Iranian Cyber Espionage Against Human Rights Activists, Academic Researchers and Media Outlets – ClearSky Cyber Security

Published: 2017-12-05 · Archived: 2026-04-05 14:04:46 UTC

Charming Kitten is an Iranian cyberespionage group operating since approximately 2014. This report exposes their vast espionage apparatus, active during 2016-2017. We present incidents of company impersonation, made up organizations and individuals, spear phishing and watering hole attacks. We analyze their exploitation, delivery, and command-and-control infrastructure, and expose DownPaper, a malware developed by the attackers, which has not been publicly documented to date.

Incidents documented in this report are likely a small fraction of the actual amount of targeted attacks, which may reach thousands of individuals. We expose more than 85 IP addresses, 240 malicious domains, hundreds of hosts, and multiple fake entities – most of which were created in 2016-2017. The most recent domains (*com-archivecenter[.]work*, *com-messengerservice[.]work* and *com-videoservice[.]work*) were registered on December 2nd, 2017, and have probably not been used in attacks yet.

We present the connection between Behzad Mesri, an Iranian national recently indicted for his involvement in hacking HBO, and Charming Kitten. We also identify other members of the group.

Targets

The attackers' focus appears to be individuals of interest to Iran in the fields of Academic research (i.e. Iranists – Scholars who study Iran), Human right and media. Emphasis is given to Iranian dissidents living in Iran or abroad, and people who come in touch with Iranians or report on Iranian affairs such as journalists and reporters, media outlets covering Iran, and political advisors.

Most targets known to us are individuals living in Iran, the United States, Israel, and the UK. Others live in Turkey, France, Germany, Switzerland, United Arab Emirates, India, Denmark and other countries.

Notably, the attackers usually try to gain access to private email and Facebook accounts. They seek to infiltrate the targets' social network as a hop point to breach other accounts in their social network, or to collect information about their targets. Sometimes, they aim at establishing a foothold on the target's computer to gain access into their organization, but, based on our data, this is usually not their main objective, as opposed to other Iranian threat groups, such as Oilrig and CopyKittens.

Report and indicators

Read the full report: Charming Kitten: Iranian Cyber Espionage Against Human Rights Activists, Academic Researchers and Media Outlets – And the HBO Hacker Connection

Indicators of compromise are available for subscribers of the ClearSky threat intelligence service in MISP events: 352, 336, 243, 241, 238, 233, 209, 182, 180, 178, 175, 169, 136, 125, 119, 94, 86, 83.

Indicators are also available in the following CSV file: Charming-Kitten-2017.csv and on PassiveTotal.
