Related news

cyberscoop.com/cobalt-dickens-iran-mabna-institiute-dell-secureworks/

August 24, 2018

government

Cobalt Dickens threat group looks to be similar to indicted hackers

A night shot of Tehran, Iran. Secureworks says hackers from Iran similar to those indicted in March have been trying to steal credentials. (Flickr user daniyal62)
Written by Patrick Howell O'Neill
Aug 24, 2018 | CYBERSCOOP
A mass credential-stealing campaign by hackers linked to the Iranian government and targeting 76 universities around the world was discovered this month by Secureworks, an Atlanta-based cybersecurity company owned by Dell.

The campaign involved 16 domains, 300 spoofed websites and fake login pages, 76 targeted universities and 14 countries including the United States, Canada, United Kingdom and Japan, the company announced.

“Universities are attractive targets for threat actors interested in obtaining intellectual property,” Secureworks’ researchers said on Friday. “In addition to being more difficult to secure than heavily regulated finance or healthcare organizations, universities are known to develop cutting-edge research and can attract global researchers and students.”

The campaign is ongoing with the most recent domain having been registered on Aug. 19.

Carried out by hackers that Secureworks researchers dub Cobalt Dickens, this campaign used some of the same infrastructure as the Iranian hackers indicted by the United States in March 2018, according to the company's research, indicating a strong link to Tehran.

Nine Iranian nationals were indicted on March 23 for allegedly hacking into the networks of multiple U.S. universities, government agencies and businesses in an effort to steal intellectual property and use the high bandwidth networks for future operations. Deputy Attorney General Rod Rosenstein said the hackers, who stole more than 31 terabytes of data from U.S. targets, acted at the command of the Iranian Revolutionary Guard Corps.

The hackers work for the Mabna Institute, a quasi-government technology firm in Iran.

"We're focusing on people who support IRGC (Islamic Revolutionary Guard Corps) in some of their cyber operations," a senior U.S. official told CyberScoop in March. "They have this dual personality where they've been hacking for profit as well as hacking information, which they sell to the Iranian government, as well as provide capabilities to the Iranian government."

In addition to the shared infrastructure, the researchers at Secureworks pointed to the similar goals and tactics.

"The targeting of online academic resources is similar to previous cyber operations by COBALT DICKENS, a threat group associated with the Iranian government," the researchers wrote. "In those operations, which also shared infrastructure with the August attacks, the threat group created lookalike domains to phish targets and used credentials to steal intellectual property from specific resources, including library systems."