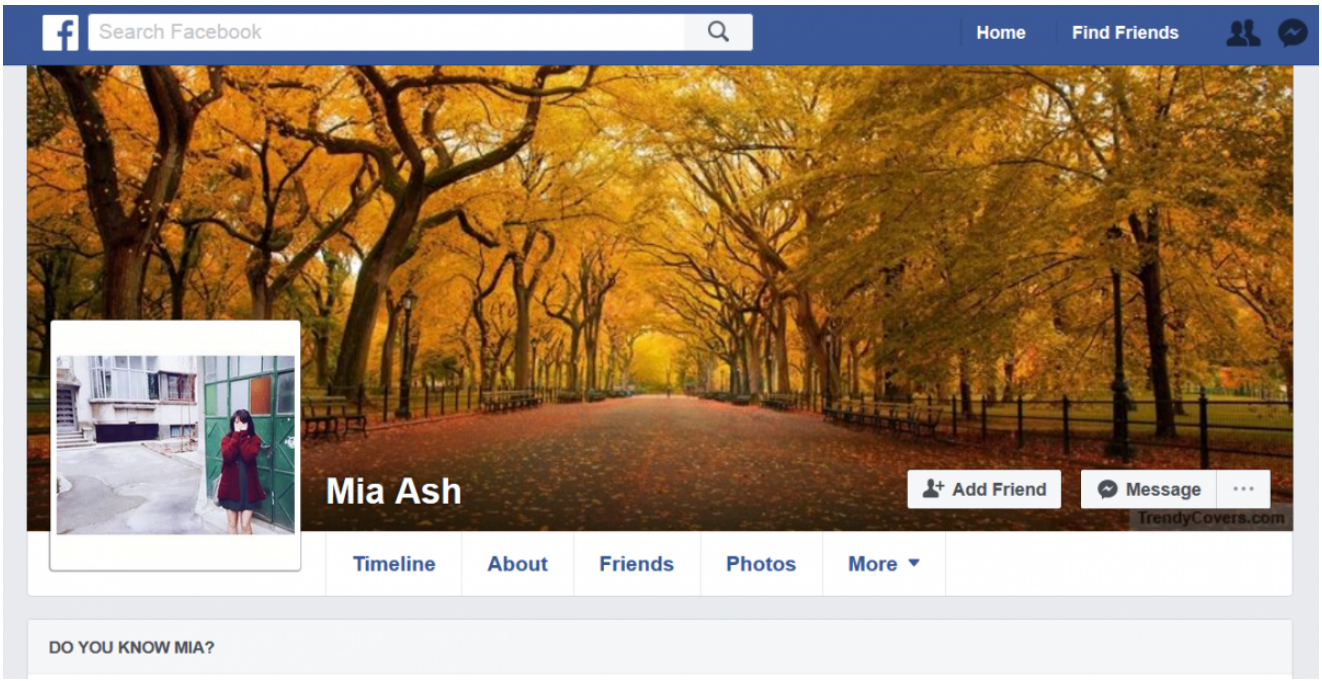
With Fake News And Femmes Fatales, Iran's Spies Learn To Love Facebook

forbes.com/sites/thomasbrewster/2017/07/27/iran-hackers-oilrig-use-fake-personas-on-facebook-linkedin-for-cyberespionage/

Thomas Brewster July 27, 2017



Thomas Brewster
Forbes Staff

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Jul 27, 2017,10:33am EDT|

This article is more than 4 years old.

Iran is honing its Facebook fakes, according to research.
SecureWorks

Before she disappeared from Facebook, Mia Ash was a fun-loving, young photographer who used the world's biggest social network to showcase her work. Ash was popular too. Stretching back to April 2016, she'd befriended a lot of individuals, as many as 500, with similar interests. Her looks almost certainly helped her apparent popularity.

Ash was thrown off of Facebook earlier this year, though. Not for any obvious infraction. But because Facebook had been handed proof by SecureWorks researcher Allison Wikoff that convinced them Ash was a fake. Not only that, her persona has been tied by Wikoff to one of

Iran's busiest cyberespionage groups, known as OilRig.

Alongside profiles across LinkedIn and DeviantArt, Ash was one of the most developed fakes Wikoff had ever seen in her years researching spy activity on the web. “What we’ve seen in the past is just a fake LinkedIn profile, but this had LinkedIn, Facebook, a Blogger profile, two domains, two email addresses, and WhatsApp. Traditionally we haven’t seen across the board," Wikoff told *Forbes*.

According to the researcher, Ash was active shortly after a surge in hacker activity from OilRig in December, as previously reported by *Forbes*. Using stolen images of a real young woman from Romania, Ash reached out to an employee of a targeted organization in the Middle East, the name of which SecureWorks isn’t reporting, sharing an interest in photography, shifting initial contact from her LinkedIn profile with more than 500 connections to her Facebook account. A relationship, albeit a fake one, was established, with chats over WhatsApp too. (*Forbes* and SecureWorks have attempted to contact the woman whose images were used, but with no success).

Eventually, she sent an email to the unwitting target, containing an Excel file, a supposed survey to do with photography. She asked him to open it on his corporate network, which he did. Then OilRig’s signature malware, known as PupyRAT, attempted to run and steal passwords for the corporate network. Fortunately, in that case, the security products of the organization sprung into action and prevented any data loss.

Despite the failure of the attack, Ash provides proof that OilRig has become adept at creating fake online personas. Wikoff says Ash tried and in many cases succeeded in grooming a range of technical individuals working for Middle East and Africa, most working in the oil and gas field. She was convincing enough to befriend an oil and gas cybersecurity pro with 10 years experience, according to Wikoff.

Fake news from Iran?

But Ash was one of a large number of fake profiles developed by Iranian-linked hacker groups over recent years, as they hone their craft. In recent months they've been experimenting with fake news outlets too. A separate group believed to be of Iranian origin, known as Charming Kitten, set up the blandly-named BritishNews, spamming a significant amount of content earlier this year, up to a sudden stop in April, according to a report handed to *Forbes* by Israeli security firm ClearSky.

The fake agency used stolen content from across the web and was designed to draw in targets to visit the official BritishNews website, from where malware would be delivered. The fake agency had a fake employee too. Again, LinkedIn was key to creating the persona, though it's unclear just who Charming Kitten was trying to target with BritishNews.

The only employee of the fake BritishNews agency, according to ClearSky.

ClearSky also reported on another fake profile earlier this week, believed to have been established by yet another Iranian-linked hacker crew called CopyKitten. Back in 2013, the crew had set up a handful of Facebook profiles to spread links to a copy of Israeli news site Haaretz. One Facebook fraud, named Amanda Morgan, was still active up to this month and was also promoting a fake news service called Emet Press. No malware were delivered over the sites and ClearSky believes they were only set up to establish trust. Most have now had their social sites cut down, others simply remain dormant, said ClearSky head of intelligence Eyal Sela.

Iran's use of personas isn't new. Historically, Iran's defense and intelligence units have long been linked to social media-led campaigns. The Newscaster attacks of 2014, for instance, saw myriad LinkedIn personas set up profiles posing as journalists. It's only the quality of the fakes that's increasing.

Facebook response

For its part Facebook has been responsive to requests to remove fake profiles. Alex Stamos, chief security officer for Facebook, told *Forbes* the company would be taking more of a manual approach rather than relying on automated technologies for dealing with nation state-sponsored fakes.

"A lot of that work ... is more about looking for the patterns of malicious behavior that are expressed by those kinds of grooming attacks by advanced nation state adversaries," Stamos said. "That would be more of a manual process that's helped by automation."

With Iran not giving up on its social exploitation, expect that game of whack-a-mole to continue.

Follow me on Twitter. Check out my website. Send me a secure tip.

Thomas Brewster