

Pursuit of hackers who took credit reports expands

March 13 2013, by Anne Flaherty



In this Feb. 10, 2013 file photo, Jay-Z poses backstage with the awards for best rap/sung collaboration for "No Church in the Wild" and best rap performance for "N****s in Paris" at the 55th annual Grammy Awards, in Los Angeles. Jay-Z is among 11 celebrities and government officials whose private financial information appears to have been posted online by a site that began garnering attention on Monday, March 11, 2013. (Photo by Matt Sayles/Invision/AP, File)

(AP)—The pursuit of hackers who audaciously stole and published credit reports for Michelle Obama, the attorney general, FBI director and other U.S. politicians and celebrities crisscrossed continents and included a San Francisco-based Internet company, Cloudflare, The Associated Press has learned.

The sensational crime caught the attention of Congress and President [Barack Obama](#), who said "we should not be surprised."

Obama said he could not confirm that the first lady's credit report was published earlier this week on a Russian website, along with what appeared to be the credit reports of nearly two dozen others, including Republican presidential candidate [Mitt Romney](#), real estate mogul Donald Trump and celebrities [Britney Spears](#), Jay Z, Beyonce and [Tiger Woods](#).

The president said determined hackers are a persistent threat.

"We should not be surprised that if you've got hackers who want to dig in and devote a lot of resources, that they can access people's private information," Obama told [ABC News](#) in an interview aired Wednesday. "It is a big problem."

Obama added: "It would not shock me if some information among people who presumably have pretty good [safeguards](#) against it, still gets out. That's part of the reason why we've got to continually improve what we do and coordinate between public and private sectors to make sure that people's information is safe."

In Congress, the Republican chairman of the House Judiciary Committee cited the breach Wednesday at a congressional hearing about the government prosecuting hackers. Rep. Bob Goodlatte said the leaks of financial information was "just the beginning of the problem" when it

comes to the vulnerability of U.S. computer networks. Goodlatte said the U.S. has billions of dollars at stake, as foreign hackers try to steal sensitive information from businesses.

"The truth is that all citizens are vulnerable to these kinds of cyberattacks," Goodlatte said.

A spokesman for one of the largest U.S. credit bureaus, Tim Klein of Equifax, said an initial investigation showed that hackers used a website designed to give consumers a free credit report. The hackers apparently used personal details about their victims to impersonate them and generate the credit reports.

Representatives for Experian, Equifax and TransUnion have all said they were cooperating with the U.S. criminal investigation being conducted by the FBI and Secret Service.

In San Francisco, Cloudflare operates the directory computers, known as name servers, used behind the scenes to send visitors to the Russian website where the stolen credit reports were being published, according to Internet registration records. Without that service, few Internet users would be able to visit the Russian website or view the stolen credit reports.

A company spokeswoman, Carol Carrubba, told the AP that Cloudflare, which she described as a performance and security company, doesn't comment on its customers. But Carrubba said: "Even if we delete a customer's account, the content remains in place, though the site may load more slowly."

Internet directories on Wednesday continued to identify Cloudflare as directing traffic to the Russian website, although any technical changes could take hours or days to update across the Internet.

Last month, the chief executive at Cloudflare, Matthew Prince, said in a speech that he had been victimized last year by hackers associated with the group UGNazi. They tricked Google into giving them access to his Gmail account, Prince said, and left voicemails taunting him that they had bought his Social Security number from an underground Russian website. Prince said the break-in of his personal email account also allowed the hackers to take over Cloudflare's corporate email systems.

In his speech, Prince said his company traced the attackers within 24 hours, and the [hackers](#) turned out to be among Cloudflare's customers.

The FBI in San Francisco declined to tell AP whether investigators have contacted Cloudflare to review payments or communications that had been used to set up the service.

The website address uses an Internet suffix originally assigned to the former Soviet Union, and many of the pages feature unflattering pictures of the person featured and taunting messages to them. A counter on the website indicated that it had received more than 450,000 views since its existence was revealed on Monday.

Social Security numbers posted on Jay-Z, Mel Gibson and others matched records in public databases. Social Security numbers are not public records, although they used to be included in some court filings. Many courts require the information be redacted from filings since the numbers can be used to steal a person's identity and open credit accounts in their name.

Copyright 2013 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: Pursuit of hackers who took credit reports expands (2013, March 13) retrieved 31 March 2023 from <https://phys.org/news/2013-03-pursuit-hackers-credit.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.