

ORIGINAL

Approved: Christopher J. DiMase
Christopher J. DiMase
Assistant United States Attorney

Before: HONORABLE ANDREW J. PECK
United States Magistrate Judge
Southern District of New York

16 MAG 7004

DOC # _____

UNITED STATES OF AMERICA

- v. -

JONATHAN POWELL,

Defendant.

SEALED COMPLAINT
Violations of
18 U.S.C. §§ 1030(a)(5)(B)
and 1030(c)(4)(A)(i)(I)

COUNTIES OF OFFENSE:
NEW YORK & WESTCHESTER

SOUTHERN DISTRICT OF NEW YORK, ss.:

Christopher Merriman, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE

1. From in or about October 2015, up to and including in or about September 2016, in the Southern District of New York and elsewhere, JONATHAN POWELL, the defendant, intentionally accessed a protected computer without authorization, and as a result of such conduct, recklessly caused damage, causing loss to one and more persons during any one-year period aggregating at least \$5,000 in value, to wit, POWELL accessed without authorization the computer network systems of a university located in New York, New York, and thereby obtained unauthorized access to data and impaired the availability of the email accounts of students and other account holders.

(Title 18, United States Code, Sections
1030(a)(5)(B), 1030(c)(4)(A)(i)(I).)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

2. I have been a Special Agent with the FBI since January 2015. I am currently assigned to a group at the FBI's New York Field Office that is responsible, among other things, for the

investigation of cyber intrusions. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with law enforcement agents and other witnesses, and my examination of reports, records, and other evidence. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

OVERVIEW OF POWELL'S CRIMINAL SCHEME

3. From at least in or about October 2015, up to and including at least in or about September 2016, JONATHAN POWELL, the defendant, obtained unauthorized access to email accounts hosted by at least two United States-based educational institutions, including one which maintains its servers in the Southern District of New York. POWELL obtained unauthorized access to these accounts by accessing password reset utilities maintained by the email servers at the victim institutions, which are designed to allow authorized users to reset forgotten passwords to accounts. POWELL utilized the password reset utilities to change the email account passwords of students and others affiliated with those educational institutions. Once POWELL gained access to the compromised email accounts (the "Compromised Accounts"), he obtained unauthorized access to other password-protected email, social media, and online accounts to which the Compromised Accounts were registered, including, but not limited to, Apple iCloud, Facebook, Google, LinkedIn, and Yahoo! accounts. Specifically, utilizing the Compromised Accounts, POWELL requested password resets for linked accounts hosted by those websites (the "Linked Accounts"), resulting in password reset emails being sent to the Compromised Accounts, which allowed POWELL to change the passwords for the Linked Accounts. POWELL then logged into the Linked Accounts, and gained access to private and confidential content stored in the Linked Accounts.

POWELL'S UNAUTHORIZED ACCESS OF UNIVERSITY EMAIL ACCOUNTS

4. I have spoken with representatives of a university that has its primary campus located in New York, New York ("University-1"), who informed me of the following, in sum and substance and in part:

a. In or about August 2016, several University-1 students reported to University-1 that their University-1 email account passwords had been changed without their permission or authority, resulting in their inability to access their email accounts. University-1 began investigating the unauthorized password resets reported by the students.

b. University-1 maintains a password reset utility for its email accounts (the "Reset Utility"), which at all times relevant to the Complaint, operated as follows:

i. The Reset Utility allowed any University-1 email account user who had forgotten his/her email password to, upon successfully entering the user's email username and the answers to two security questions, reset his/her email account password. The new password would allow the user to re-access his/her University-1 email account.

ii. As part of the process of setting up a University-1 email account, the user was responsible for choosing the two security questions from a discrete list of available security questions. As part of that same process, the user was also responsible for supplying answers to the two security questions.

iii. The Reset Utility was accessible on a public-facing University-1 website.

c. University-1's email servers, which support institutional email access for University-1 students, staff, and alumni, are located in Westchester County, New York.¹ The University-1 server that hosts the Reset Utility is also located in Westchester County, New York.

d. After becoming aware of the above-described access to the Reset Utility, University-1 retained the services

¹ A server is a centralized computer that provides services for other computers connected to it via a network or the Internet. For example, a server that is configured so that its sole task is to support a website is known simply as a "Web server." A server that only stores and processes email is known as an "email server." The computers that use the server's services are sometimes called "clients." When a user accesses email, web pages, or files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network or Internet.

of a forensic consulting firm (the "Consulting Firm") to analyze data related to the suspected network intrusion. To date, University-1 has paid the Consulting Firm in excess of \$5,000 to perform the requested analysis and to assist in remediating network system issues in connection with the intrusion.

5. A fellow FBI Special Agent working together with me on the investigation ("Agent-1") and I have spoken with representatives of the Consulting Firm, who informed us of the following, in sum and substance and in part:

a. An analysis of Reset Utility logs and other data performed by the Consulting Firm revealed that an external IP address (the "IP Address") accessed the Reset Utility approximately 18,640 different times between approximately October 2015 and September 2016.² During that timeframe, those Reset Utility accesses resulted in approximately 18,600 attempted password changes in connection with approximately 2,054 unique University-1 email accounts, and approximately 1,378 successful password changes in connection with approximately 1,035 unique University-1 email accounts (the "Compromised Accounts").³

b. The Consulting Firm also reviewed email logs, containing email header and email subject line data, in connection with the Compromised Accounts, along with other University-1 network logs. That review revealed that after the passwords for the Compromised Accounts were successfully changed using the Reset Utility, the user of the IP Address logged into the Compromised Accounts using the new passwords. In many cases, the user of the IP Address then identified password-protected accounts hosted by other internet service providers

² An Internet Protocol address ("IP address") is a unique numeric address used to identify computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its sources to its destination.

As detailed later in this complaint, the investigation revealed that JONATHAN POWELL, the defendant, was the user of the IP Address at all times relevant to this conduct.

³ The number of successful password changes is greater than the number of compromised University-1 email accounts because certain University-1 email accounts were compromised more than once.

("ISPs"),⁴ including but not limited to Apple iCloud, Facebook, Google, LinkedIn, and Yahoo! (the "Linked Accounts"), to which a Compromised Account was linked as a registration email address.

c. The user of the IP Address next connected to website portals maintained by the Linked Account ISPs. Password reset emails from the Linked Accounts found in the Compromised Accounts demonstrated that the user of the IP Address requested password changes for the Linked Accounts. The user of the IP Address connected to the Linked Account websites again, using web-links provided in the Linked Account password reset emails. In some cases, the Consulting Firm located emails in the Compromised Accounts demonstrating that a Linked Account had been successfully accessed from a new device, following a Linked Account password reset.

d. Thus, utilizing the above-described process, it appears that the user of the IP Address gained unauthorized access not only to the Compromised Accounts, but also to a large number of Linked Accounts, allowing the user of the IP Address to login to the Linked Accounts and obtain access to private and confidential content stored by users in the Linked Accounts.

e. The Consulting Firm identified various Linked Accounts believed to be compromised following the unauthorized access of the Compromised Accounts.

6. The Consulting Firm provided the FBI with a list containing details related to the Compromised Accounts and various Linked Accounts also believed to be compromised, following the unauthorized access of the Compromised Accounts.

7. Agent-1 has spoken to a representative of a second university ("University-2"), located in Pennsylvania, who informed Agent-1 of the following, in sum and substance and in part:

a. In or about September 2016, University-2's publicly-available password reset utility was repeatedly accessed by the IP Address, in a similar fashion to University-1. During that timeframe, the individual connecting to University-2's password reset utility from the IP Address

⁴ An ISP is a commercial service that, depending on the particular ISP, provides Internet connectivity, Internet email accounts, social media accounts, and/or other Internet-connected services to its subscribers.

c. The Device was assigned to JONATHAN POWELL, the defendant, an employee at the Arizona Branch.

d. POWELL has worked for the Company at the Arizona Branch since in or about November 2012. POWELL generally worked regular weekday business hours at the Company.

e. On or about October 3, 2016, as part of a ruse to obtain the Device, a representative of the Company's information technology department sent a message to POWELL, informing POWELL that the Device had been infected with malware, that it would be disabled within the next hour, and that it would be replaced as soon as possible. The Device was subsequently disabled and collected by the Company's information technology department, and replaced with a new device.

10. After becoming aware of the use of the Device to access University-1 email accounts without authorization, the Company retained a private computer forensics firm (the "Forensics Firm") to analyze data obtained from the Device. Based on my review of a report produced by the Forensics Firm in connection with that analysis (and attachments appended to that report), along with a review of the analysis performed by the Consulting Firm retained by University-1, Agent-1 and I learned the following, in sum and substance and in part:

a. A review of the Device's web browser history (the "Browser History"), conducted by the Forensics Firm, demonstrated a repeated cycle of: (1) searching for biographical information about an individual victim; (2) leveraging that information to gain access to the individual victim's email accounts via password reset utilities - for example, questions about the individual's high school mascot and the names of the individual's grandparents; (3) leveraging the compromised email accounts to compromise linked social media accounts; and (4) searching the linked accounts for additional password information, along with images, particularly sexually explicit images.

b. For example, based on the analysis performed by the Consulting Firm, the user of the IP Address accessed the University-1 Reset Utility on or about July 6, 2016, at approximately 4:46 p.m., Mountain Standard Time ("MST"), and successfully changed the password for the University-1 email account of a particular student (the "Student"). Subsequent emails sent from Google to the Student's email account show that the password for the Student's linked Google account was changed shortly thereafter.

c. An excerpt of the Browser History from July 6, 2016, showed, among other things, the following:

i. Initial internet research regarding the Student, occurring between approximately 4:44 p.m. and 4:45 p.m. MST;

ii. Access to the University-1 Reset Utility at approximately 4:45 p.m. MST;

iii. Access to the University-1 email system at approximately 4:46 p.m. MST, representing the intrusion into the Student's email account;

iv. Access to the Student's Google Gmail webmail account, including access to the Gmail password reset functionality, between approximately 4:48 p.m. and 4:51 p.m. MST;

v. Searches within the Student's Gmail account between approximately 4:52 p.m. and 4:59 p.m. MST, including a search of email in the Gmail account labeled "Personal," and the following keyword searches of email and saved Gmail chat history: (1) "jpg OR jpeg OR png";⁶ (2) "password"; (3) "naked"; (4) "cum"; and (5) "horny".

11. I have learned from another member of law enforcement who reviewed the Browser History that, according to the Browser History, the Device accessed student directories and login portals associated with more than 75 other colleges or universities located in various locations across the United States (the "Other Universities"), during the period of July 5, 2016 to October 3, 2016.

12. The Company provided the FBI with the Device, along with a network backup of certain files on the Device created on or about September 30, 2016 (the "Device Backup"), which were analyzed by me, Agent-1, and FBI computer scientists. That analysis revealed the following, in sum and substance and in part:

a. The Device and Device Backup contained a number of documents containing University-1 email account usernames and passwords. The documents also contained credentials - i.e.,

⁶ The filename extensions ".jpg", ".jpeg", and ".png", are filename extensions commonly associated with digital photographs.

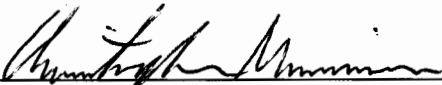
usernames and passwords - for logging into various ISP accounts appearing to belong to the same University-1 email account users. For example, the Device contained a file which listed a number of University-1 email account usernames, along with login credentials for what appear to be linked email accounts hosted by other ISPs, including Google and Yahoo! Based on the forensic analysis conducted by the Consulting Firm retained by University-1, the passwords for more than 10 of the University-1 email account usernames listed in the file on the Device were compromised by the user of the IP Address, utilizing the Reset Utility.

b. The Device Backup contained a spreadsheet listing members of a University-1 sorority chapter, along with usernames and passwords for logging into the sorority's national website. The University-1 email accounts of least four of those sorority members were among the 1,035 Compromised Accounts reported by University-1.

c. The Device Backup contained a document with a filename that included the name of University-2, which appears to contain Facebook profile pages and other information relating to University-2 email account users.

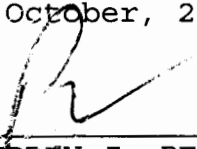
d. The Device Backup contains several documents with filenames that refer to certain of the Other Universities, whose login portals appear to have been accessed by the device, as described above in paragraph 10(d). Those documents contain what appear to be login credentials for a variety of password-protected accounts linked to Other University email accounts.

WHEREFORE, I respectfully request that an arrest warrant be issued for JONATHAN POWELL, the defendant, and that he be arrested and imprisoned or bailed, as the case may be.



Christopher Merriman
Special Agent
Federal Bureau of Investigation

Sworn to before me this
31st day of October, 2016



HONORABLE ANDREW J. PECK
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK