Telefónica

INSIDE ELECTIONS_

Threats to the Iranian Electoral Process

09.06.2017

CYBER SECURED BY ElevenPaths

elevenpaths.com

Threats to the Iranian Electoral Process

Analyst's View

Iran has been accused of creating different tools for obtaining sensitive information or taking control of systems belonging both to individuals (including defenders of human rights) and to foreign powers. These include **MacDownloader**, **Infy** and **RocketKitten** campaigns **I** and **II**, all with recently-active sessions coinciding with the electoral period. On the other hand, in order to avoid the sort of influence false news stories on Facebook had on the American presidential elections, Iran has limited certain functions of social networks such as Telegram and Instagram.

Principal Country Keys

Official name	Islamic Republic of Iran
Capital	Tehran
Official language	Farsi o persa
Religion	Islam is the official religion. The majority of Muslims in Iran are Shiite.
Form of Government	**Islamic Republic**. The system is based on an Executive branch led by the President of the Republic (Hassan Rouhani) and a Legislature that approves laws. Nevertheless, both are overseen by the figure of the Supreme Leader (Ali Khamenei), who has the capacity to set general policy.
Principal clients	China, India, Turkey
Principal providers	China, UAE, South Korea and Turkey
Principal exports	Petroleum and gas products (73%) and rubber and plastic products (5.3%), principally.

Severing of relations with the United States after the **storming of the American Embassy** in Iran **[1979]**

The Ahmadinejad presidency and the **Iranian nuclear program** further strained relations with the Western world **[2005-2013]**

First Rouhani mandate as President of the Republic. The key points of his exterior policy were **[2013-2017]**:

Removal of economic sanctions in exchange for halting the *nuclear program*. This resulted in warmer relations with the EU

Middle East peace process: softening of tone against Israel

Relationship with *neighbouring Arab countries* influenced by the Syrian conflict

Tension with *Afghanistan* as a result of Afghani immigration over the border

Member of OPEP and Gas Exporting Countries Forum

New relationship of strength with *Russia*. After sanctions were removed, Russia became the first sponsor of Iranian petroleum

Second Rouhani mandate as President of the Republic **[19 May 2017]**

Types of Threats Identified

Threats from external agents

We must go back to 2010 to identify possible attacks on the Islamic Republic of Iran by foreign powers that are capable of affecting the country's interior and exterior policy. Stuxnet, a worm affecting SCADA systems, was discovered in 2010. Duqu was discovered one year later: this was very similar to Stuxnet, although its mission was to obtain information on industrial control systems. Both affected critical infrastructures, especially the development of the Iranian nuclear program.

Furthermore, in 2012 Flame was discovered; this was a malware aimed at cyber-espionage operations in the Middle East with Iran as one of its objectives. Flame was capable of spreading to other systems through local networks (LAN) and through USB flash drives.

Threats from internal agents

Internet use among Iranians is at about 68.5%, [1] and at least 47% of the population is in the age range of 25 - 34 [2]. With this in mind, Iranian presidential candidates have used social networks as the principal means of spreading news about their campaigns.

Table I. Principal networks used by candidates.

Candidate	Twitter	Facebook	Telegram	Aparat	Instagram
Rouhani	X	X	X	-	X
Jahangiri	X	-	X	-	X
Raisi	-	-	X	X	X
Ghalibaf	-	-	X	X	X
Hashemitaba	-	-	-	-	-
Mirsalim	X	X	X	X	X

Keeping in mind that Twitter, Facebook and Youtube are banned, the messaging application Telegram and the photograph- and video-sharing platform Instagram are the most frequently used social networks, both by the candidates themselves (see **Error! Reference ource not found.**) and by citizens in general [3]. Nevertheless, the authorities placed certain limits on these social networks, such as the government being notified whenever public groups have more than 5,000 users. As a result, according to the Centre for Human Rights [4] in Iran, at least twelve Telegram channel administrators were arrested in mid-march.

In order to avoid the sort of influence false news stories on Facebook had on the American presidential elections, Iran also banned Telegram voice calls, as well as Instagram's function for transmitting live video [5]. Nevertheless, in spite of strict controls, two cases of false news being spread over Telegram were registered. The first spoke of the murder of 27 people in a shopping centre in Tehran, while the second was related to supposed warnings of the illegal activities of the Iranian Internet Police (FATA) through the social network.

Not only social networks were subject to bans. Some web pages have also been the victims of censure, with constant repression being used against informers, according to Reporters Without Borders [6]. A certain degree of repression was also exercised against student movements in universities. 92 student organizations wrote a letter to President Rouhani expressing their concern over threats against students after Supreme Leader Ali Khamenei spoke about the politicization of students. Dozens of students were expelled for political reasons between 2005 and 2016, and have been unable to resume their studies at the end of 2016 [7].

Iran has been accused by different security investigators [8] of creating several tools for obtaining sensitive information or taking control of systems belonging both to individuals and foreign powers. One example of this is MacDownloader, a piece of malware developed for Mac systems that has been used to attack United States defence contractors and human rights defenders. Disguised as a false Flash Player software installer or a false antivirus, this piece of malware has certain design errors and uses obsolete

persistence techniques, but has nevertheless been effective at obtaining user credentials.

Another tool in their arsenal is Infy, which according to investigators from Palo Alto has been in operation for ten years. This type of malware is habitually transmitted by email, using attachments on Word documents or PowerPoint presentations, which contain executable compressed files that are self-extracting. It includes keylogging functions in order to obtain data and tools for the exfiltration of the same, with recent variants enabling remote control of infected systems. The most recent samples are from 19 March 2017, appearing in a whole series of business sectors, principally in companies aimed at wholesale, high technology, telecommunications and governments. The geographic distribution of the same is limited, with victims in Ireland, the United States, the Netherlands and Turkey. Infy operators have principally used IP addresses from attacked countries to place C&Cs as means of evasion.

Iran is also believed to be behind the RocketKitten I and II campaigns, where web browsing was used as an infection path. The principal affected sectors were high technology companies, government organisations and companies aimed at wholesale. Similarly, the countries attacked were Ireland, the United States, the Netherlands, Turkey and Spain.

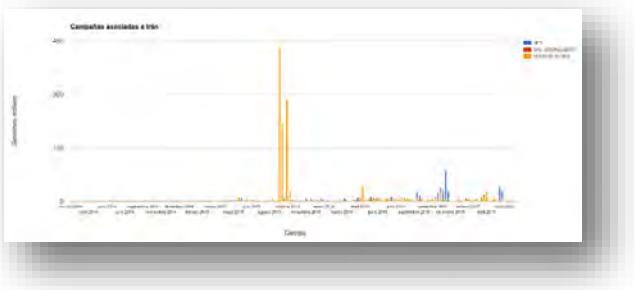

Figure 1. Number of active sessions of each piece of malware or campaign associated with Iran.

Furthermore, specific campaigns like Woolen-GoldFish (also associated with the Rocket Kitten group) used phishing attacks to penetrate victims' systems. In this case, the defence industry, the information technology sector, government organisations and academic organisations were the most affected. One of the associated samples is GHOLE, which uses macros for infection. This malware is spread to a remote server using HTTP, and, once installed, it allows complete control over the victim's machine. The origin of this family of malware is associated with a cracked version of the legitimate software Core Impact, used by pentesters.

Other Considerations

Hassan Rouhani was candidate for president in 2013, and focused his message on the promise of improved access to the internet and information. He was re-elected in May, and his internet policy continues to be key. His success in this area has been mixed, since the Supreme Council of Cyberspace has the final word on decisions involving the Internet. This body includes judicial powers and the Revolutionary Guard, and is directly subject to Ali Khamenei.

[1] Internet World Stats, «Iran Internet Stats and Telecommunications Reports», 30-jun-2016. [En línea]. Disponible en: http://www.internetworldstats.com/me/ir.htm. [Accedido: 31-may-2017].

[2] Central Intelligence Agency, «The World Factbook — Central Intelligence Agency». [En línea]. Disponible en: https://www.cia.gov/library/publications/the-world-factbook/fields/2010.html. [Accedido: 31-may-2017].

[3] «¿Cómo ha logrado Telegram conquistar Irán?», *Intereconomia*, 10-mar-2017. .

[4] «Admins of 12 Reformist Telegram Channels Arrested in Iran Ahead of May 2017 Election», *Center for Human Rights in Iran*, 21-mar-2017. .

[5] «Iran's Judiciary Blocks Instagram's Live Video Service Weeks Before May 2017 Elections», *Center for Human Rights in Iran*, 28-abr-2017. .

[6] «Irán :: Informe Anual 2015 - Reporteros Sin Fronteras». [En línea]. Disponible en: http://www.informeanualrsf.es/news/iran/. [Accedido: 31-may-2017].

[7] «OHCHR United Nations Human Rights Council». [En línea]. Disponible en: http://www.ohchr.org/EN/HRBodies/HRC/Pages/HRCIndex.aspx. [Accedido: 31-may-2017].

[8] «Iran Threats: Documenting Iranian State Sponsored Hacking». [En línea]. Disponible en: https://iranthreats.github.io/. [Accedido: 04-jun-2017].

About ElevenPaths

At ElevenPaths we believe in the idea of challenging the current state of security, a characteristic which should always be present in technology. We are continually rethinking the relationship between security and people, with the aim of creating innovative products capable of transforming the concept of security and thereby keeping one step ahead of our attackers, who are increasingly present in our digital lives.

Further Information

www.elevenpaths.com

@ElevenPaths

blog.elevenpaths.com