Iranian APT Charming Kitten impersonates ClearSky, the security firm that uncovered its campaigns

cyware.com/news/iranian-apt-charming-kitten-impersonates-clearsky-the-security-firm-that-uncovered-its-campaigns-7fea0b4f

Iranian cyberespionage group Charming Kitten, which has been operating since 2014, has impersonated the cybersecurity firm that exposed its operations and campaigns. Israeli firm ClearSky Security said the group managed to copy its official website hosted on a similar-looking domain - clearskysecurity[.]net.

ClearSky's actual website is Clearskysec.com.

Fake ClearSky website

"Charming Kitten built a phishing website impersonating our company," ClearSky said. "They copied pages from our public website and changed one of them to include a 'sign in' option with multiple services. These sign in options are all phishing pages that would send the victim's credentials to the attackers."

ClearSky's official website does not feature any sign-in options. Researchers noted the fake website is likely still under construction.

"It seems that the impersonating website is still being built because some of the pages have error messages in them," ClearSky said.

ClearSky added that Charming Kitten was hosting the fake domain on an older server that the researchers had ousted on June 12. They also found one page on the fake ClearSky website that wasn't customized yet, but contained content from the attackers' earlier campaign. This also further indicates Charming Kitten is likely behind the fake website.

Since the website was still incomplete, ClearSky does not believe the hackers managed to phish anyone, adding that its employees, systems and clients were not affected by the incident. The fake website was marked as a suspicious website via the Safe Browsing API shortly after it was uncovered and has since been taken down.

Charming Kitten behavior

The advanced persistent threat (APT), also known as Newscaster or Newsbeef, has long targeted academic researchers, human rights activists , political advisors, and media outlets that are of interest to Iran.

The group usually attacks its targets leveraging made up organizations and people to lure people into malicious websites, impersonating real companies, watering hole attacks and spear-phishing.

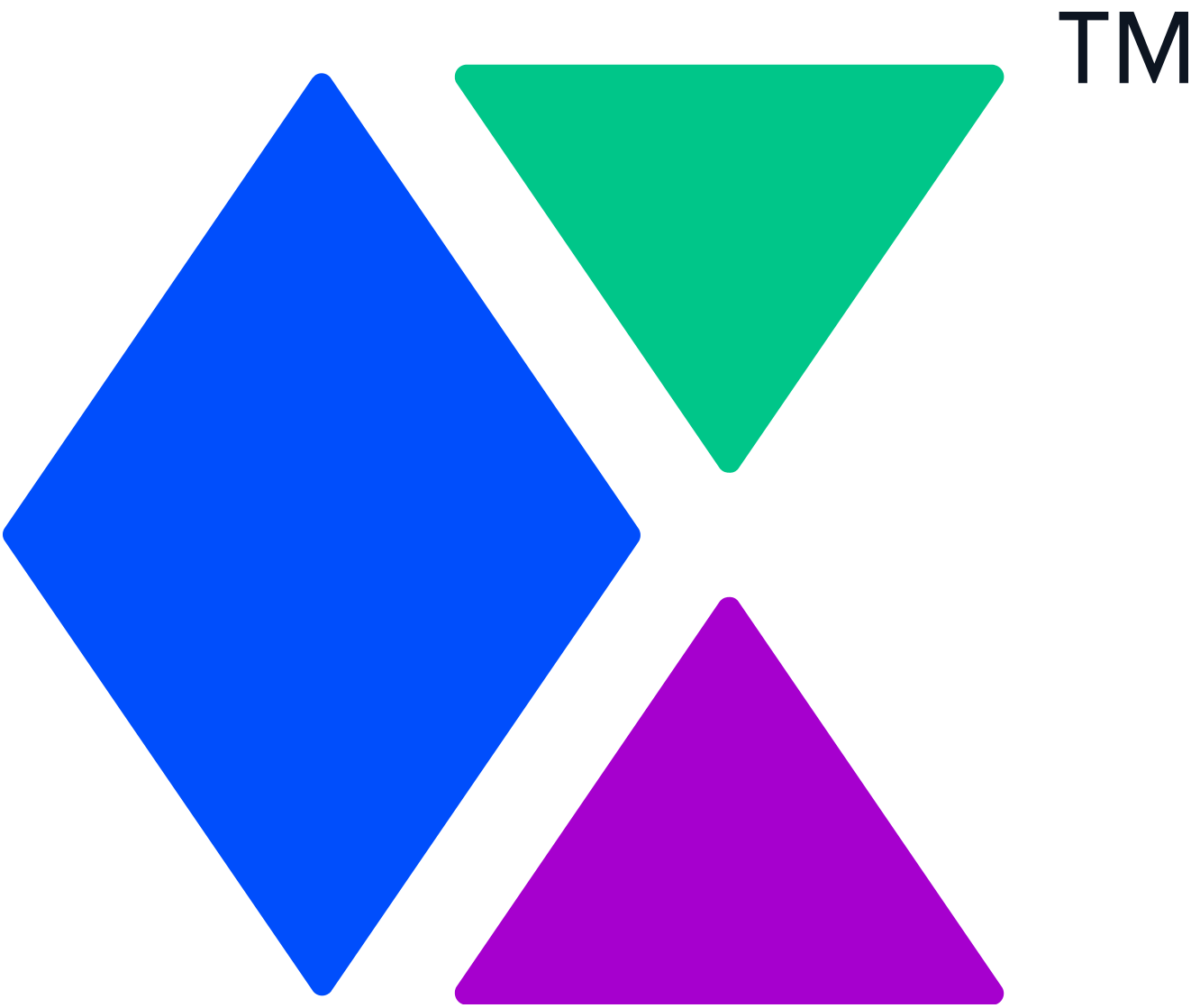
As one of Iran's oldest APTs, Charming Kitten has typically attacked targets in Iran, the United States, Israel and the UK among others. Some of the group's campaigns over the past few years include Saffron Rose, Newscaster and the StoneDrill wiper.

Other legitimate companies impersonated by the hacking group include United Technologies (UTC). In early 2017, the attackers created a fake UTC website that claimed to offer "Free Special Programs and Courses for Employees of Aerospace companies" that designed to dupe visitors into downloading a fake Flash Player that was actually the group's DownPaper malware.

Iranian national Behzad Mesri, who was charged in the US with hacking HBO and stealing multiple Game of Thrones files, is believed to be a part of the Charming Kitten entourage.

"While Iranian threat actors have been well documented by security researchers, the inner workings of the ecosystem of Iran's hackers is not entirely clear," ClearSky researchers wrote in an earlier report. "Groups can be vigorously active for years and then disappear abruptly, sometimes due to being publicly outed. Researchers make a best-faith effort to assign operations to certain groups, but the instability in the field makes the process challenging."

ClearSky Security | Impersonation Attack | Iranian Cyber Espionage | Iranian Hackers | Fake Website



Publisher

Cyware