Iran's APT35 targeting individuals tied to US 2020 elections

Reference: Memo [191009-1] – Version: 1.0
Keywords: Targeted intrusion, Iran, US, election targeting, cloud services, social media, Microsoft O365
Sources: Publicly available information

Key Points

- An Iranian state-sponsored threat actor reportedly targeted accounts associated with the US presidential campaign.
- The group has also reportedly targeted academic researchers focusing on Iran in France, the US and the Middle-East.
- Attempts by state-sponsored threat actors from various countries to compromise business or personal cloud-based email or social media accounts remain a significant threat.
- Even if not technically sophisticated, social engineering enabled attempts to compromise cloud based email or social network accounts remain an efficient method for motivated attackers.

Summary

On October 4, Microsoft released a message[1] warning about a state-sponsored group attempting to take over Microsoft accounts. More specifically, over a period of 30 days, the likely Iran-based threat actor APT35 (aka Phosphorus, Charming Kitten, Newscaster) executed reconnaissance activities (user identification) on 2.700 specific Microsoft user accounts, attempted to take over 241 of them, and succeeded to compromise 4 of them.

Targeted accounts are reportedly associated with "the US presidential campaign, journalists covering global politics and prominent Iranians living outside Iran." Although this threat actor seems to be especially interested in US entities, APT35 also reportedly[2] targeted non-Iranian researchers from the Middle East and France, focusing on academic research of Iran.

The attackers reportedly conducted these account takeovers manually, using information (likely obtained via social engineering) such as telephone numbers and secondary email addresses to exploit legitimate account recovery processes.

Microsoft as well as other cloud service providers notify users when "unusual activity" has been discovered on their account. Attackers are capitalising on this by sending emails that pretend to be "unusual sign-in activity" alerts from Microsoft[3], even seemingly originating from the legitimate sender address "account-security-noreply@accountprotection.microsoft.com". The cyber security company Clearsky[4] backed Microsoft's assertions and detailed additional credential harvesting techniques recently employed by APT35. These include: (1) spoofing of Google Drive to deliver malicious URLs, (2) sending fake SMS alert messages about attempts to compromise the victim's Google mail, (3) sending fake Yahoo alert messages about attempts to compromise the victim's Yahoo mail, (4) impersonation of security teams of social networks (e.g. Instagram, Facebook and Twitter) in order to get authentication details.

Comments

State-sponsored APT groups are actively looking for credentials of business or personal, cloud-based, email accounts of specific individuals. In the case of APT35, social engineering methods used by attackers to harvest victims' credentials are not sophisticated but have proven to be efficient with 4 Microsoft accounts compromised per 241 attempts.

There had already been warnings by Microsoft, recently, about various state-sponsored actors attempting to take over accounts. In July, the company said[5] that 10.000 users had been targeted by nation state attacks in 2018 (84% of these attacks aimed at enterprise users). Microsoft added that "the majority of nation-state activity in this period originated from actors in three countries – Iran, North Korea, and Russia."

The US government and several IT security companies have historically been tracking and attempting to disrupt APT35 cyberattacks. In December 2018, the Associated Press reported[6] that APT35 was behind a spear phishing campaign targeting US Department of the Treasury officials, nuclear scientists, Iranian civil society figures, US think tank employees, and prominent supporters and critics of the Iranian nuclear deal. In April 2019[7], Microsoft announced it had disrupted attacks run by APT35, after suing the group's members in the US District Court for Washington D.C. and taking over 99 domains the hackers had used in their malicious campaigns.

Although Microsoft's message at this point is not specific, it is likely that APT35 was attempting to compromise email accounts associated with the Office 365 (O365) platform. In any case, Microsoft and other such companies have a broad portfolio of online services. Even if the attackers were not directly going for O365, acquiring the credentials would still give them significant access to the individuals targeted through associated services, such as email, skype, etc.

[1] https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/
2 https://www.clearskysec.com/the-kittens-are-back-in-town/
3 https://www.bleepingcomputer.com/news/security/beware-of-fake-microsoft-account-unusual-sign-in-activity-emails/
4 https://www.clearskysec.com/the-kittens-are-back-in-town-2/
[5] https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/
6 https://www.apnews.com/od4dcaaboe134cf6a1c6ce6be3b7b6a8
7 https://www.bleepingcomputer.com/news/security/microsoft-retaliates-against-apt35-hacker-group-by-seizing-99-domains/