Iranian Hackers Have Been Infiltrating Critical Infrastructure Companies

wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/

Lily Hay Newman December 7, 2017

The international intelligence agency always has a keen interest in Iran's hacking activity. And new research published by the security firm FireEye on Thursday indicates the country's efforts show no signs of slowing. In fact, a new network reconnaissance group— FireEye calls them Advanced Persistent Threat 34—has spent the last few years burrowing deep into critical infrastructure companies.

Given how aggressively Iran has pursued infrastructure hacking, previously targeting the financial sector and even a dam in upstate New York, the new findings serve as a warning, and highlight the evolving nature of the threat.

FireEye researchers tracked 34 of the group's attacks on institutions in seven Middle Eastern countries between 2015 and mid-2017, but says APT 34 has been operational since at least 2014. The group appears to target financial, energy, telecommunications, and chemical

companies, and FireEye says it has moderate confidence that its hackers are Iranians. They log into VPNs from Iranian IP addresses, adhere to normal Iranian business hours, their work has occasionally leaked Iranian addresses and phone numbers, and their efforts align with Iranian interests. Namely, targeting the country's adversaries.

New APT in Town

There isn't definitive evidence of a direct link between APT 34 and APT 33, an Iranian hacking group and malware distributor FireEye published findings on in September. But researchers have seen APT 34 operating concurrently inside many of the same target networks as other Iranian hackers.

> 'The more we divulge things we know about them, the more they'll shift and change.'

Jeff Bardin, Treadstone 71

"We have seen, and this is with a lot of the Iranian actors, a very disconcerting or aggressive posture towards critical infrastructure organizations," says John Hultquist, director of intelligence analysis at FireEye. "APT 33 has targeted a lot of organizations in critical infrastructure in the Middle East and so has APT 34. They obviously represent opportunities for intelligence collection. But we always have to think about the alternative use of those intrusions or accesses as possible means for disruption and destruction, especially given the destructive incidents we've already seen with other Iranian actors."

To establish what Hultquist describes as beachheads, APT 34 uses involved operations to move deeper and deeper into a network, or exploit a toehold within one organization to pivot into another. FireEye has observed the group compromising someone's email account at a target company, rifling through their archive, and restarting threads as old as a year, to trick the recipient into clicking a malicious attachment. The hackers also use compromised email accounts to spearphish other companies, and leapfrog into their systems as well.

While the APT 34 Iranian hacking activity doesn't appear to target the United States, any Iranian efforts in that space are noteworthy. The countries have a long history of cyber antagonism, which includes the deployment of Stuxnet, malware thought to be a product of the NSA and their Israeli counterparts, to cripple Iran's uranium enrichment activities. Tensions between the countries have escalated recently as well, with President Donald Trump recently taking steps to decertify the nuclear agreement between the US and Iran.

'A Multilayered Approach'

APT 34 uses malicious Excel macros and PowerShell-based exploits to move around networks. The group also has fairly extensive social media operations, deploying fake or compromised accounts to scope out high-profile targets, and using social engineering to get closer to particular organizations. FireEye researchers speculate that APT 34 may be a reconnaissance and persistence unit, focused on finding ways into new networks and

broadening access within existing targets. Some evidence indicates that the group may work directly for the Iranian government, but it's also possible that the hackers are effectively contractors, selling backdoors to the government as they find them.

"When you look at this, it’s a multilayered approach," says Jeff Bardin, the chief intelligence officer of the threat-tracking firm Treadstone 71, which monitors Iranian hacking activity. "They get in and make a lot of modifications, download new malware, manipulate the memory, so it’s definitely pretty sophisticated. And the Powershell activity has been largely a hallmark of Iranian activity lately. They change their tactics constantly. The more we divulge things we know about them, the more they’ll shift and change."

Though much remains unknown about APT 34, its capabilities and prowess make the group's interest in critical infrastructure targets all the more noteworthy, whether it's tasked with carrying out full operations itself, or charged with laying the groundwork for others to do so.

"This is yet another example of Iranian cyber capability, which only seems to grow every day," FireEye's Hultquist says. "It’s a challenge for people who are concerned with Iranian actors, and as geopolitics shifts, the number of people who should be concerned with Iranian actors will probably only increase."