UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	
	:	**CRIMINAL COMPLAINT**
v.	:	
	:	Mag. No. 11-6084
JASON CORNISH,	:	
	:	Hon. Michael A. Shipp
Defendant	:	
	:	UNDER SEAL

I, Russell A. Ficara, being duly sworn, state the following is true and correct to the best of my knowledge and belief. On or about February 3, 2011, in the District of New Jersey and elsewhere, defendant Jason Cornish did:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

Russell A. Ficara, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,
June 30, 2011, in Essex County, New Jersey

HONORABLE MICHAEL A. SHIPP
UNITED STATES MAGISTRATE JUDGE

Signature of Judicial Officer

ATTACHMENT A

knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, that is, a computer used in interstate commerce and communication, and cause loss to one or more persons during any 1-year period aggregating at least $5,000 in value

In violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B)(i).

ATTACHMENT B

I, Russell A. Ficara, a Special Agent of the Federal Bureau of Investigation, have knowledge of the following facts based upon evidence collected during the investigation and discussions with witnesses and other law enforcement agents. Since this affidavit is submitted for the purpose of establishing probable cause to support the issuance of a complaint and arrest warrant, I have not included each and every fact known by the government concerning this investigation. Statements attributed to individuals are provided in substance and in part.

BACKGROUND

1. At all times relevant to the Complaint:

   a. Defendant Jason Cornish ("Cornish") resided in or near Smyrna, Georgia. Cornish used the e-mail account caveman****@gmail.com ("the Caveman Account").

   b. Shionogi Inc. ("Shionogi") was a United States subsidiary of a Japanese pharmaceutical company with operations located in New Jersey and Georgia.

   c. Between at least as early as 2009 and in or about July 2010, Cornish worked for Shionogi as an information technology employee. He reported to B.N., a close friend whom Cornish had known for approximately 15 years.

   d. Cornish resigned from Shionogi in or about July 2010 after a dispute with a senior manager. At B.N.'s suggestion, however, Shionogi continued to employ Cornish as a paid consultant because of Cornish's knowledge of Shionogi's computer network.

   e. Cornish stopped working for Shionogi as a paid consultant in or about September 2010. At no time after October 1, 2010 was Cornish permitted to access Shionogi's computer network.

   f. In late September 2010, Shionogi announced layoffs that would affect B.N. On or about October 1, 2010, B.N. refused to return certain network passwords to Shionogi officials, which led the company to suspend and later fire him.

THE FEBRUARY 3, 2011 ATTACK

2. At approximately 6:05 a.m. (EST) on or about February 3, 2011, Cornish gained unauthorized access to Shionogi's computer network ("the February 3 Attack").

3. During the February 3 Attack, Cornish used a Shionogi user account named CVAULT to access a Shionogi server named SPVC01 ("the SPVC01 Server").

4. Once he accessed the SPVC01 Server, Cornish took control of vSphere, a piece of software that he had secretly installed on the SPVC01 Server several weeks earlier.

5. Cornish then used the vSphere program to delete, one by one, the contents of each of 15 "virtual hosts" on Shionogi's computer network. These 15 virtual hosts housed the equivalent of 88 different computer servers.[1] Cornish used his familiarity with Shionogi's network to identify each of these virtual hosts by name or by its corresponding Internet Protocol ("IP") address.

6. The deleted servers housed most of Shionogi's American computer infrastructure, including the company's e-mail and Blackberry servers, its order tracking system, and its financial management software. The February 3 Attack effectively froze Shionogi's operations for a number of days, leaving company employees unable to ship product, to cut checks, or even to communicate via email.

7. Shionogi sustained at least $300,000 in losses responding to the February 3 Attack, conducting damage assessments, and restoring the company's network to its condition prior to the attack.

THE INVESTIGATION

8. In the wake of the February 3 Attack, the FBI examined Shionogi's remote access firewall logs ("the Firewall Logs").[2] The Firewall Logs, which survived the February 3 Attack, recorded, among other things: (1) the date and time that any outside computer gained access to Shionogi's network; (2) the date and time that any outside computer unsuccessfully attempted to gain access to Shionogi's network; (3) the Shionogi user account accessed; and (4) the Internet Protocol ("IP") address from which the access or attempted access to Shionogi's network originated.

9. The FBI also reviewed event logs and records of activity on the SPVC01 Server, the particular Shionogi computer that appeared to be a launching pad for the February 3 Attack.

10. According to the Firewall Logs, access to the SPVC01 Server immediately prior

---

[1] A "virtual host" is a method by which one physical computer can be subdivided into several "virtual" computers, giving the one computer the capability and functionality of many computers. Virtual hosts eliminate the need to have separate computers for different functions within a company's computer infrastructure.

[2] A "firewall" is a security feature that controls access to a computer or computer network.

to the February 3 Attack originated from the IP address 64.134.184.162, which the FBI's public source research revealed to belong to AT&T Internet Services.

11. AT&T provided the FBI with records indicating that on or about February 3, 2011, the IP address 64.134.184.162 was assigned to a free wireless Internet connection located at a McDonald's restaurant located in Smyrna, Georgia ("the Smyrna McDonald's"). (The IP address 64.134.184.162 will hereinafter be referred to as "the McDonald's IP Address").

12. According to McDonald's business records, a Visa credit card number ending in 8921 ("the 8921 Visa") was used at the Smyrna McDonald's to make an approximately $4.96 purchase on February 3, 2011 at 6:00:46 a.m. (EST) — approximately 5 minutes before the attack on Shionogi from the McDonald's IP Address.

13. According to documents provided by Google, Inc., a Visa credit card number ending in 8921 was provided to it in connection with Cornish's Caveman Address.

14. According to documents provided by Bank of America, Jason Cornish is an accountholder for a Bank of America debit card that was used on February 3, 2011 at the Smyrna McDonald's to make an approximately $4.96 purchase.

Other Unauthorized Access to the SPVC01 Server

15. Further review of the Firewall Logs and SPVC01 Server records revealed that on or about January 13, 2011, defendant Cornish accessed the CVAULT account and used that access to install vSphere — the software program believed to have been used to delete Shionogi's virtual hosts — on the SPVC01 Server ("the January 13 Access"). Shionogi officials advised that there was no legitimate business reason for vSphere to be installed or running on the SPVC01 Server.

16. According to the Firewall Logs, the January 13 Access originated from the IP Address 68.184.94.214, which FBI public source research revealed to belong to Charter Communications, an Internet Service Provider in the Atlanta area ("Charter").

17. On or about February 22, 2011, Charter advised the FBI that at the time of the January 13 Access, the IP Address 68.184.94.214 was assigned to Jason Cornish, its named subscriber at Cornish's Smyrna, Georgia residence (hereinafter, "the Cornish IP Address").

18. Further review of the Firewall Logs revealed that between on or about October 1, 2010 and on or about January 19, 2011, the Cornish IP Address was used approximately twenty (20) times to gain access to Shionogi's network through the CVAULT account, the same account used for the January 13 Access and the February 3 Attack.

19. Similarly, between on or about October 1, 2010 and on or about October 14, 2010, the Cornish IP Address was also used unsuccessfully to attempt to gain access to various user

accounts at Shionogi, including accounts assigned to the company's Blackberry server, Cornish's user account, and other administrative accounts of which Cornish would have been aware as an information technology employee.