Fox Kitten – Widespread Iranian Espionage-Offensive Campaign – ClearSky Cyber Security

Published: 2020-02-16 · Archived: 2026-04-06 00:27:24 UTC

During the last quarter of 2019, ClearSky research team has uncovered a widespread Iranian offensive campaign which we call “Fox Kitten Campaign”; this campaign is being conducted in the last three years against dozens of companies and organizations in Israel and around the world.

Read the full Report: Fox Kitten – Widespread Iranian Espionage-Offensive Campaign

Though the campaign, the attackers succeeded in gaining access and persistent foothold in the networks of numerous companies and organizations from the IT, Telecommunication, Oil and Gas, Aviation, Government, and Security sectors around the world.

We estimate the campaign revealed in this report to be among Iran’s most continuous and comprehensive campaigns revealed until now. Aside from malware, the campaign enfolds an entire infrastructure dedicated to ensuring the long-lasting capability to control and fully access the targets chosen by the Iranians. The revealed campaign was used as a reconnaissance infrastructure; however, it can also be used as a platform for spreading and activating destructive malware such as ZeroCleare and Dustman, tied to APT34.

During our analysis, we have found an overlap, with medium-high probability, between this campaign’s infrastructure and the activity of an Iranian offensive group APT34-OilRig. Additionally, we have identified, with medium probability, a connection between this campaign and the APT33-Elfin and APT39-Chafer groups. The campaign was first revealed by Dragos, named “Parisite” and attributed to APT33; we call the comprehensive campaign revealed in this report “Fox Kitten”.

We assess with a medium probability that the Iranian offensive groups (APT34 and APT33) have been working together since 2017, though the infrastructure that we reveal, vis-à-vis a large number of companies in Israel and around the world.

The campaign infrastructure was used to:

- Develop and maintain access routes to the targeted organizations
- Steal valuable information from the targeted organizations
- Maintain a long-lasting foothold at the targeted organizations
- Breach additional companies through supply-chain attacks

The campaign was conducted by using a variety of offensive tools, most of which open-source code-based and some – self-developed.

Our main insights:

- The Iranian APT groups have succeeded to penetrate and steal information from dozens of companies around the world in the past three years.
- The most successful and significant attack vector used by the Iranian APT groups in the last three years has been the exploitation of known vulnerabilities in systems with unpatched VPN and RDP services, in order to infiltrate and take control over critical corporate information storages.
- This attack vector is not used exclusively by the Iranian APT groups; it became the main attack vector for cybercrime groups, ransomware attacks, and other state-sponsored offensive groups.
- We assess this attack vector to be significant also in 2020 apparently by exploiting new vulnerabilities in VPNs and other remote systems (such as the latest one existing in Citrix).
- Iranian APT groups have developed good technical offensive capabilities and are able to exploit 1-day vulnerabilities in relatively short periods of time, starting from several hours to a week or two.
- Since 2017, we identify Iranian APT groups focusing on IT companies that provide a wide range of services to thousands of companies. Breaching those IT companies is especially valuable because through them one can reach the networks of additional companies.

- After breaching the organizations, the attackers usually maintain a foothold and operational redundancy by installing and creating several more access points to the core corporate network. As a result, identifying and closing one access point does not necessarily deny the capability to carry on operations inside the network.
- We assess with a medium-high probability that Iranian APT groups (APT34 and APT33) share attack infrastructures. Furthermore, it can be one group that was artificially marked in recent years as two or three separate APT groups.
- The time needed to identify an attacker on a compromised network is long and varies between months to not at all. The existing monitoring capability for organizations to identify and block an attacker that entered through remote communication tools is difficult to impossible.

We would like to thank **researchers from Dragos** who found the first signs of the campaign (which they call “Parisite”) and shared with us valuable information that helped us reveal the whole Fox Kitten campaign presented in this report.
