My regional focus is Iran because of my linguistic ties to the country. As such I found one notable APT with various names known as charming kitten (crowdstrike), APT35 (FireEye), group 83 (CISCO), G0058 (MITREATT&CK), and iKittens. It is most commonly known as charming kitten. Based on my understanding of naming conventions each organization has a different method. For instance crowdstrike use of kitten denotes that it is an Iranian threat actor, while FireEye, CISCO and Mitre Att&ck appear to just use a standard numbering system. The other common name, iKittens, indicates a little more. Following crowdstrikes naming convention I understand that it is an Iranian threat actor, and the use of "i" suggest a relationship to apple devices. After a little reading "charming kitten" also alludes to more in which the attackers use some method of social manipulation to gain the trust of the victim in order to gain access into a system

## FireEye

#### https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

APT35 aka the "Newscaster Team" uses unsophisticated tools to employ fake social media personas with convincing backgrounds claiming to be part of a news organization and uses these complex social engineering campaigns to compromise systems in efforts to conduct reconnaissance and steal credentials. Their targets include telecommunications, business services, energy, construction and engineering, government, defense, and the media. A case study on APT35 in 2017 targeting an energy company through a spear-phishing email showed the IOCs for APT35 targets. Based on my understanding of IOCs, one of the major ones for APT35 regarding this case study are email addresses and malware hashes.

## iKittens

#### https://iranthreats.github.io/resources/macdownloader-macos-malware/

This articles suggest my guess on the naming convention wasn't too far off. The Iranian actor resurfaces with a malware for Mac targeting the defense industrial base. Through social engineering the attacker convinces victims to download a MacOS malware agent, named MacDownlaoder that poses as both an installer for Adobe Flash and a Bitdefender Adware Removal Tool. It may have been first a fake virus removal tool and then repurposed to a fake Flash Player to fit a particular social engineering attempt. It was identified through these IOCs that were labeled at the bottom of the report:

- Hashes:

addone flashplayer.app.zip

52efcfe30f96a85c9c068880c20663db64f0e08346e0f3b59c2e5bbcb41ba73c

Bitdefender Adware Removal Tool

7a9cdb9d608b88bd7afce001cb285c2bb2ae76f5027977e8635aa04bd064ffb7

- Network

46.17.97[.]37

officialswebsites[.]info

utc.officialswebsites[.]info

## Comparision

The similarities that unite these two reports are the targets and the method of attack. Using complex social engineering and unsophisticated technology, this APT infiltrates and compromises systems in order to conduct reconnaissance and transmit files specifically credentials. Between the two reports I did not see a similar IOCs, though in the iKitten report similarities between naming conventions alluded to Persian grammar structure and I quote the "continuity in certain infrastructure and rends in targeting" suggest relationship to Charming Kittens. Another notable identifier is something called "snc" that is shared in victims of concurrent spear phishing campaigns. I am not sure what "snc" means but it has something to do with communicating to the C2 in exfiltrating data from the victim. Additionally, the researchers in this report were able to identify more ties to Iran namely a software and hosting firm, Novin Pardaz Zenderod, in Isfahan, Iran as well as wireless networks complicit in earlier Iranian campaigns specifically Jok3r and mb\_1986.