KIM ZETTER SECURITY 10.19.15 6:14 PM

TEEN WHO HACKED CIA DIRECTOR'S EMAIL TELLS HOW HE DID IT

CIA director John Brennan. CHRIS MADDALONI/AP

A HACKER WHO claims to have broken into the AOL account of CIA Director John Brennan says he obtained access by posing as a Verizon worker to trick another employee into revealing the spy chief's personal information.

Using information like the four digits of Brennan's bank card, which Verizon easily relinquished, the hacker and his associates were able to reset the password on Brennan's AOL account repeatedly as the spy chief fought to regain control of it.

News of the hack was first reported by the *New York Post* after the hacker contacted the newspaper last week. The hackers described how they were able to access sensitive government documents stored as attachments in Brennan's personal account because the spy chief had forwarded them from his work email.

The documents they accessed included the sensitive 47-page SF-86 application that Brennan had filled out to obtain his top-secret government security clearance. Millions of SF86 applications were obtained recently by hackers who broke into networks belonging to the Office of Personnel Management. The applications, which are used by the government to conduct a background check, contain a wealth of sensitive data not only about workers seeking security clearance, but also about their friends, spouses and other family members. They also include criminal history, psychological records and information about past drug use as well as potentially sensitive information about the applicant's interactions with foreign nationals—information that can be used against those nationals in their own country.

The hacker, who says he's under 20 years old, told WIRED that he wasn't working alone but that he and two other people worked on the breach. He says they first did a reverse lookup of Brennan's mobile phone number to discover that he was a Verizon customer. Then one of them posed as a Verizon technician and called the company asking for details about Brennan's account.

"[W]e told them we work for Verizon and we have a customer on scheduled callback," he told WIRED. The caller told Verizon that he was unable to access Verizon's customer database on his own because "our tools were down."

After providing the Verizon employee with a fabricated employee Vcode—a unique code the he says Verizon assigns employees—they got the information they were seeking. This included Brennan's account number, his four-digit PIN, the backup mobile number on the account, Brennan's AOL email address and the last four digits on his bank card.

"[A]fter getting that info, we called AOL and said we were locked out of our AOL account," he said. "They asked security questions like the last 4 on [the bank] card and we got that from Verizon so we told them that and they reset the password." AOL also asked for the name and phone number associated with the account, all of which the hackers had obtained from Verizon.

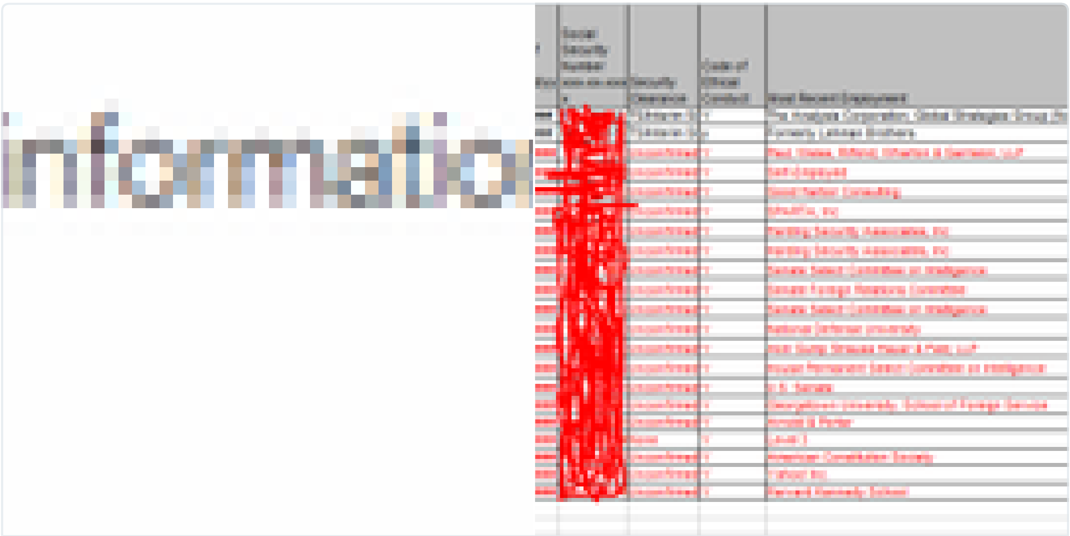
On October 12, they gained access to Brennan’s email account, where they read several dozen emails, some of them that Brennan had forwarded from his government work address and that contained attachments. The hacker provided WIRED with both Brenann’s AOL address and the White House work address used to forward email to that account.

Among the attachments was a spreadsheet containing names and Social Security numbers—some of them for US intelligence officials—and a letter from the Senate asking the CIA to halt its use of harsh interrogation techniques—that is, its controversial use of torture tactics.

These documents appear to come from 2009. The Associated Press has speculated that the spreadsheet might be a list of guests who were visiting the White House that year when Brennan was President Obama’s counter-terrorism adviser.

The hackers posted screenshots of some of the documents on their Twitter account, @phphax. Among the items posted were links to a file the hackers say contained portions of Brennan’s contact list as well as a log of phone calls by former CIA deputy director Avril Haines. They also posted a reduced page from the spreadsheet.

The hackers were in Brennan’s account for three days before it was disabled last Friday.



cracka
@phphax

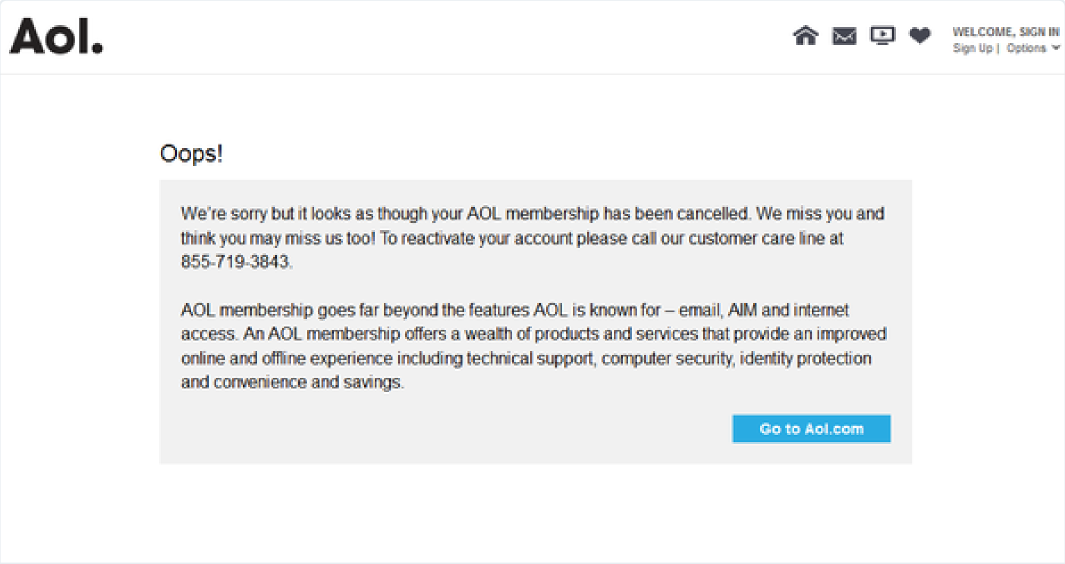
Follow

"It does not appear that any classified information was accessed" meanwhile..

12:59 AM - 20 Oct 2015

59 45

On October 16, the hacker Tweeted that Brennan had deleted his AOL account after they had notified him of the breach.



Oops!

We're sorry but it looks as though your AOL membership has been cancelled. We miss you and think you may miss us too! To reactivate your account please call our customer care line at 855-719-3843.

AOL membership goes far beyond the features AOL is known for – email, AIM and internet access. An AOL membership offers a wealth of products and services that provide an improved online and offline experience including technical support, computer security, identity protection and convenience and savings.

cracka
@phphax

Follow

Well, John Brennan deleted his email because we kept jacking it LOL

8:56 PM - 16 Oct 2015

11 ★ 6

The hacker told WIRED that Brennan had tried to access the account and couldn't.

He told WIRED that Brennan re-set the password, and they hijacked it again. "[H]e took back access and we re-jacked it. That happened 3 times," he said.

So they called Brennan's mobile number, using VoIP, and told him he'd been hacked. The conversation was brief.

"[I]t was like 'Hey,.... its CWA.' He was like 'What do you want?' We said '2 trillion dollars hahhaa, just joking,'" the hacker recounted to WIRED.

Brennan, the hacker says, replied, "How much do you really want?"

They told Brennan "We just want Palestine to be free and for you to stop killing innocent people."

In addition to Brennan's AOL account, the hackers also broke into the Comcast account of Homeland Security Secretary Jeh Johnson.

The news of the breach, of course, comes in the midst of another email scandal involving Hillary Clinton who has been under fire for months over a private server and email account she maintained to do official work. Clinton has been accused of maintaining the server to bypass public records requests involving her government email address.

It's unclear if Brennan was using his personal email to conduct government business or if he simply used it to occasionally store email and documents from his work account.

The hack, using social-engineering techniques to pull information from tech support, is reminiscent of the epic hack that targeted former WIRED writer Mat Honan. In that case, Apple tech support gave a hacker named Cosmo access to Honan's iCloud account, and Amazon tech
nan's credit
Ionan's
access to a
series of other accounts.

#CIA #CYBERSECURITY #HACKS AND CRACKS #JOHN BRENNAN

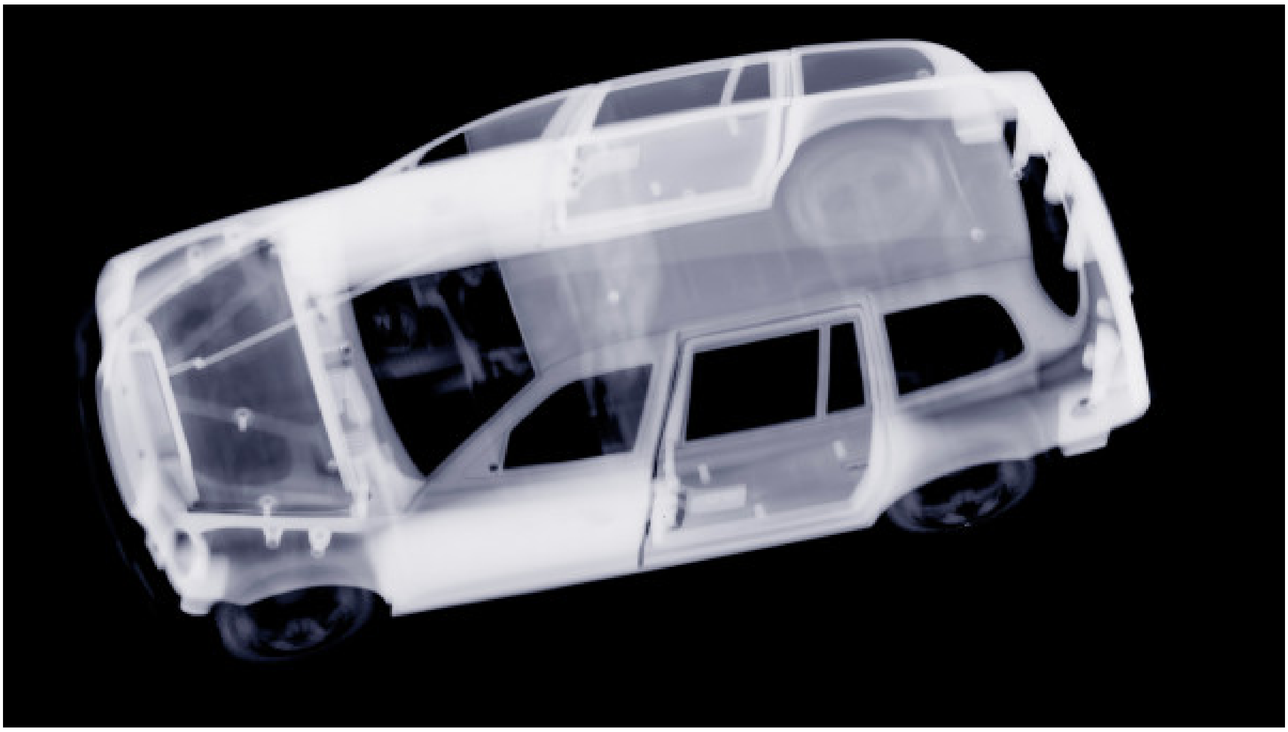
VIEW COMMENTS

MORE SECURITY

CYBERCRIME

X-Ray Scans Expose an Ingenious Chip-and-Pin Card Hack

17 HOURS



SECURITY THIS WEEK

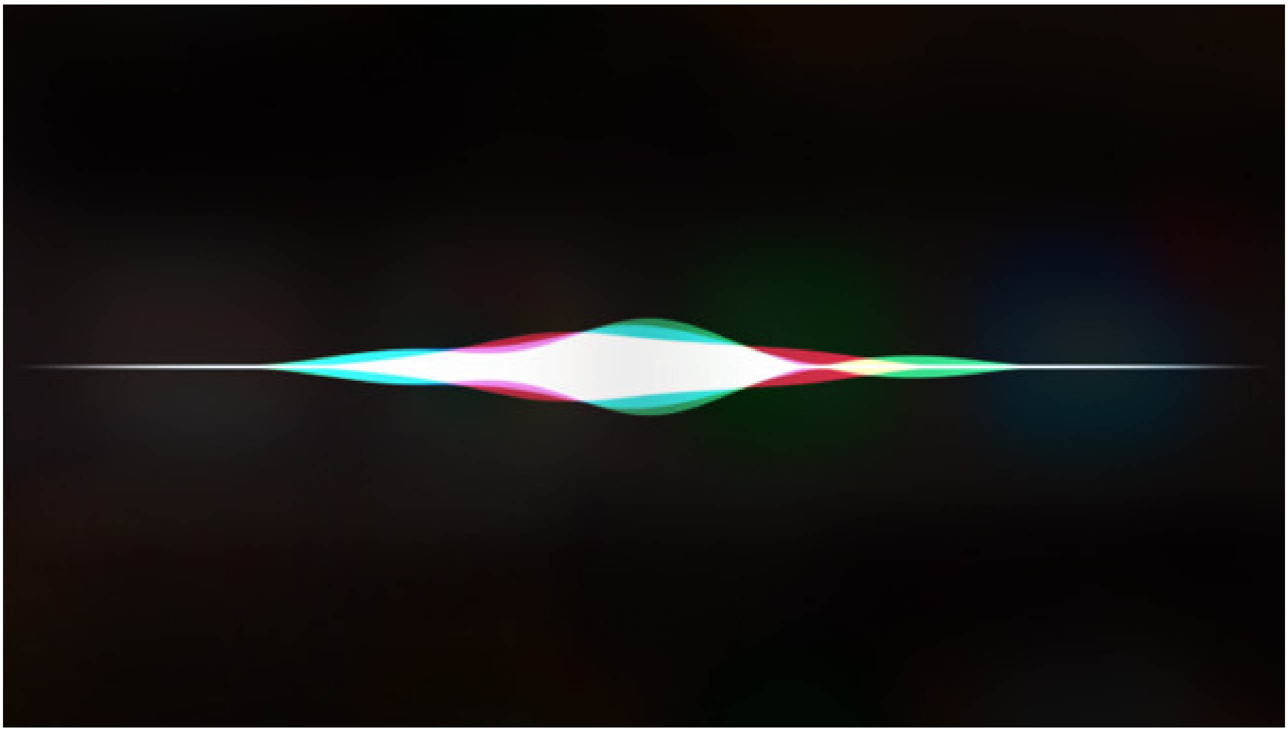
Security News This Week: The NYPD Doesn't Want You to Know About Its X-Ray Spy Vans

10.17.15

EXPLAINED

Answers to Your Burning Questions on the Ashley Madison Hack

08.21.15



SECURITY

Hackers Can Silently Control Siri From 16 Feet Away

10.14.15

PRIVACY

A New Way for Tech Firms to Fight Orders to Unlock Devices

10.13.15

WE RECOMMEND

LIZ STINSON

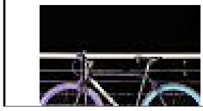
NASA's Logo From The '70s Was Ridiculously Cool

CADE METZ

The Porn Business Isn't Anything Like You Think It Is

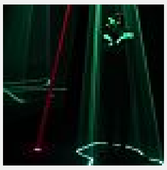
NATHAN MATTISE

Quick! Chug Your Liquor Before It Goes Weird



WIRED INSIDER

An Un-stealable Bike Has Arrived



DWELL

Digital Revolution: The Immersive Future of Art and Technology

POWERED BY OUTBRAIN

FOLLOW US ON YOUTUBE

Don’t miss out on WIRED’s latest videos.

FOLLOW

WIRED

SUBSCRIBE

ADVERTISE

SITE MAP

PRESS CENTER

FAQ

CUSTOMER CARE

CONTACT US

NEWSLETTER

WIRED STAFF

JOBS

RSS