JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051

http://oversight.house.gov

May 26, 2016

The Honorable Devin Nunes, Chairman
The Honorable Adam Schiff, Ranking Member
Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Nunes and Ranking Member Schiff:

Thank you for your letter on June 23, 2015, making a referral to the Oversight Committee of claims that CyTech Services discovered last year's cyber-attacks against the Office of Personnel Management (OPM) before OPM discovered them. The Committee has now investigated these claims, obtaining thousands of pages of documents and conducting multiple transcribed interviews. The evidence obtained by the Committee indicates that OPM first discovered the intrusion into its networks—not CyTech—and claims that CyTech was responsible for first detecting these attacks are inaccurate.

Referral from Intelligence Committee to Oversight Committee

On June 23, 2015, you sent a referral letter and memorandum to the Oversight Committee relaying claims made by CyTech employees during a meeting with your staff on June 19, 2015.[1]

Your referral stated that CyTech employees met with OPM officials on April 21, 2015, to demonstrate their product, known as CyFIR, which your referral described as a "high-speed forensic analytic tool."

Your referral stated that, during this product demonstration, CyTech employees "were allowed to rack-mount one of their servers loaded with CyFIR tools onto the OPM system" and that they "launched a 'snapshot' scan of the OPM system."

Your referral stated that the scan "identified some known malware and adware as well as some 'unknown processes' that required further examination" and that these unknown processes "were of high interest to OPM."

---

[1] Letter and Memorandum from Chairman Devin Nunes and Ranking Member Adam Schiff, House Permanent Select Committee on Intelligence, to Chairman Jason Chaffetz and Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform (June 23, 2015).

Your referral acknowledged, however, that your staff "have not independently verified this information."

Oversight Committee Hearing and Requests for Information

The day after we received your referral, on June 24, 2015, the Oversight Committee held a previously scheduled hearing on the OPM data breach.[2]

During that hearing, Committee Members questioned then-OPM Director Katherine Archuleta and then-Chief Information Officer Donna Seymour about CyTech's claims. Both responded that OPM had identified the breach a week before CyTech did, but that the agency allowed CyTech to run its scan in order to determine whether the product the company was selling would have identified the breach.

For example, during the hearing, Rep. Michael Turner asked Director Archuleta and Ms. Seymour: "Was CyTech involved in the discovery of this data breach?" In response, Ms. Seymour explained that "OPM discovered the breach." With respect to CyTech's subsequent scan, she explained: "We wanted to see if that tool set would also discover what we had already discovered." Rep. Turner then replied:

> Well, clearly, you are going to have to give us all an additional briefing and certainly the Intel Committee staff an additional briefing on exactly how you did this because, you know, CyTech's relating what they did is very compelling. And, quite frankly, what you say sounds highly suspicious, that you would have brought them in, tricked them to see if they could discover it, something you have already discovered.

On July 24, 2015, we sent a letter to OPM requesting a wide range of documents relating to this issue.[3] The Committee also requested documents from CyTech on August 14, 2015.[4] In addition, we requested documents from the federal agencies and contractors involved with OPM's incident response and remediation efforts, specifically, the United States Computer Emergency Readiness Team (US-CERT) and Cylance, Inc., the contracting company that directly participated in incident response efforts at OPM.[5]

---

[2] House Committee on Oversight and Government Reform, *Hearing on OPM Data Breach: Part II* (June 24, 2015).

[3] Letter from Chairman Jason Chaffetz and Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform, to Beth Cobert, Acting Director, Office of Personnel Management (July 24, 2015).

[4] Letter from Chairman Chaffetz, House Committee on Oversight and Government Reform, to Ben Cotton, President and CEO, CyTech Services (Aug. 14, 2015).

[5] Letter from Chairman Jason Chaffetz, House Committee on Oversight and Government Reform, to Ann Barron-DiCamillo, Director, United States Computer Emergency Readiness Team (Aug. 19, 2015); Letter from Chairman Jason Chaffetz and Ranking Member Elijah E.

The Committee also conducted transcribed interviews of CyTech's President and CEO, OPM's Director of Security Operations, one of his support personnel, and two representatives from a different vendor known as Cylance.

Results of Oversight Committee Investigation

The evidence obtained by the Committee indicates that OPM discovered the breach on April 15 or 16, 2015—five or six days before CyTech conducted its product demonstration and its scan of OPM's systems.

As part of our investigation, the Committee obtained a report issued by US-CERT on April 24, 2015, stating that OPM discovered suspicious activity on its networks on April 16, 2015. On that date, OPM "requested that US-CERT conduct digital media analysis of three server images/hard drives." The report states that between April 16 and 20, 2015, "OPM also provided US-CERT with a document containing information on suspicious IP Addresses and domains that may have been involved with the incident."[6]

The Committee also obtained a follow-on report issued by US-CERT on June 9, 2015, stating that on April 15, 2015, OPM discovered an unknown Secure Sockets Layer (SSL) certificate on its network that was being used to communicate with the known malicious domain "opmsecurity.org."[7] The SSL decryption functionality was a component of hardware previously installed by OPM as part of its enhanced security measures.[8]

On February 17, 2016, Committee staff conducted a transcribed interview of Brendan Saulsbury, the OPM contract engineer who actually detected the breaches as part of his work in OPM's Security Operations Center (SOC). When asked how OPM first became aware of the breaches, Mr. Saulsbury had this exchange with Committee staff:

Q: Who specifically within OPM, SOC first detected the malicious activity that was behind the April 2015 cyber intrusion?

A: Myself.

Cummings, House Committee on Oversight and Government Reform, to Stuart McClure, CEO, President, and Founder, Cylance, Inc. (Dec. 3, 2015).

[6] United States Computer Emergency Readiness Team, *Preliminary Digital Media Analysis Report (PDMAR) No. INC 465355* (Apr. 24, 2015).

[7] United States Computer Emergency Readiness Team, *Digital Media Analysis Report (DMAR) No. 465355* (June 9, 2015).

[8] Letter from Jason K. Levine, Director, Congressional, Legislative and Intergovernmental Affairs, Office of Personnel Management, to Chairman Jason Chaffetz and Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform (Sept. 25, 2015).

Q: And was it on April 16, 2015, that you recall detecting the malicious activity?

A: I believe so.

Q: Can you tell us what specifically was the malicious activity you detected on OPM's network on April 16, 2015?

A: We observed malware beaconing out to a command and control server from, at the time, two different servers.[9]

Mr. Saulsbury also explained that the malware he detected was disguised as McAfee antivirus files:

> [W]e were able to determine that the actual malware was a DLL file that was called mcutil.dll. It was basically trying to fly under the radar as if it was a McAfee antivirus executable. The problem is that OPM doesn't use McAfee, so that stood out right there to us that, at that point, I was 100 percent certain that this is malware that is beaconing out.[10]

On February 18, 2016, Committee staff conducted a transcribed interview with Jeff Wagner, OPM's Director of Security Operations, who confirmed Mr. Saulsbury's account. Mr. Wagner had this exchange with Committee staff:

Q: Earlier you mentioned that on April 15, 2015, OPM recognized an unknown certificate attached to a sophisticated attacker. So how did you first come to learn on April 15, 2015, that OPM's network may have been compromised?

A: My first indication was in the discussion of an unknown certificate through email.

...

Q: So we're clear, was it folks working in OPM's Security Operations Center, or SOC, that first detected malicious activity on OPM's network?

A: Yes.

Q: And do you recall any of the names of folks within the SOC who were responsible for first detecting the malicious activity on April 15, 2015?

---

[9] House Committee on Oversight and Government Reform, Transcribed Interview of Brendan Saulsbury, Senior Cybersecurity Engineer, SRA International (Feb. 17, 2016).

[10] *Id.*

> A: Jon Tonda, my lead engineer, would have been doing log investigation, and Brendan Saulsbury would have been the one pulling the forensics logs and doing the reverse engineering.[11]

Mr. Wagner also explained that the tool used to identify the malware was developed by a different contractor, Cylance, that Ms. Seymour had hired previously to enhance OPM's cybersecurity:

> Because of the unique capability of Cylance in mapping binary files as opposed to looking at direct signatures, we knew it was going to be able to immediately find any malware no matter what the indicators were.[12]

On April 17, 2015, Mr. Wagner sent an email to Ms. Seymour reporting that Cylance officials were "coming in to help with the forensics" because it was "their tool that found the Malware."[13] He sent this email five days before CyTech conducted its product demonstration.

On September 30, 2015, Committee staff conducted a transcribed interview of Ben Cotton, the President and CEO of CyTech, who stated: "I had discovered that they were not using McAfee as an anti-virus. But three of these processes were masquerading as McAfee executables."[14]

The evidence obtained by the Committee confirmed that the malware OPM identified was the same malware CyTech identified during its product demonstration a week later. As Mr. Saulsbury, the OPM contract engineer who discovered the breach a week earlier, explained, CyTech "didn't detect anything that we didn't already know about."[15]

Conclusion

The evidence obtained by the Committee confirms that OPM discovered the data breach five or six days before CyTech conducted its product demonstration on April 21, 2015, and that the malware OPM identified was the same malware that was later identified by CyTech. As a result, claims that CyTech was responsible for first detecting the OPM data breaches are inaccurate.

---

[11] House Committee on Oversight and Government Reform, Transcribed Interview of Jeff Wagner, Director of Security Operations, Office of Personnel Management (Feb. 18, 2016).

[12] *Id.*

[13] Email from Jeff Wagner, Director of Security Operations, Office of Personnel Management, to Donna Seymour, Chief Information Officer, Office of Personnel Management (Apr. 17, 2015).

[14] House Committee on Oversight and Government Reform, Transcribed Interview of Ben Cotton, President and CEO, CyTech Services (Sept. 30, 2015).

[15] House Committee on Oversight and Government Reform, Transcribed Interview of Brendan Saulsbury, Senior Cybersecurity Engineer, SRA International (Feb. 17, 2016).

For your information, the majority staff on the Committee asked that I make clear that although I asked Chairman Chaffetz to join this letter, he declined.

If you have any further questions about this matter, please contact Tim Lynch or Jesse Reisman of my staff at (202) 225-5051.

Sincerely,

Elijah E. Cummings
Ranking Member

cc: The Honorable Jason Chaffetz, Chairman