The Kittens Are Back in Town 2 – Charming Kitten Campaign Keeps Going on, Using New Impersonation Methods

clearskysec.com/the-kittens-are-back-in-town-2

by ClearSky Research Team October 7, 2019

On the 15th of September 2019, we have published a report[1] about a sharp increase in Charming Kitten attacks against researchers from the US, Middle East, and France, focusing on Iranian academic researchers, Iranian dissidents in the US. In our last report, we exposed a new cyber espionage campaign that was conducted in July 2019. Since then, we observed another wave of these attacks, leveraging new impersonating vectors and IOCs.

Until these days, Iran was not known as a country who tends to interfere in elections around the world. From a historical perspective, this type of cyber activity had been attributed mainly to the Russian APT groups such as APT28 (known as Fancy Bear). The group is infamous for hacking American Democratic National Committee emails and targeting German and French campaign members, in an attempt to circumvent the elections in the US, Germany, and France.

Microsoft's October announcement exposes, for the first time, that **Charming Kitten, an Iranian APT group, plays a role in the domain of cyber-attacks for the purpose of interfering with democratic procedures.**

On 4th of October 2019[2], Microsoft has announced that Phosphorus (known as Charming Kitten) attempted to attack email accounts that are associated with the following targets: U.S. presidential campaign, current, and former U.S. government officials, journalists covering global politics, and prominent Iranians living outside Iran. These spear-phishing attacks were conducted by Charming Kitten in August and September. **We evaluate in a medium-high level of confidence, that Microsoft's discovery and our findings in our previous and existing reports is a congruent operation.**

Read the full report: The Kittens Are Back in Town 2

Our evaluation based on the following issues:

1. **Same victim profiles** – In both cases, the victims were individuals of interest to Iran in the fields of academic research, human rights, opposition to the Islamic Republic of Iran's regime (such as NIAC) and journalists. Although the congruent is not exactly similar, our sample is mainly based on Israeli victims.
2. **Time overlapping** – In our latest report, we mentioned that we have observed an escalation of the attacks in July-August 2019. In their announcement, Microsoft mentioned that the attacks occurred on 'In a 30-day period between August and September'.

3. **Similar attack vectors** – In both cases, Charming Kitten used similar attack vectors which are:
    1. Password recovery impersonation of the secondary email belonging to the victims in both cases.
    2. Both attack vectors used spear-phishing emails in order to target Microsoft, Google and Yahoo services.
    3. In our research, we identified a spear-phishing attack via SMS messages, indicating that Charming Kitten gathers phone numbers of the relevant victim. Microsoft found that Charming Kitten gathers phone numbers for password recovery and two-factor authentications of the relevant victims to gain control of their email accounts.

In this report, we uncovered four new spear-phishing methods used by this group, alongside with new indicators of this operation.

Indicators of compromise are available for subscribers of the ClearSky threat intelligence service in MISP events 1745.

---

[1] https://www.clearskysec.com/the-kittens-are-back-in-town/

[2] https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/
