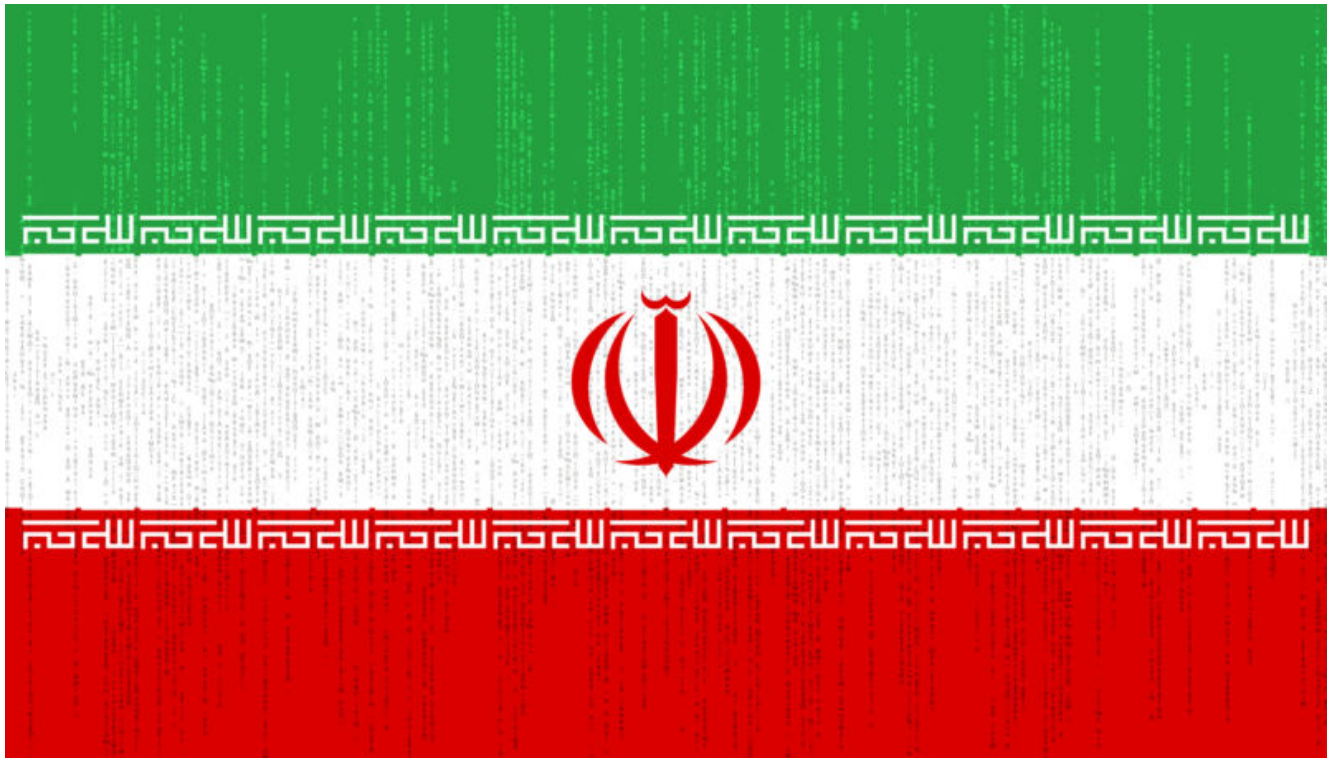


Iran courted US security expert for years, seeking industrial hacking training



reader comments

23 with 20 posters participating

Share this story

Iran has over the past decade built up its own organic hacking and cyberwarfare capabilities. But the groups associated with orchestrating Iran's various cyberwarfare and cyber-espionage activities have also relied significantly on mining the work of others—and in at least one case, they have tried to bring in outside help for the ostensible purpose of training would-be hackers.

According to Chris Kubecka—a security researcher who played a prominent role in Saudi Aramco's response to the Iran-

attributed Shamoon “wiper” malware—officials with the Telecommunication Company of Iran emailed and messaged her on behalf of the Iranian government, attempting “to recruit me to teach hacking in country against critical Infrastructure with focus on nuclear facilities,” she told Ars.

These efforts, which Kubecka alluded to briefly in a presentation at AppSec California in 2018, spanned over 2.5 years—during which Kubecka informed the FBI. “I was collecting evidence and communicating with them directly until last January when the FBI stepped in,” she said. “The last contact we had, the Iranians wanted my home address to send me ‘a gift’.”

The TCI contact offered Kubecka “up to \$100,000 for one month” to come to Iran, Kubecka explained, to teach a Global Information Assurance Certification (GIAC) penetration tester advanced course for industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. The trip included a scheduled “VVIP tour with pictures with their military,” Kubecka claimed. She showed some of the messages to Ars, including some of her communication with FBI.

Iran’s access to US information security tools and training is in theory blocked by sanctions against the country, though there have certainly been loopholes that could be exploited to get around those barriers. And when Iran approached Kubecka, UN sanctions had been partially lifted with the signing of the Joint Comprehensive Plan of Action (JCPA) in 2015—though US sanctions remained in place.

Though the Trump administration’s exit from the JCPA significantly impeded legitimate trade with Iran, the government can use proxies to gain technology that is restricted—including tools used by the TCI to censor Iran’s Internet and surveil Internet users. In the meantime, Iran has built its own organic capabilities atop off-the-shelf tools—some open source, some “cracked” commercial software—and

lessons learned from its campaigns in Saudi Arabia and other Gulf states as well as against Western companies.

CISA has warned industry of Iran's escalated activities, including new potential destructive attacks. And since then, there has been an uptick in the past few months in efforts to gain access and collect account information. In October and November of 2019, the Iranian-attributed threat group APT33 targeted a total of about 4,000 organizations, mostly in the industrial controls space, with "password-spraying" attacks against hundreds of accounts at each organization.

In August and September of 2019, another Iranian threat group, APT35, was observed making thousands of attempts to breach the email accounts of the Trump presidential campaign organization. APT35 was also spotted trying to breach the email accounts of current and former US government officials and of journalists and Iranian expatriates.

<https://arstechnica.com/?p=1640503>