Iranian Hackers Charged in March Are Still Actively Phishing Universities

bleepingcomputer.com/news/security/iranian-hackers-charged-in-march-are-still-actively-phishing-universities/

Catalin Cimpanu

By
Catalin Cimpanu

- August 24, 2018
- 09:00 AM
- 1

An Iranian hacking group has continued its phishing operations undeterred by indictments from the US Department of Justice.

The group's name is Cobalt Dickens or Silent Librarian. In March 2018, the US DOJ charged nine hackers it believed were behind the group's activity.

DOJ officials said the suspects were "hackers-for-hire or affiliates of the Mabna Institute, an Iran-based company that, since at least 2013, conducted a coordinated campaign of cyber intrusions," at the behest of Iran's Islamic Revolutionary Guard Corps (IRGC), one of the country's intelligence agencies.

The nine were charged with carrying out cyber-attacks against 144 US universities and 176 universities in 21 foreign countries, but also attacks against 47 US and foreign companies active in various private sectors.

According to court documents, the group primarily targeted universities. A PhishLabs report described the group's modus operandi. Their favorite tactic, albeit not the only one, was to use phishing pages for a university's online library portal.

Hackers used the collected logins to steal intellectual property from the university's library, which they later resold online on various portals, such as Megapaper.ir (Megapaper) and Gigapaper.ir (Gigapaper), two websites operated by a company controlled by one of the nine suspects.

New Cobalt Dickens campaign discovered

But according to a report shared with Bleeping Computer in advance, US cyber-security firm Secureworks says it detected new phishing attacks carried out by the same Cobalt Dickens group.

Secureworks researchers say they initially discovered one URL spoofing a login page for a university but after further investigations, they uncovered a broader campaign aimed at multiple targets.

"Sixteen domains contained over 300 spoofed websites and login pages for 76 universities located in 14 countries, including Australia, Canada, China, Israel, Japan, Switzerland, Turkey, the United Kingdom, and the United States," revealed Secureworks experts.

They also say the domains were registered between May and August 2018, a clear indicator that the indictment hasn't phased the group's members or forced them underground, as most hackers tend to do after being publicly ousted.

> After getting run off of @Namecheap, #SilentLibrarian actors are now using straight-up Iranian-hosted websites for their phishing sites. The group recently switched over to the domain UNTC[.]IR. Today's targets: @LancasterUni @ucl @Stockholm_Uni
>
> Really covert guys!
>
> — Crane Hassold (@CraneHassold) August 24, 2018

> These guys are busy today! Another #SilentLibrarian actor has just activated #phishing sites targeting @NCState and @tcddublin on the domain LLLF[.]NL hosted on Freenom (@dottk). pic.twitter.com/tGwJ3XKkhb
>
> — Crane Hassold (@CraneHassold) August 24, 2018

Related Articles:

Cyberspies use IP cameras to deploy backdoors, steal Exchange emails

Austin Peay State University resumes after ransomware cyber attack

Phishing campaign targets Russian govt dissidents with Cobalt Strike

FBI warns of hackers selling credentials for U.S. college networks

Intuit warns of QuickBooks phishing threatening to suspend accounts

- APT
- Cyber-espionage
- Education
- Iran
- Phishing
- University

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Comments

Warthog-Fan - 3 years ago

  - ○
  - ○

Why shouldn't these hackers keep up their phishing activity? It's not like they are going to get extradited to the U.S. to face criminal charges.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: