Charming Kitten

By Contributors to Wikimedia projects

Published: 2019-09-10 · Archived: 2026-04-05 21:14:02 UTC

From Wikipedia, the free encyclopedia

Charming Kitten

Formation	c. 2004–2007[1]
Type	Advanced persistent threat
Purpose	Cyberespionage, cyberwarfare
Region	Middle East
Methods	Zero-days, spearphishing, malware, Social Engineering, Watering Hole
Membership	At least 5
Official language	Persian
Parent organization	IRGC
Affiliations	Rocket Kitten APT34 APT33
Formerly called	APT35 Turk Black Hat Ajax Security Team Phosphorus

Charming Kitten, also called **APT35** (by Mandiant), **Phosphorus** or **Mint Sandstorm** (by Microsoft[1]), **Ajax Security** (by FireEye[2]), and **NewsBeef** (by Kaspersky[3][4]) is an Iranian government cyberwarfare group, described by several companies and government officials as an advanced persistent threat (APT).

The United States Cybersecurity and Infrastructure Security Agency (CISA) has identified Charming Kitten as one of several Iranian state-aligned actors that target civil society organizations, including journalists, academics, and human rights defenders, in the United States, Europe, and the Middle East, as part of efforts to collect intelligence, manipulate discourse, and suppress dissent.[5]

The group is known to conduct phishing campaigns that impersonate legitimate organizations and websites, using fake accounts and domains to harvest user credentials.[6]

The entire national mass surveillance "Kashef" database software and its domain " built by the IRGC CYBER COM to spy on Iranian public was hacked in 2025 as well real life identities of the entire chain of command from the hacker groups, with its CEO main runner of a front corporation "Amn Afzar company " being IRGC commander Nilofar Bagheri.[7]

National mass surveillance software used by Unit40, by Iran International
https://vimeo.com/1137702960/faabbbf3a4

Witt defection (2013)

[edit]

In 2013, former United States Air Force technical sergeant and military intelligence defense contractor Monica Witt defected to Iran[8] knowing she might incur criminal charges by the United States 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.[*citation needed*]

HBO cyberattack (2017)

[edit]

In 2017, following a cyberattack on HBO, a large-scale joint investigation was launched on the grounds that confidential information was being leaked. A conditional statement by a hacker going by alias **Sokoote Vahshat** (Persian سکوت وحشت lit. 'Silence of Fear') said that if money was not paid, scripts of television episodes, including episodes of *Game of Thrones*, would be leaked. The hack caused a leak of 1.5 terabytes of data, some of which was shows and episodes that had not been broadcast at the time.[9] HBO has since stated that it would take steps to make sure that they would not be breached again.[10]

Behzad Mesri was subsequently indicted for the hack. He has since been alleged to be part of the operation unit that had leaked confidential information.[11]

According to Certfa, Charming Kitten had targeted US officials involved with the 2015 Iran Nuclear Deal. The Iranian government denied any involvement.[12][13]

Second indictment (2019)

[edit]

A federal grand jury in the United States District Court for the District of Columbia indicted Witt on espionage charges (specifically "conspiracy to deliver and delivering national defense information to representatives of the Iranian government"). The indictment was unsealed on February 19, 2019. In the same indictment, four Iranian

nationals—Mojtaba Masoumpour, Behzad Mesri, Hossein Parvar and Mohamad Paryar—were charged with conspiracy, attempting to commit computer intrusion, and aggravated identity theft, for a campaign in 2014 and 2015 that sought to compromise the data of Witt's former co-workers.[14]

In March 2019, Microsoft took ownership of 99 DNS domains owned by the Iranian government-sponsored hackers, in a move intended to decrease the risk of spear-phishing and other cyberattacks.[15]

Media impersonation campaign (2019-2020)

[edit]

In 2020, *Reuters* reported that Charming Kitten targeted critics of the Iranian government, academics, and journalists, such as Erfan Kasraie and Hassan Sarbakhshian, who received fake interview requests designed to harvest email credentials. The emails impersonated reporters from outlets like *The Wall Street Journal*, *CNN*, and *Deutsche Welle*, sometimes asking recipients to enter Google passwords or sign bogus contracts. Cybersecurity firms Certfa, ClearSky, and Secureworks attributed the operation to Charming Kitten based on tactics, infrastructure, and targeting.[16]

2020 election interference attempts (2019)

[edit]

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.[17] 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.[18] This assertion is corroborated by the fact that only the Trump campaign used Microsoft Outlook as an email client.

Iran denied any involvement in election meddling, with the Iranian Foreign Minister Mohammad Javad Zarif stating "We don't have a preference in your election [the United States] to intervene in that election," and "We don't interfere in the internal affairs of another country," in an interview on NBC's "Meet The Press".[19]

Cybersecurity experts at Microsoft and third-party firms such as ClearSky Cyber Security maintain that Iran, specifically Charming Kitten, was behind the attempted interference, however. In October 2019, ClearSky released a report supporting Microsoft's initial conclusion.[20] In the report, details about the cyberattack were compared to those of previous attacks known to originate from Charming Kitten. The following similarities were found:

- **Similar victim profiles.** Those targeted fell into similar categories. They were all people of interest to Iran in the fields of academia, journalism, human rights activism, and political opposition.
- **Time overlap.** Verified Charming Kitten activity was ramping up within the same timeframe that the election interference attempts were made.

- **Consistent attack vectors.** The methods of attack were similar, with the malicious agents relying on spear-phishing via SMS texts.

Operational exposure (2020)

[edit]

In 2020, IBM's X-Force IRIS team uncovered over 40GB of data from Charming Kitten, including training videos showing operatives hacking email and social media accounts. The footage included access to accounts of US and Hellenic Navy personnel, failed phishing attempts on US officials, and use of tools like Zimbra to manage stolen credentials. Researchers described the discovery as a rare insight into the group's methods and suggested it showed limited ability to bypass multi-factor authentication.[21]

HYPERSCRAPE data theft tool (2022)

[edit]

On August 23, 2022, a Google Threat Analysis Group (TAG) blog post revealed a new tool developed by Charming Kitten to steal data from well-known email providers (i.e. Google, Yahoo!, and Microsoft).[22] This tool needs the target's credentials to create a session on its behalf. It acts in such a way that using old-style mail services looks normal to the server and downloads the victim's emails, and does some changes to hide its fingerprint.

Per the report, the tool is developed on the windows platform but not for the victim's machine. It uses both command line and GUI to enter credentials or other required resources like cookies.

Activist targeting in Europe (2023)

[edit]

In September 2023, Germany's domestic intelligence agency issued a public warning about "concrete spying attempts" by the Iranian-linked hacker group Charming Kitten, according to *The Guardian*. The report followed incidents documented across several European countries in which Iranian activists experienced hacking attempts, cyberattacks, online harassment, and threats of physical harm. Activists in Germany, France, the UK, and Spain were reportedly warned by local authorities about threats allegedly linked to Iranian cyber actors.[23]

- Sony Pictures hack
- Monica Witt

1. ^ *"Microsoft uses court order to shut down APT35 websites". CyberScoop. March 27, 2019. Archived from the original on February 6, 2023. Retrieved September 10, 2019.*
2. ^ *"Ajax Security Team lead Iran-based hacking groups". Security Affairs. May 13, 2014. Archived from the original on December 2, 2022. Retrieved September 10, 2019.*
3. ^ *"Freezer Paper around Free Meat". securelist.com. April 27, 2016. Archived from the original on January 28, 2023. Retrieved September 10, 2019.*

4. ^ *Bass, Dina. "Microsoft Takes on Another Hacking Group, This One With Links to Iran". news.bloomberglaw.com. Archived from the original on December 2, 2022. Retrieved September 10, 2019.*
5. ^ *"Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society" (PDF). U.S. Cybersecurity and Infrastructure Security Agency (CISA). May 14, 2024. Retrieved April 25, 2025.*
6. ^ *"Iranian Charming Kitten ATP group poses as Israeli cybersecurity firm in phishing campaign". Security Affairs. July 3, 2018. Archived from the original on December 4, 2022. Retrieved September 10, 2019.*
7. ^ *"افشای هویت مدیران «اداره ۴۰» اطلاعات سپاه؛ بزرگترین بانک اطلاعاتی جاسوسی تهران". content.iranintl.com. Retrieved December 5, 2025.*
8. ^ *Blinder, Alan; Turkewitz, Julie; Goldman, Adam (February 16, 2019). "Isolated and Adrift, an American Woman Turned Toward Iran". The New York Times. ISSN 0362-4331. Archived from the original on February 17, 2019. Retrieved April 23, 2022.*
9. ^ *"The HBO hack: what we know (and what we don't) - Vox". August 5, 2017. Archived from the original on April 23, 2019. Retrieved September 10, 2019.*
10. ^ *Petski, Denise (July 31, 2017). "HBO Confirms It Was Hit By Cyber Attack".*
11. ^ *"HBO Hacker Was Part of Iran's "Charming Kitten" Elite Cyber-Espionage Unit". BleepingComputer.*
12. ^ *"Iranian Hackers Target Nuclear Experts, US Officials". Dark Reading. December 15, 2018.*
13. ^ *Satter, Raphael (December 13, 2018). "AP Exclusive: Iran hackers hunt nuclear workers, US targets". AP NEWS.*
14. ^ *"Former U.S. Counterintelligence Agent Charged With Espionage on Behalf of Iran; Four Iranians Charged With a Cyber Campaign Targeting Her Former Colleagues" (Press release). United States Department of Justice, Office of Public Affairs. February 13, 2019.*
15. ^ *"Microsoft seizes 99 domains owned by Iranian state hackers". News @ WebHosting.info. March 28, 2019. Archived from the original on January 19, 2021. Retrieved September 10, 2019.*
16. ^ *"Exclusive: Iran-linked hackers pose as journalists in email scam". Reuters. February 5, 2020. Retrieved April 25, 2025.*
17. ^ *"Recent cyberattacks require us all to be vigilant". Microsoft On the Issues. October 4, 2019. Archived from the original on October 4, 2019. Retrieved December 10, 2020.*
18. ^ *Bing, Christopher; Satter, Raphael (October 4, 2019). "Exclusive: Trump campaign targeted by Iran-linked hackers - sources". Reuters.*
19. ^ *AP. "Iran denies US election meddling, claims it has no preference". The Times of Israel. ISSN 0040-7909. Retrieved December 10, 2020.*
20. ^ *"The Kittens Are Back in Town 2" (PDF). ClearSky Cyber Security. October 2019. Archived (PDF) from the original on September 9, 2024. Retrieved September 9, 2024.*
21. ^ *"Iranian state hackers caught with their pants down in intercepted videos". Ars Technica. July 17, 2020. Retrieved April 25, 2025.*
22. ^ *Bash, Ajax (August 23, 2022). "New Iranian APT data extraction tool". Threat Analysis Group (TAG). Archived from the original on September 9, 2024. Retrieved September 9, 2024.*
23. ^ *"Iranian activists across Europe are targets of threats and harassment". The Guardian. September 22, 2023. Retrieved April 25, 2025.*

Source: https://en.wikipedia.org/wiki/Charming_Kitten