CHARMING KITTEN

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON CHARMING KITTEN: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Charming Kitten is an Iranian cyber espionage group that has been active since approximately 2014. They appear to focus on targeting individuals of interest to Iran who work in academic research, human rights, and media, with most victims having been located in Iran, the US, Israel, and the UK. [Charming Kitten often tries to access private email and Facebook accounts, and sometimes establishes a foothold on victim computers as a secondary objective.

II. TARGETS

Charming Kitten (aka Parastoo, aka Newscaster) is an group with a suspected nexus to Iran that targets organizations involved in government, defense technology, military, and diplomacy sectors.

III. METHODS USED

- Ending an email message leveraging social engineering methods.
- Impersonating social media websites, such as Facebook, Twitter and Instagram, as well as using these social media to spread malicious links. Experts also has observed a few social media entities that used social media to contact their victims in order to trick them into visiting malicious websites.
- Sending SMS messages to the cellular phone of the victim. The messages include a link and claim to inform the recipient of an attempt to compromise their email account. The link points to a malicious phishing website.

IV. CAMPAIGNS

- **2013** : In 2013, former United States Air Force technical sergeant and military intelligence defense contractor Monica Witt defected to Iran knowing she might incur criminal charges by the United Stages for doing so.[citation needed] Her giving of intelligence to the government of Iran later caused Operation Saffron Rose, a cyberwarfare operation that targeted US military contractors.
- **2015** : ClearSky discovered the first wave of phishing attacks, named "Thamar reservoir".
- **2017** : • ClearSky exposed a vast espinage operation against Iranian experts working in the academy, human rights activists and media personnel.
- **2018** : Charming Kitten attempted to attack ClearSky and our customers directly via a fraudulent website impersonating the ClearSky portal. ClearSky identified new wave of attacks against researchers in the Middle East, using fake emails and look alike webistes.
- **2019** : • March - Microsoft filed an official complaint against the group for “establishing an internet-based cyber theft operation referred to as 'Phosphorus'.”
- September- ClearSky published a report about a sharp increase in Charming Kitten attacks. It appears that group has initiated a new cyber espionage campaign comprised of two stages.
- October - Microsoft announced that ‘the group is making attempts to identify consumer email accounts belonging to specific Microsoft customers, including a US Presidential Candidate . ClearSky exposed new impersonation vectors.
- **2020** : According to Microsoft, in a 30-day period between August and September 2019, Charming Kitten made 2,700 attempts to gain information regarding targeted email accounts. This resulted in 241 attacks and 4 compromised accounts. Although the initiative was deemed to have been aimed at a United States presidential campaign, none of the compromised accounts were related to the election.Microsoft did not reveal who specifically was targeted, but a subsequent report by Reuters claimed it was Donald Trump's re-election campaign.[15] This assertion is corroborated by the fact that only the Trump campaign used Microsoft Outlook as an email client.

AX1AL

V. IOCS

C2's

my[.]en-gb[.]home-access[.]online
notification-accountservice[.]com
recovery-services[.]info
recoverysuperuser[.]info
see-us[.]info
sessions-identifier-memberemailid[.]network
smarttradingfast[.]com
system-services[.]site
telagram[.]net
uploaddata[.]info
verification-services[.]info
40[.]112[.]253[.]185
91[.]109[.]22[.]53
136[.]243[.]195[.]229
178[.]32[.]58[.]182
185[.]177[.]59[.]240
46[.]166[.]151[.]209
51[.]68[.]200[.]126
51[.]89[.]229[.]215
51[.]255[.]157[.]110
181[.]177[.]59[.]240

TTP's

Application Layer Protocol: Web Protocols.
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder,
Command and Scripting Interpreter: PowerShell
Command and Scripting Interpreter: Windows Command Shell, Query Registry,
System Information Discovery,
System Owner/User Discovery

VI. References / Sources

https://securityaffairs.co/wordpress/92469/apt/charming-kitten-impersonation-methods.html#:~:text=As%20part%20of%20the%20recently,media%20to%20spread%20malicious%20links.
https://www.clearskysec.com/wp-content/uploads/2019/10/The-Kittens-Are-Back-in-Town-2.pdf
https://attack.mitre.org/groups/G0058/
https://en.wikipedia.org/wiki/Charming_Kitten