21,201 views | Jul 22, 2019, 03:35am

Warning As Iranian State Hackers Target LinkedIn Users With Dangerous New Malware

Zak Doffman Contributor

Cybersecurity

I write about security and surveillance.

GETTY

Cookies on Forbes

As I reported over the weekend, the multidimensional cyber warfare playing out in the Middle East has taken a shape we have not seen at this scale before—a mix of military offensive and defensive capabilities with state-sponsored attacks on civilian targets. With cyber warfare becoming "an interchangeable battlefield tool," an attack in one domain can lead to

retaliation in another. And the catalyst has been the continuing escalation of tensions between the U.S. (and its allies) and Iran.

Iran understands that retaliation against the U.S. military in the cyber domain "might be akin to throwing rocks at a tank," but it can hit the vast and under-protected U.S. corporate sector at will. Two weeks after U.S. Cyber Command hit Iran's command and control structure in the aftermath of the downing of a U.S. surveillance drone, came a warning that an Iranian-led hack was targeting the millions of unpatched Microsoft Outlook systems.

Now, U.S. cybersecurity firm FireEye has warned of a malicious phishing campaign that it has attributed to the Iranian-linked APT34—whose activity has been reported elsewhere as OilRig and Greenbug. The campaign has been targeting LinkedIn users with plausible but bogus invitations to join a professional network and emailed attachments laced with malware that seeks to infect systems with a hidden backdoor and steal data and credentials.

According to a FireEye blog post published on Thursday (July 18), the campaign targets specific industries that are clearly of interest to the regime in Teheran: "This threat group has conducted broad targeting across a variety of industries operating in the Middle East—however, we believe APT34's strongest interest is gaining access to financial, energy, and government entities."

In the reference case cited by FireEye, the counterfeit invitations masqueraded as coming from a Cambridge University researcher, with a plausible URL for the download of malicious attachments. "The targeted employee conversed with 'Rebecca Watts', allegedly employed as 'Research Staff at the University of Cambridge.' This is not the first time we've seen APT34 utilize academia and/or job offer conversations in their various campaigns."

Cookies on Forbes

In exposing this campaign, FireEye identified new malware variants that target infected systems to collect information through a hidden backdoor installed to facilitate data exchange. There was also a tool to steal credentials stored in a Windows Vault. This is notable because the nefarious cyberattacks on high-profile targets—including government, resources and critical infrastructure—rely on credentials to open "real-world" vulnerabilities. It is a chain, and you target one link at a time.

LinkedIn is seen as solid hunting ground for APT34, given that so many of us will link and engage without the same level of skepticism we might apply to an email from an unknown sender, FireEye describe social media platforms "as an effective delivery mechanism if a targeted organization is focusing heavily on e-mail defenses to prevent intrusions."

This is unsurprising. It is yet another example of Iran turning to non-military targets as it continues its cyber war against the West. "The activity," FireEye reports, "is a well-known Iranian threat actor utilizing their tried-and-true techniques to breach targeted organizations."

Last month, the Cybersecurity and Infrastructure Security Agency (CISA) within the DHS issued a blanket warning about a"recent rise in malicious cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies... using destructive ‘wiper’ attacks, looking to do much more than just steal data and money."

CISA warned that "these efforts are often enabled through common tactics like spear-phishing, password spraying, and credential stuffing. What might start as an account compromise, where you think you might just lose data, can quickly become a situation where you’ve lost your whole network."

Also last month, the National Security Agency confirmed to AP that "there have been serious issues with malicious Iranian cyber actions in the past. In these times of heightened tensions, it is appropriate for everyone to be alert

Cookies on Forbes

to signs of Iranian aggression in cyberspace and ensure appropriate defenses are in place."

"We suspect this will not be the last time APT34 brings new tools to the table," FireEye warns. "Threat actors are often reshaping their TTP [Tactics, Techniques and Procedures] to evade detection mechanisms, especially if the target is highly desired. For these reasons, we recommend organizations remain vigilant in their defenses, and remember to view their environment holistically when it comes to information security."

Follow me on Twitter or LinkedIn.

Zak Doffman

I am the Founder/CEO of Digital Barriers, providing surveillance solutions to defense, security and law enforcement agencies worldwide. Contact me at zakd@me.com.

Cookies on Forbes