to use for international communications (Stratfor Worldview, 2018). In 2014, Iran announced a cooperation with China, which also tightly controls internet content within its territory, in the development of a "National Information Network", a similar system of content control as the Chinese Great Firewall (Crowdstrike, 2016; Stratfor Worldview, 2018).

All of these online monitoring and surveillance measures are evidence of the Iranian government's determination to maintain its monopoly and narrative in the Iranian information sphere. Iranian authorities learned from the protests of the Green Movement in 2009, where protesters organized using social media and messaging applications. Since then, the Iranian government has adapted its surveillance of the internet and other means of communication, and increased repression to avoid a reoccurrence of such protests. Surveillance will most likely continue, and Iranian President Rouhani's government has significantly invested in the development and acquisition of technology to ensure control over communications (Auchard, 2017; Siboni and Kronenfeld, 2012).

4.2 Economic effects

Economic effects of cyber-activities relating to Iran concern economic losses from destructive cyberattacks and DDoS attacks. Both types of attacks generate significant costs for targets.

The first wave of destructive cyberattacks perpetrated by the Shamoon Group in August 2012 partially or entirely wiped the hard drives of more than 30,000 computers (approximatively three quarters of Saudi Aramco's computers) (Perlroth, 2012). These computers were useless after the attack and needed to be replaced, which caused additional costs for the company. Moreover, while the cyberattack did not affect Saudi Aramco's oil production, it did interfere with supply management, shipping and contracts with governments and private partners. Saudi Aramco was unable to communicate with partners or contractors, which slowed down the business for some time and caused additional economic losses. It took approximately five months for Saudi Aramco to get back to normal (Pagliery, 2015b). It was estimated that the cyberattack on this Saudi Arabian firm cost the company between US$10 million and US$100 million in damaged goods (Anderson and Sadjadpour, 2018). Based on this evaluation, the Shamoon attack on Saudi Aramco cost the economy more than the Sony hack by the Lazarus Group from The Democratic Republic of North Korea in 2014 (Pagliery, 2015b). After 2012, the Shamoon malware reappeared in 2016 and 2018, again causing significant damage. However, the estimated cost of these attacks remains unclear.

DDoS attacks are also costly for targets. For businesses, the estimated cost of DDoS attacks is US$22,000 per minute of website unavailability. This estimate only includes the direct economic losses for the target, but businesses also suffer in terms of reputation (NSFocus Inc., 2016). In Operation Ababil, which was launched in September 2012, Iranian patriotic hackers targeted major US banks with DDoS attacks in several waves until January 2013. The attacks disrupted access to the banks' websites and caused delays in banking operations (Nakashima, 2012). However, US banks were quick to apply countermeasures, and the final waves of DDoS attacks only had limited consequences. Operation Ababil was considered one of the largest DDoS attack at the time, larger than the one that hit Estonia in 2007 (Anderson and Sadjadpour, 2018; Perlroth and Hardy, 2013). It was estimated that banks were forced to spend approximately US$10 million to apply countermeasures to these DDoS attacks (Anderson and Sadjadpour, 2018), and the attacks may have cost approximately US$100 million worth of damage to one of the targeted US banks (Kovacs, 2013).

4.3 Technological effects

Low technical sophistication of Iranian APTs

Cybersecurity experts on Iranian APT groups agree on the fact that the majority of these groups are not technically advanced but still managed to steal credentials and spy on adversaries. Iranian APTs have mostly used a mix of publicly available and commercial tools and custom-made malware, sometimes reusing code found on hacker forums. The fact that these groups employ open-source tools is not something specific to Iranian APTs, as Indian and Pakistani APTs have also used freely available tools.[21] However, the difference between Iranian APTs and their South Asian counterparts lies in the Iranian groups' persistence and investments in delivery methods. Iranian APTs have not employed technically sophisticated methods, but have demonstrated a sustained effort to gain their victims' trust to induce them to download attachments or click on links in spear phishing emails. Iranian groups have also demonstrated the ability to reuse compromised emails or social media accounts to lure their targets. Creating fake personas on social networks and fake

[21] For more information on cyber-activities in the context of India's and Pakistan's regional rivalry, please see: Baezner, Marie (2018): Hotspot Analysis: Regional rivalry between India-Pakistan: tit-for-tat in cyberspace, August 2018, Center for Security Studies (CSS), ETH Zürich.

websites is not particularly technically advanced but requires a significant amount of resources and commitment. By offsetting their relatively limited technical sophistication with strong persistence, Iranian APTs have managed to achieve their strategic goals. They were able to steal information and destroy hard drives. Nevertheless, Anderson and Sadjadpour (2018) state that Iranian groups' cyber-operations have been more successful against domestic targets than against foreign ones. These researchers argue that Iranian domestic targets may be less aware of cyberthreats and less well protected than international targets. Anderson and Sadjadpour (2018) add that, while Iranian APTs managed to steal information from a variety of targets, these targets were not considered to be high-level (e.g. classified networks or critical infrastructure). Therefore, Iranian APTs' limited technical sophistication can be considered to be an obstacle for more daring strategic objectives.

Stuxnet as a turning point

Stuxnet acted as a wakeup call for the international and cybersecurity communities. Stuxnet was the first exposed example of a highly sophisticated offensive tool developed by a state. Until Stuxnet, reported state-sponsored cyberattacks were limited to DDoS attacks on strategic targets (e.g. DDoS attacks on Estonian banks in 2007 and DDoS attacks on Georgian websites in 2008). Stuxnet revealed to the international community that it was technically possible for actors with the requisite resources to develop such tools. This piece of malware was successfully deployed to infect the air-gapped network of the Natanz nuclear site. This particularity, among other sophisticated features of Stuxnet, demonstrated that air-gapped networks were no longer sufficient to protect critical networks. Finally, as Stuxnet spread to computers outside Iran and therefore became available in the wild, qualified software developers would have been able to reuse and repurpose its code for cybercrime activities or other malicious purposes (Collins and McCombie, 2012). However, Stuxnet has not been repurposed since its discovery in 2010. Neither have new versions of the malware appeared in the wild, most likely because zero-day exploits used by Stuxnet have since been patched and repurposing malware designed for such a specific target demands significant expertise and resources.

4.4 International effects

The international aspects of cyber-activities relating to Iran can be categorized into four elements. First, Iran uses cyber-operations as a tool in asymmetrical warfare against the US and its allies. Second, Iran uses proxies in cyberspace in regional conflicts in precisely the same manner as in the physical realm. Third, the signature of the JCPOA in 2015 had an impact on Iranian cyber-activities. Finally, Iran has engaged more actively in online influence campaigns with the objective of shaping political opinion in favor of its national interests.

Iranian use of cyber-operations as asymmetrical warfare technique

In cyber-operations, Iran has found a way to cause damage to more powerful military powers while limiting the risk of retaliation. Iran authorities are aware that the Iranian armed forces cannot obtain a comparative advantage over more powerful enemies such as the US through military action. In addition, cyber-operations are relatively cheap to set up and give plausible deniability to attackers. Consequently, cyber-operations provide an opportunity for Iran to inflict damage on its enemies while limiting the risk of retaliation. Similarly to the DPRK, the Iranian government understands that states targeted by cyberattacks are unlikely to respond with military intervention. Therefore, Iran benefits from the lack of clear norms on state-sponsored cyberattacks and plausible deniability to act with relative impunity in cyberspace. Unlike nuclear development, cyber-operations allow Iran to attract some international attention while containing the risk of economic sanctions (Park, 2016).

However, Iran's limited cyber capabilities have restricted the impact of its operations. Anderson and Sadjadpour (2018) underline the fact that Iranian APTs did not manage to infect critical infrastructures or confidential networks. This lack of capabilities also caused Iranian APTs to focus on easier targets such as US allies. If the Iranian APTs' intent was to indirectly inflict damage on the US, their cyberattacks missed their objective. However, if it was to attract the attention of the US and disrupt US allies in the Middle East, it seems that their goal would have been achieved.

Proxy wars with regional rivals in physical and cyber realms

Iran is involved in indirect wars with its adversaries in both the physical space in Syria and Yemen and in cyberspace. Iran's cultural and religious heritage differentiate the Islamic Republic from its neighboring Arabic countries. However, its military power, its size and its economy make Iran a regional power which is perceived as a threat by neighboring states. Some of Iran's neighbors seek the help of the US and hope that the presence of US bases will deter potential Iranian expansionist ambitions. Therefore, Iran and its regional rivals have transposed their physical fights to other places through proxy wars. In Syria, Iran supports Syrian President Bashar al-Assad, whereas

Saudi Arabia, UAE, Qatar[22], Bahrain and Jordan, led by the US, support the anti-Syrian government forces. Similarly, in Yemen, Iran supports the Houthi Movement against the Hadi government, which Saudi Arabia, UAE, and other Arabic countries support. This logic of proxy wars between regional rivals is also transposed to cyberspace. Iranian authorities are aware that the US's most important networks are well protected and difficult to infiltrate. Therefore, targeting less protected networks of regional rivals seems more attractive and likely to be successful for Iranian cyber-operations. Saudi Arabian networks have become regular targets of Iranian APTs. In addition to regular spear phishing and cyberespionage campaigns, Iranian APTs have targeted Saudi Arabian and Qatari oil and gas companies with destructive cyberattacks (e.g. multiple waves of the Shamoon malware). These cyberattacks are believed to be in retaliation for Stuxnet and Flame attacks on Iranian networks (Anderson and Sadjadpour, 2018).

However, this transposition of proxy wars to cyberspace presents several risks. First, an increased number of cyber-activities between Iran and its regional rivals increases the risk of escalation in the region. While these regional rivals conduct cyberattacks and cyberespionage against one another, their activities augment the risk of misperception in cyberspace: If a cyberespionage activity is perceived as a hostile act by the targeted state, tensions may escalate into a conventional conflict. Second, some of Iran's neighbors are US allies. If a cyberattack triggers an escalation in the physical realm, the US may be dragged into a conflict between Iran and its regional rivals.

The JCPOA and cyber-activities

Cybersecurity experts claim that Iranian cyber-activities against US targets decreased after the JCPOA was signed and increased after the US withdrew from the agreement. The discovery of Stuxnet reduced tensions in the region and created an opportunity for a diplomatic solution to the Iranian nuclear development. Negotiations started in 2013 after Iranian President Rouhani's election, and Iran, the US, the UK, China, France, Germany and Russia signed the Iran nuclear deal in July 2015. Cybersecurity experts confirm that Iranian cyber-activities against the US decreased after the signature of the JCPOA (Anderson and Sadjadpour, 2018). However, when US President Trump announced in May 2018 that the US was withdrawing from the Iran nuclear deal, cybersecurity experts were expecting a surge of Iranian cyber-activities against US targets. This increase did in fact materialize in November 2018, when Iranian APTs targeted US federal employees working on the reinstatement of economic sanctions on Iran (Certfa Lab, 2018; Perlroth, 2019). Crowstrike (2019) also stated that it remained unclear if the resurgence of the Shamoon malware in December 2018 was in retaliation for the reinstatement of US economic sanctions against Iran. Nevertheless, the decrease and subsequent resurgence of Iranian cyber-activities against the US demonstrate that cyber-operations are primarily linked to the political and international contexts.

Iranian international influence campaigns

Similarly to Iranian domestic influence campaigns, Iranian actors also conduct international influence campaigns promoting news and stories aligned with Iranian interests. Iranian actors have constructed complex networks of fake websites and social media personas to promote anti-Saudi Arabia, anti-Israel, pro-Palestinian stories and news on US policies in favor of Iran. These influence campaigns most likely serve the goal of swaying political opinion on issues related to Iran or Iran's regional rivals (Crowdstrike, 2019; FireEye Inc., 2018). The change to international influence campaigns is rather new for Iranian actors, though, who imitate Russian techniques by creating news websites and promoting Iranian narratives. However, their sophistication has not reached the level of Russian influence campaigns. Consequently, Iranian influence campaigns are easier to spot (Sanger, 2018). While Iranian online influence campaigns seek to support anti-Trump narratives, it does not seem that these online campaigns have managed to influence the outcome of elections. The influence campaigns fit in with the Iranian authorities' narrative of focusing on soft power to promote Iranian discourses (Crowdstrike, 2019). However, a link between these influence campaigns and the Iranian government has not been confirmed (Sanger, 2018).

[22] Interestingly, in the spring of 2017, Saudi Arabia and its allies isolated the state of Qatar on the grounds that it was financing terrorism. Qatar and Iran have increased their economic exchanges since in order to circumvent economic sanctions imposed on both states (Therme and Margueritte, 2019).

5 Policy Consequences

This section suggests some generic measures that states can implement to mitigate the risks of being impacted by malicious cyber-activities similar to the ones described in this Hotspot Analysis.

5.1 Improving cybersecurity

Cyber-activities observed in the context of Iranian rivalry with its neighbors and the West often started with spear phishing emails. Therefore, it is important to improve awareness of this infection vector. Campaigns to raise awareness of spear phishing would allow users to recognize spear phishing emails and messages. Users would then be less likely to click on malicious links or download malicious attachments without thinking about the possible consequences. This type of awareness campaign would be especially useful for users with access to sensitive information. State institutions and enterprises could establish standard procedures for responding to incidents of people identifying phishing emails. It is important that such procedures be communicated within institutions to ensure that employees are familiar with them. Relevant training should additionally be provided so that employees know how to identify and report phishing emails.

Because Iranian actors seem to be difficult to deter by public disclosure and / or public attribution, states should focus their mitigation on securing their systems.

5.2 Information sharing

The nebulous structure of Iranian APTs makes these groups difficult to define and track. Cybersecurity firms, industries and intelligence services should favor information sharing on these groups' techniques, tactics and procedures to ensure that information about any specific groups reaches potential targets. Furthermore, a better understanding of these APTs' structures could make it easier to design security measures against them, even when the groups are discovered and subsequently dissolved, and members disband to join other groups. The creation of sector-specific Information Sharing and Analysis Centers (ISAC) could help to spread information within economic sectors. ISACs could also assist smaller enterprises in raising awareness of specific threats in that sector. ISACs could also bring together public and private actors and help to improve public-private partnerships in cybersecurity.

5.3 Building awareness of Iranian influence campaigns

Iranian influence campaigns focusing on other states are a rather novel technique for Iranian actors and are still relatively easily recognized. However, they may become more sophisticated with time and more difficult to spot. Regulating news is a difficult task for democratic states, as it would infringe on free speech and be associated with censorship. While states should not try to build their own counter-propaganda narratives to Iranian online influence campaigns, they could raise awareness of the origin of news websites and expose disinformation and propaganda materials. Also, given that influence campaigns are problems that concern the whole of society, states could develop education programs to educate the population, enabling them to recognize influence campaigns and critically analyze news articles. Education programs and increased awareness of influence campaigns would help the population to build their own opinions about stories found on the internet.

5.4 Monitoring of US – Iran relations

The dynamic between the US and Iran in cyberspace is strained. Iranian destructive cyberattacks are often regarded as retaliation for Stuxnet. More recently, cybersecurity experts have considered it possible that the latest wave of the Shamoon malware was launched in retaliation for the reinstatement of US economic sanctions on Iran. While we have no information on current US actions against Iran in cyberspace, the US recently indicted several Iranian citizens. Tit-for-tat actions in cyberspace and in the physical realm increase risks of misperception in cyberspace and escalation of the situation into open conflict. States should monitor the situation between the US and Iran in cyberspace to avoid being impacted by a possible escalation. An escalation between the two countries could imply an increase in destructive cyberattacks such as Shamoon on US allies that Iranian APTs perceive to be easier targets than US networks. Therefore, by regularly monitoring the situation between the two states, other states and more particularly US allies can anticipate and prepare their systems against possible Iranian cyberattacks.

6 Annex 1

Non-exhaustive list of cyber-incidents related to Iranian geopolitical events.

B = Business, E = Energy companies, G = Government and government institutions, I = Iranian dissidents, M = Media (including social media), MIL = Military institutions, NGO = Non-Governmental Organizations, O = Others				
Date	**Victim(s)**	**Type of victim(s)**	**Alleged perpetrator**	**Technique / Tool**
2000	Websites	Unknown	Iranian Cyber Army (ICA) (Iranian patriotic hacker)	Patriotic hacking (most likely website defacement and DDoS) (Cylance, 2014)
2005	A former Iranian vice-president (dissident to Ahmadinejad's government)	I	Unknown	Website defacement (Anderson and Sadjadpour, 2018)
2005	Website of US Naval Station Guantanamo	MIL	Iran Hackers Sabotage (Iranian patriotic hacker)	Website defacement (Denning, 2017)
09.2008	Iranian websites	Unknown	United Arab Emirates (UAE) patriotic hackers	Website defacements (Anderson and Sadjadpour, 2018)
09.2008	UAE websites	Unknown	Iranian patriotic hackers	Website defacements (Anderson and Sadjadpour, 2018)
12.2009	Twitter	M	ICA (Iranian patriotic hacker)	Disabling access to Twitter website in Iran as retaliation for the Green Movement (Anderson and Sadjadpour, 2018)
01.2010	Baidu (Chinese search engine)	B	ICA (Iranian patriotic hacker)	Website defacement (Center for Strategic and International Studies, 2018)
03.2010	Human rights activists' websites	NGO	Iranian government	Made the website inaccessible with most likely DDoS attack (Anderson and Sadjadpour, 2018)
06.2010 (date of discovery)	Iranian uranium enrichment plant in Natanz	E/G	USA and Israel	Stuxnet (Nakashima, 2012; Zetter, 2011a)
07.2010	Baluchi minority in Iran	I	Unknown (most likely an Iranian actor)	Baluchi social media accounts used as watering hole for delivering malware (Anderson and Sadjadpour, 2018)
22.02.2011	Voice of America website	M	ICA (Iranian patriotic hacker)	Website defacement (Denning, 2017)
09.2011	DigiNotar	B	Iranian government actor	Stole certificate to get access to the content of Gmail accounts (Anderson and Sadjadpour, 2018)

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique / Tool
01.09.2011	Computers around the world, including in Iran	Unknown	USA and Unit 8200	Espionage (Carr, 2016; Zetter, 2011b)
2012	Computers of the IAEA	O	Parastoo (Iranian patriotic hacker)	Claims to have compromised computers (Crowdstrike, 2016)
03.2012	BBC Persian service	M	ICA (Iranian patriotic hacker)	Cyberattack (Center for Strategic and International Studies, 2018)
04.2012	Iran's Oil Ministry and other targets in the Middle East	G	Equation Group (USA)	Flame malware (Center for Strategic and International Studies, 2018; Cylance, 2014)
06.2012	Individuals in Iran, Israel and Afghanistan	Unknown	Madi group (Iranian APT)	Madi malware (GReAT, 2012a, 2012b)
08.2012	AT&T and Saudi oil companies' websites	E/O	Iranian actor	DDoS attack (Nakashima, 2012)
15.08.2012	Saudi Aramco	E/G	The Shamoon Group (Iranian APT)	Shamoon wiper (wiped data on 30,000 computers)(Cylance, 2014; GReAT, 2012c)
30.08.2012	Qatari RasGas	E/G	The Shamoon Group (Iranian APT)	Shamoon wiper (Cylance, 2014; Mills, 2012; Perlroth, 2012)
09.2012	US banks' websites	B	IRGC and / or Izz ad-Din al-Qassam hacker group	DDoS attack campaign called Operation Ababil; lasted until January 2013 (Center for Strategic and International Studies, 2018; Cylance, 2014; Perlroth and Hardy, 2013)
11.2012	Members of the International Atomic Energy Agency (IAEA)	O	Parastoo (Iranian patriotic hacker)	Website defacement or DDoS attack (Anderson and Sadjadpour, 2018)
2013	Iranian opposition websites	I	ICA (Iranian patriotic hacker)	Website defacement (Denning, 2017)
05.2013	Iranian military branch Basij	MIL	Unknown	(Center for Strategic and International Studies, 2018)
05.2013	US electric grid	E/G	Iranian and other hacker groups	Attempts to breach networks (Center for Strategic and International Studies, 2018)
09.2013	More than 300 academic institutions in Western countries	O	Mabna Institute group (Iranian APT)	Spear phishing to steal credentials (Hassold, 2018)
09.2013	US Navy unclassified computers	MIL	Cutting Kitten (Iranian APT)	Spear phishing and malware (Cylance, 2014)
2014	NewrozTV (Kurdish television channel)	M	Flying Kitten (Iranian APT)	Espionage (Anderson and Sadjadpour, 2018)

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique / Tool
02.2014	Eurasia Foundation (US NGO)	NGO	Flying Kitten (Iranian APT)	Espionage (Anderson and Sadjadpour, 2018)
02.2014	Sands Las Vegas Corporation	B	An Iranian hacker	Data theft and destruction of data (Pagliery, 2015a; Vijay, 2014)
04.2014	Israeli academic institution	O	Rocket Kitten (Iranian APT)	Espionage (Pernet and Sela, 2015)
04.2014	Israeli defense-industry-adjacent company	B	Rocket Kitten (Iranian APT)	Espionage (Pernet and Sela, 2015)
05.2014	EU defense-related institution	G	Rocket Kitten (Iranian APT)	Espionage (Pernet and Sela, 2015)
05.2014	US senior military personnel	MIL	Charming Kitten (Iranian cyber-group)	Fake personas and fake websites and IRC malware (Check Point Software Technologies, 2015; iSightPartners, 2014)
05.2014	US diplomatic personnel	G	Charming Kitten (Iranian cyber-group)	Fake personas and fake websites and IRC malware (Check Point Software Technologies, 2015; iSightPartners, 2014)
05.2014	Defense contractors in the US and Israel	B	Charming Kitten (Iranian cyber-group)	Fake personas and fake websites and IRC malware (Check Point Software Technologies, 2015; iSightPartners, 2014)
06.2014	EU government institution	G	Rocket Kitten (Iranian APT)	Espionage (Pernet and Sela, 2015)
06.2014	Israel Defense Forces (IDF)	MIL	Iranian actors	DDoS attack (Anderson and Sadjadpour, 2018)
07.2014	Israeli academic institution	O	Rocket Kitten (Iranian APT)	Espionage (Pernet and Sela, 2015)
08.2014	German government institution	G	Rocket Kitten (Iranian APT)	Espionage (Pernet and Sela, 2015)
08.2014	Israeli defense contractor	B	Rocket Kitten (Iranian APT)	Espionage (Pernet and Sela, 2015)
18.08.2014	Major Saudi oil company	E/G	Cutting Kitten (Iranian APT)	Espionage (Cylance, 2014)
23.08.2014	Major oil and gas companies in Qatar and Kuwait, ministries of foreign affairs in Persian gulf countries and an airline in UAE	B/E/G	Cutting Kitten (Iranian APT)	Espionage (Cylance, 2014)
09.2014	Israeli targets	Unknown	An Iranian APT	Spear phishing campaign delivering Gholee malware (Check Point Software Technologies, 2015; ClearSky Research Team, 2014)
09.09.2014	Major US universities	O	Cutting Kitten (Iranian APT)	Espionage (Cylance, 2014)

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique / Tool
11.2014	Israeli academic institution	O	Rocket Kitten (Iranian APT)	Espionage (Pernet and Sela, 2015)
12.2014	Israeli academic institution	O	Rocket Kitten (Iranian APT)	Espionage (Pernet and Sela, 2015)
2015	Telecoms and airlines in the Middle East	B/G	Chafer and Cadelle (Iranian APTs)	Malware infection to surveil end users (Symantec Security Response, 2015)
2015	Iranian industrial infrastructure	B/G	USA	Cyberattack (Anderson and Sadjadpour, 2018)
04.2015	Kurdistan Free Life Party (PJAK)	I/PP	Unknown	Malware designed to target the Kurdish minority in Iran (Anderson and Sadjadpour, 2018)
06.2015	Israeli academic institution	O	Rocket Kitten (Iranian APT)	Espionage (Check Point Software Technologies, 2015; Pernet and Sela, 2015)
06.2015	Expatriated Iranian professor	O	Rocket Kitten (Iranian APT)	Espionage (Pernet and Sela, 2015)
08.2015	US Department of Defense website	G/MIL	Remember EMAD (Iranian patriotic hacker)	Claims to have defaced the website but no evidence (Crowdstrike, 2016)
09.2015	US Department of Energy network	G	SOBH Cyber Jihad (Iranian patriotic hacker)	Claimed to have hacked the Department's network but no evidence (Crowdstrike, 2016)
10.2015	Saudi defense industry company	B	Helix Kitten (Iranian APT)	Spear phishing emails delivering the Helminth backdoor (Falcone and Lee, 2016)
11.2015	Emails and social media accounts of US President Obama's officials	G	IRGC	Hack (Center for Strategic and International Studies, 2018)
12.2015	Unknown websites	Unknown	Charming Kitten (Iranian APT)	Compromised websites to transform them into watering holes for delivering the BeEF malware (GReAT, 2016)
05.2016	Al-Elm, a Saudi Arabian communications and defense organizations	B/G	Helix Kitten (Iranian APT)	Hack (Brewster, 2017b; Lee and Falcone, 2018)
05.2016	Saudi Arabian financial and technology organizations	B	Helix Kitten (Iranian APT)	Hack (Brewster, 2017b; Lee and Falcone, 2018)
17.11.2016	11 Saudi Arabian businesses and government organizations	B/G	The Shamoon Group (Iranian APT)	1st wave of Shamoon 2.0 wiper (Bing, 2017; GReAT, 2017)
29.11.2016	11 Saudi Arabian businesses and government organizations	B/G	The Shamoon Group (Iranian APT)	2nd wave of Shamoon 2.0 wiper (Bing, 2017; GReAT, 2017)

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique / Tool
12.2016	Defense industries	B	Charming Kitten (Iranian APT)	MacDownloader malware (Guarnieri and Anderson, 2017b)
12.2016	Human rights advocate	NGO	Charming Kitten (Iranian APT)	MacDownloader malware (Guarnieri and Anderson, 2017b)
2017	Telecoms and airline companies in Israel, Jordan, UAE, Saudi Arabia and Turkey	B	Chafer (Iranian APT)	Spear phishing emails delivering malware, some being publicly available (Symantec Security Response, 2018)
01.2017	Defense organizations in Middle East	B	Cutting Kitten (Iranian APT)	Spear phishing campaign and use of fake personas on social media (DellSecureWorks, 2017)
01.2017	AI Squared	B	Helix Kitten (Iranian APT)	Theft of digital certificate to make Helix Kitten's malware look legitimate (Brewster, 2017b)
01.2017	Saudi Arabian firm National Technology Group	B	Helix Kitten (Iranian APT)	Spear phishing emails with PupyRAT (Brewster, 2017b)
01.2017	Egyptian firm ITWorx	B	Helix Kitten (Iranian APT)	Spear phishing emails with PupyRAT (Brewster, 2017b)
23.01.2017	11 Saudi Arabian businesses and government organizations	B/G	The Shamoon Group (Iranian APT)	3rd wave of Shamoon 2.0 wiper (Bing, 2017; GReAT, 2017)
04.2017	Iranian dissidents and activists	I	Charming Kitten (Iranian APT)	Targeting for surveillance prior to Iranian elections (Crowdstrike, 2018)
06.2017	Nearly 90 British members of parliaments' email accounts	G	Iranian hacker group	Hack (Center for Strategic and International Studies, 2018)
07.2017	Iraqi Kurds	O	Charming Kitten (Iranian APT)	Targeting for surveillance prior to a vote on independence (Crowdstrike, 2018)
08.2017	Western think tanks	O	Charming Kitten (Iranian APT)	Espionage (Crowdstrike, 2018)
11.2017	Engineering industry company	B	APT33 (Iranian APT)	Most likely for cyberespionage (Ackerman et al., 2018)
05.2018	Technology services providers in the Middle East	B	Helix Kitten (Iranian APT)	Espionage (Lee and Falcone, 2017)
05.2018	Government agencies in the Middle East	G	Helix Kitten (Iranian APT)	Espionage (Lee and Falcone, 2017)
06.2018	Entities in Bahrain and Kuwait	Unknown	Helix Kitten (Iranian APT)	Espionage (Meyers, 2018)

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique / Tool
26.06.2018	Middle Eastern government agency	G	Helix Kitten (Iranian APT)	Espionage (Lee and Falcone, 2017)
07.2018	Same engineering industry company as in 11.2017	B	APT33 (Iranian APT)	Attempt to enter the network (Ackerman et al., 2018)
07.2018	Industrial control systems in electric companies in USA, Europe, Asia and Middle East	E	Iranian hacker group	Attempts to enter the networks (Center for Strategic and International Studies, 2018)
08.2018	Same engineering industry company as in 11.2017 and 07.2018	B	APT33 (Iranian APT)	Attempt to enter the network (Ackerman et al., 2018)
09.2018	Iranian supporters of the Islamic State and Kurdish minority in Iran	I	Iranian hacker group	Surveillance campaign (Center for Strategic and International Studies, 2018)
09.2018	Middle Eastern government agencies	G	Helix Kitten (Iranian APT)	Spear phishing with OopsIE Trojan (O'Neill, 2018a)
10.2018	US political figures working on economic sanctions against Iran	G	Charming Kitten (Iranian APT)	Spear phishing campaign (Certfa Lab, 2018)
10.2018	Iran nuclear facilities	E/G	Unknown	Iran declared to have stopped a new Stuxnet attack (Center for Strategic and International Studies, 2018)
11.2018	Telecom customers in the Middle East	Unknown	Helix Kitten (Iranian APT)	Surveillance (Meyers, 2018)
11.2018	Iranian dissidents	I	Iranian hacker group	Surveillance campaign on Telegram and Instagram (Center for Strategic and International Studies, 2018)
12.2018	Saudi and Emirati oil companies	E	The Shamoon Group (Iranian APT)	3rd version of the Shamoon wiper (Hay Newman, 2018)
10.12.2018	Saipem (Italian Oil Company)	E	The Shamoon Group (Iranian APT)	3rd version of the Shamoon wiper (Hay Newman, 2018)

7 Annex 2

Table representing the main Iranian actors in cyberspace, their targets, their types of cyberattacks and their infection vectors.

X = Targets or uses, - = Does not target or does not use, ? = likely but unverified targets or uses

	Iranian actors	Targets											Types of cyberattack				Infection vectors			
		Energy	Aerospace	Finance	Telecom	Government	Defense organizations	Media	Academia	Critical infrastructure	Domestic opposition groups	Others	Defacement	DDoS attack	Cyberespionage	Data destruction	Watering hole	Phishing / spear phishing	Website vulnerabilities	Others (e.g.: USB drive)
APTs	Helix Kitten	X	X	X	X	X	-	-	-	-	-	-	-	-	X	-	-	X	-	-
	Cutting Kitten[23]	X	-	-	X	X	X	-	-	-	-	X	-	-	X	-	X	X	X	-
	Rocket Kitten	-	-	-	-	-	-	-	X	-	X	-	-	-	X	-	-	X	X	-
	Flying Kitten	-	-	-	-	-	-	-	-	-	X	X	X	-	X	-	-	X	-	-
	Magic Kitten	-	-	-	-	-	-	-	-	-	X	-	-	-	X	-	-	X	-	-
	Chafer	-	X	-	X	-	-	-	-	-	X	-	-	-	X	-	-	X	X	-
	Cadelle	-	X	-	X	-	-	-	-	-	X	-	-	-	X	-	-	?	?	-
	APT33[24]	X	-	-	-	X	-	-	-	-	-	X	-	-	X	-	X	X	-	-
	Charming Kitten	X	X	-	X	X	X	X	X	-	X	X	-	-	X	-	X	X	-	-
	Shamoon Group	X	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	X
	Copy Kitten[25]	-	-	-	X	X	X	-	X	-	-	X	-	-	X	-	X	X	X	-
	Static Kitten[26]	X	-	X	X	X	X	-	X	-	-	-	-	-	X	-	-	X	-	-
	APT39	-	-	-	X	-	-	-	-	-	-	X	-	-	X	-	-	X	-	-
	Mabna Institute Group[27]	-	-	-	-	-	-	-	X	-	-	-	-	-	X	-	-	X	-	-
	Madi[28]	-	-	X	-	X	-	-	-	X	X	-	-	-	X	-	-	X	-	-
	Infy	-	-	-	-	X	-	-	-	-	X	X	-	-	X	-	X	X	-	-
	IRGC	?	-	-	-	-	-	-	-	-	X	-	-	-	X	?	-	X	-	-
Patriotic hackers	Iranian Cyber Army	-	-	-	-	-	-	X	-	-	X	X	X	-	-	-	-	X	-	-
	Cyber Fighters of Izz ad-Din al-Qassam	-	-	X	-	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-
	IRGC	-	-	-	-	-	-	-	-	-	-	X	X	-	-	-	-	-	-	-
	Other Iranian patriotic hackers	-	-	-	-	-	-	-	-	-	X	X	X	-	-	-	-	-	-	-

[23] Cutting Kitten is also known as the Cleaver Team and Ghambar.

[24] APT33 is also known as Magic Hound.

[25] Copy Kitten is also known as Slayer Kitten and DarkHydrus.

[26] Static Kitten is also known as MuddyWater, Seedworm and TEMP.Zagros.

[27] The Mabna Institute is also known as Silent Librarian.

[28] Madi is also known as Mortal Kombat Underground Security Team.

8 Annex 3

Table representing the main Iranian APTs and patriotic hackers and their potential connections and / or overlaps.

X = is connected to or overlaps with, - = is not connected to or does not overlap with,
? = could be connected to or could overlap with but unverified

Is connected to / overlaps with	Helix Kitten	Cutting Kitten	Rocket Kitten	Flying Kitten	Magic Kitten	Chafer	Cadelle	APT33	Charming Kitten	Shamoon Group	Mabna Institute Group	Madi	Infy	IRGC	CopyKittens	Static Kitten	APT39	Iranian government	Hezbollah (Lebanon)	ICA	Iran Cyber Security Group	Basij Cyber Council	Ashiyane Digital Security
Helix Kitten	-	-	-	-	-	X	-	-	-	-	-	-	-	-	X	-	X	X	-	-	-	-	-
Cutting Kitten	-	-	-	-	-	-	-	-	-	-	-	-	-	?	-	-	-	-	-	X	-	-	-
Rocket Kitten	-	-	-	X	-	-	-	X	X	-	-	-	-	?	-	-	-	?	-	-	-	-	-
Flying Kitten	-	-	X	-	-	-	-	-	X	-	-	-	X	-	-	-	-	?	-	-	-	-	-
Magic Kitten	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	X	-	-	-	-
Chafer	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-
Cadelle	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
APT33	-	-	X	-	-	-	-	-	?	?	-	-	-	-	-	-	-	-	-	-	-	-	-
Charming Kitten	-	-	X	X	-	-	-	?	-	X	-	-	-	-	-	-	-	-	-	-	X	-	-
Shamoon Group	-	-	-	-	-	-	-	?	X	-	-	-	-	?	-	-	-	-	-	-	-	-	-
Mabna Institute Group	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Madi	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Infy	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	?	-	-	-	-	-
IRGC	-	?	?	-	-	-	-	-	-	?	-	-	-	-	-	-	-	-	-	-	-	X	X
CopyKittens	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Static Kitten	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
APT39	X	-	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Iranian government	X	-	?	?	X	-	-	-	-	-	-	-	?	-	-	-	-	-	-	X	-	-	-
Hezbollah (Lebanon)	-	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ICA (patriotic hackers)	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-	-
Iran Cyber Security Group (patriotic hackers)	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Basij Cyber Council	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-	-
Ashiyane Digital Security Team (patriotic hackers)	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-	-

9 Glossary

Advanced Persistent Threat (APT): A threat that targets critical objectives to gain access to a computer system. Once inside a network, it tries to remain hidden and is usually difficult to remove when discovered (Command Five Pty Ltd, 2011; DellSecureWorks, 2014).

Air-gapped network: A security measure that implies physical separation between a network and the Internet or other insecure local networks (Zetter, 2014).

Botnet or bot: Network of infected computers which can be accessed remotely and controlled centrally in order to launch coordinated attacks (Ghernaouti-Hélie, 2013, p. 427).

Centrifuge: A centrifuge is a cylinder with a rotating rotor into which uranium is fed in the form of isotopic gas. The goal is to use centrifugal force to separate heavier from lighter gas. The former becomes depleted and the latter enriched uranium (Institute for Science and international Security, n.d.).

Chinese Great Firewall: Legal and technical measures to control the flow of information and access to websites for internet users in China (Wired Staff, 1997).

Command and Control infrastructure (C&C): A server through which the person controlling malware communicates with it in order to send commands and retrieve data (QinetiQ Ltd, 2014, p. 2).

Distributed Denial of Service (DDoS): The act of overwhelming a system with a large number of packets through the simultaneous use of infected computers (Ghernaouti-Hélie, 2013, p. 431).

Internet Protocol (IP) address: A numerical address assigned to each device that uses the internet communications protocol, allowing computers to communicate with one another (Internet Corporation For Assigned Names and Numbers, 2016).

Internet Relay Chat (IRC) malware, Trojan, backdoor, botnets or rootbot: A set of scripts or executable code that connects to IRCs as clients to pass as a regular user to other IRC users (Satpathy, 2015).

Macro: Group of commands put together as one single command to run automatic command sequences (Microsoft, 2019).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012, p. 81).

Patch: Software update that repairs one or several identified vulnerabilities (Ghernaouti-Hélie, 2013, p. 437).

Patriotic hacking: Sometimes also referred to as nationalistic hacking. A group of individuals originating from a specific state engage in cyberattacks in defense against actors that they perceive to be enemies of their country (Denning, 2011, p. 178).

Proxy: In computing, an intermediate server acting in place of end-users. This allows users to communicate without direct connections. This is often used for greater safety and anonymity in cyberspace (Ghernaouti-Hélie, 2013, p. 438). They are also used in the physical realm when one actor in a conflict uses third parties to fight in their place.

Supervisory Control And Data Acquisition (SCADA): Computer programs used to control industrial processes (Langner, 2013, p. 9).

Spear phishing: A sophisticated phishing technique that not only imitates legitimate webpages, but also selects potential targets and adapts malicious emails to them. Emails often look like they come from a colleague or a legitimate company (Ghernaouti-Hélie, 2013, p. 440).

Trojan horse: Malware hidden in a legitimate program in order to infect and hijack a system (Ghernaouti-Hélie, 2013, p. 441).

Virtual Private Network (VPN): Private network within a public network that uses encryption to remain private (PCmag, 2016).

Watering hole attack: Attack where a legitimate website is injected with malicious code that redirects users to a compromised website which infects users accessing it (TechTarget, 2015).

Website defacement: Cyberattack replacing website pages or elements by other pages or elements (Ghernaouti-Hélie, 2013, p. 442).

Wiper: Feature that completely erases data from a hard disk (Novetta, 2016, p. 57).

Zero-day exploit / vulnerabilities: Security vulnerabilities of which software developers are not aware and which can be used to hack a system (Karnouskos, 2011, p. 2).

10 Abbreviations

APT	Advanced Persistent Threat
CIA	Central Intelligence Agency - USA
C&C	Command and Control infrastructure
DDoS	Distributed Denial of Service
DPRK	Democratic Republic of North Korea
FATA	Iranian Cyber Police
IAEA	International Atomic Energy Agency
ICA	Iranian Cyber Army
ICS	Industrial Control System
IDF	Israel Defense Force
IP	Internet Protocol
IRC	Internet Relay Chat
IRGC	Iranian Revolutionary Guard Corps
ISAC	Information Sharing and Analysis Center
ISIS	Islamic State in Iraq and Syria
JCPOA	Joint Comprehensive Plan of Action
MeK	Mojahedin-e-Khalq (Iranian dissident group)
NGO	Non-Governmental Organization
NSA	National Security Agency - USA
PJAK	Kurdistan Free Life Party
SCADA	Supervisory Control And Data Acquisition
UAE	United Arab Emirates
UN	United Nations
VPN	Virtual Private Network

11 Bibliography

Ackerman, G., Cole, R., Thompson, A., Orleans, A., Carr, N., 2018. OVERRULED: Containing a Potentially Destructive Adversary [WWW Document]. FireEye. URL https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html (accessed 07.01.19).

Anderson, C., Sadjadpour, K., 2018. Iran's Cyber Threat Espionage, Sabotage and Revenge. Carnegie Endowment for International Peace, Washington, DC.

Associated Press, 2011. Syria nuclear weapons site revealed by UN investigators [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2011/nov/01/syria-nuclear-arms-site-revealed (accessed 24.02.17).

Auchard, E., 2017. Once "kittens" in cyber spy world, Iran gains prowess: security experts [WWW Document]. Reuters. URL https://www.reuters.com/article/us-iran-cyber/once-kittens-in-cyber-spy-world-iran-gains-prowess-security-experts-idUSKCN1BV1VA (accessed 23.01.19).

Bamford, J., Weaver, M., 2013. NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us Into Cyberwar [WWW Document]. WIRED. URL https://www.wired.com/2013/06/general-keith-alexander-cyberwar/ (accessed 23.01.19).

BBC News, 2018. Iran profile - timeline [WWW Document]. BBC News. URL https://www.bbc.com/news/world-middle-east-14542438 (accessed 04.12.18).

BBC News, 2012. Iran's Supreme Leader sets up body to oversee internet [WWW Document]. BBC News. URL https://www.bbc.com/news/world-middle-east-17288785 (accessed 24.01.19).

BBC News, 2011. Iran: Scientist shot dead in Tehran [WWW Document]. BBC News. URL https://www.bbc.com/news/world-middle-east-14263126 (accessed 10.01.19).

Behar, R., 2016. Inside Israel's Secret Startup Machine [WWW Document]. Forbes. URL https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#599258bb1a51 (accessed 01.03.19).

Bing, C., 2017. Shamoon 2.0 and StoneDrill are separate campaigns, but target the same country [WWW Document]. Cyberscoop. URL https://www.cyberscoop.com/shamoon-stonedrill-kaspersky-iran-saudi-arabia/ (accessed 25.01.19).

Brewster, T., 2017a. With Fake News And Femmes Fatales, Iran's Spies Learn To Love Facebook [WWW Document]. Forbes. URL https://www.forbes.com/sites/thomasbrewster/2017/07/27/iran-hackers-oilrig-use-fake-personas-on-facebook-linkedin-for-cyberespionage/#12d220949af8 (accessed 16.01.19).

Brewster, T., 2017b. Inside OilRig -- Tracking Iran's Busiest Hacker Crew On Its Global Rampage [WWW Document]. Forbes. URL https://www.forbes.com/sites/thomasbrewster/2017/02/15/oilrig-iran-hackers-cyberespionage-us-turkey-saudi-arabia/#52632542468a (accessed 17.01.19).

Brewster, T., 2017c. Meet APT33: A Gnarly Iranian Hacker Crew Threatening Destruction [WWW Document]. Forbes. URL https://www.forbes.com/sites/thomasbrewster/2017/09/20/iran-hacker-crew-apt33-heading-for-destructive-cyberattacks/#53f5877e4a48 (accessed 22.03.19).

Brodkin, J., 2011. Spotted in Iran, trojan Duqu may not be "son of Stuxnet" after all [WWW Document]. Ars Tech. URL https://arstechnica.com/information-technology/2011/10/spotted-in-iran-trojan-duqu-may-not-be-son-of-stuxnet-after-all/ (accessed 23.01.19).

Carr, J., 2016. NSA, Unit 8200, and Malware Proliferation [WWW Document]. Medium.com. URL https://medium.com/@jeffreyscarr/nsa-unit-8200-and-malware-proliferation-dd6e075ce26e (accessed 23.01.19).

Center for Strategic and International Studies, 2018. Significant Cyber Incidents.

Certfa Lab, 2018. The Return of The Charming Kitten [WWW Document]. Certfa. URL https://blog.certfa.com/posts/the-return-of-the-charming-kitten/ (accessed 17.01.19).

Check Point Software Technologies, 2015. Rocket Kitten: A Campaign with 9 lives, Threat intelligence and research. Check Point Software Technologies.

ClearSky Cyber Security, 2017. Charming Kitten. ClearSky Cyber Security.

ClearSky Cyber Security, 2015. Thamar reservoir An Iranian Cyber-Attack campaign Against targets In The Middle East. ClearSky Cyber Security.

ClearSky Research Team, 2017. Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford [WWW Document]. Clear. Cyber Secur. URL

https://www.clearskysec.com/oilrig/ (accessed 07.01.19).
ClearSky Research Team, 2014. Gholee – a "protective edge" themed spear phishing campaign [WWW Document]. Clear. Cyber Secur. URL https://www.clearskysec.com/gholee-a-protective-edge-themed-spear-phishing-campaign/ (accessed 01.03.19).
Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. https://doi.org/10.1080/18335330.2012.653198
Command Five Pty Ltd, 2011. Advanced Persistent Threats: A Decade in Review.
Crowdstrike, 2019. 2019 Global Threat Report Adversary Tradecraft and The Importance of Speed. CrowdStrike.
Crowdstrike, 2018. 2018 Global Threat Report: Blurring the lines between statecraft and tradecraft. CrowdStrike.
Crowdstrike, 2016. 2015 Global Threat Report. CrowdStrike.
Cylance, 2014. Operation CLEAVER. Cylance.
Davenport, K., 2016. Timeline of nuclear Diplomacy With Iran [WWW Document]. Arms Control Assoc. URL https://www.armscontrol.org/factsheet/Timeline-of-Nuclear-Diplomacy-With-Iran#2006 (accessed 19.10.16).
De Falco, M., 2012. Stuxnet Facts Report: A Technical and Strategic Analysis. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.
Dehghan, S.K., 2012. Iran nuclear scientist killed in Tehran motorbike bomb attack [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2012/jan/11/iran-nuclear-scientist-killed (accessed 10.01.19).
DellSecureWorks, 2017. The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets [WWW Document]. Secureworks. URL https://www.secureworks.com/research/the-curious-case-of-mia-ash (accessed 06.12.18).
DellSecureWorks, 2014. Advanced Threat Protection with Dell SecureWorks Security Services. Dell Inc.
Denning, D., 2017. Following the developing Iranian cyberthreat [WWW Document]. The Conversation. URL https://theconversation.com/following-the-developing-iranian-cyberthreat-85162 (accessed 23.01.19).
Denning, D.E., 2011. Cyber Conflict as an Emergent Social Phenomenon, in: Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications. Holt and Schell, pp. 170–186.
Department of Justice, 2019. Former U.S. Counterintelligence Agent Charged With Espionage on Behalf of Iran; Four Iranians Charged With a Cyber Campaign Targeting Her Former Colleagues [WWW Document]. U. S. Dep. Justice. URL https://www.justice.gov/opa/pr/former-us-counterintelligence-agent-charged-espionage-behalf-iran-four-iranians-charged-cyber (accessed 01.03.19).
Falcone, R., Lee, B., 2016. The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor [WWW Document]. Paloalto Netw. URL https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/ (accessed 07.01.19).
Farwell, J.P., Rohozinski, R., 2011. Stuxnet and the Future of Cyber War. Survival 53, 23–40. https://doi.org/10.1080/00396338.2011.555586
FireEye Inc., 2018. SUSPECTED IRANIAN INFLUENCE OPERATION Leveraging Inauthentic News Sites and Social Media Aimed at U.S., U.K., Other Audiences (Special Report). FireEye Inc., Milpitas, CA, USA.
Fisher, M., Keller, J., 2011. Syria's Digital Counter-Revolutionaries [WWW Document]. The Atlantic. URL https://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/ (accessed 08.02.17).
Ghernaouti-Hélie, S., 2013. Cyberpower: crime, conflict and security in cyberspace, 1. ed. ed, Forensic sciences. EPFL Press, Lausanne.
GReAT, 2017. FROM SHAMOON TO STONEDRILL Wipers attacking Saudi organizations and beyond. Kaspersky Lab HQ.
GReAT, 2016. Freezer Paper around Free Meat Repackaging Open Source BeEF for Tracking and More [WWW Document]. Kaspersky Lab. URL https://securelist.com/freezer-paper-around-free-meat/74503/ (accessed 16.01.19).
GReAT, 2012a. The Madi Campaign – Part I [WWW Document]. Kaspersky Lab. URL https://securelist.com/the-madi-campaign-part-i-5/33693/ (accessed 11.12.18).
GReAT, 2012b. The Madi Campaign – Part II [WWW Document]. Kaspersky Lab. URL https://securelist.com/the-madi-campaign-part-ii-53/33701/ (accessed 11.12.18).
GReAT, 2012c. Shamoon the Wiper - Copycats at Work [WWW Document]. Securelist. URL https://web.archive.org/web/20120820041239/http://www.securelist.com/en/blog/208193

786/Shamoon_the_Wiper_Copycats_at_Work (accessed 07.12.18).
Guarnieri, C., Anderson, C., 2017a. Flying Kitten to Rocket Kitten, A Case of Ambiguity and Shared Code [WWW Document]. Iran Threats. URL https://iranthreats.github.io/resources/attribution-flying-rocket-kitten/ (accessed 08.01.19).
Guarnieri, C., Anderson, C., 2017b. iKittens: Iranian Actor Resurfaces with Malware for Mac (MacDownloader) [WWW Document]. Iran Threats. URL https://iranthreats.github.io/resources/macdownloader-macos-malware/ (accessed 16.01.19).
Gundert, L., Chohan, S., Lesnewich, G., 2018. Iran's Hacker Hierarchy Exposed [WWW Document]. Rec. Future. URL https://www.recordedfuture.com/iran-hacker-hierarchy/ (accessed 09.01.19).
Halliday, J., 2010. Stuxnet worm is the "work of a national government agency" [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency (accessed 01.03.19).
Hassold, C., 2018. Silent Librarian: More to the Story of the Iranian Mabna Institute Indictment. PhishLabs Blog. URL https://info.phishlabs.com/blog/silent-librarian-more-to-the-story-of-the-iranian-mabna-institute-indictment (accessed 5.12.18).
Hawley, S., Read, B., Brafman-Kittner, C., Fraser, N., Thompson, A., Rozhansky, Y., Yashar, S., 2019. APT39: An Iranian Cyber Espionage Group Focused on Personal Information [WWW Document]. FireEye. URL https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html (accessed 04.02.19).
Hay Newman, L., 2018. The Iran Hacks Cybersecurity Experts Feared May Be Here [WWW Document]. WIRED. URL https://www.wired.com/story/iran-hacks-nuclear-deal-shamoon-charming-kitten/ (accessed 07.01.19).
Institute for Science and international Security, n.d. What is a Gas Centrifuge? [WWW Document]. Inst. Sci. Int. Secur. URL http://exportcontrols.info/centrifuges.html (accessed 20.10.16).
Internet Corporation For Assigned Names and Numbers, 2016. Glossary [WWW Document]. ICANN. URL https://www.icann.org/resources/pages/glossary-2014-02-03-en#i (accessed 04.11.16).
iSightPartners, 2014. NEWSCASTER: An Iranian Threat Within Social Networks, Threat Scape Intelligence report. iSightPartners.
Karnouskos, S., 2011. Stuxnet worm impact on industrial cyber-physical system security. IEEE, pp. 4490–4494. https://doi.org/10.1109/IECON.2011.6120048
Kovacs, E., 2013. Official Says Chinese Hacking Operations Have Cost the US $2TN / €1.5TN [WWW Document]. Softpedia. URL https://news.softpedia.com/news/Official-Says-Chinese-Hacking-Operations-Have-Cost-the-US-2TN-1-5TN-370302.shtml (accessed 24.01.19).
Langner, R., 2013. To kill a centrifuge: a technical analysis of what Stuxnet's creators tried to achieve.
Lee, B., Falcone, R., 2018. OilRig Targets Technology Service Provider and Government Agency with QUADAGENT [WWW Document]. Paloalto Netw. URL https://unit42.paloaltonetworks.com/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/ (accessed 18.01.19).
Lee, B., Falcone, R., 2017. Magic Hound Campaign Attacks Saudi Targets [WWW Document]. Paloalto Netw. URL https://unit42.paloaltonetworks.com/unit42-magic-hound-campaign-attacks-saudi-targets/ (accessed 15.01.19).
Lukich, A., 2011. The Iranian Cyber Army [WWW Document]. Cent. Strateg. Int. Stud. URL https://web.archive.org/web/20130606084937/https:/www.csis.org/blog/iranian-cyber-army (accessed 23.01.19).
Mabon, S., 2018. Muting the trumpets of sabotage: Saudi Arabia, the US and the quest to securitize Iran. Br. J. Middle East. Stud. 45, 742–759. https://doi.org/10.1080/13530194.2017.1343123
Mandiant, 2018. MTrends 2018 (Special Report). FireEye Inc., Milpitas, CA, USA.
Meyers, A., 2018. Meet CrowdStrike's Adversary of the Month for November: HELIX KITTEN [WWW Document]. CrowdStrike Blog. URL https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/ (accessed 11.12.18).
Microsoft, 2019. Create or run a macro [WWW Document]. Microsoft. URL https://support.office.com/en-us/article/create-or-run-a-macro-c6b99036-905c-49a6-818a-dfb98b7c3c9c (accessed 21.01.19).
Mills, E., 2012. Virus knocks out computers at Qatari gas firm RasGas [WWW Document]. CNet. URL

https://www.cnet.com/news/virus-knocks-out-computers-at-qatari-gas-firm-rasgas/ (accessed 21.01.19).

Nakashima, E., 2012. Iran blamed for cyberattacks on U.S. banks and companies [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html?utm_term=.f37bfab0ef64 (accessed 11.12.18).

Novetta, 2016. Operation Blockbuster: Unraveling the long thread of the Sony attack. Novetta, McLean,Virginia, USA.

NSFocus Inc., 2016. Distributed Denial-of-Service (DDoS) Attacks: An Economic Perspective (Whitepaper). NSFocus Inc., Santa Clara, CA.

O'Neill, P.H., 2018a. A well-known hacking group is getting better at evading detection [WWW Document]. Cyberscoop. URL https://www.cyberscoop.com/oopsie-oilrig-iran-evading-detection/ (accessed 18.01.19).

O'Neill, P.H., 2018b. Well-known Middle Eastern hacking group keeps updating its arsenal [WWW Document]. Cyberscoop. URL https://www.cyberscoop.com/oilrig-bondupdater-palo-alto-technologies/ (accessed 21.01.19).

Paganini, P., 2015. Animal Farm APT and the Shadow of French Intelligence [WWW Document]. Infosec Inst. URL https://resources.infosecinstitute.com/animal-farm-apt-and-the-shadow-of-france-intelligence/#gref (accessed 08.02.19).

Pagliery, J., 2015a. Iran hacked an American casino, U.S. says [WWW Document]. CNN Bus. URL https://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html (accessed 11.01.19).

Pagliery, J., 2015b. The inside story of the biggest hack in history [WWW Document]. CNN Bus. URL https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html (accessed 21.01.19).

Park, D., 2016. North Korea Cyber Attacks: A New Asymmetrical Military Strategy [WWW Document]. Henry M Jackson Sch. Int. Stud. URL https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/ (accessed 16.02.18).

PCmag, 2016. Definition of: virtual private network [WWW Document]. PCmag. URL http://www.pcmag.com/encyclopedia/term/53942/virtual-private-network (accessed 25.04.17).

Perlroth, N., 2019. Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html (accessed 28.02.19).

Perlroth, N., 2012. In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html (accessed 07.12.18).

Perlroth, N., Hardy, Q., 2013. Bank Hacking Was the Work of Iranians, Officials Say [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html (accessed 11.12.18).

Pernet, C., Lu, K., 2015. Operation Woolen-Goldfish When Kittens go phishing (Research paper). Trend Micro, Irving, Texas, USA.

Pernet, C., Sela, E., 2015. The Spy Kittens Are Back: Rocket Kitten 2 (Research paper). Trend Micro and ClearSky Cyber Security, Irving, Texas, USA.

QinetiQ Ltd, 2014. Command & Control: Understanding, denying, detecting. QinetiQ Ltd.

Sanger, D.E., 2018. Mystery of the Midterm Elections: Where Are the Russians? [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2018/11/01/business/midterm-election-russia-cyber.html?rref=collection%2Fbyline%2Fdavid-e.-sanger (accessed 01.03.19).

Sanger, D.E., 2012. Obama Order Sped Up Wave of Cyberattacks Against Iran [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (accessed 23.01.19).

Sanger, D.E., Mazzetti, M., 2016. U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html (accessed 21.01.19).

Satpathy, R., 2015. IRC botnets have evolved to steal passwords and avoid detection [WWW Document]. Emsisoft. URL https://blog.emsisoft.com/en/15698/irc-botnets-have-evolved-to-steal-passwords-and-avoid-detection/ (accessed 14.03.19).

Shamoon 2.0 [WWW Document], 2016. . Counc. Foreign Relat. URL https://www.cfr.org/interactive/cyber-operations/shamoon-20 (accessed 10.01.19).

Siboni, G., Kronenfeld, S., 2012. Iran's Cyber Warfare [WWW Document]. Inst. Natl. Secur. Stud. URL https://www.inss.org.il/publication/irans-cyber-warfare/ (accessed 23.01.19).

Stratfor Worldview, 2018. For the Iranian Internet, It's High Speed, High Control [WWW Document]. Stratfor. URL https://worldview.stratfor.com/article/iranian-internet-its-high-speed-high-control (accessed 13.03.19).

Symantec Security Response, 2018. Chafer: Latest Attacks Reveal Heightened Ambitions [WWW Document]. Symantec Secur. Response. URL https://www.symantec.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions (accessed 30.11.18).

Symantec Security Response, 2015. Iran-based attackers use back door threats to spy on Middle Eastern targets [WWW Document]. Symantec Secur. Response. URL https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets (accessed 05.12.18).

TechTarget, 2015. watering hole attack [WWW Document]. TechTarget. URL http://searchsecurity.techtarget.com/definition/watering-hole-attack (accessed 29.11.16).

The Economist, 2002. George Bush and the axis of evil [WWW Document]. The Economist. URL http://www.economist.com/node/965664 (accessed 18.10.16).

Therme, C., Margueritte, L., 2019. Le Qatar et l'Iran face au blocus : une entente conjoncturelle [WWW Document]. Areion24News. URL https://www.areion24.news/2019/01/18/le-qatar-et-liran-face-au-blocus-une-entente-conjoncturelle/ (accessed 21.01.19).

Vijay, 2014. Biggest Las Vegas Casino Network hacked by Iranian Hackers [WWW Document]. TechWorm. URL https://www.techworm.net/2014/12/las-vegas-casino-network-hacked-by-iranian-hackers.html (accessed 25.01.19).

Villeneuve, N., Moran, N., Haq, T., Scott, M., 2014. Operation Saffron Rose (Special Report). FireEye Inc., Milpitas, CA, USA.

Volz, D., Finkle, J., 2016. U.S. indicts Iranians for hacking dozens of banks, New York dam [WWW Document]. Reuters. URL https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF (accessed 23.01.19).

Wired Staff, 1997. The Great Firewall of China [WWW Document]. WIRED. URL https://www.wired.com/1997/06/china-3/ (accessed 19.07.17).

Zetter, K., 2014. Hacker Lexicon: What Is an Air Gap? [WWW Document]. Wired. URL https://www.wired.com/2014/12/hacker-lexicon-air-gap/ (accessed 04.11.16).

Zetter, K., 2012. Meet "Flane" the massive spy malware infiltrating Iranian computers [WWW Document]. WIRED. URL https://www.wired.com/2012/05/flame/ (accessed 23.01.19).

Zetter, K., 2011a. How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History [WWW Document]. Wired. URL https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ (accessed 18.10.16).

Zetter, K., 2011b. Son of Stuxnet found in the wild on systems in Europe [WWW Document]. WIRED. URL https://www.wired.com/2011/10/son-of-stuxnet-in-the-wild/ (accessed 23.01.19).

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.