

18 months after indictment, Iranian phishers are still targeting universities

Aurich Lawson / Getty

reader comments

18 with 15 posters participating

Share this story

In March 2018, nine Iranians were criminally charged for their involvement with the Mabna Institute, a company federal prosecutors said was created in 2013 for the express purpose of using coordinated cyber intrusions to steal terabytes of academic data from universities, academic journal publishers, tech companies, and government organizations. Almost 18 months later, the group's hacking activities are still going strong, Secureworks, a Dell-owned security company, said on Wednesday.

The hacking group, which Secureworks researchers call Cobalt Dickens, has recently undertaken a phishing operation that targeted more than 60 universities in countries including the US, Canada, the UK, Switzerland, and Australia, according to a report. Starting in July, Cobalt Dickens used malicious webpages that spoofed legitimate university resources in an attempt to steal the passwords of targeted individuals. The individuals were lured through emails like the one below, dated August 2.

Secureworks

The emails informed targets that their online library accounts would expire unless they reactivated them by logging in. Recipients who clicked on the links landed on pages that looked almost identical to library resources that are widely used in academic settings. Those who entered passwords were redirected to the legitimate library site being spoofed, while behind the scenes, the spoof site stored the password in a file called pass.txt. Below is a diagram of how the scam worked:

Secureworks

The links in the emails led directly to the spoofed pages, a departure from a Cobalt Dickens operation from last year that relied on link shorteners. To facilitate the change, the attackers registered more than 20 new domains to augment a large number of domains used in previous campaigns. To make the malicious sites harder to spot, Cobalt Dickens protected many of them with HTTPS certificates and populated them with content pulled directly from the spoofed sites.

The group members used free services or software tools from domain provider Freenom, certificate provider Let's Encrypt, and Github. In some cases, they also left clues in the comments or metadata of spoofed pages that they were indeed Iranians.

Secureworks

Secureworks

Federal prosecutors said 18 months ago that the attack group had targeted more than 100,000 professor accounts around the world and successfully compromised about 8,000 of them. The defendants allegedly stole almost 32 terabytes of academic data and intellectual property. The defendants then sold the stolen data on websites. Secureworks said that Cobalt Dickens to date has targeted at least 380 universities in more than 30 countries.

The brazenness of the new operation underscores the limited results criminal indictments have against many types of attackers. A much more effective countermeasure would be the use of multi-factor authentication, which would immediately neutralize the operations and require the attackers to devote considerably more resources. The most effective form of MFA is the industry-wide WebAuthn standard, but even time-based one-time passwords from an authenticator app or, if nothing else is possible, a one-time password sent by SMS message would have defeated the campaigns.

<https://arstechnica.com/?p=1567475>