

CIO TODAYGet **EXPERT ADVICE**
from CSO InsightsDownload
the whitepaper[HOME](#) [ENTERPRISE SOFTWARE](#) [ENTERPRISE HARDWARE](#) [TECH TRENDS](#) [NETWORK SECURITY](#) [CLOUD COMPUTING](#) [MORE](#)**TRENDING TOPICS:** [Security](#) • [Cybercrime](#) • [Microsoft](#) • [Google](#) • [Data Centers](#) • [Android](#) • [Net Neutrality](#) • [Apple](#)

NETWORK SECURITY

Report Links Sophisticated Hacking Scheme to Iran

Posted August 28, 2015

 **EARLIER**
**University Student Pleads Guilty To Making
Android Spy App****THIS STORY**
**Report Links Sophisticated Hacking Scheme to
Iran****LATER**
**Ashley Madison Breach Spawns Malicious
Spammers** YOU ARE HERE: [HOME](#)[NETWORK SECURITY](#)[THIS STORY](#)**neustar.** [Want to block DDoS? Here's how.](#)**NEWS OPS****By Bree Fowler.**
*Updated August 28,
2015 4:00AM***SHARE**

Researchers have linked a sophisticated hacking scheme targeting Iranian dissidents 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.

CERTIFICATION EXAM DATE
12 September 2015***REGISTER EARLY AND
SAVE US \$50!****EARLY REGISTRATION DEADLINE:**
17 JUNE 2015**REGISTER >****ISACA***CISA and CISM only. Held in select locations.



Microsoft

THIS IS
BUSINESS IN THE
NOW

Learn how
with your
free CRM trial



ALSO SEE

Hacking

Phishing

Iran

Network Security

Cybercrime

Cyberattack

Citizen Lab

Gmail

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 notification containing personal details and stating that the login attempt had been from "The Iran," boosting the fears of people already worried about Iranian hackers.

The emails contained links directing the target to a page where they could reset their password. But in fact, the links were to phishing sites designed to collect the target's password. The hackers would then, in real time, use the password to login to the user'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, collect it through the fraudulent website, and then use it to take control of the account.

In other cases, the targets were contacted by phone by a person speaking English or Farsi, the predominate language in Iran, who would make a "proposal" related to the target's business activities. The fake 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.

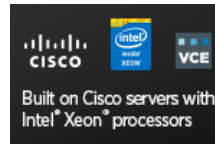
When the target clicked on the drive, they would be prompted to login with the Google credentials and ultimately the two-factor identification code, just like in the cases of the text messages.

While attempts to circumvent two-factor authentication security are nothing new when it comes to financial fraud -related hackings, the practice is fairly new to politically motivated attacks.

"It may be that, as a growing number of potential targets have begun using two-factor authentication on their email accounts out of a concern for their security, politically motivated attackers are borrowing from a playbook that financial criminals have written over the past decade," the report reads.

The report emphasizes that these kinds of attacks are increasing, boosting the importance of two-factor authentication.

It notes that in the case of these hackers, the existence of the code significantly increased the amount of work required. The hackers were forced to actively monitor the phishing site and enter the information they collected in real time in order to take control of the



TOP OF THE NEWS SATURDAY AUGUST 29



Windows 10 Now on 75 Million Devices, Microsoft Says

Microsoft says that its new Windows 10 software is running on more than 75 million computers, tablets and other devices -- in just under a month since the operating system was released.



Spammers Prey on Cheat Site Users



U.S. Funding New High-Tech Venture



Appeals Court Reverses NSA Ruling



Facebook Hits 1B Users in One Day

CERTIFICATION EXAM DATE
12 September 2015*

REGISTER EARLY AND SAVE US \$50!

EARLY REGISTRATION DEADLINE:
17 JUNE 2015

[REGISTER >](#)

ISACA

*CISA and CISM only. Held in select locations.

Learn the vulnerabilities your website likely faces: Discover why it probably can't handle a large DDoS attack. Plus, learn how [Neustar](#) is an AWS Technology Partner offering the solutions and expertise to keep your site safe. Defend your Internet presence. [Download the e-book now!](#)

MORE IN NETWORK SECURITY

- **Ashley Madison CEO Quits Amid Hack**

accounts.

Without the existence of the code, the hackers could have just collected passwords through the fake website at their leisure, the report says.

© 2015 Associated Press syndicated under contract with NewsEdge. All rights reserved.

Tell Us What You Think

Comment:

Name:

- **Spammers Prey on Cheat Site Users**
- **Audit: California at Risk for IT Breach**
- **Guilty Plea in Android Spy App Case**
- **Amazon Bans Flash Ads from Site**

CERTIFICATION EXAM DATE
12 September 2015*

REGISTER EARLY AND
SAVE US \$50!

EARLY REGISTRATION DEADLINE:
17 JUNE 2015

[REGISTER >](#)

ISACA

*CISA and CISM only. Held in select locations.

[Next Article >](#)



GET THE SELLING GUIDE



TECHNOLOGY MARKETPLACE / BUYER'S GUIDE

▼ advertisement

Big Data

- VCE VBlock - more productivity with less cost. Download the paper.

CRM Systems

- Transform your sales teams with the CSO Insights whitepaper.

Cloud Computing

- VCE VBlock - more productivity with less cost. Download the paper.
- Next Generation Data Center Is Here! Vblock™ Systems from VCE.

Customer Service

- Experience CRM and Business Success today with Salesforce.com.

Cybercrime

- Think you're safe from DDoS attacks? Get Neustar's e-book now!

Data Storage

- Next Generation Data Center Is Here! Vblock™ Systems from VCE.

Sales & Marketing

- Transform your sales teams with the CSO Insights whitepaper.

Security Solutions

- Think you're safe from DDoS attacks? Get Neustar's e-book now!

Get **EXPERT ADVICE**
from CSO Insights



Download
the whitepaper 



INSIDE CIO TODAY

- ENTERPRISE SOFTWARE
- ENTERPRISE HARDWARE
- TECH TRENDS
- NETWORK SECURITY
- CLOUD COMPUTING
- DATA STORAGE
- OPERATING SYSTEMS
- UNIFIED
- COMMUNICATIONS
- CIO ISSUES
- MOBILE TECH
- BIG DATA
- WORLD WIDE WEB
- BUSINESS BRIEFING
- CRM SYSTEMS
- AFTER HOURS
- PRESS RELEASES

NETWORK SITES

- CIO TODAY
- TOP TECH NEWS
- MOBILE TECH TODAY
- DATA STORAGE TODAY
- ABOUT OUR NETWORK

SERVICES

- FREE NEWSLETTERS
- ARTICLE REPRINTS
- CONTACT US
- PRIVACY POLICY
- TERMS OF SERVICE

BENEFITS

- ADVERTISE WITH US
- PUBLIC RELATIONS (PR) SERVICES
- (In Partnership with NewsFactor)



*Daily Briefing for Technology's Top
Decision-Makers*

Copyright 2015 CIO Today Network. All rights reserved. Member of **Accuserve Ad Network**.