

JOHN BOLTON WILL GET TO START HIS IRAN WAR BECAUSE NINE IRANIANS STOLE ACADEMIC DISSERTATIONS

Earlier today, Rod Rosenstein rolled out a dangerously vague indictment of nine Iranians, allegedly tied to the Revolutionary Guard, for hacking hundreds of universities and some private companies and NGOs.

I say it's dangerously vague because, while it's clear the Iranians compromised thousands of university professors, it's not clear precisely what they stole. But it appears that most of data stolen from universities (some privacy companies, government agencies, and NGOs were targeted too) consists of scholarship.

[M]embers of the conspiracy used stolen account credentials and obtained unauthorized access to victim professor accounts, through which they then exfiltrated, or transferred to themselves, academic data and documents from the systems of compromised universities, including, among other things, academic journal, these, dissertations, and electronic books.

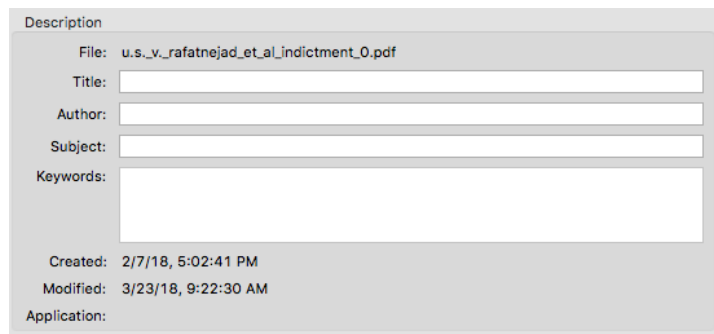
The indictment describes the stolen data benefitting (along with the IRGC) "Iran-based universities." And it specifies that the hackers sold the information so that Iranians could access US academic online libraries.

Magapaper sold stolen academic resources to customers within Iran, including Iran-based public universities and institutions, and Gigapaper sold a service to customers within Iran whereby purchasing customers could use

compromised university professor accounts to directly access the online library systems of particular United States-based and foreign universities.

The indictment claims the Iranians stole “academic data and intellectual property” which cost the affected 144 US universities “\$3.4 billion to procure and access.” But that’s reminiscent of the Aaron Swartz case (to which several people have likened this), where the prosecutor justified pursuing Swartz because he had downloaded “intellectual property that cost millions to create,” something like 4.75 million articles and 87 Gigabytes of data (See the extensive discussion about cost and damages in this MIT report.) DOJ accuses the Iranians of stealing 31 terabytes of data.

As I said, this is a dangerously vague indictment. And, from the metadata, it appears that the indictment may be more than a month old. (h/t z3dster)



Description

File: u.s._v._rafatnejad_et_al_indictment_0.pdf

Title:

Author:

Subject:

Keywords:

Created: 2/7/18, 5:02:41 PM

Modified: 3/23/18, 9:22:30 AM

Application:

There are also not dates on any of the signature lines, so it may be this indictment has just been sitting in a drawer in southern Manhattan, waiting to serve as a casus belli.

Perhaps there was more sensitive data stolen here. Perhaps the professors who got hacked were more selectively targeted than the sheer number of academics targeted – 100,000 got phished, with almost 8,000 responding – suggests.

But absent far more details, this indictment seems to make an international incident out of people in a very closed society trying to access

academic information that is readily available here.

I've long written about the potential downsides of indicting nation-state hackers, which is effectively what these guys are – particularly the possibility that doing so will invite retaliation against our own official hackers. But in some cases – with the OPM hack, with hacks of national security information, with the Russians who targeted the election – that might make sense.

But indicting nation-state hackers for stealing dissertations?

Update: This confirms what z3dster noted: this thing has been sealed since February 7. Why? And why did it get unsealed the day after Bolton was hired?