Targets & Methods [Adversary Profile]

crowdstrike.com/blog/who-is-pioneer-kitten/

Alex Orleans August 31, 2020

PIONEER KITTEN at a Glance

Origins	Islamic Republic of Iran
Target Nations	Israel, Middle East North Africa (MENA), North America, United States
Last Known Activity	July 2020 (earliest: 2017)
Target Industries	Highly opportunistic with a focus on Technology, Government, Defense and Healthcare
Community Identifiers	PARISITE, UNC757, Fox Kitten
Motivations	Espionage

PIONEER KITTEN Origins

PIONEER KITTEN is an Iran-based adversary that has been active since at least 2017 and has a suspected nexus to the Iranian government. This adversary appears to be primarily focused on gaining and maintaining access to entities **possessing sensitive information of likely intelligence interest to the Iranian government**.

Behavioral indicators and other traits suggest PIONEER KITTEN is likely **a contract element operating in support of the Iranian government**, rather than one operated by the government itself. Industry reporting has linked PIONEER KITTEN activity to multiple Iranian adversaries; however, CrowdStrike® Intelligence considers these claims to be circumstantial and lacking in sufficient corroborative data to enable confirmation of such relationships.

In late July 2020, an actor assessed to be associated with PIONEER KITTEN was identified as advertising to sell access to compromised networks on an underground forum. That activity is suggestive of a potential attempt at revenue stream diversification on the part of PIONEER KITTEN, alongside its targeted intrusions in support of the Iranian government. The types of entities the actor associated with PIONEER KITTEN claims to have compromised would be of significant intelligence value to the Iranian government. As such, it is unlikely this commercial activity by PIONEER KITTEN is sanctioned by the Iranian government, since the commercial sale of such access would have significant negative impacts on potential intelligence collection operations.

PIONEER KITTEN Methods

PIONEER KITTEN tradecraft is characterized by a pronounced **reliance on exploits of remote external services** on internet-facing assets to achieve initial access to victims, as well as an almost total reliance on open-source tooling during operations.

The adversary is particularly interested in **exploits related to VPNs and network appliances**, including CVE-2019-11510, CVE-2019-19781, and most recently CVE-2020-5902; reliance on exploits such as these lends to an opportunistic operational model.

PIONEER KITTEN's namesake operational characteristic is its **reliance on SSH tunneling**, through open-source tools such as *Ngrok* and the adversary's custom tool *SSHMinion*, for communication with implants and hands-on-keyboard activity via Remote Desktop Protocol (RDP).

PIONEER KITTEN's Targets

Identified PIONEER KITTEN targeting to date has centered around North American and Israeli entities of likely intelligence interest to the Iranian government. Target sectors include technology, government, defense, healthcare, aviation, media, academic, engineering,

consulting and professional services, chemical, manufacturing, financial services, insurance, and retail.

The widespread nature of PIONEER KITTEN's target scope is likely a result of the adversary's opportunistic operational model; the entities apparently of most interest to the adversary are technology, government, defense, and healthcare organizations.

Other Known "ADVERSARIES"

PIONEER KITTEN is just one of many adversaries tracked by CrowdStrike Intelligence. Some of the other threat adversaries that CrowdStrike monitors include the following:

- HELIX KITTEN
- FANCY BEAR
- MYTHIC LEOPARD
- GOBLIN PANDA

Curious about other eCrime, hacktivist or nation-state adversaries? Visit our threat actor center to learn more about adversaries that the CrowdStrike threat Intelligence team tracks.

Additional Resources

- *Download: CrowdStrike 2020 Global Threat Report.*
- *To learn more about how to incorporate intelligence on threat actors like PIONEER KITTEN into your security strategy, please visit the Falcon X Threat Intelligence page.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*