Iran's domestic espionage: Lessons from recent data leaks

intel471.com/blog/irans-domestic-espionage

By the Intel 471 Global Research Team.

In the last decade, Iran has undergone a quiet revolution. Since the"Green Movement" uprising in 2009, more Iranians have dared to openly oppose their regime. The reasons include accusations of elections tampering, global sanctions, increased inflation, heavy investment of state funds in the nuclear and arming programs, and ambitious regional policies in Lebanon, Syria, Iraq, Yemen and others, amid a deteriorating socioeconomic situation of the average Iranian.

There was a lot of talk in the past about Iran's espionage measures and offensive cyber activities targeting other countries. However, growing domestic unrest prompted the Iranian regime to invest more resources in developing espionage capabilities aimed against its own citizens. Additionally, the regime carried out tough measures against civil uprisings such as cutting off the internet in the country for long periods of time and killing hundreds of protestors.

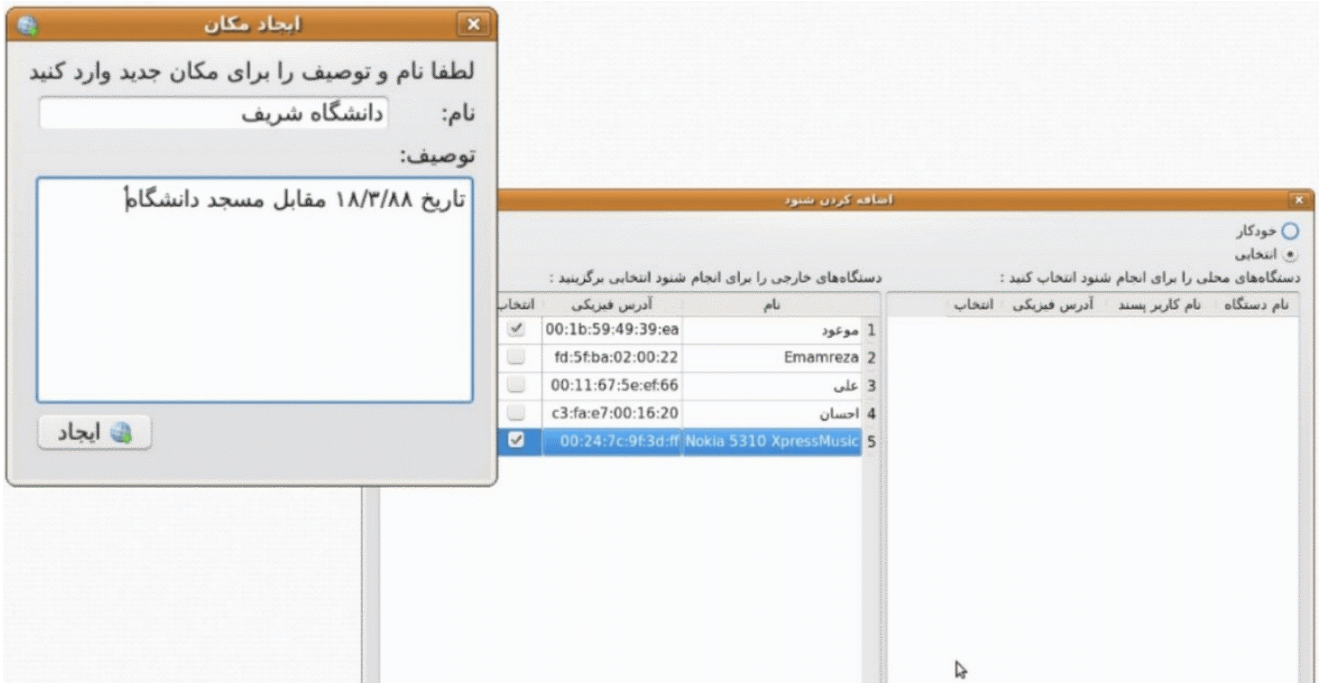
During the past year, a number of online activists have leaked what they claim to be inside information about the regime's surveillance methods, in an attempt to expose the unethical tactics used by Iranian security forces. Among the top whistleblowers are operators of the Lab Dookhtegan (translated in Persian as "stitched lips") Telegram channel and an activist named Masoud Molavi. Molavi, assassinated by Iranian agents in November 2019, was a former cybersecurity official behind the Black Box Telegram channel that was responsible for many notable leaks of Iranian government information.

The series of leaks uncovered hundreds of documents that offer a glimpse into the way Iran is spying on its own people. According to the leaked information, the Islamic Revolutionary Guard Corps (IRGC) and the Iranian Ministry of Intelligence Services (MOIS) developed numerous tools, malicious software, surveillance systems and data analysis platforms, in order to control citizens in Iran and abroad. Much of this activity allegedly was conducted in the Rana Intelligent Computing Institute, an organization working under the Iranian MOIS, involved in internal espionage by developing unique tools and gaining access to a variety of foreign countries' infrastructure.

Tools and Techniques used for Domestic Espionage

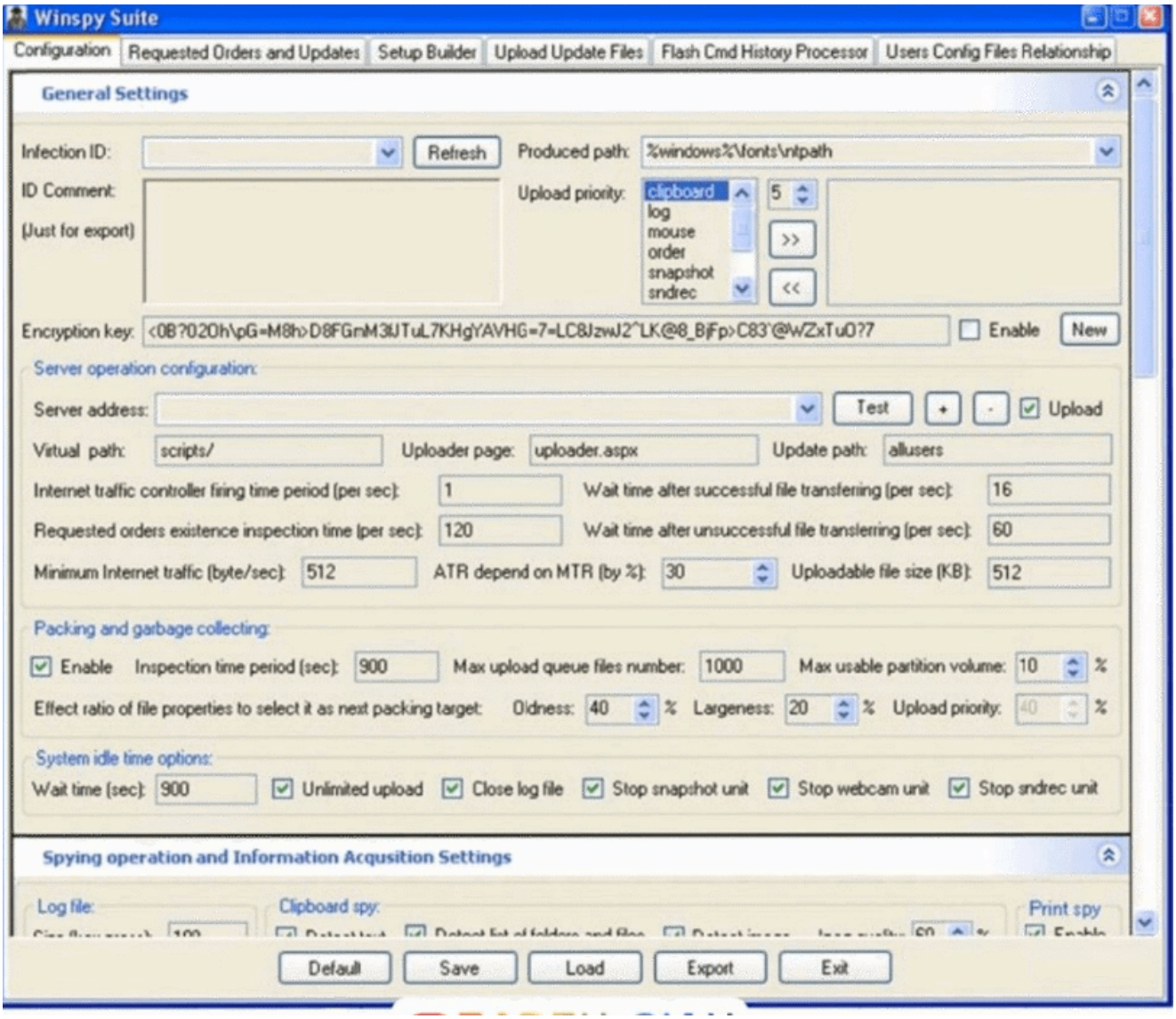
According to the information shared by these whistleblowers, Iran is heavily investing in the development of customized tools and malicious software for domestic espionage. For example, the Iranian regime developed a surveillance system dubbed Abi, which allegedly

was used to spy on political activists, human rights lawyers, regime opponents and protesters by intercepting Bluetooth communications. According to an Iranian blog called Arezooyenatamam, (translated in Persian as 'an unfinished dream"), this system has been installed on pickup trucks posted in strategic locations in Iran such as university campuses or protest centers.



A screenshot from the Abi system monitoring of Sharif University

The Iranian regime also developed customized malware used for stealing information from citizens. One example found in those leaks was called WinspySuite, a remote access and information stealing malware that reportedly was used specifically to spy on suspects arrested by the regime. Internally referred to as Peyvand, the malware allegedly was loaded onto a target's computer via a USB flash drive during interrogations or sent via a malicious link to a victim's email address. The regime also developed a remote access tool for Android and iPhone mobile devices as part of a project dubbed Project 220. The malware purportedly was able to steal sensitive data from a victim's device, including call data, text messages, contacts and locations.



A screenshot from the Winspy Suite control panel

Another malware project dubbed Project 420 aka Dolphin developed, deployed and controlled an undisclosed mobile malware capable of collecting and analyzing information about the activities of individuals and groups on social media networks including Facebook, Twitter, and Instagram, and on messaging applications such as Telegram.

According to leaked information, the regime not only developed tools for stealing sensitive data from its citizens, but also created designated platforms for the collection and analysis of the data. A system dubbed Payamak was developed to store and analyze text messages from targeted subjects. A software called Seraj was used as an analytical search engine for data on suspects, employees, intelligence operations and arrests related to the MOIS. Another system mentioned in reports dubbed Shojreh includes a mapping of family relations of Jewish people in Iran and abroad.

Additionally, the IRGC and MOIS gained unauthorized access to legitimate services or websites to spy on Iranian citizens. For example, the MOIS would compromise Iran's National Library computer network seeking to obtain personal information about users, mainly students and political prisoners, and their topics of interest. The MOIS allegedly also abused this access to send phishing emails with malicious attachments from the library's official email account.

Tracking Iranians Abroad

In addition to all of the above, the Iranian government is making great efforts to monitor citizens going abroad by surveying and analyzing location data obtained from Iranian cellular operators with a system called Pouya, and by compromising the infrastructure of foreign companies.

A screenshot from the Pouya system

In 2019, an unknown activist or group of activists launched a site called "Vagheyatepenhaan" (translated in Persian as 'the hidden facts') to expose Iranian regime espionage-related activity. The site contains a large section about espionage enterprises outside Iran that was conducted to monitor the movement of Iranians traveling abroad. According to this information, the regime gained access to computer systems of numerous airline companies in Bahrain, Dubai, India, Indonesia, Malaysia, Pakistan, the Philippines, Qatar, Saudi Arabia, Thailand and the United Arab Emirates (UAE) for data collection on flights of Iranian citizens. In another case, leaked documents showed the government worked on a project that aimed to compromise hotel websites in the Republic of Georgia, a neighboring country and a popular holiday destination for Iranians.

While they can be considered revealing, It should be noted that these leaks provide a very narrow window into the full extent of the Iranian regime's priorities. However, the information disclosed provides evidence that as time goes by, motivation to expose these activities likely will remain high.