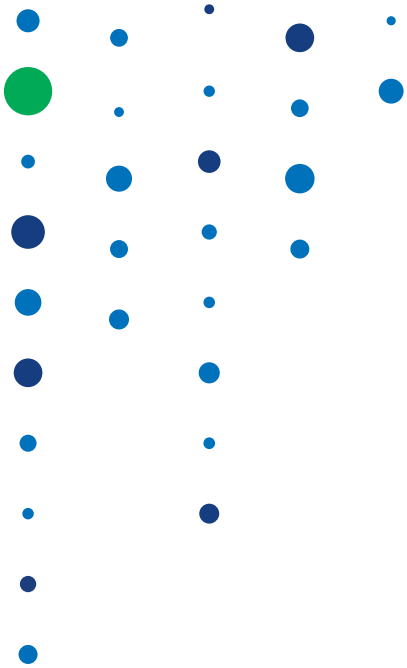
Recorded Future

CYBER THREAT ANALYSIS

Iran's Hacker Hierarchy Exposed

How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations

By Levi Gundert, Sanil Chohan, and Greg Lesnewich
Recorded Future



Scope Note: Insikt Group conducted interviews with a former Iranian hacker with first-hand knowledge of the information shared and was living in Iran when he started one of Iran's first security forums. This source's commentary forms the basis for the background on the genesis of Iran's offensive cyber efforts. Additional research was facilitated with Recorded Future and by leveraging third-party metadata and open source intelligence (OSINT) techniques using a variety of tools. While we address historical background and precedent in the piece, the technical analysis regarding organizations and institutes in Iran's offensive cyber program is based on data collected from March 1, 2018 to April 30, 2018.

Executive Summary

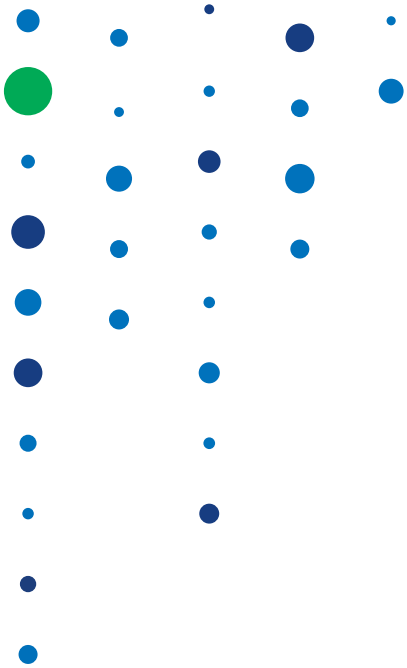
Since at least 2009, the Islamic Republic of Iran has regularly responded to sanctions or perceived provocations by conducting offensive cyber campaigns. The Islamic Republic has historically preferred to use proxies or front organizations both in physical conflict — Hezbollah against Israel and Yemen rebels against Saudi Arabia — and cyberattacks to achieve their policy goals.

Currently, Iran faces the prospect of negative economic impact via renewed sanctions. On May 8, 2018 President Trump announced that the United States would not renew the waivers on sanctions against Iran. The U.S will instead impose additional economic penalties , the combination of which amounts to a de facto U.S. withdrawal from the 2015 Joint Comprehensive Plan of Action (JCPOA) (commonly referred to as the "Iran nuclear deal".

We assess, based on Iran's previous reactions to economic pressure, that with President Trump's exit from the JCPOA, Iran is likely to respond by launching cyberattacks on Western businesses within months, if not faster. Judging from historical patterns, the businesses likely to be at greatest risk are in many of the same sectors that were victimized by Iranian cyberattacks between 2012 and 2014 and include banks and financial services, government departments, critical infrastructure providers, and oil and energy.

Key Judgments

- The Islamic Republic has abandoned its typically deliberate and methodical approach to cyber operations on only two known occasions, in 2012 and in 2014, when a quick reactionary response was required. We assess that when Iranian cyber operators respond to the U.S. withdrawal from the JCPOA that the operations will be staffed and executed by capable, but less trusted contractors.
- Further, we assess that staffing these operations with less trusted contractors could result in a scenario where the Islamic Republic has difficulty controlling the scope and scale of the destructive cyberattacks once they have begun.



- Iranian cyber operations are administered via a tiered approach, where an ideologically and politically trusted group of middle managers translate intelligence priorities into segmented cyber tasks which are then bid out to multiple contractors. This creates a quasi-capitalistic system that pits contractors against each other for influence with the Iranian government.
- The Islamic Republic operates with embedded paranoia, where ultimately, no one can be trusted. The situation creates unique trade-offs in Iran's government-sanctioned offensive cyber campaigns; individuals with demonstrated adherence to the government's ideology and individuals with the greatest offensive cyber skills are almost always mutually exclusive.
- Based on our source's conversations with other hackers in Iran, there are over 50 estimated contractors vying for Iranian government-sponsored offensive cyber projects. Only the best individuals or teams succeed, are paid, and remain in business.
- Insikt Group analyzed internet traffic relating to various institutes affiliated with the Iranian cyber ecosystem from March 1, 2018 to April 30, 2018. As this is the first profiling of Iranian internet activity for these institutes, we cannot determine whether the suspicious activity we analyzed was in preparation of the U.S. announcement.
- According to Insikt Group's source, to find and retain the best offensive cyber talent, Iranian government contractors are forced to mine closed-trust communities. The links between the forums and contractors may illustrate that the trust communities begin with the Iranian security forums.

The History of Iranian Geopolitical Response and the Nuclear Agreement Decision

Editor's Note: Where applicable, information in this section was provided by a former Iranian hacker with direct access to the information provided. Based on additional corroboration, we assess high confidence in this information. We refer to this individual as "Insikt Group's source" in other sections where their information is cited.

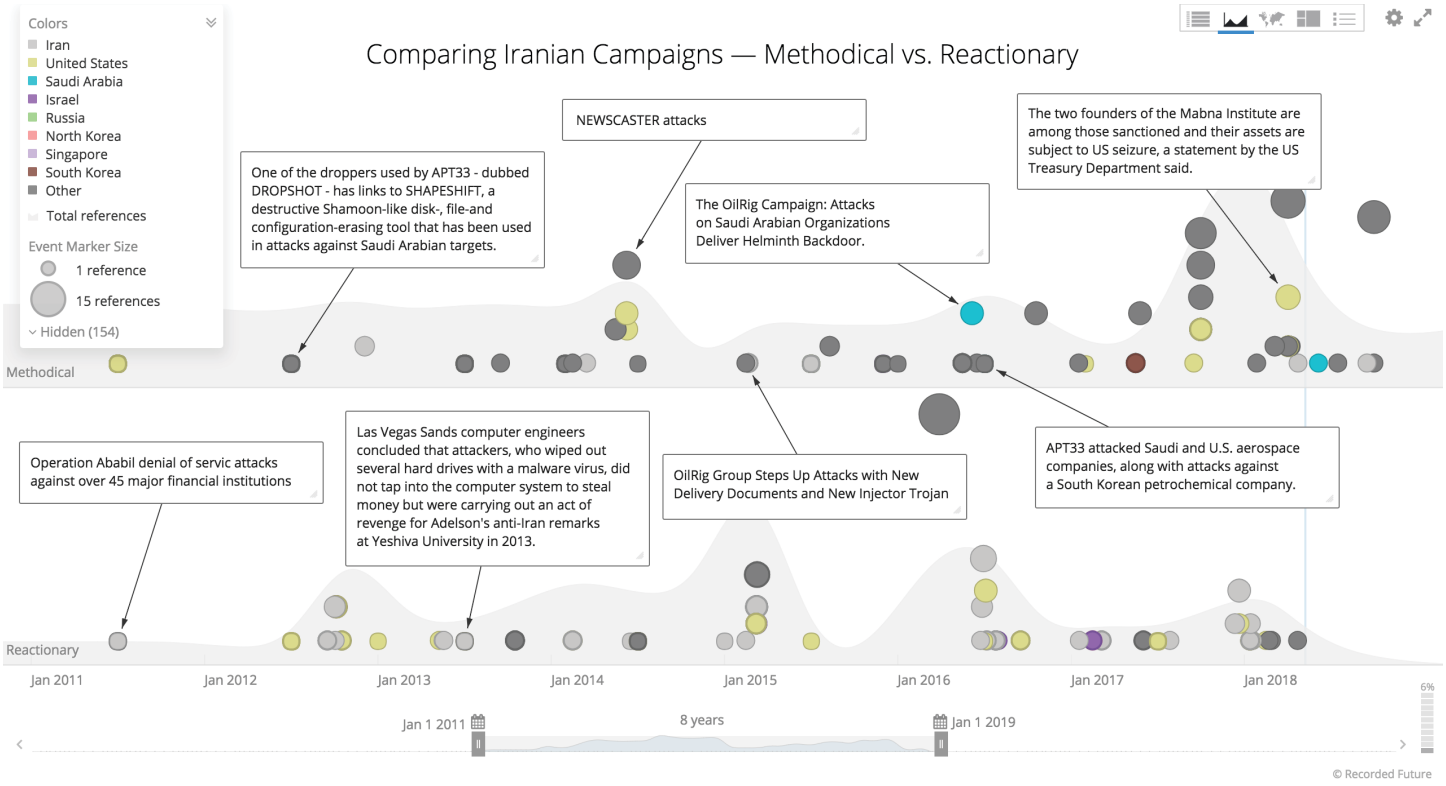
Since 1979, Iran's reactions to perceived Middle Eastern adversaries' foreign policy has been a study in the use of proxies. Specifically, Israel, Saudi Arabia, United States, and Iraq have been frequent targets of Iranian-funded military actions, most recently through Houthi rebels in Yemen, and Hezbollah everywhere else.

Since 2009, Iran has developed proxies in the cyber domain to partially obfuscate government fingerprints from foreign attacks. Subsequent to starting a cyber operations program in 2009, the Iranian government had an immediate need to use the program in the fall of 2012 after U.S. President Obama imposed severe financial sanctions on Iran, including removing Iran from the SWIFT money transfer system.

According to Insikt Group's source, the Iranian government authorized denial-of-service attacks on America's largest financial services companies as an immediate response to the sanctions in a campaign dubbed Operation Ababil. A quick response was top priority, so time and planning were forgone luxuries for the Iranian government. Instead, the Iranian government opted for speed and the most capable actors, regardless of demonstrated ideology.

Similarly, a year later in the fall of 2013, Sheldon Adelson (the CEO of Sands Corporation) publicly suggested that the United States should attack Iran with an atomic weapon. In February 2014, Iran launched a destructive attack on the Sands Las Vegas Corporation that caused significant network damage. This was the second public Iranian attack campaign on an American business, where the response called for speed over time and preparation.

The Iranian attacks in 2012 and 2014 were in contrast to the relatively slow and methodical work of APT 33, APT 34, and APT 35, developing custom malware, targeting data exfiltration from strategic intelligence targets such as U.S. military contractors, Middle East energy companies, and university research networks.



Comparing Iranian campaigns — methodical versus reactionary.

Building a National Capability — History and Relationships Between Proxies

The Iranian Revolution replaced the Persian monarchy and transitioned the Shah's power to the Islamic Republic, led by Ayatollah Ruhollah Khomeini. Loyalty to the resulting theocracy was defined by alignment to the Supreme Leader's moral precepts.

The new leaders of Iran also established an intelligence and security organization, the Islamic Revolutionary Guard Corps (IRGC), "charged with defending the Islamic Republic against internal and external threats." Currently, the IRGC is Iran's premier security organization and possesses an army, navy, and air force, and manages "Iran's ballistic missile arsenal and irregular warfare operations through its elite Quds Force and proxies such as Hezbollah."

The IRGC has a vast domestic information security and monitoring mandate, as well as broad foreign mission, and has been linked to cyberattacks against Western institutions since at least 2011.

According to Insikt Group's source, during the 2009 Green Revolution, Gerdab.ir emerged as the IRGC's domestic hacking group tasked with targeting opposition news websites and individuals considered immoral by the regime. Iranian hackers targeting Iranian government resources (one example was defacing Khamanei.ir) were identified by Gerdab and imprisoned. Gerdab continues to act as the Iranian government's internal censor.

Following the Green Revolution, the Iranian government considered adding a formal offensive cyber component to its existing intelligence apparatus, and was forced to address a personnel problem. Iran needed a talented, but politically and religiously reliable workforce. Stuxnet and scientist assassinations reminded Iran of the efficacy of Mossad and CIA programs, and according to Insikt Group's source, fervent religious ideology was the only way to demonstrate loyalty and build trust.

The emergence of the Iranian Cyber Army (ICA) as an extension of the IRGC was an initial attempt by the Islamic Republic at conducting internationally focused operations. These operations were a departure from Gerdab's focus on maintaining domestic moral values and defending government rhetoric. In 2011, the IRGC's ICA formed the foundation of the Khaybar Center for Information Technology. According to a former IRGC cyber commander, the Khaybar Center was established in 2011 and has been linked to a number of attacks against the United States, Saudi Arabia, and Turkey.

Even today, the balance between ideology and cyber skills remains problematic. One example of the conflict between ideology and skill was Mohammad Hussein Tajik, a former cyber commander within the IRGC. According to Insikt Group's source, Tajik's father maintained a strong religious background and was a veteran of Iran's ministry of intelligence. Yet Tajik was arrested and killed because the Iranian government feared that Tajik was not ideologically aligned and posed a betrayal and flight risk.

Following the Green Revolution, Iran's government needed to quickly improve its cyber capabilities, but according to Insikt Group's source, the talent was primarily young and focused on financial benefits. This motivation bred government mistrust, as the Islamic Republic feared that the financially motivated could be bought by foreign intelligence services. Additionally, many of the original Iranian hackers responsible for mass defacements hated authority and lacked the discipline necessary for government work.

According to Insikt Group's source, the government answer was a tiered approach, with a network of people unofficially associated with the IRGC and Iranian government — a type of ideologically aligned middle management — that were loyal to the regime and demonstrated sufficient religious commitment. This middle tier translated intelligence priorities into segmented cyber tasks which were then bid out to multiple contractors. Sometimes the contractors would compete with each other, sometimes they would work together, but payment was only made once the objective was completed. The result was (and presently remains) a quasi-capitalistic system that pitted contractors against each other for influence with the Iranian government.

In the Islamic Republic, influence can lead to security and wealth, but it can also lead to a false sense of security (no one is above being imprisoned and questioned at any given time). Thus, contractors must learn to play the game — enough surface-level adherence to the regime's ideology — to gain temporary reprieves from suspicion long enough to be given contracted work. To the Iranian government, ideology is more important than skills. Deep belief in the Ayatollah's precepts and the government's goals helps to avoid defections and traitors.

Obfuscating Iranian government involvement in offensive campaigns.

Today, based on ongoing contact between Insikt Group's source and Iranian hackers, it is estimated that there are over 50 organizations vying for government-sponsored offensive cyber projects. Only the best teams succeed, are paid, and remain in business. The government does its best to compartmentalize — one job might be creating a remote code exploit (RCE) for a popular software application, while another job might be using the RCE and establishing persistent unauthorized access. Two different contractors (or more) are typically required to complete the government-defined objective.

Public knowledge has also established that Iranian academic institutions play a contractor-like role. Specific examples include Shahid Beheshti University (SBU) and the Imam Hossein University (IHU), which have comprehensive science and technology departments attracting some of the best academic talent in Iran. In fact, the SBU has a specific cyberspace research institute dedicated to such matters, and the IHU was founded by the IRGC.

As the Mabna Institute indictments highlight, despite the lifting of sanctions and an appetite to re-engage with the international community, Iran has continued a subversive and aggressive global cyber operations campaign. This ongoing campaign, which targets universities for scientific and technological intellectual property theft, demonstrates a fundamental lack of trust in the international agreements, including the Joint Comprehensive Plan of Action (JCPOA).

Relationship Between the Iranian Government, Contractors, and Security Forums

Clearsky, FireEye, Symantec, and PhishLabs have all performed significant research on Iranian nation-state-sponsored campaigns that provide historical insight into technical capabilities and relationships between the Iranian government and contractors.

The work of the aforementioned security companies and recent U.S. Department of Justice indictments provides consistent evidence that Iranian government-sponsored offensive campaigns are executed by contractors.

FireEye disclosed that the Nasr Institute was an APT 33 contractor in an operation that used publicly available backdoors and remote access trojans. The handle "xman_1365_x" (self-identified on security forums as Mahdi Honarvar) was found by FireEye in malware artifacts, which open sources linked to the Nasr Institute. Previously, Nasr Institute had been associated with Operation Ababil's distributed denial-of-service attacks against American banks, an organization which a U.S. Department of Justice indictment confirms had been hired to build attack infrastructure by the Iranian government.

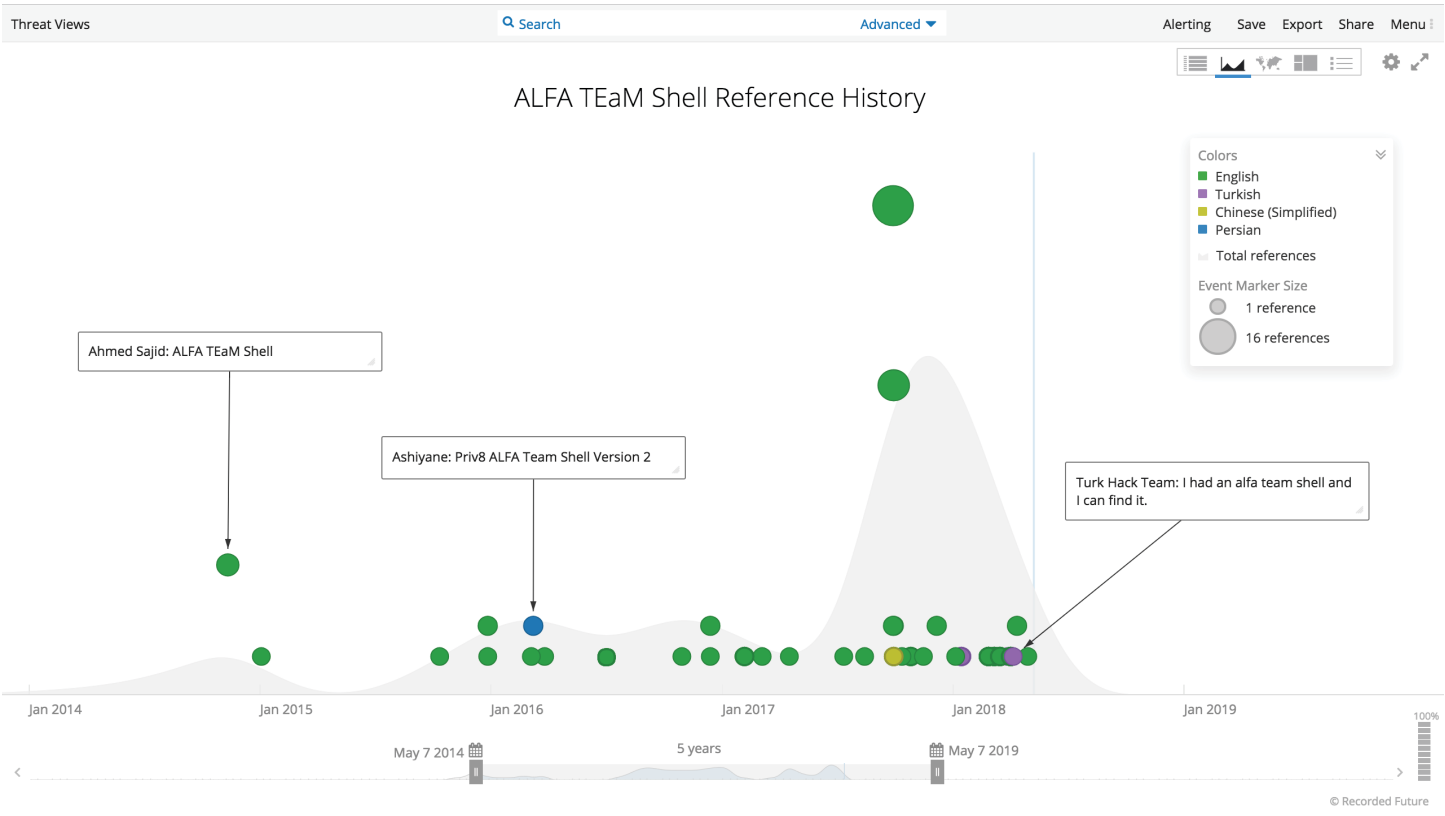
The actor xman_1365_x was then linked to a security company called Kavosh Security via OSINT by Iran Cyber News Agency. The actor was linked to a destructive operation, which used NewsBeef and StoneDrill malware families. According to Kaspersky, the latter data wiping operation targeted sectors across Saudi Arabia and Europe.

Command and control (C2) domains used by StoneDrill and NewsBeef in Kaspersky's findings were found to share an SSL certificate, which surfaced an additional three domains in research by the Iran Cyber News Agency. WHOIS information was then connected via open sources to Imam Hossein University (IHU). IHU was named in sanctions by the U.S. Treasury "for providing, or attempting to provide technological, or other support for and services in support of the IRGC."

Additional publicly known Iranian contractors include ITSecTeam (ITSEC) and Mersad Company, also linked to Operation Ababil.

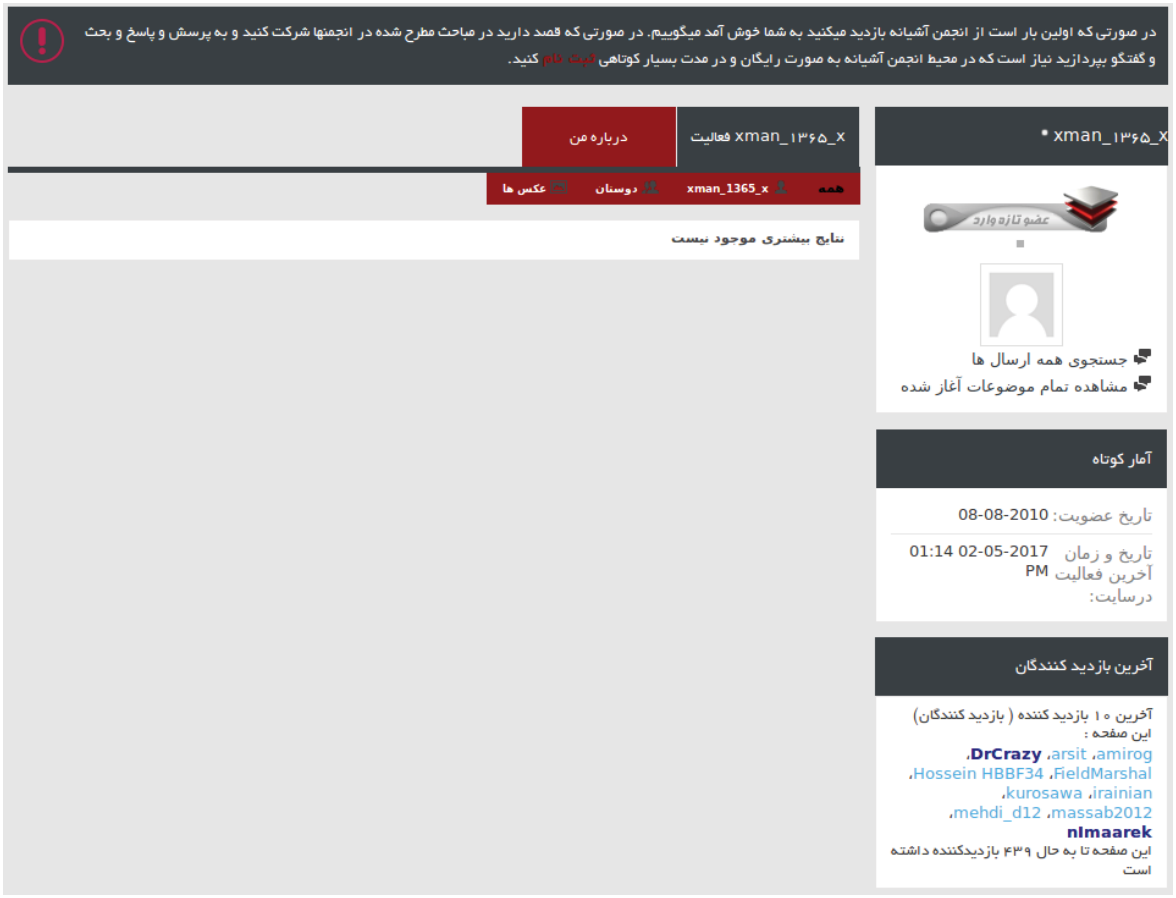
The links between the Iranian government and contractors are well documented; however, the identity of specific groups and individuals within the Iranian government and IRGC responsible for offensive cyber campaigns is murky, as is the relationship between contractors and security forums.

Yet, our research and analysis suggest that Iranian security forums may play a role in staffing and knowledge sharing for Iranian contractors. First, FireEye referenced the publicly available ALFA TEaM Shell in APT33 spear phishing email campaigns. The ALFA Shell is discussed in multiple web locations, including Ashiyane and Iranian Dark Coders Team Forum.



ALFA TEaM shell history.

Second, xman_1365_x created an Ashiyane profile on August 8, 2010, allegedly not long after Ashiyane temporarily became the primary security forum in Iran, following Behrooz Kamalian's visit to prominent cleric, Ayatollah Naser Makarem Shirazi.



xman_1365_x created an Ashiyane profile in 2010.

Finally, according to Insikt Group's source, Iranian contractor ITSEC specifically employed hackers from the respective online forums Simorgh and Delta Security. Further, Hossein Asgari, a self-proclaimed Iranian hacker, managed the Simorgh forum and worked with his father, who was employed by the IRGC.

```
**************************************************************************
Iranian Hackers : WWW.SIMORGH-EV.COM
Programer : Hossein Asgary
Note : SimAttacker  Have copyright from simorgh security Group
please : If you find bug or problems in program , tell me by :
e-mail : admin(at)simorgh-ev(dot)com
Enjoy :) [Only 4 Best Friends ]
**************************************************************************

OS :Windows NT 6.1 build 7601 (Windows 7 Home Premium Edition Service Pack 1) i586
IP :::1
```

Source: http://hackingscripts.com/simattacker-shell/

Zone-h captured website defacements committed by Hossein Asgari
Source: http://www.zone-h.org/mirror/id/4479919

According to Insikt Group's source, to find and retain the best offensive cyber talent, Iranian government contractors are forced to mine closed-trust communities. The links between the forums and contractors may illustrate that the trust communities begin with the Iranian security forums.

Analyzing Iranian Cyber Institute Internet Traffic

Insikt Group analyzed internet traffic relating to various institutes affiliated with the Iranian cyber ecosystem from March 1, 2018 to April 30, 2018. Our goal was to determine whether any of these institutes had forecasted Iran's intentions in cyberspace leading up to the U.S. decision to withdraw from the 2015 JCPOA.

This is Insikt Group's first profiling of internet activity for Iranian cyber institutes. While we cannot assess whether this level of activity is typical or not, monitoring it over time to determine changes in response to international pressure could be revealing.

Cyberspace Research Institute of Iran

Iran's Cyberspace Research Institute (CSRI) is a research center affiliated with the prestigious Shahid Beheshti University in Iran. The institute commands a significant proportion of the university's allocated IP space, with no fewer than eight /24 IP ranges registered to the CSRI in Iran, according to regional RIPE NCC records. The ranges are listed below:

netname	inetnum_start	inetnum_end	country	mnt-by	created
CyberSpace-Research-Institute	31.184.130.0	31.184.130.255	IR	MNT-MABNA	2013-08-31T06:02:20Z
CyberSpace-Research-Institute	31.184.131.0	31.184.131.255	IR	MNT-MABNA	2013-09-15T04:57:21Z
CyberSpace-Research-Institute	31.184.132.0	31.184.132.255	IR	MNT-MABNA	2013-09-15T05:02:03Z
CyberSpace-Research-Institute	31.184.133.0	31.184.133.255	IR	MNT-MABNA	2013-09-15T05:10:24Z
CyberSpace-Research-Institute	31.184.134.0	31.184.134.255	IR	MNT-MABNA	2013-09-15T05:11:21Z
CyberSpace-Research-Institute	31.184.135.0	31.184.135.255	IR	MNT-MABNA	2017-05-23T05:30:27Z

Source: RIPE NCC database, ripe.net.

Insikt Group identified several activities of concern emanating from these ranges.

We discovered over 400 previously unreported SSH sessions between CSRI ranges and Spanish government and university networks from April 4, 2018 to April 9, 2018. These exchanges involved the transfer of a large volume of data between the two networks. The Spanish networks resolved to departments supporting the digital transformation of Spanish public services and multi-disciplined universities. Direct network connectivity between the Iranian and Spanish institutions demonstrates that they either have a deep academic relationship and are sharing data with one another, or the large transfer of data from the Spanish institutes is unwarranted. It is unlikely that CSRI would have a valid business interest with Spanish government departments, so the large volume of data transferred between the two networks over such a short period of time is a conspicuous indicator of possibly malicious activity.

Throughout April, Iran's CSRI simultaneously demonstrated an increased interest in the Philippine Department of Science & Technology (DOST). Similar to the Spanish network interactions, very large data volumes were exchanged between the two networks, denoting strong interest.

This level of engagement and interaction, particularly in light of the reduction of sanctions, and the thawing of relations between Iran and the West following the 2015 JCPOA, was expected between academia. In fact, in 2015 and 2017, Philippine and Spanish universities agreed to expand scientific cooperation with Iranian institutions. However, given CSRI's background, Iran's demonstrated interest in using cyber operations to steal academic and intellectual property, and our evidence of ongoing campaigns targeting universities for theft worldwide, we assess that this activity between CSRI and these Spanish and Philippine universities may be malicious.

CSRI was also observed in a large number of events dispatching the Parsijoo bot to crawl websites of interest. According to Wikipedia, Parsijoo.ir is the second most popular search engine in Iran after Google and it uses the Parsijoobot to crawl websites for indexing purposes. During our research, we noted repeated crawls of a specialist Canadian-Iranian immigration website, www.itc-canada[.]com, using Parsijoo bot from CSRI IP ranges. The crawls were observed throughout our data period from early March continuing right through to the end of April, suggesting a strong, persistent interest in this particular site.

Finally, we identified CSRI interacting with IPs registered to Ravand Cybertech Inc. Ravand Cybertech offers, via its website ravand[.]com, cloud hosting solutions, among other services. Ravand Cybertech has strong ties to the Iranian regime. Historically, it hosted the website of the conservative news agency Fars which is affiliated with the Iranian military. The company's registered IP ranges sit under AS12212 with the following prefixes ranged 198.55.48.0 – 198.55.61.255, 198.55.63.0 – 198.55.63.255 and 207.176.216.0 – 207.176.219.255.

Ravand Cybertech hosted a number of domains used by an Iranian Ministry of Intelligence Services (MOIS) agent, Massoud Khodabandeh, in a disinformation campaign conducted in Western media. The campaign attempted to discredit and demonize the main Iranian opposition party, the People's Mojahedin Organization of Iran/Mojahedin-e Khalq (PMOI/MEK). According to an opinion piece written for The Hill, the websites were found by the Pentagon to be created by order from Tehran. Ravand Cybertech was identified as being an "Iranian state-run" company, which hosted fake news sites aimed at disseminating Iranian propaganda to undermine the efforts of Iranian-American lobbyists.

Based on the volume of activity observed during our research, we assess the CSRI may be engaged in supporting the malicious disinformation activities of Ravand Cybertech.

Imam Hossein University (Imam Hussein University)

The Imam Hossein Comprehensive University (IHU) is an Iranian university based in Tehran that is affiliated with the Iranian Revolutionary Guard Corps (IRGC), the Iranian Ministry of Science, Research and Technology, and the Iranian Ministry of Defense and Armed Forces Logistics.

Our research focused on the publicly noted IP ranges for the university, listed below:

netname	inetnum_start	inetnum_end	country	mnt-by	created
IMAMHOSSEINUNI	217.218.175.0	217.218.176.255	IR	AS12880-MNT	2008-12-28T10:20:37Z
IHUO	78.39.164.160	78.39.164.167	IR	AS12880-MNT	2015-09-05T04:48:32Z

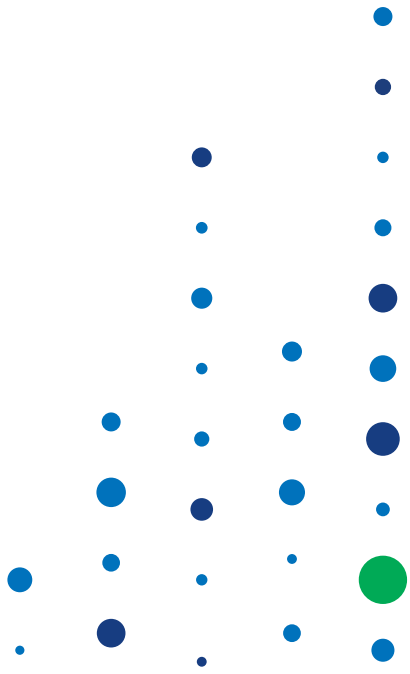
Source: RIPE NCC database, ripe.net.

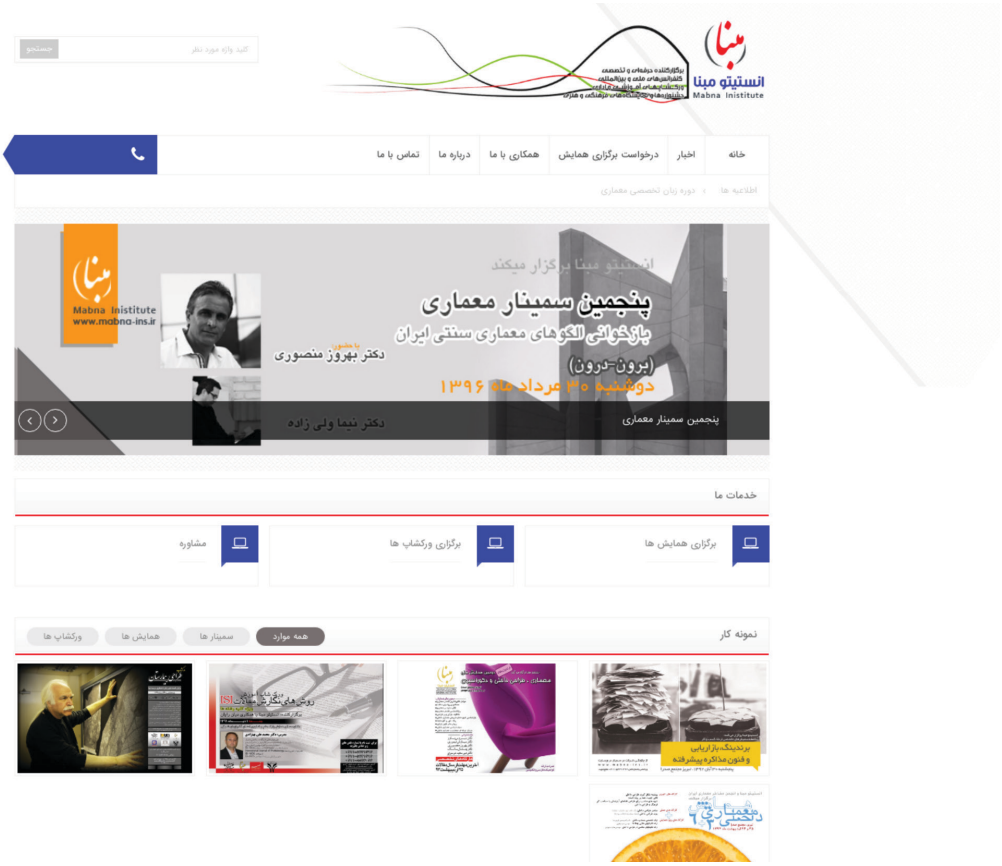
During our research, we found that IHU was also very interested in Spanish higher educational establishments and specific government departments. In fact, two of the same Spanish establishments exchanged high data volumes with the IHU source range IPs.

Further web browsing activity from IHU ranges was noted to the website of a U.S.-based multinational engineering software company, Gamma Technologies. The browsing activity was centered on its GT-SUITE software. Gamma Technologies specializes in the development of simulation software for a wide variety of worldwide industries, including power generation.

Mabna Institute

As previously detailed, the Mabna Institute was publicly identified in an FBI indictment as a front company engaged in hostile state-sponsored cyberespionage on behalf of the Iranian state. Our OSINT research identified a single domain, mabna-ins[.]ir, which could correspond to the group. The domain was previously hosted on an Iranian IP 5.144.130[.]23 and since April 22, 2017, points at German VPS IP 144.76.87[.]86. This VPS also hosts over 2,000 other domains, most of which are .ir domains.





Source: mabna-ins[.]ir

Intent, Scenarios for Retaliation, and Recommendations

According to the terms of the JCPOA, Tehran agreed to restrictions on its nuclear weapons program in exchange for sanctions relief. However, various provisions of the accord expire at different times over the next 25 years, with some expiring as soon as 2025.

On May 8, 2018, President Trump decided not to renew the waivers suspending some U.S. sanctions against Iran and initiated a de facto U.S. withdrawal from the agreement. As a result of this action, we assess that Iran will likely respond quickly by launching destructive attacks on American, European, and rival nation (countries such as Saudi Arabia and Israel) businesses.

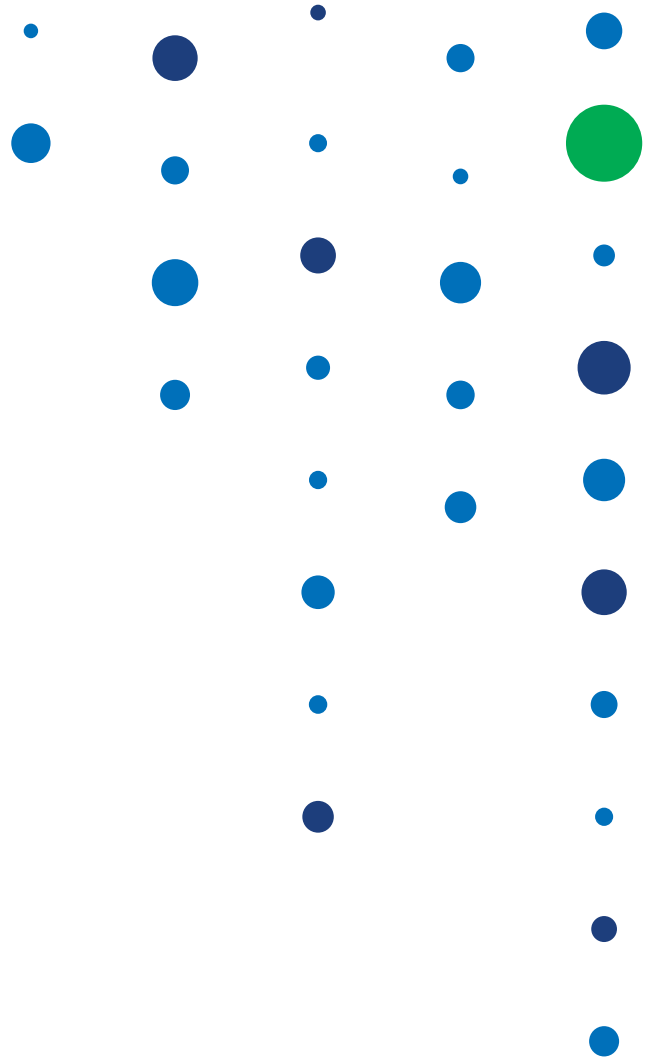
Conversely, Iran may also retaliate (exclusively or in conjunction with destructive attacks) through cyber proxies in more methodical and sustained campaigns. Given the impact of re-applied and expanded economic sanctions, it is likely that American, European, and rival nation businesses will also be targeted with more sustained destructive attacks.

As documented above, when pursuing quick-turn cyber operations, the Iranian regime will weigh religious and political reliability against offensive skills. The best operators are not always the most devout or loyal to the regime and we assess that, in this case, the IRGC may forgo careful contractor selection and planning in an attempt to deliver a destructive attack within a short period of time.

Further, our research indicates that because of the need for a quick response, the Islamic Republic may utilize contractors that are less politically and ideologically reliable (and trusted) and as a result, could be more difficult to control. It is possible that this dynamic could limit the ability of the government to control the scope and scale of these destructive attacks once they are unleashed.

Western businesses should closely monitor geopolitical events initiated by the United States or Europe that affect Iran. As demonstrated above, Western businesses are the logical victims of Iranian retaliation for perceived American policy transgressions; specifically businesses in financial services, government departments, critical infrastructure providers, and oil and energy sectors.

In addition to carefully monitoring Iranian geopolitical developments, tracking emerging tactics, techniques, and procedures (TTPs) on Ashiyane, specifically, is wise for any Western commercial threat intelligence program to determine the efficacy of existing security controls.



Recorded Future

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.