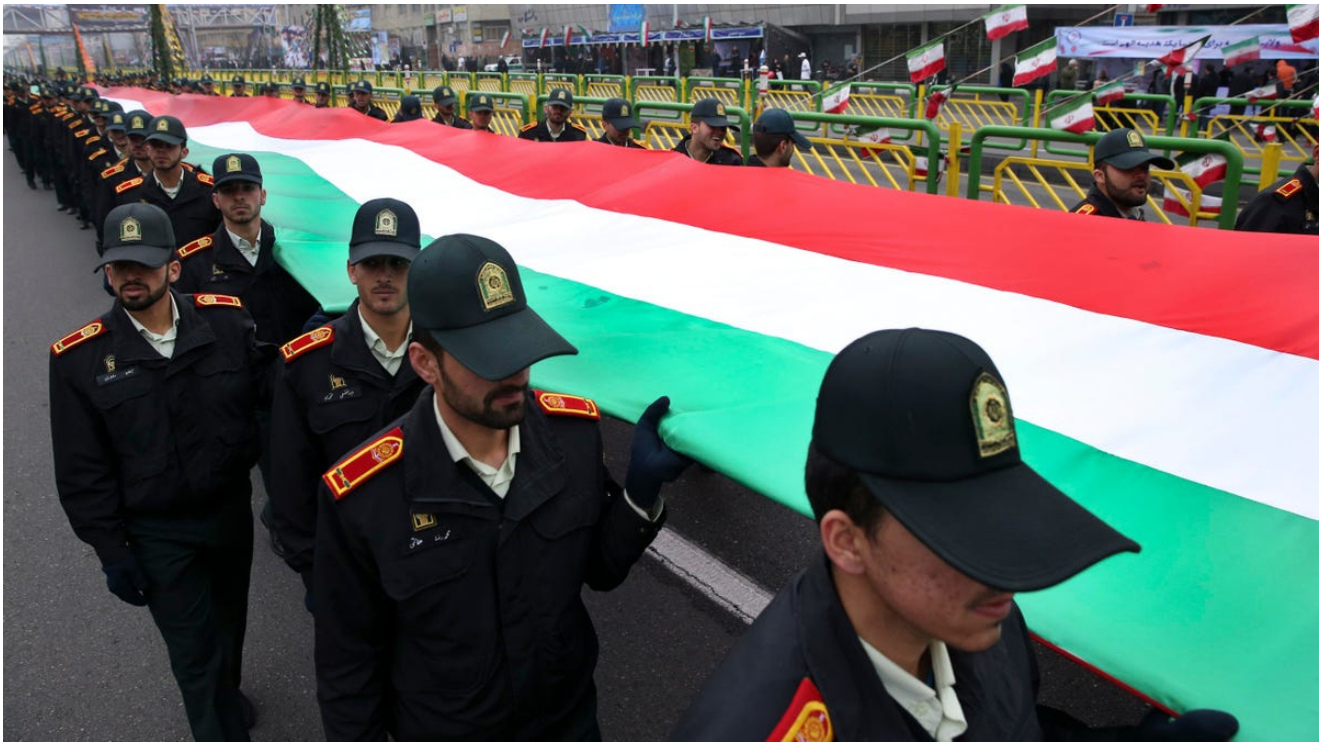
Inside OilRig -- Tracking Iran's Busiest Hacker Crew On Its Global Rampage

forbes.com/sites/thomasbrewster/2017/02/15/oilrig-iran-hackers-cyberespionage-us-turkey-saudi-arabia/

Thomas Brewster February 15, 2017



This article is more than 5 years old.

Iran has become one of the more prolific nations when it comes to cyberespionage, according to U.S.... [+] experts. (AP Photo/Vahid Salemi)

AI Squared, a small, mission-driven tech firm based in a verdant corner of Vermont, builds software that alters websites to help those with visual impairment use the internet. It never expected to become an innocent victim in an international cyberespionage campaign allegedly perpetrated by Iran.

But AI Squared is now living proof that any American business, be it Microsoft-sized or a minnow, is a potential victim of Iran's increasingly sophisticated and prolific digital army. Indeed, AI Squared has become the only known private American business to have been targeted by a young crew from Iran known as OilRig. Since its birth in late 2015, OilRig has become one of the most active hacking organizations to be sponsored by the Iranian government, according to cybersecurity experts and to U.S. and Israeli intelligence firms. FORBES is revealing a handful of its targets for the first time on Wednesday, showing its rapid infiltration of systems across the globe in little over a year.

While most Iranian groups have typically targeted a niche set of domestic and foreign targets, in particular government agencies and dissidents, OilRig is far more focused on private industry outside of Iran. "What's interesting about OilRig is how much it's just foreign focused and is interested in the private sector as much as it's interested in the diplomatic establishment," said Collin Anderson, a Washington D.C.-based researcher who is drawing up a report for Carnegie Mellon on Iran's overall cyber power. And though it's unclear just what data OilRig has siphoned off target systems, the unit is representative of a shift in Iran's cyber strategy, from destructive attacks, such as the infamous hit on the Las Vegas Sands Casino in 2014, to stealthy monitoring of targets.

An American platform for attack

AI Squared's problems started in the second week of January, when the company received a startling warning from security giant Symantec: Certificates for its technology that are designed to guarantee its authenticity had been compromised. What Symantec didn't say, and what AI Squared is now investigating after FORBES' disclosed the Iranian link to the company, was that OilRig was believed to have been responsible.

The crew stole AI Squared certificates and used them to disguise their own malware. The goal was to make their surveillance tools appear legitimate to security systems of their many targets across the Middle East, Europe and the U.S., as noted in a report from Israeli security provider ClearSky in early January. The OilRig hackers pushed those espionage tools over two fake Oxford University pages in November 2016, one claiming to offer jobs at the institution, the other a conference sign-up website, ClearSky said. Both encouraged visitors to download documents, one to complete registration for the fake event, the other for an Oxford University CV creator. Once clicked, the crew's malware, named Helminth, would run, allowing the OilRig crew to control targets' PCs and steal data.

A fake Oxford University jobs site created by OilRig. Malware signed by an American firm's... [+] certificates was delivered from the domain.

AI Squared, owned by Florida-based VFO Group since a June 2016 acquisition, only received vague details on the compromise from Symantec and is only now launching an investigation. "Could someone else have hacked into our systems? We're pretty secure here, but they hacked the White House, they can hack anywhere they want," said Scott Moore, marketing VP at VFO Group, which claims to be "the world's leading assistive technology provider for the visually impaired." The company is yet to find any conclusive findings.

Gunning for government officials

Many other organizations have become victims of OilRig's crew in recent years. Intelligence firms believe OilRig has taken control of multiple email accounts of public and private organizations. With that access, they've expanded their phishing campaigns in the U.S., Saudi Arabia, Turkey, and beyond.

One OilRig phishing email viewed by FORBES, dated July 2016, was addressed to three officials at Turkey's foreign ministry. They included an adviser to the Permanent Mission of Turkey to the United Nations, based in New York, a staffer at the Turkish embassy staff in Riga, Latvia, and another official based in Turkey. It was sent from an official Turkish Airlines check-in address, indicating the hackers had either compromised the airline's email or spoofed the account. The message encouraged the recipient to provide login details via an attached Excel file. Once opened, the group's Helminth malware would run.

The Turkish adviser in New York said he had never seen the phishing email and so couldn't have clicked on the link. At the time of publication, the other targets had not responded to multiple requests for comment. Turkish Airlines also had not returned requests. Despite the phishing email itself showing who OilRig was trying to expose, it's not known if either organization was successfully hacked.

But similar malicious documents were sent to multiple other government organizations across the world, according to Palo Alto Networks, which first published the phishing email without naming the parties involved.

Private industry attacks

OilRig has gone after multiple private companies too. Another phish was attempted in May 2016 by the hackers that, according to the metadata in the email headers, was sent from servers within Saudi Arabian government contractor and IT security supplier Al-Elm. That could indicate a breach at Al-Elm, according to the security researcher who showed FORBES the email.

The message was injected into an ongoing email thread between Al-Elm and Samba, part of the Samba Financial Group, the kingdom's third largest lender that reported $290 million profit last quarter. The message contained a version of OilRig's Helminth surveillance kit, which would launch as soon as a recipient opened an attached document, in this case an Excel file called "notes.xls." Neither Al-Elm nor Samba had responded to requests for comment.

According to a report released Wednesday by cyber intelligence firm SecureWorks, which has dubbed the OilRig crew Cobalt Gypsy, the group was active this January, sending out messages loaded with malware from legitimate email addresses belonging to one of Saudi Arabia's biggest IT suppliers, the National Technology Group, and an Egyptian IT services firm, ITWorx. From those email accounts, an unnamed Middle East entity was targeted with messages promising links to job offers. Hidden in the attachments was PupyRAT, an open source remote access trojan (RAT) that works across Android, Linux and Windows platforms.

One of OilRig's favorite methods of infection is sending out job ads. In this case, Egypt's ITWorx... [+] was used as a lure.

Neither the National Technology Group nor ITWorx had responded to requests for comment. Just as in the case of Al-Elm, analysis of the headers of the phishing emails indicated they originated from within the sender's organization, and were not spoofed, SecureWorks said. That indicated "the threat actor previously compromised those organizations," according to SecureWorks intelligence analyst Allison Wikoff.

The SecureWorks Counter Threat Unit has repeatedly informed its customers across government and private sector with "high confidence" that OilRig "is associated with Iranian government-directed cyber operations." CrowdStrike, which dubs the group Twisted Kitten, has connected it with Iran too. And Israeli firm ClearSky has also traced the crew back to the Middle East nation.

"They're very active, possibly the most active group [in Iran]," said Rafe Pilling, security researcher at SecureWorks. "They are capable and have demonstrated that capability to leverage their phishing ops."

The Iranian government hadn't responded to a request for comment on the OilRig group at the time of publication. In the past, Iran has denied involvement in cyberespionage and digital attacks on foreign systems.

Iran's freewheeling cyber spies

Outside of OilRig, other reports of Iranian activity have caused alarm across the security community in the last year, for both their sophistication and their novelty. One of only a handful of Mac malware samples was attributed to the Iranian government earlier this month. Just last year, the U.S. indicted seven Iranians for their alleged participation in an attacks on U.S. financial institutions. One was also charged with an attempt to hack the Bowman Dam in New York. The accused reside in Iran and are not expected to be extradited to stand trial. Iran denied involvement in the attacks.

Anderson, who uncovered the Mac malware, said Iran had created a hodgepodge of hackers, some of whom were capable of causing severe harm. "It's chaotic, five or six-man shops that produce mediocre malware," said Anderson, who tracks a substantial amount of Iran cyber activity with fellow researcher Claudio Guarnieri. "Sometimes they do some catastrophic damage, most of the time not so much."

U.S. cyber experts are now looking at how OilRig and its sister crews will respond to the Trump administration's stance on Iran, which will be looking at how the president's meeting with Israeli prime minister Benjamin Netanyahu. "The Iranians are being cautious about provoking the US until they see how the Trump administration lines up on Iran policy," said James Lewis, an intelligence and security specialist at the Center for Strategic and International Studies. "Let's see what happens with the Netanyahu visit."