Menu

The Cyber Shafarat – Treadstone 71

We See What Others Cannot – WWW.TREADSTONE71.COM

Farzin Karimi Moves From Pure MOIS to Ravin Academy

12 MAY 2020

#MOIS #VAJA #IRAN #RAVINACADEMY #LAB_DOOKHTEGAN #ESFANDIYAR #FAJR #APT33 #MUDDYWATER #PossibleDeception #DECEPTION #INFLUENCEOPERATIONS #PSYOPS

April of last year (Farzin Karimi on Cyber Shafarat) we discussed Mr. Karimi via multiple posts from #Lab_Dookhtegan. In our direct discussions with Iranian insiders, we have updates on Farzin's status. We can call this storyline, My Conversation with Esfandiyar. Esfandiyar claims to be an Iranian citizen concerned over the situation in Iran. We do not have any historical record with Esfandiyar to either prove or disprove the data provided. We have found the individuals

named with backgrounds in computer science, past alignments with Ashiyane, claims of defacements and other hacks. Information provided by Esfandiyar related to each named individual has to date proven true. In his words:

"Iranian government was in really bad situation, Sanctions, economic pressure, corona, all come together to paralyze the Islamic Republic, and this terrorist government is currently considering using cyberspace to consolidate its position, so you can also disclose information that we cannot. You will be of great help to the world and to the people of Iran who are hostages of this government. … exposing of information such as Snowden's done, Because the Iranian government is a terrorist government. Supports Hezbollah, persecutes his people, assassinates his opponents in every country, disturbed Yemen, destroyed Syria to protect Bashar al-Assad. I think one of these is enough to become a terrorist state. "

Mr. Karimi opened Ravin Academy. Ravin Academy provides services in the following areas:

> Information Security Training, Threat Hunting, Cyber Security, Red Team, Digital Forensics, Malware Analysis, Security Audit, Penetration Testing, Network Defense, Incident Response, Vulnerability Analysis, Mobile Penetration Testing, Reverse Engineering, and Security Research

Previously identified as working directly for the Ministry of Intelligence (MOIS or VAJA), Farzin now runs his new company while reportedly continuing to support the MOIS. Seyyed Bagher Hosseini also works at Ravin and is known as an author of malware. His work in developing malware for the MOIS included attacks against #Saudi #UAE #Turkey, and #Azerbaijan

Specifically, the group (MOIS Cyberteam or FAJR as they called themselves) attacked Saudi Aramco, the Turkish Defense Ministry, and the Turkish immigrant network. The attacks on Turkey were the most successful according to Esfandiyar. Turkish customs resulted in the exfiltration of approximately 500GB of data directly sent to the MOIS. Another feather in their cap was the theft of technology from Azerbaijan used to generate electricity from waste (waste-to-energy). FAJR also attack sites in the United States, Israel, and neighboring states to gather information and technical knowledge Iran was unable to acquire due to sanctions.

Sites Esfandiyar was able to provide:

- mfa.gov.tr
- mod.gov.ae
- enec.gov.ae

There were other sites usually under the high level of Ministry of Foreign Affairs or MFA.

- https://cybershafarat.com/2020/03/15/iranian-hackers-leak-turkish-citizen-data/
- https://cybershafarat.com/2020/03/18/iranians-targeting-turkey/

The main players on the team working directly for the MOIS:

- Farzin Karimi – Team Lead

- Masoud Aghdasifam
- Ghader (Qader) Ahmadi
- Mohammad Farhadzadeh
- Seyed Bagher Hosseini

Why Farzin as the lead?

Farzin was selected as the lead due to skill, but that came with a price. Farzin ran a strict shop coupled with an extremely sensitive nature. Farzin did not share anything other than MOIS orders with the team and had a high level of trust with intelligence officials. The team did have internal conflicts that lead to some members being removed. There was also tension between this team working on behalf of the MOIS, and the Islamic Revolutionary Guard Corp. The team did not have a high opinion of MOIS members drawn from the Basij since they did not have the necessary expertise.

Seyyed Bagher Hosseini reportedly purchased tools using Bitcoin possibly via Binance Coin. One known handle used by Hosseini was EB_DARYA.

For each operation, team tasking including site reconnaissance with sites categorized based on level of difficulty to penetrate. Certain team members developed malware based the levels of difficulty. The levels were measured against organizations who used up-to-date defensive measures including current patching levels. There is the assumption these defensive measures included continuous tuning of various sensors. Preparation for attacks included adjustments based on target security systems and tools, their network structure and any other information gathered during surveillance and reconnaissance actions. Normally, Ghader Ahmadi (malware development and attack preparation) and Mohammad Farha Zadeh (attack preparation) performed these activities.

Fear permeated the team's activities since discovery by the target could result in death for the homeland. Explained by Esfandiyar, according to religious beliefs, an Iranian who is killed because of what is considered a religious act, will go directly to heaven. Since all operations of this type were on behalf of the theocratic government, the operations were considered a war of good versus evil. Anyone killed because of a failure would be granted direct access to #Firdaus or paradise. Regardless, any information, whether valuable or worthless served to boost the team's annual budget. That amount was not shared with the team.

The teams were fixed in nature (no new members or trainees along the way) and geographically segmented by city, treated like a separate cell only known to the MOIS. Each city has its own independent operations center usually with one professional hacker directly working with the MOIS. The rest of the team are pulled from local universities. Detailed education was taught by local experts cover topics like reverse engineering and exploit development. The most expert groups are in Tehran. In fact, each city in Iran has teams that are known by APT names. Esfandiyar's team was part of APT33 or Muddywater as named by Western groups although they called themselves FAJR or Dawn. The location of his group will remain confidential. A word of note, the team struggled whenever they encountered Trend Micro in a target's environment.

Link Analysis of Iranian Cyber Actors

Our conversation continued to discussions on the risk of discovery. Esfandiyar said there was no real plan for handling a discovery, likely do to the fact that almost all operations suffered discovery eventually. He indicated this was due to the lack of professional hackers. The training of hackers of this type is not formalized but performed by local experts identified during university classes, recognized prowess, or other such method of skill identification. According to Esfandiyar, most were "university geniuses" and therefore "militarily selected."

I asked Esfandiyar if there had been operations not associated with known advanced persistent threats (APTs). Within his group, an attack on the government of Azerbaijan targeting United States technologies in use there were both successful and largely undetected. The United States provides advanced technology to the government of Azerbaijan.

Most all orders for targeting came via phone or in person. Farzin Karimi received the orders directly from an MOIS officer. Farzin then informed the team of the new tasking. Many of the initial attacks used phishing with macro-infected documents specifically prepared for each target. Other social engineering actions consisted of phone calls to target organizations followed up by emails with resumes containing malware. An expectation after the call that an email would follow.

Esfandiyar said some of the tools used were Empire, PowerSploit, PyRat, and inhouse developed remote access trojans, and one-day exploits. The team desperately searched for zero-day vulnerabilities saying that their efforts failed in finding any. Tools used in combination were the norm depending upon the targets defensive posture and the relative success or failure of the tools during the attack. When asked about following some type of structured approach once inside a target network, Esfandiyar responded with a comment saying the activities were mostly erratic in nature. This corresponds to the irregular mode of non-kinetic means of attack, mostly due to a lack of maturity in their country's overall offensive cyber capabilities. Operations focused on stealing information to gain some type of advantage while avoiding a situation that leads to harsh response. The team did venture into influence operations after the death of Jamal #Khashoggi sending malicious documents under the title "Secret of Khashoggi Death."

Any information collected was sent to the MOIS. Malware developers received technical data but nothing of intelligence value. All such data had a direct path to the MOIS via Farzin Karimi. Only internal reconnaissance information and information on internal target defenses made their way to the malware developers who then had two days to prepare and test the malware, updating their payloads. Final malware testing was the final step before moving to the next phase, that being a hand off to the attack unit for operational attack.

Esfandiyar said most malware was written in #PowerShell and #Delphi, with some in #Python. Lateral movement processes used #Mimikatz and #Lazagne. One such tool used for hiding payloads may be found on Github at https://github.com/3NC0D/Powershell-Obfuscator. Esfandiyar said they received no outside help (non-Iranian) for their efforts. Of no surprise, Kali and Ubuntu flavors of Linux represented the desired development platform of choice while Windows was used for testing due to target usage. One area of difficulty for this team was the inability to penetrate access domain controllers.

Many on the team performed their tasks due to the desire to learn and the ability to earn a particularly good wage in Iran. Team members were paid 12,000,000 Tomans or 120,000,000 Iranian Rials monthly. Just under $3K USD per month. Another benefit was unlimited technology and in return, the team provided simulated network environments

used to perform pre-attack tests. This included information security defensive technologies and associated training. (Something Treadstone 71 has railed against repeatedly on the Cyber Shafarat).

- https://cybershafarat.com/2019/07/06/sansirancehciscomicrosoft/
- https://cybershafarat.com/2020/02/14/course-name-certified-ethical-hacker-ceh-v10-312-50-professor-fariborz-fallahzadeh/
- https://cybershafarat.com/2019/08/26/8041/
- https://cybershafarat.com/2019/08/06/offensiveroadmapiran/
- https://cybershafarat.com/2020/02/05/vistaac/
- https://cybershafarat.com/2020/01/01/esets-criminal-cooperation-with-the-repugnant-islamic-republic-lab_dookhtegan/
- https://cybershafarat.com/2019/05/12/mcafee-institute-next-company-to-reward-and-support-iranian-hackers-who-target-the-us-and-our-allies/
- https://cybershafarat.com/2019/04/25/iran-hackers-cyber-security-training/

Internal security is tight with team members unable to perform anything remotely 'personal' while in the MOIS safe house. Internet access was tightly controlled and only used for operational activities. No external devices allowed in the safe house. When the team did communicate with others, they normally used Signal and Telegram with constantly changing handles and groups. Team members held the identity of these groups and handles private although Esfandiyar provided a couple of group names: Jendekhana and Okozlaar used in the past but deleted monthly.

Our conversations with Esfandiyar will likely continue.

Team Brief

Note: This is a very limited view. We have scores of pages on each team member.

Farzin Karimi – Known to participate in the past as a cyber mercenary for the IRGC targeting internal Iranian websites who did not profess the revolutionary ideals. Karimi also trained IRGC cyber mercenaries through a company named Noora Net, a company he lists on his resume. His actions during his time with Noora Net include identifying Iranian civil activities to the IRGC, many of whom disappeared. (noora.ir noorasec.com). Farzin Karimi, co-founder of Ravin Academy, shared how to evaluate and explore the vulnerability of CVE_2020_0688 on Exchange server along with the Exploit script. Karimi enhanced code for DLL Function Proxy. Possible email used by Farzin is 0x0darkcoder@gmail.com



Ravin Academy is located at No. 36, Naqdi Street, North Sohrevardi Ave, Tehran, Tehran IR

He graduated in 1985 from K.N. Toosi University of Technology. Khajeh Nasir Toosi University of Technology, also known as K. N. Toosi University of Technology, is a public university in Tehran, Iran, named after medieval Persian scholar Khajeh Nasir Toosi. The university is considered one of the most prestigious, government-sponsored institutions of higher education in Iran.





Mohammad Farhadzadeh studied Engineering at the Islamic Azad University of Tehran-Central and speaks Farsi, Turkish, and English.

Massoud Aqdasi Fam is a PhD student in Computer Science at Tabriz University having earned his Master of Science in Computer Science from Tabriz University and his Bachelor's Degree in Software Engineering, Computer Software from Tabriz Higher Education Institute after receiving an Associate's degree in Applied Mathematics from Tabriz University.

Ghader (Qader / GH4D3R) Ahmadi claims to be a Red Team Operator after being the APA Moshaver CEO for 3.4 years in East Azerbaijan, Iran. He is a Certified Network Security Specialist (ICSI – from the International CyberSecurity Institute – UK). Ghader participated in hacks with former Ashiyane members as well as Kheshtak. He studied civil engineering and likes to target ICS-SCADA systems.

Treadstone 71 Training

Treadstone 71

Related

Iranian MOIS - Vaja hacks Turkish Government Site Tracking dissidents
5 Jun 2019
In "2009"

Green Leakers - InfoSec & Beyond - Lotusint - STANDBY for a possible leak on MuddyWater
23 Apr 2019
In "2009"

Iran Internet Communication Status - MOIS
11 May 2020
In "Iran"

Categories:

CYBER OPERATIONS HACK INTELLIGENCE ANALYSIS IRAN LAB DOOKHTEGAN MOIS MUDDYWATER OFFSEC OSINT PASDARAN SAUDI SCADA SEPAH VAJA

Published by Treadstone 71
@Treadstone71LLC cyber intelligence, counterintelligence, infiltration, OSINT, Clandestine Cyber HUMINT, cyber intel and OSINT training and analysis, cyber psyops, strategic cyber security, Interim CISO Services **View all posts by Treadstone 71**