June 2021

INVESTIGATION OF IRANIAN CYBER HIERARCHY

Prepared by: Argonyte
Intelligence Researcher
AXIAL

Introduction

Iranian Government has constantly prided itself in askew military capacity, composing the use of terrorist proxies and cost-effective technology to go against the more technologically advanced countries. Though International Sanctions, such as those from the US, may have delayed Iran's ability to generate or buy technologies in every quarter this hasn't prevented them from continually expanding and advancing their cyber capabilities.

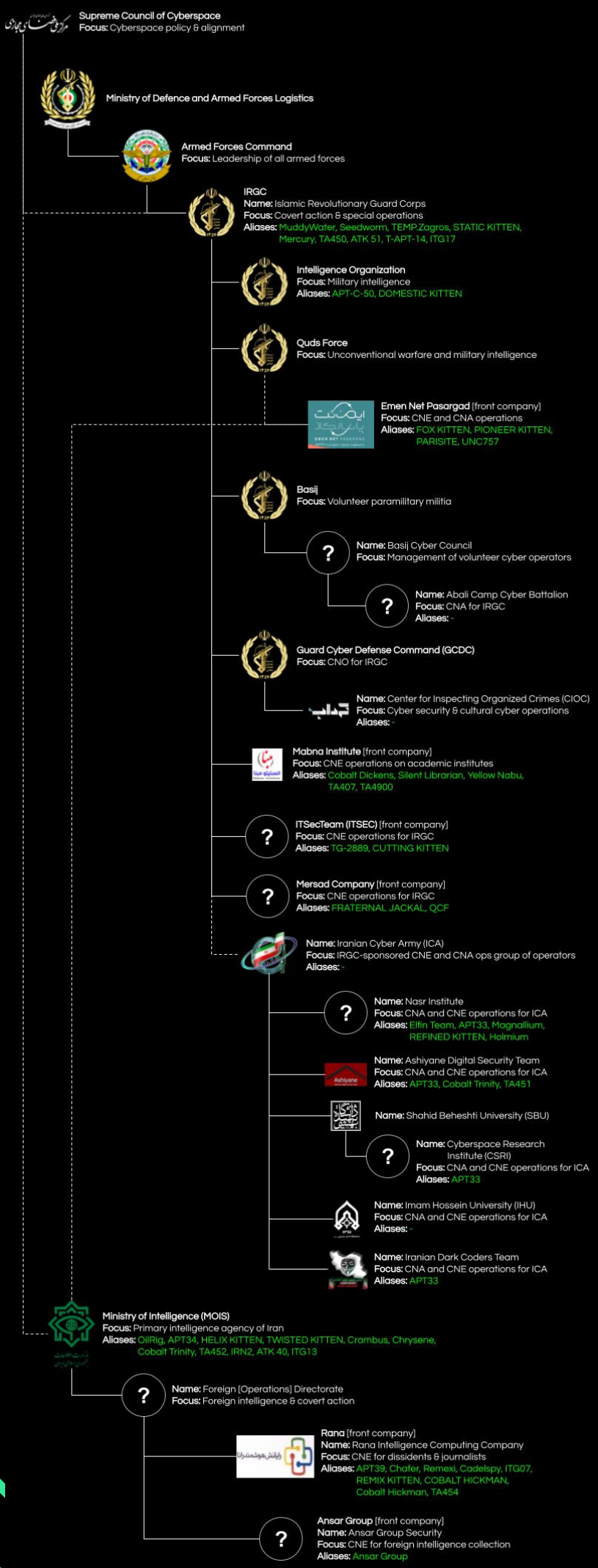
The best teacher for Iran in terms of its Cyber capabilities was Stuxnet in 2010. A malicious covert worm spread throughout Iran’s nuclear enrichment plant at Natanz. It is believed that Stuxnet caused substantial damage and setbacks to Iran’s nuclear program. The full Iranian response to Stuxnet is unknown but would have certainly led to significant costs and added time to repair the damages inside the IT systems, many of which would require isolation for purging of the malware or perhaps would even need to be destroyed.

In 2012, malware called Flame was identified on Iranian computer networks, where it was covertly extracting and erasing data including documents, social media conversations, and keystrokes.

Iran also used cyber repression to crush online protests during the 2009 rise of the “Green Revolution” by limiting Internet access and censoring or defacing Web content posted by protesters. The protests were aggressively challenged by Iran’s security forces. However, Iran’s youth continued the protest through the use of Web content and social media, and in the process revealed this new, Internet-based battlefield as a key weakness in Iran’s ability to respond. Following the Green Revolution, the Iranian government deemed adding a formal offensive cyber division to its existing intelligence sector and was forced to address a personnel problem. Iran needed a talented, but politically and religiously reliable workforce.

Iran Cyber Operations Groups

Author: Anastasios Pingios (@xorlgr)
Version: 1.5



Iran's Cyber Groups Hierarchy (Image Source: xorlgr)

An Overview of the Hierarchy

Iranian Threat Groups have been predominantly active over the last decade, wreaking destruction across nations. The Islamic Republic of Iran is unique in that its most powerful officials—namely Supreme Leader Khamenei and the Islamic Revolutionary Guard Corps—are inaccessible, while its most accessible officials—including Foreign Minister Javad Zarif—are far less powerful. Iran's offensive cyber activities are almost exclusively overseen by the Islamic Revolutionary Guard Corps or Ministry of Intelligence of the Islamic Republic of Iran—likely without the overlooking of the country's publicly "elected" officials—and composed of a scattered, but an elaborate network of autonomous contractors. While the relationships within proxies and governments can range from passive assistance to complete administration, Iran's indigenous threat actors maintain an arms-length connection to the state, with special operations organized to meet the requirements of the government. These contractor associations are not homogenous, and their forces are sometimes blended for attacks, which makes it challenging to distinguish and track the specific perpetrators.

Iranian cyberattacks typically practice a mix of methods requiring minimal skills (e.g., phishing) coupled with additional sophisticated techniques to covertly access a target's network. This results in several attacks that are scattershot and amateurish, raising the likelihood of exposure by the target. Iran also performs productive use of open-source investigation to engineer further targeted cyber-attacks on individuals and to diffuse propaganda. The bulk of Iranian cyberattacks are on PCs, although Iran also has the basic ability to steal data from mobile devices. The latter is limited yet has already been seen to calibrate from only domestic use in the past to international targeting. In addition, Iran will unquestionably continue the development and deployment of Shamoon. It is working to develop a means of ICS attack by stealing information from ICS suppliers to learn more about the vulnerabilities in such equipment. Iran may also be getting support from Russia, supported by a public cyber bilateral memorandum of understanding and the detection of uncharacteristic Russian cyber activity in the Middle East.

Iran proceeds to improve its cyberattack capacity by developing both technical ability and innovations in targeting. Where traditional targets have become more aware of IT security, Iran now attacks more vulnerable organizations in the supply chains of these targets, attacking at a global scale to obtain information or to find “backdoors” through steal from its primary targets.

The Insikt Group concluded that over fifty companies are contending for Iranian government-sponsored cyber projects. These projects are frequently compartmentalized such that two separate contractors (or more) are typically expected to complete the government-defined objective. These groups have been given diverse names by the cybersecurity research community, typically beginning with the word “Kitten” to signify Iranian origin.

Analysis of Iran's Cyberspace

1. Iran's ASN numbers

Iran is known for its strict censorship of the Internet, so it should be no surprise that every single one of the top ISPs is controlled by the government.

The list of Iranian ISP are:

- Mobile Communication Company of Iran PLC - AS197207
- Iran Telecommunication Company PJS - AS58224
- Information Technology Company (ITC) - AS12880
- Aria Shatel Company Ltd - AS31549
- Iran Cell Service and Communication Company - AS44244
- Mobin Net Communication Company - AS50810
- Pars Online PJS - AS16322
- Rightel Communication Service Company PJS - AS57218

According to reports, 12,412,468 IP Addresses (approximately 12.5 million IP addresses) belong to Iran.

References:

- https://www.nirsoft.net/countryip/ir.html
- https://mainfacts.com/ip-address-space-addresses/IR-IRN-Iran
- https://ipinfo.io/countries/ir
- https://lite.ip2location.com/iran-(islamic-republic-of)-ip-address-ranges
- https://en.wikipedia.org/wiki/Internet_censorship_in_Iran

2. Iranian Goverment Domains

The most common domain used by the government is .gov.ir, but several websites just use the .ir top level alone. It is managed by the Institute for Research in Fundamental Sciences.

The list of Second Level Domains:

- .ir – public
- .ac.ir – academic (tertiary education and research establishments) and learned societies.
- .co.ir – commercial/companies
- .gov.ir – government (Islamic Republic of Iran)
- .id.ir – personal, everyone has a National Number from Islamic Republic of Iran
- .net.ir – ISPs and network companies approved by IRTCT
- .org.ir – non-profit organisations
- .sch.ir – schools, primary and secondary education

Few Governmental Domains are:

- Iranian Intelligence - http://www.vaja.ir (IP- 2.187.252.17)
- Communications and Information Technology – https://www.ict.gov.ir/ (IP: 78.38.249.221)
- Justice – https://www.justice.ir/ – 62.193.12.10
- Foreign Affairs – https://www.mfa.gov.ir/ – 185.143.233.5
- Defense Armed Forces Logistics — https://irangov.ir/cat/545 IP: 194.225.148.179
- Science, Research and Technology – https://www.msrt.ir/ – 94.184.236.55
- Petroleum – https://www.mop.ir/ – 217.174.16.48
- Energy – https://moe.gov.ir/ – 78.157.43.50

3. Iran's Social Media

Iranian’s are very active on the global social media platforms like Twitter, Facebook, Instagram or TikTok. However, there are also several local social media sites whose popularity is unique to Iran.

Here are some popular Iranian social media sites:

- Aparat – an Iranian version of Youtube, works in a very similar way with video sharing and comments.
- Balatarin – link sharing website, dominated by political themes. Good for online handles searching.
- Cloob – a rather dated social media site that combines discussion forums and chat rooms.
- Digikala – online marketplace that looks and feels like eBay or Amazon.
- Divar – classified ads site, useful for searching usernames, but can be a hit and miss.
- Facenama – an Iranian clone of Facebook. Nowhere near close to the real thing in terms of usability.
- Sheypoor – classified ads site for mobile and desktop.
- Wisgoon – a photo sharing platform, clone of Instagram.

References:

- https://www.alexa.com/topsites/countries/IR

The Islamic Revolutionary Guard Corps and Groups under its control

- The Islamic Revolutionary Guard Corps (IRGC) is a branch of the Iranian Armed Forces, founded after the Iranian Revolution on 22 April 1979. 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 is designated as a terrorist organization by the governments of Bahrain, Saudi Arabia and the United States. They 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.

- IRGC comes under the Supreme Council of Cyberspace which has a prime focus on Cyberspace Policy and alignment. IRGC's primary focus orbits around Covert Actions and Special Operations. They command campaigns focused against both government and corporate targets globally. They are supported by several paramilitaries, semi-professional militias like The Basij, who also formed their cyber offense wing called the Basij Cyber Units (BCU).

- According to Insikt Group's source, during the 2009 Green Revolution, Gerdab.ir emerged as the IRGC's domestic hacking team 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. Currently, IRGC actively sponsors MuddyWater threat group which are also known as SeedWorm, Static Kitten, TA450, T-APT-41 and ITG17 who has actively targeted victims in Middle East with in-memory vectors leveraging on Powershell. They emerged in 2017 and was initially thought to be part of the financially motivated criminal group commonly referred to as FIN7 due to the use of an open source tool that was used by both sets of activity.

- The overall sophistication and commitment observed in such campaigns have not significantly altered in the decade that Iran has interlaced in offensive cyber operations. While sophistication alone can be a partial metric of posed threat, Iranian operations do not exhibit the typical technical forethoughts taken by other nation-state actors (such as obfuscating malware), and, even with strong social engineering abilities, attacks are frequently misguided by a lack of financing in nontechnical resources (such as fluency in English or personal tailoring of messages). These resource restrictions also account for why Iranians are more efficient at jeopardizing dissidents—Iranian threat actors understand their target's context and language, as opposed to when they are tasked with European languages or other cultures.

IRGC's Affliations and Contractors:

- Intelligence Organization: Going by the Alias, Domestic Kitten or APT-C-50, Check Point researchers revealed an extensive and targeted attack that has been taking place since 2016 and, until now, has remained under the radar due to the artful deception of its attackers towards their targets. The targets include dissidents and opposition forces in a certain Middle East country, as well as ISIS Supporters and Kurdish minorities mainly settled in the western part of a country in the Middle East. IRGC, Ministry of Intelligence, Ministry of Interior had provided its support to the organization to carry out their operations.

- Quds Force: They are one of five branches of Iran's Islamic Revolutionary Guard Corps (IRGC) specializing in unconventional warfare and military intelligence operations. The Quds Force reports directly to the Supreme Leader of Iran, Ayatollah Khamenei.

- Basij: A paramilitary volunteer militia established in Iran in 1979 by order of Ayatollah Khameini, leader of the Iranian Revolution, the organization originally consisted of civilian volunteers who were urged by Khomeini to fight in the Iran–Iraq War. It was an autonomous group from inception until 17 February 1981, when it was officially incorporated into the Revolutionary Guards organization structure by the Iranian Parliament to end the interservice dispute between the two. The Basij are subordinate to and receive their orders from the Islamic Revolutionary Guard Corps (IRGC) and the Supreme Leader of Iran, to whom they are known for their loyalty. As of July 2019, Gholamreza Soleimani is the commander of the Basij. The Basij Cyberspace Headquarters, founded in 2014, is one of a generation of organizations within Iran's bureaucracy charged with controlling Iranians' cyber activities.

Gholamreza Soleimani- Commander of Basij
(Image Source: Wikipedia)

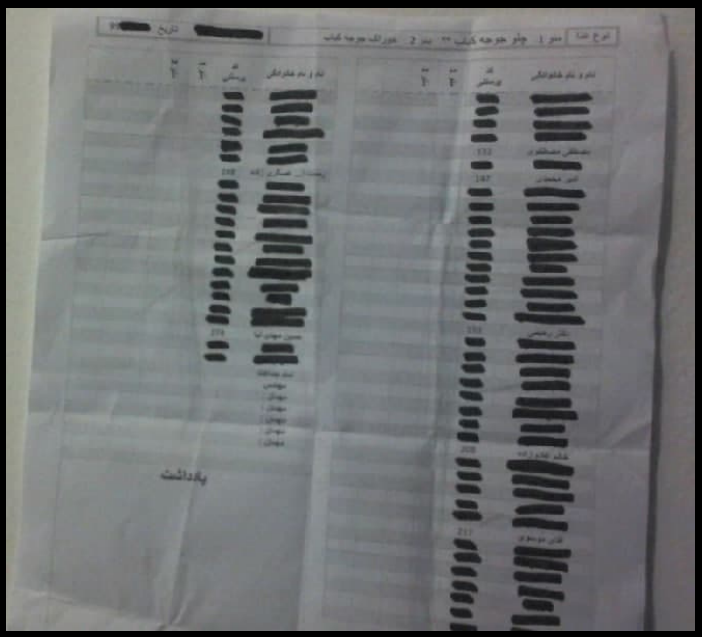
- Guard Cyber Defence Command (GCDC): Since November 2010, an organization called "The Cyber Defense Command" has been operating in Iran under the supervision of the country's "Passive Civil Defense Organization" which is itself a subdivision of the Joint Staff of Iranian Armed Forces.

- Emen Net Pasargad: A front company (aka “Imannet Pasargad,” “Iliant Gostar Iranian,” “Eeleyanet Gostar Iraniyan”) for operations conducted by IRGC and MOIS, and their aliases is Fox Kitten, Pioneer Kitten, UNC757, ENP were the ones behind AVAT System, and Project Signal. Lab Dookhtegan declassified the AVAT System and they state that it's a modelling system that identifies threats to the malwares developed by the company. AVAT System is exclusively sold to the security and espionage divisions of Islamic Republic of Iran in order to detect vulnerabilities in their malicious cyber tools, and customize them accordingly. The purchase of most of the anti-virus products was done through manipulations and deceit, using front companies, in order to bypasses the sanctions imposed by the UNSC against the terrorist regime.

Leaked files detailing AVAT System (Source: Treadstone71)

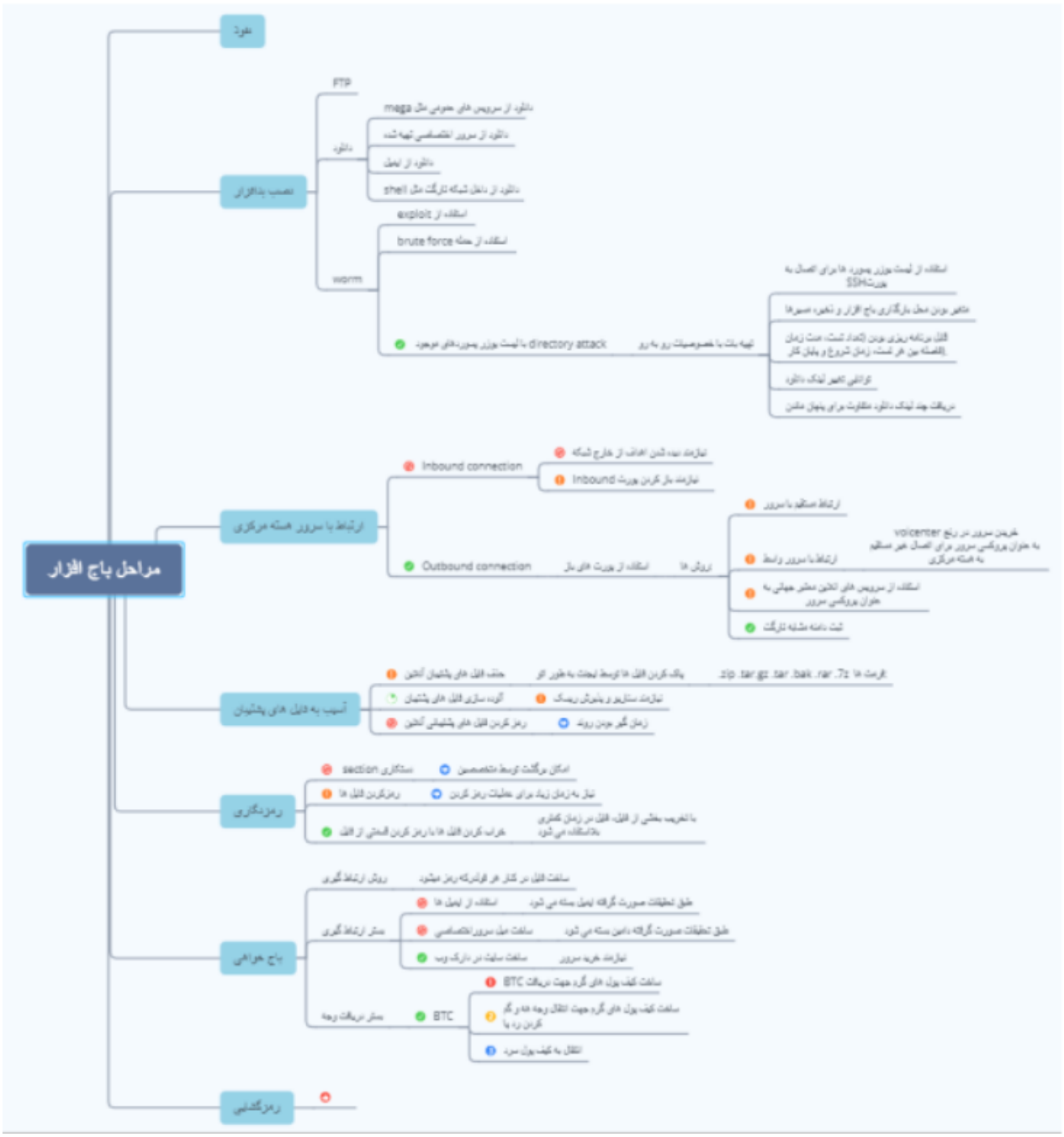
Managers of Emen Net Pasargad were declassified last year. The members were:

- Mostafa Mostafavi (employee #132): Head of administration and finance department
- Amir Mohammadi (employee #147): Head of cyber department
- Dr. Rahimi (employee #193): Shirinkar's senior advisor
- Gholam-Zadeh (employee #208): Head of research center
- Mousavi (employee #217): Head of security
- Rahmatollah Asgari-Zadeh (employee #248): Head of general-manager's office
- Hossein Mehdi-Nia (employee #274): Head of information technology



ENP's staff details leaked

ENP's ransomware project dubbed "Project Signal" began sometime between late July 2020 and early September 2020, when ENP's internal research organization the "Studies Center" began investigating unspecified target websites with the goal of "preparing for operations." Project Signal was also referenced in another spreadsheet showing that the project had been assigned to ENP's "Cyber Directorate," responsible for carrying out ENP's offensive cyber operations. The transfer of the Signal project from the Studies Center to the Cyber Directorate demonstrated that the ransomware project had progressed from the research and planning phase to the operational phase. In the spreadsheet, the word "ransom" was listed as the goal for the Signal project and the project was slated to take place between October 18 to 21, 2020, with a listed completion date of October 21, 2020.



ENP's Ransomware Workflow a.k.a. Project Signal

- Mabna Institute: A threat actor which has been associated with the Iran's Islamic Revolutionary Guard Corps (IRGC) focuses its operations specifically against academic and research sector institutions. Gholamreza Rafatnejad and Ehsan Mohammadi, founded the Mabna Institute in 2013 to assist Iranian universities and scientific and research organizations in stealing access to non-Iranian scientific resources. In furtherance of its mission, the Mabna Institute employed, contracted, and affiliated itself with hackers-for-hire and other contract personnel to conduct cyber intrusions to steal academic data, intellectual property, email inboxes and other proprietary data. The U.S. Department of Justice indicted nine officials from the Mabna Insititute in 2018. They are alleged to have compromised the networks of over 144 U.S. universities, 176 universities in over twenty-one other countries, as well as private sector, government, and multilateral entities.

  Members of Mabna Institure were:
  - Gholamreza Rafatnejad - Founder
  - Ehsan Mohammadi - Founder
  - Seyed Ali Mirkarimi - Mabna Institute Contractor
  - Mostafa Sadeghi - Affiliate
  - Sajjad Tahmasebi - Contractor
  - Abdollah Karima a.k.a Vahid Karima - Businessman
  - Abuzar Gohari Moqadam - Professor
  - Roozbeh Sabahi - Contractor
  - Mohammed Reza Sabahi - Contractor

  The members also sold data through two websites, Megapaper.ir and Gigapaper.ir. Megapaper was operated by a company named Falinoos Company, which was controlled by Abdollah Karima. Gigapaper was also affiliated with Karima.

References:

- https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

- ITSecTeam (ITSEC): One of the threat actors responsible for the denial of service attacks against U.S in 2012–2013. Victims included major banks such as Bank of America, Capital One, J.P. Morgan Chase, Wells Fargo, BB&T, PNC Bank, American Express, Citibank, and the New York Stock Exchange.

  Members of this group were:
  - Ahmad Fathi, Age - 37;
  - Hamid Firoozi, Age - 34;
  - Amin Shokohi, Age - 25;

  They were responsible for ITSEC's portion of the DDoS campaign against the U.S. financial sector and were indicted by the Justice Department in 2016

From Left To Right: Ahmed Fathi, Hamid Firoozi, Amin Shokohi (Wanted by the FBI)

References:
- https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

Ministry of Intelligence of the Islamic Republic of Iran and Groups under its control

Ministry of Intelligence of the Islamic Republic of Iran is the primary intelligence agency of Iran. MOIS is the most powerful and well-supported ministry among all Iranian ministries in terms of logistics, finances, and political support. It is a non-military governmental organization that operates both inside and outside of Iran. Intelligence experts rank MOIS as one of the largest and most dynamic intelligence agencies in the Middle East. Reliable and valid information on the ministry is often difficult to obtain. The Ministry of Intelligence and Security (MOIS) uses all means at its disposal to protect the Islamic Revolution of Iran, utilizing such methods as infiltrating internal opposition groups, monitoring domestic threats and expatriate dissent, arresting alleged spies and dissidents, exposing conspiracies deemed threatening, and maintaining liaison with other foreign intelligence agencies as well as with organizations that protect the Islamic Republic's interests around the world.

MOIS has sposored to APT34 aka OilRig, Helix Kitten, Twisted Kitten, ATK40. They have targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its cyber operations within the Middle East. It appears that they actively carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. 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).

MOIS has sposored to APT34 aka OilRig, Helix Kitten, Twisted Kitten, ATK40. They have targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its cyber operations within the Middle East. It appears that they actively carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. 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).

References:

- https://trends.builtwith.com/hosting/Ravand-Cybertech/Iran
- https://www.moisdisinformation.com/en/index.php/hyperlinks/108-massoudkhodabandeh

The regime's civilian intel wing of the government with cyber capabilities is the Ministry of Intelligence and Security (MOIS). They conduct a wide variety of operations, from signals interception, Internet censorship, digital counter-intelligence and disinformation warfare. Iranian cyber capabilities also include companies and NGOs, such as the Mabna Institute (private tech and IT company located in Tehran, suspected of hacking activities on behalf of the regime) and The Nejat Society (NGO involved in online PR and propaganda efforts for the Iranian authorities).

Connected Groups are:

- Foreign [Operations] Directorate: No links to any threat group

- Rana Intelligence Computing Company: A front company to APT39, it was created to bring together previous activities and methods used by this actor, and its activities largely align with a group publicly referred to as "Chafer." APT39 primarily leverages the SEAWEED and CACHEMONEY backdoors along with a specific variant of the POWBAT backdoor. They are one of the few operators directly controlled by MOIS. 45 associated individuals linked to Rana Intelligence Computing Company were found.

The 45 designated individuals served in various capacities while employed at Rana, including as managers, programmers, and hacking experts. These individuals provided support for ongoing MOIS cyber intrusions targeting the networks of international businesses, institutions, air carriers, and other targets that the MOIS considered a threat.

Rana Intelligence Computing Company: MOIS and APT39's Disguise

On the left, Rana's logo is detailed. Rana is a front company for APT39 actors working for the Iranian MOIS, the logo for which is detailed on the right.

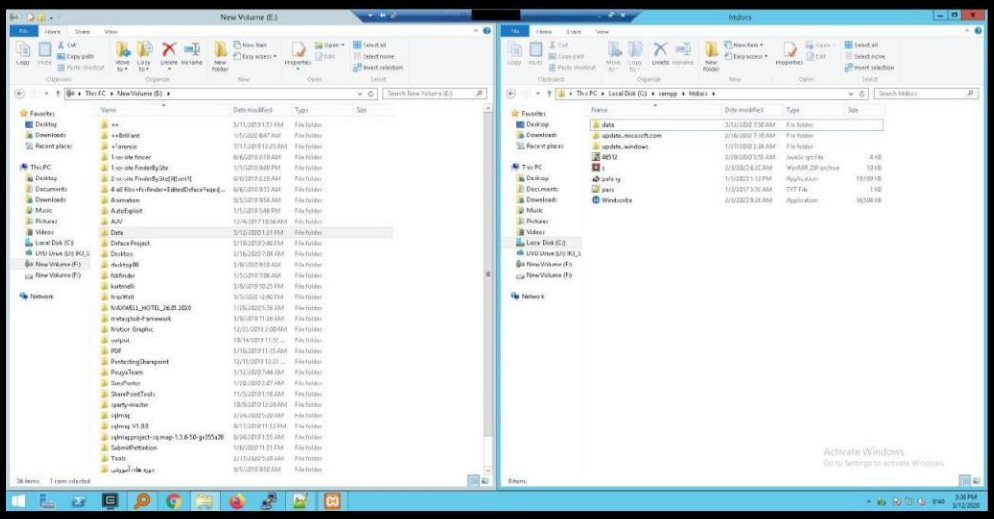
References:

- https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20200917

- Ansar Group Security: A front company for MOIS operations, Ansar Group was identified because of an Operations Report that were leaked. It declassfied military projects, telecom projects, energy projects and RnD of Malware. Furthermore, in these slides Social Engineering attacks are shown and they aim to steal private information and use them for its illegal activities, started in March 2018.

Several members have been identified: one of them is “sir shahroukh“, who is also CEO of the company “Pishgaman-e dad-e-tala-ei haraz” and he has close ties with the IRGC. Another member identified is "satanic2000" who was known from Stars Hacking Team of 2013. They had collaborated on writing an exploit of Arbitary File upload Vulnerability of Joomla. Because of the efforts of Labdookhtegan group, satanic2000's servers were hacked and evidence of former members of Ashiyane threat group were discovered.

Ansar Group also attacked a satellite company Thuraya which provided telecommunications coverage in more than 161 countries in Europe, the Middle East, Africa, Oceania and Asia. This hack provides this group the capabilities for stealing customers’ information, locating, intercepting and monitoring millions of civilians.



satanic2000's server which was hacked

Ansar Group presentations leaked

Translated Summary of few of the slides

1. Hacking hotels in Turkey, Georgia, Armenia, and access to the hotel reservations to follow our innocent compatriots outside the country (here the translated document).
2. Hacking websites for searching our compatriots according to their mobile phone numbers.
3. Hacking websites in Saudi Arabia and Jordan.
4. Hacking important companies in Arab countries.
5. Hacking infrastructures in Arab countries, Israel and Turkey.
6. Hacking oil fields and airports in the region.
7. Hacking the website on sanctioning medicine in order to influence the public opnion and to mislead them and to divert the responsibility for the medicine crisis from this desperate regime.
8. Sending out fake emails in order to attack the computers of compatriots in the region and steal their information.
9. Hacking news websites in Iraq in order to publish fake news and influence the public opinion in Iraq, even if that hurts the national interests of an ally country such as Iraq.

Iranian Cyber Army and Groups under its control

The Iranian Cyber Army is an IRGC sponsored division. It is thought to be connected to Iranian government, although it is not officially recognized as an entity by the government. It has pledged loyalty to Supreme Leader of Iran. The group has claimed responsibility for several attacks conducted over the Internet since 2009, most notably attacks against Baidu and Twitter.

Operating since 2013, APT-33 has been directing operations against targets that comprise of military and commercial aviation industries in the United States as well as the Kingdom of Saudi Arabia. They also targeted the petrochemical sectors of the KSA and South Korea. They have regularly shown a distinct interest in Aviation and Aerospace sectors in both military as well as commercial capacities. Evaluation of these attacks on multiple companies with partnerships to Saudi Arabia affirms that APT-33 may be viewing to gain intelligence on Saudi Arabia's military aviation capacities. APT33 has a reputation for engaging in destructive cyberattacks, utilizing TTP that has remained dormant within the context of cyber espionage campaigns. This ability not only sets apart APT33 from many other Iranian Threat Actors but further highlights it due to its small subset of industries and nations.

APT33 actively utilized Nasr Institute, a branch of the Iranian Cyber Army (ICA) both of which are affiliated with the Iranian Government and Supreme Council of Cyberspace. Iranian Cyber Army also regulates the group Cobalt Trinity which handled the team named Ashiyane Digital Security Team, Cyberspace Research Institute (CSRI) a part of Shahid Beheshti University (SBU) as well as Iranian Dark Coders Team. These teams actively administered Computer Network Attacks (CNA) and Computer Network Exploitation (CNE) of their Victims.

In 2017, FireEye's Operation against this APT exposed that an online moniker "xman_1365_x" was discovered in the PDB path of a backdoor sample. This moniker is associated with an individual at the Cyber Army Institute of Nasr. The moniker was also connected to the operations that involved NewsBeef and StoneDrill Malware.

The actor xman_1365_x, self-identified himself as Mahdi Honarvar on security forums. He also stated that he's from Mashhad, Iran. He's associated with the security company called Kavosh Security. Due to his poor Security Procedures and OPSEC, researchers were easily able to link the malware back to the Iranian State.

Some additional affiliates of the Kavosh Security group were also exposed, namely:

- Malek Mohammedinezhad
  - The Head of the Kavosh Security Group. His emails were found on barnamenevis.org forums which has a large number of Iranian Users.
  - Emails- mmndeveloper@yahoo.com, vranonymous@yahoo.com
- Behzad Shamsi Achachluei
  - A spyware and malware developer for smartphones
  - Email- behzadshams2005@gmail.com
- Saeid Beiki
  - Discovers Vulnerabilities and informs IRGC. His resume states that in past he's been a ‘Malware Analyst, Kavosh Security Center, Tehran’
  - Email- cephexin@gmail.com
- Mehdi Hoseinzadeh
  - Hoseinzadeh is a spyware developer.
  - Email - mehdi.hosseinzadeh86@gmail.com
- Milad Torkashvan
  - Involved with research and development of cloud-based attack systems, working as a malware developer.
  - Email- milad.torkashvan@gmail.com
- Sayyed Javad Sayyedhamzeh
  - Sayyedhamzeh is a spyware and destructive malware developer
  - Email- xabcmex@hotmail.com
- Javad Heidariyan
  - Heidariyan codes malware to spy on Iranians
  - Email- j.heydarian@gmail.com
- Nima Nikjoo Tabrizi
  - works on coding malware to spy on Iranians
  - Email- gladiyator_cracker@yahoo.com
- Mohammad Paryar
  - Codes malware to spy on Iranians
  - Email- I_bush_I@yahoo.com

Command and control (C2) domains used by StoneDrill and NewsBeef in Kaspersky's conclusions were seen to share an SSL certificate, which surfaced a further three domains in the investigation by the Iran Cyber News Agency. WHOIS information was then correlated 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." The connections between the Iranian government and contractors are thoroughly documented; however, the identity of definite groups and individuals within the Iranian government and IRGC responsible for offensive cyber campaigns is murky, essentially like the connection between contractors and security forums.

Though, Iranian security forums may play a function in staffing and knowledge sharing for Iranian contractors. First, FireEye referenced the publicly obtainable ALFA TEaM Shell in APT33 spear phishing email campaigns. The ALFA Shell is addressed in multiple web locations, including Ashiyane and Iranian Dark Coders Team Forum. 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 the prominent cleric, Ayatollah Naser Makarem Shirazi.

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.

Group-IB's Analysis of a campaign targeting Turkish Military Electronics manufacturer was done by the threat actor MUDDYWATER. "Nima Nikjoo" an employee of Kavosh Security Group between 2006-2014, was one of the perpetrators behind this campaign as metadata from maldocs revealed the author as "Gladiyator_CRK". Additionally, an email address suspected to be related, "gladiyator_cracker@yahoo.com," was associated with "نیما نیکجو," which translates to "Nima Nickjou," in a 2014 blog that exposed the names and email addresses of individuals allegedly employed at the Nasr Institute.

Malware Analysis - System Programmer

Kavosh Security Center

март 2006 – июнь 2014 · 8 лет 4 мес.

Tehran

Duqu Analysis
Flame Analysis
Red-October Analysis
Malware Development (Just for Research and test our product's safety)
System Programming
Development of Virtual Machine Protection
Development of Orange Metamorphic Engine (With 1% Similarity)
Development of Improved Nanomits Technology
Programming Anti-Reversing Frameworks such as Obfuscators and RISC Virtualizer
Reversing Anything to Find some thing we need it Свернуть

Previous Job entry of Nima Nikjoo which is now removed

In 2019, Maldocs were discovered created by a windows user with the nickname "Gladiyator_CRK". These documents also distributed the POWERSTATS backdoor and connected to the C2 server with the similar name gladiyator[.]tk.

Nima Nikjoo is the owner of the Gladiyator_CRK profile on Iranian video hosting sites dideo.ir and videoi.ir. He actively demonstrates PoC exploits for disabling AVs of various vendors and bypassing Sandboxes.

On March 19, 2019, Nima Nikjoo on Twitter changed his username to Malware Fighter, and also deleted related posts and comments. The Gladiyator_CRK profile on the video hosting dideo.ir was also deleted, as on YouTube, and the profile itself was renamed N Tabrizi. However, after almost a month (April 16, 2019), the Twitter account again began to use the name Nima Nikjoo.

Google Search of Gladiyator_CRK

https://www.dideo.ir › Gladiyator_CRK · Translate this page

Nima Nikjoo دیدئو dideo

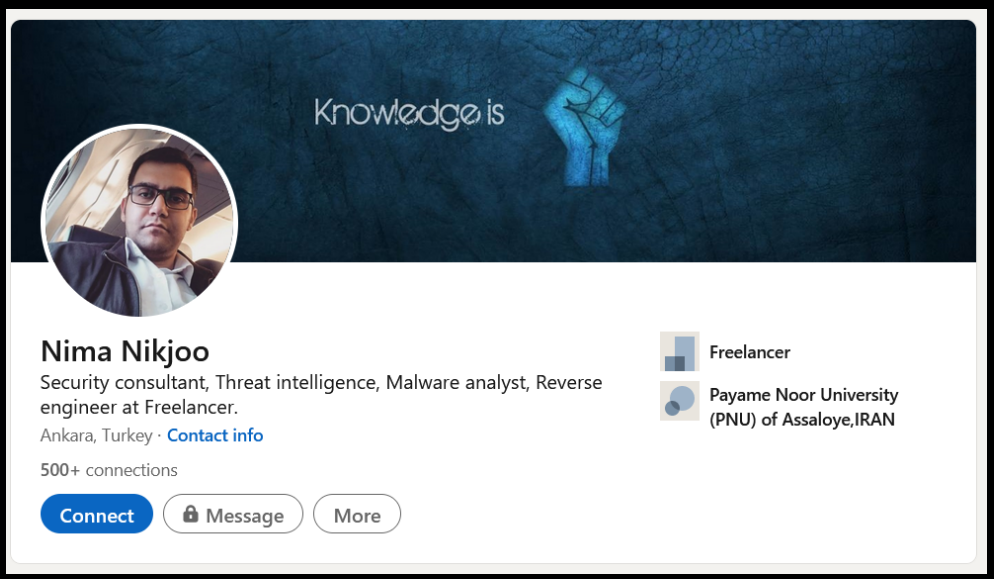
یافته های شخصی در رابطه با حوزه امنیت اطلاعات دیدئو dideo.

https://www.dideo.ir › cuckoo-sandbox-installation-part-3

Cuckoo Sandbox Installation Part 3 دیدئو dideo

emad.jahad.73. 3 years ago. Cuckoo Sandbox Installation Part 1 · Bypass cuckoo sandbox **Nima Nikjoo**. 3 years ago. Bypass cuckoo sandbox. Show More.

Nima Nikjoo's Current Twitter

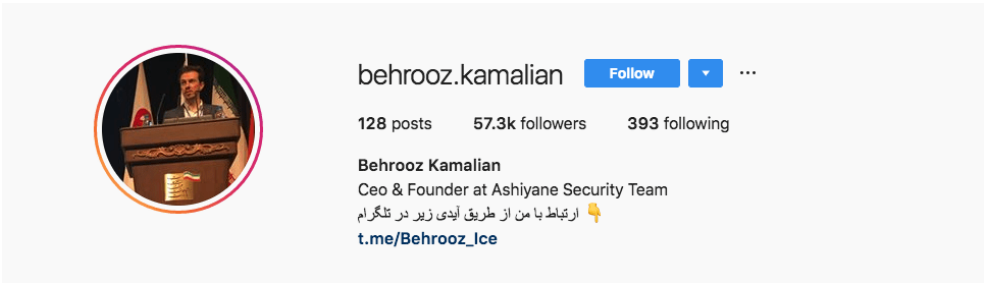


LinkedIn Connected to Nima Nikjoo

Some notable members of APT33:

- Ashiyane Digital Security Team: The Creators of Main Security Forums in Iran, Ashiyane Forums, held key sources for Iranian contractors to identify talent and share knowledge on successful offensive tools and tactics. Based on archived web page data, Ashiyane Forum initially started as a section of Ashiyane Digital Security Team's original website, ashiyane.com, in early 2003. The forum expanded into its website, ashiyane.org, in 2006. Ashiyane.org contained segments for general questions, tool sharing, defacements, training sessions, and news. Several of these original sections persisted as the forum grew and shifted to one of the largest hacking forums in Iran. In August of 2018, Ashiyane Forum was shut down. Behrooz Kamalian, recognized as the "father of Iranian hacking," is the CEO and founder of Ashiyane Digital Security Team. Behrooz is well regarded among the Iranians for his willingness to share his knowledge with younger hackers. Behrooz is also popular among many Iranian actors and actresses who claim he has helped protect their Instagram access, specifically by helping to regain control of previously compromised accounts. When asked about Ashiyane Digital Security Team's potential involvement with Iranian state-sponsored efforts, Behrouz has claimed that while Ashiyane Forum functions independently and automatically, they contribute with Iranian military apparatuses in advising and improving security, and "have always operated in the framework of the goals of the state."

Ashiyane Forums



Behrooz Kamalian's Instagram

References:

- https://www.recordedfuture.com/ashiyane-forum-history/

- Imam Hossein Comprehensive 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.

- Cyberspace Research Institute: 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.

Tools used by Elfin include their custom malware: AutoIt backdoor, Notestuk, StoneDrill. They have also used commodity and publically malware and tools such as DarkComet, DistTrack, EmpireProject, Filerase, JuicyPotato, LaZagne, Mimikatz, NanoCore RAT, NetWire RC, PoshC2, PowerBand, PowerSploit, POWERTON, PsList, PupyRAT, QuasarRAT, RemcosRAT, Ruler, SHAPESHIFT, TURNEDUP.

References:

- https://www.recordedfuture.com/iranian-cyber-operations-infrastructure/

Resources

- https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf
- https://apt.thaicert.or.th/cgi-bin/listgroups.cgi
- https://henley-putnam.national.edu/article/irans-real-threat/
- https://www.recordedfuture.com/iran-hacker-hierarchy/
- https://www.recordedfuture.com/iranian-cyber-operations-infrastructure/
- https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
- https://en.wikipedia.org/wiki/Internet_censorship_in_Iran
- https://xorl.wordpress.com/2021/05/06/iran-cyber-operations-groups/
- https://fas.org/irp/world/iran/mois-loc.pdf