Elfin Team

By Contributors to Wikimedia projects

Published: 2017-09-20 · Archived: 2026-04-05 22:49:14 UTC

From Wikipedia, the free encyclopedia

Advanced Persistent Threat 33 (**APT33**) is a hacker group identified by FireEye as being supported by the government of Iran.[1][2] The group has also been called **Elfin Team**, **Refined Kitten** (by Crowdstrike), **Magnallium** (by Dragos), **Peach Sandstorm**,[3] and **Holmium** (by Microsoft).[4][5][6] It is categorized as an advanced persistent threat.

FireEye believes that the group was formed no later than 2013.[1]

APT33 has reportedly targeted aerospace, defense and petrochemical industry targets in the United States, South Korea, and Saudi Arabia.[1][2]

APT33 reportedly uses a dropper program designated DropShot, which can deploy a wiper called ShapeShift, or install a backdoor called TurnedUp.[1] The group is reported to use the ALFASHELL tool to send spear-phishing emails loaded with malicious HTML Application files to its targets.[1][2]

APT33 registered domains impersonating many commercial entities, including Boeing, Alsalam Aircraft Company, Northrop Grumman and Vinnell.[2]

FireEye and Kaspersky Lab noted similarities between the ShapeShift and Shamoon, another virus linked to Iran.[1] APT33 also used Farsi in ShapeShift and DropShot, and was most active during Iran Standard Time business hours, remaining inactive on the Iranian weekend.[1][2]

One hacker known by the pseudonym of xman_1365_x was linked to both the TurnedUp tool code and the Iranian Nasr Institute, which has been connected to the Iranian Cyber Army.[7][1][2][8] xman_1365_x has accounts on Iranian hacker forums, including Shabgard and Ashiyane.[7]

- Charming Kitten

1. ^ Jump up to: *a b c d e f g h* *Greenberg, Andy (September 20, 2017). "New Group of Iranian Hackers Linked to Destructive Malware". Wired.*
2. ^ Jump up to: *a b c d e f* *O'Leary, Jacqueline; Kimble, Josiah; Vanderlee, Kelli; Fraser, Nalani (September 20, 2017). "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware". FireEye.*
3. ^ *"Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets". Microsoft. 14 September 2023.*
4. ^ *"Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S."*

5. ^ *"MAGNALLIUM | Dragos". 30 May 2020.*
6. ^ *"Microsoft says Iran-linked hackers targeted businesses". Associated Press. 6 March 2019.*
7. ^ Jump up to: ***a*** ***b*** *Cox, Joseph (20 September 2017). "Suspected Iranian Hackers Targeted U.S. Aerospace Sector". The Daily Beast. Archived from the original on September 21, 2017. "Included in a piece of non-public malware APT33 uses called TURNEDUP is the username "xman_1365_x." xman has accounts on a selection of Iranian hacking forums, such as Shabgard and Ashiyane, although FireEye says it did not find any evidence to suggest xman was formally part of those site's hacktivist groups. In its report, FireEye links xman to the "Nasr Institute," a hacking group allegedly controlled by the Iranian government."*
8. ^ *Auchard, Eric; Wagstaff, Jeremy; Sharafedin, Bozorgmehr (September 20, 2017). Heinrich, Mark (ed.). "Once 'kittens' in cyber spy world, Iran gaining hacking prowess: security experts". Reuters. "FireEye found some ties between APT33 and the Nasr Institute - which other experts have connected to the Iranian Cyber Army, an offshoot of the Revolutionary Guards - but it has yet to find any links to a specific government agency, Hultquist said."*
