Helix Kitten

Published: 2017-12-10 · Archived: 2026-04-05 20:03:02 UTC

From Wikipedia, the free encyclopedia

Helix Kitten

بچه گربه هلیکس	
Formation	c. 2004–2007[1]
Type	Advanced persistent threat
Purpose	Cyberespionage, cyberwarfare
Methods	Zero-days, spearphishing, malware
Official language	Persian
Affiliations	APT33
Formerly called	APT34

Helix Kitten (also known as **APT34** by FireEye, **OILRIG**, **Crambus**, **Cobalt Gypsy**, **Hazel Sandstorm**,[1] or **EUROPIUM**)[2] is a hacker group identified by CrowdStrike as Iranian.[3][4]

The group has reportedly been active since at least 2014.[3] It has targeted many of the same organizations as Advanced Persistent Threat 33, according to John Hultquist.[3]

In April 2019, APT34's cyber-espionage tools' source code was leaked through Telegram.[5][6]

The group has reportedly targeted organizations in the financial, energy, telecommunications, and chemical industries, as well as critical infrastructure systems.[3]

APT34 reportedly uses Microsoft Excel macros, PowerShell-based exploits and social engineering to gain access to its targets.[3]

1. ^ *"How Microsoft names threat actors"*. *Microsoft. Retrieved 21 January 2024.*
2. ^ *"Iranian State-Sponsored OilRig Group Deploys 3 New Malware Downloaders"*.

3. ^ Jump up to: ***a*** ***b*** ***c*** ***d*** ***e*** *Newman, Lily Hay (December 7, 2017). "APT 34 Is an Iran-Linked Hacking Group That Probes Critical Infrastructure". Wired. Archived from the original on December 10, 2017.*
4. ^ *Sardiwal, Manish; Londhe, Yogesh; Fraser, Nalani; Fraser, Nicholas; O'Leary, Jaqueline; Cannon, Vincent (December 7, 2017). "New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit". FireEye. Archived from the original on December 10, 2017.*
5. ^ *Catalin Cimpanu (April 17, 2019). "Source code of Iranian cyber-espionage tools leaked on Telegram; APT34 hacking tools and victim data leaked on a secretive Telegram channel since last month". ZDNet. Retrieved April 24, 2019.*
6. ^ *"How companies – and the hackers themselves – could respond to the OilRig leak". 18 April 2019.*
