Report links hacking scheme to Iran (Update)

August 27 2015, byBree Fowler

Researchers have linked a sophisticated hacking scheme targeting Iranian dissidents and at least one freedom of expression activist back to Iran.

A report released Thursday by the Citizen Lab at the University of Toronto's Munk School of Global Affairs describes how the hackers used text message and phone-based phishing to try to get around the security of Google's Gmail and access the accounts of their targets.

The attacks studied by the Citizen Lab were very similar to others connected to Iranian hackers, the report says.

Omid Memarian, an exiled Iranian journalist living in New York, says the hackers contacted him in June through Google Chat messages, phone calls and emails, telling him he needed to change his Gmail password. He realized it was a phishing attempt and didn't hand over his information, but the hackers' repeated attempts made him fear that his account had been compromised.

Memarian, who speaks out frequently through mainstream and social media about jailed reporters in Iran and other human-rights issues, says that while he's received generic phishing emails before, it was "terrifying" to know that he had been personally targeted by the hackers.

"There's no doubt that this comes from Iran's Revolutionary Guard, which has been very vicious against the free press and free speech," Memarian says.

Officials for the Iranian government and the Revolutionary Guard didn't immediately return emails seeking comment. Google also didn't immediately return an email seeking comment.

According to the report, some of the attacks began when the targets received text messages that appeared to be from Google saying that there had been an unauthorized attempt to access their Gmail accounts.

The hackers would then follow up with a carefully crafted email that included a link to a website where the target could reset their password. But the links actually took the targets to phishing sites. After the target entered their password on the phony site, the hackers would use it right away to login to the target's account and trigger the sending of an identification code to the target.

Gmail uses the code as a form of two-factor authentication, which adds a second layer of security on top of a person's password. The hackers would then wait for the target to enter the code on the fake website, collect it, and then use it to take control of the account.

In other cases, the targets were contacted by phone by a person who would make a "proposal" related to the target's business activities. The proposal, usually promising thousands of dollars, would then be sent to the target's Gmail in the form of an email containing a fake Google Drive link.

When the target clicked on the drive, they would be prompted to login with the Google credentials and ultimately the two-factor identification code, just like in the cases of the text messages.

Jillian York, director of international freedom of expression at the Electronic Frontier Foundation, was the only non-Iranian noted in the report to be caught up in the scheme. For her, the phishing attempt

started with an early morning phone call earlier this month from a man who identified himself as a journalist wanting to interview her.

The man, who York says sounded German, sent her an email that included an attachment. After she declined to open it, he sent it again from a different address, so she knew something was up. When she still wouldn't open it, he started calling her again, ultimately a total of 34 times.

York contacted the Citizen Lab, which was already working on its report. It tied the attack on York to the Iranian phishing scam.

While York, who is based in Germany, does handle freedom of expression issues related to the Arab Middle Eastern countries, she doesn't deal much with Iran. But she is connected through social media to some notable people who do, which is her best guess as to why she was targeted in the scheme.

Regardless of the motivation behind them, phishing schemes such as this highlight how important two-factor authentication has become, the report says.

It notes that in the case of these hackers, the existence of the identification code significantly increased the amount of work required. It forced the hackers to actively monitor the fake website and enter the information they collected in real time. Without the existence of the code, the hackers could have just sent out a flood of emails and collected passwords through their website at their leisure.