Security researchers at Check Point have unravelled a six-year, ongoing surveillance operation apparently run by Iran-based threat actors against regime dissidents.

Going back as far as 2014, the attackers used multiple attack vectors to spy on their victims, including hijacking victims’ Telegram accounts, extracting two-factor authentication codes from SMS messages, recording a phone’s audio surroundings, accessing KeePass password manager account information, and distributing malicious Telegram phishing pages using fake accounts.

Malware-laced documents
The victims appear to have been hand-picked from anti-regime organisations and resistance movements such as Mujahedin-e Khalq, the Azerbaijan National Resistance Organisation, which advocate the liberation of Iranian people and minorities within Iran, and Balochistan citizens.

The attackers used malware-laced documents to lure victims into infecting their devices. The core functionality of the malware is to steal as much information as it can from the target device. The payload targets two main applications: Telegram Desktop and KeePass, the famous password storage manager. The main features of the malware include:

- **Information Stealer**
  - Uploads relevant Telegram files from victim’s computer. These files allow the attackers to make full usage of the victim's Telegram account
  - Steals information from KeePass application
  - Uploads any file it could find which ends with pre-defined extensions
  - Logs clipboard data and takes desktop screenshots

- **Unique Persistence**
  - Implements a persistence mechanism based on Telegram’s internal update procedure

### Two-factor authentication

During their investigation, Check Point researchers also uncovered a malicious Android application tied to the same threat actors. The application masquerades as a service to help Persian speakers in Sweden get their driver's license. This Android backdoor contains the following features:
Steals existing SMS messages
Forwards two-factor authentication SMS messages to a phone number provided by the attacker-controlled C&C server
Retrieves personal information like contacts and accounts details
Initiates a voice recording of the phone's surroundings
Performs Google account phishing
Retrieves device information such as installed applications and running processes

Setting up an account

Some of the websites related to the malicious activity also hosted phishing pages impersonating Telegram. Surprisingly, several Iranian Telegram channels issued warnings against the phishing websites, claiming that the Iranian regime is behind them. According to the channels, the phishing messages were sent by a Telegram bot.

The messages warned their recipient that they were making an improper use of Telegram's services, and that their account will be blocked if they do not enter the phishing link. Another Telegram channel provided screenshots of the phishing attempt showing that the attackers set up an account impersonating the official Telegram one. At first, the attackers sent a message about the features in a new Telegram update to appear legitimate. The phishing message was sent only five days later, and pointed to a malicious domain.

Cyber-security expert
A removed blog entry from 2018 accused a cyber-security expert of plagiarism, when he was interviewed by AlArabiya news to discuss Iranian cyber-attacks. Researchers believe this page was created as part of a targeted attack against this person or his associates.

The blog included a link to download a password-protected archive containing evidence of the plagiarism from `endupload[.]com`. It appears that `endupload[.]com` has been controlled by the attackers for years, as some of the malicious samples related to this attack dating to 2014 communicated with this website.

**Monitoring different geographies**

Lotem Finkelsteen, Manager of Threat Intelligence at Check Point said: “After conducting our research, several things stood out. First, there is a striking focus on instant messaging surveillance. Although Telegram is un-decryptable, it is clearly hijackable. Instant messaging surveillance, especially on Telegram, is something everyone should be cautious and aware of”

“Second, the mobile, PC and web phishing attacks were all connected to the same operation. These operations are managed according to intelligence and national interests, as opposed to technological challenges. We will continue to monitor different geographies across the world to better inform the public around cyber security.”
You may also be interested in...

**Why RMR is more important than ever for security integrators**

The security industry knows the value of recurring revenue, as it’s the foundation of the residential security monitoring market. Comm...

**Check Point Research publishes the Global Threat Index for August 2020**

Check Point Research, the Threat Intelligence arm of Check Point® Software Technologies Ltd, a provider of cyber security solutions glob...

**Be our guest: How to manage visitors with both safety and service**

In today’s fraught times, business continuity and success hinges on how you manage the visitors to your company. By prioritising safet...

**Check Point Software Technologies acquires Odo Security to provide sec...**

Check Point® Software Technologies Ltd., a provider of cyber security solutions globally, announces the acquisition of a new cloud-based...