SecureTheVillage

The Email That Hacked the Democratic National Committee … and Other Information Security Lessons from the DNC Breach

January 2017

Stan Stahl, Ph.D.
President, Citadel Information Group
President, Secure the Village

Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account [redacted]@gmail.com.

Details:

Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

September 2015: Missed Warning Signs

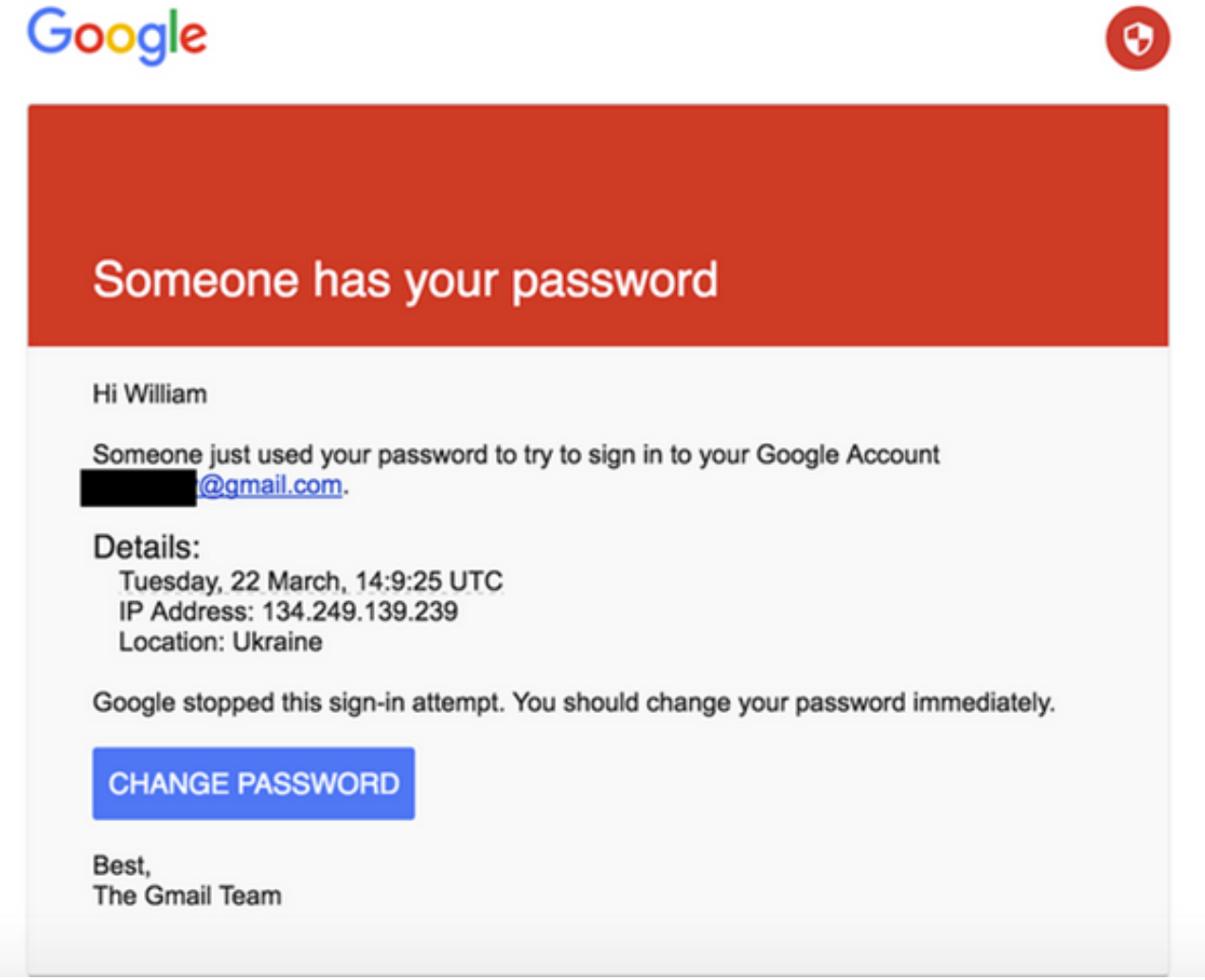
- FBI Special Agent Adrian Hawkins called the D.N.C.
- Yared Tamene, a Tech-Support contractor took the call and was told: *At least one computer system belonging to the D.N.C. had been compromised by hackers federal investigators had named "the Dukes," a cyberespionage team linked to the Russian government.*
- He checked Google for "the Dukes" and conducted a cursory search of the D.N.C. computer system logs to look for hints of a cyberintrusion.
- By his own account, he did not look too hard even after Special Agent Hawkins called back repeatedly over the next several weeks — in part because he wasn't certain the caller was a real F.B.I. agent and not an impostor.

The Perfect Weapon: How Russian Cyberpower Invaded the U.S.

November 2015: More Missed Warning Signs

- Special Agent Hawkins called with more ominous news, alerting Tamene that a D.N.C. computer was “calling home,” sending information to Moscow. Hawkins added that the F.B.I. thinks that this calling home behavior could be the result of a state-sponsored attack.
- Andrew Brown, D.N.C. Technology Director, and Tamene’s boss, knew Tamene was fielding calls from the F.B.I. but was tied up on a different problem: whether Senator Sanders campaign had improperly gained access to Clinton’s campaign data.

March 2016: A Second Attack



Oops!!

From: Charles Delavan <cdelavan@hillaryclinton.com>
Date: March 19, 2016 at 9:54:05 AM EDT
To: Sara Latham <slatham@hillaryclinton.com>, Shane Hable <shable@hillaryclinton.com>
Subject: Re: Someone has your password

Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this is done ASAP.

With another click, a decade of emails that Mr. Podesta maintained in his Gmail account — a total of about 60,000 — were unlocked for the Russian hackers. ***Mr. Delavan, in an interview, said that his bad advice was a result of a typo: He knew this was a phishing attack, as the campaign was getting dozens of them. He said he had meant to type that it was an "illegitimate" email, an error that he said has plagued him ever since.***

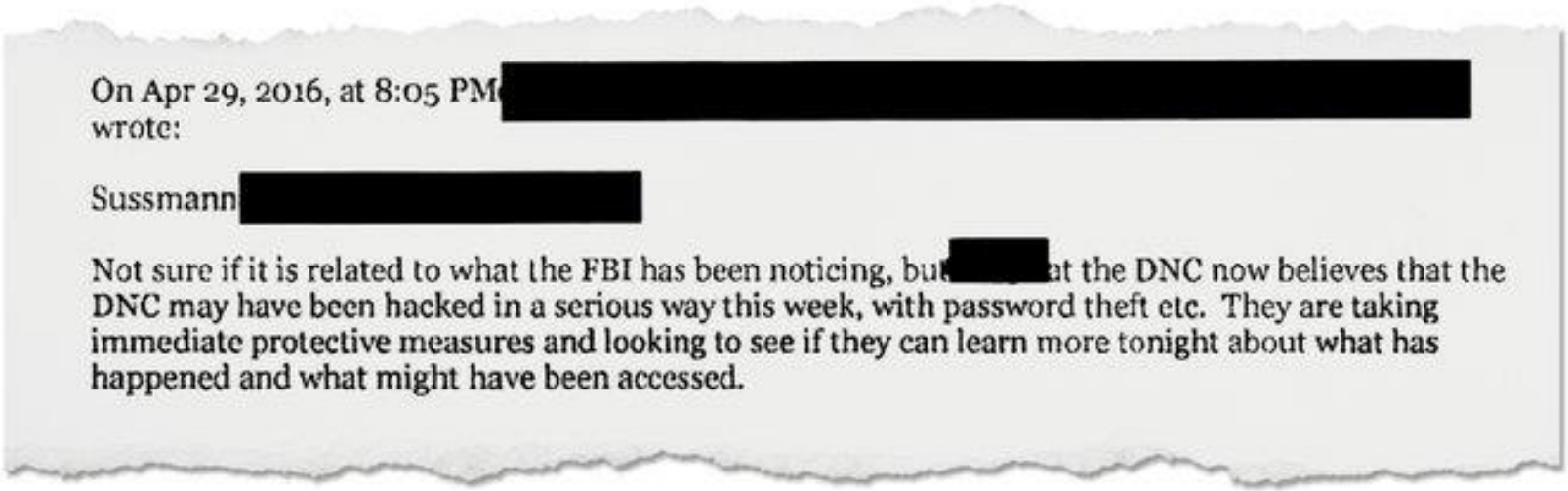
More Missed Signals

- During this second wave, the hackers also gained access to the Democratic Congressional Campaign Committee, and then, through a virtual private network connection, to the main computer network of the D.N.C.
- The F.B.I. observed this surge of activity as well, again reaching out to Mr. Tamene to warn him. *Yet Mr. Tamene still saw no reason to be alarmed*: He found copies of the phishing emails in the D.N.C.'s spam filter. But he had no reason, he said, to believe that the computer systems had been infiltrated.

Mid-April 2016: A Bit of Progress

- D.N.C., seven months after it had first been warned, finally installed a “robust set of monitoring tools,” according to Tamene
- With the new monitoring system in place, Tamene had examined administrative logs of the D.N.C.’s computer system and found something very suspicious: *An unauthorized person, with administrator-level security status, had gained access to the D.N.C.’s computers*.

April 29, 2016: The D.N.C. Finally Connects the Dots



On Apr 29, 2016, at 8:05 PM [redacted] wrote:

Sussmann [redacted]

Not sure if it is related to what the FBI has been noticing, bu[redacted]t the DNC now believes that the DNC may have been hacked in a serious way this week, with password theft etc. They are taking immediate protective measures and looking to see if they can learn more tonight about what has happened and what might have been accessed.

The Consequences

- ***The failure of the IT Contractor and the Technology Director to take the possibility of a breach seriously,*** coupled with the *"low-key approach of the F.B.I., meant that Russian hackers could roam freely through the committee's network for nearly seven months before top D.N.C. officials were alerted to the attack and hired cyberexperts to protect their systems. In the meantime, the hackers moved on to targets outside the D.N.C., including Mrs. Clinton's campaign chairman, John D. Podesta, whose private email account was hacked months later."* Italics from NYT article.

The Excuses

- **Budget:** The D.N.C. was a nonprofit group, dependent on donations, with a fraction of the security budget that a corporation its size would have.
- **F.B.I.:** Shawn Henry, ex-head of F.B.I.'s cyber division, currently CrowdStrike, the cybersecurity firm retained by the D.N.C. in April, said he was baffled that the F.B.I. did not call a more senior official at the D.N.C. or send an agent in person to the party headquarters to try to force a more vigorous response.

The Security Problems Were Structural

- **Ad Hoc Security Management:** There seems to have been no qualified person specifically tasked with information security management. Podesta reached out for support to a colleague — not a security professional — and was given misleading information.
- **IT Security Management:** Tamene was an IT contractor. He was apparently not trained in information security management of IT
- **Contractor Management:** Tamene was not a full-time D.N.C. employee; he works for a Chicago-based contracting firm called *The MIS Department*.
- **Incident Response Training:** Tamene was left to figure out, largely on his own, how to respond — and even whether the man who had called in to the D.N.C. switchboard was really an F.B.I. agent.

Krebs's Five Immutable Truths About Data Breaches

1. If you connect it to the Internet, someone will try to hack it.
2. If what you put on the Internet has value, someone will invest time and effort to steal it.
3. Even if what is stolen does not have immediate value to the thief, he can easily find buyers for it.
4. The price he secures for it will almost certainly be a tiny slice of its true worth to the victim.
5. Organizations and individuals unwilling to spend a small fraction of what those assets are worth to secure them against cybercrooks can expect to eventually be relieved of said assets."

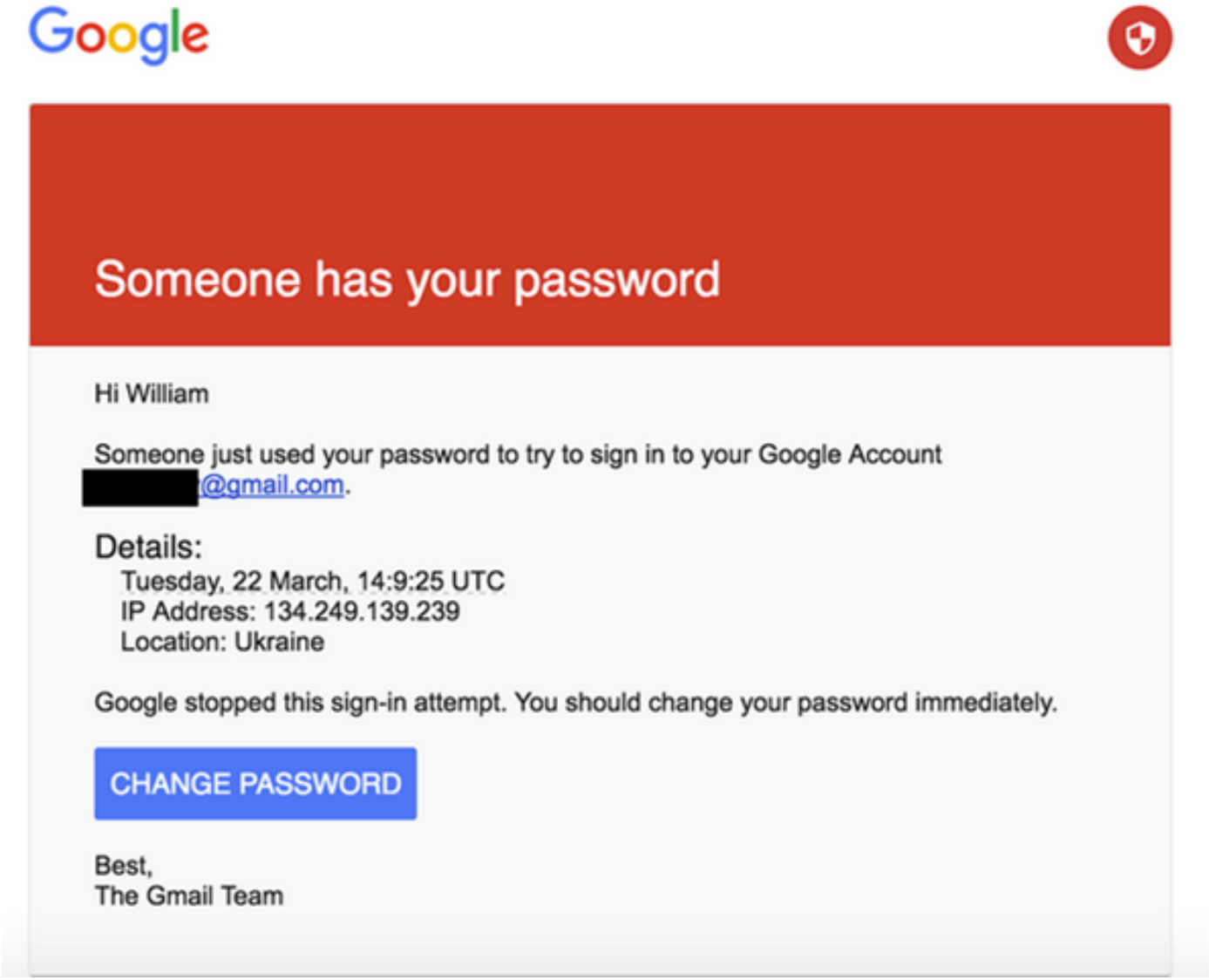
Citadel's Three Defense Truths

1. No matter how much money you spend, you will not be able to 100% protect your assets.
2. SMB's can get significant protection without spending a ton of money. *
3. You get your greatest bang-for-the-buck through formal risk management, leadership, and culture change.

* Except when needing to defend themselves against a nation-state attack or from a group specifically targeting that organization

The number one thing at the Board level and CEO level is to ***take cybersecurity as seriously as you take business operations and financial operations***. It's not good enough to go to your CIO and say "are we good to go." ***You've got to be able to ask questions and understand the answers***.

Major Gen Brett Williams, U.S. Air Force (Ret)
This Week with George Stephanopoulos, December 2014



How Many of Your People Would Click the Link in the Above Email?

How Strong Are Your Defenses When They Do?


Information Peace of Mind ®
Information Security Proactively Managed
Commercially Reasonable Information Security Practices
Lower Total Cost of Information Security SM
Support Public Interest

For More Information

Stan Stahl Stan@citadel-information.com 323-428-0441
LinkedIn: Stan Stahl Twitter: @StanStahl

Citadel Information Group: citadel-information.com

- ***Information Security Resource Library***
- ***Free: Cyber Security News of the Week***
- ***Free: Weekend Vulnerability and Patch Report***

SecureTheVillage: SecureTheVillage.org

- ***Information Security Resource Library***
- ***Join the Community***
- ***Attend a Cybersecurity Roundtable***

FBI's Southern California Cyber Fraud Unit: sccf@leo.gov.

SecureTheVillage

The Email That Hacked the Democratic National Committee … and Other Information Security Lessons from the DNC Breach

Thank You!

Stan Stahl, Ph.D.
President, Citadel Information Group
President, Secure the Village