Parisite, Fox Kitten, Pioneer Kitten

Archived: 2026-04-06 01:07:18 UTC

Description“This group has operated since at least 2017 based on infrastructure Dragos identified,” the report explained. “Parisite serves as the initial access group and enables further operations for APT 33, Elfin, Magnallium.”

(ClearSky) During the last quarter of 2019, ClearSky research team has uncovered a widespread Iranian offensive campaign which we call “Fox Kitten Campaign”; this campaign is being conducted in the last three years against dozens of companies and organizations in Israel and around the world. Though the campaign, the attackers succeeded in gaining access and persistent foothold in the networks of numerous companies and organizations from the IT,Telecommunication,Oil and Gas, Aviation, Government, and Security sectors around the world.

During our analysis, we have found an overlap, with medium-high probability, between this campaign’s infrastructure and the activity of an Iranian offensive group OilRig, APT 34, Helix Kitten, Chrysene. Additionally, we have identified, with medium probability, a connection between this campaign and the APT 33, Elfin, Magnallium and Chafer, APT 39 groups.The campaign was first revealed by Dragos, named “Parisite”and attributed to APT33; we call the comprehensive campaign revealed in this report “Fox Kitten”.

The initial breach of the targeted organizations was performed, in most cases, by exploiting 1-day vulnerabilities in different VPN services such as: Pulse Secure VPN, Fortinet VPN, and Global Protect by Palo Alto Networks. Upon gaining foothold at the target, the attackers tried to maintain the access to the networks by opening a variety of communication tools, including opening RDP links over SSH tunneling, in order to camouflage and encrypt the communication with the targets. At the final stage, after successfully infiltrating the organization, the attackers have performed a routine process of identification, examination, and filtering of sensitive, valuable information from every targeted organization.The valuable information was sent back to the attackers for reconnaissance, espionage, or further infection of connected networks.

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=9d13d133-e25a-4de0-8952-6b0cbdb92899