AO 91 (Rev. 11/11) Criminal Complaint AUSA William E. Ridgway (312) 469-6233

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA	
v.	CASE NUMBER: Hon. Daniel G. Martin
TIMOTHY JUSTIN FRENCH, also known as "Orbit," "@Orbit_g1rl," "crysis," "rootcrysis," and "c0rps3"	**UNDER SEAL**

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning no later than in or around July 2013, and continuing until at least in or about May 2014, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant, TIMOTHY JUSTIN FRENCH, also known as "Orbit," "@Orbit_g1rl," "crysis," "rootcrysis," and "c0rps3," violated:

Code Section	*Offense Description*
Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), and 1030(c)(4)(B)(i)	Conspiring to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization to a protected computer, which offense caused a loss aggregating at least $5,000 in value to one or more persons during a one-year period

This criminal complaint is based upon these facts:

_X_ Continued on the attached sheet.

Patrick M. Geahan
Special Agent, Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: June 3, 2014

Judge's signature

City and state: Chicago, Illinois

Daniel G. Martin, U.S. Magistrate Judge
Printed name and Title

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

Introduction and Agent Background

I, Patrick M. Geahan, being duly sworn, state as follows:

1. I am a Special Agent of the Federal Bureau of Investigation and am assigned to the Chicago Field Office. I have been employed as a Special Agent with the FBI since 2004. As a Special Agent, I am charged with investigating possible violations of federal criminal law, including computer crimes, in violation of 18 U.S.C. § 1030 (the Computer Fraud and Abuse Act). I have received specialized training in those areas. In particular, I hold a Bachelor of Science degree in Computer Science from Michigan Technological University, as well as a Certified Information Systems Security Professional certification from the International Information Systems Security Certification Consortium. I have attended multiple FBI and private sector training sessions and conferences on computer intrusion, network analysis, and electronic evidence recovery.

2. This affidavit is submitted in support of a criminal complaint alleging that Timothy Justin French, also known as "Orbit," "@Orbit_g1rl," "crysis," "rootcrysis," and "c0rps3," and others have conspired to knowingly

cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer, which offense caused a loss aggregating at least $5,000 in value to one or more persons during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), and 1030(c)(4)(B)(i). Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the defendant committed the offense alleged in the complaint.

3. This affidavit is based on my personal knowledge, information provided to me by other law enforcement agents and from other persons with knowledge regarding relevant facts. Moreover, throughout this affidavit in footnotes and in brackets I provide definitions and explanations for certain terms and phrases. Those definitions are based on my training and experience in the area of computers and my experience investigating the unauthorized access of computer systems, also known as computer hacking.

Definitions

4. I know from my training and experience that the following definitions apply to the activity discussed in this affidavit:

a. *IP Address*: The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic to and from that computer may be properly directed from its source to its destination.

b. *Server*: A server is a computer that provides services to other computers. Examples include web servers which provide content to web browsers and e-mail servers which act as a post office to send and receive e-mail messages.

c. *VPN*: A Virtual Private Network ("VPN") is an encrypted connection between two or more computer resources over a public computer network, such as the Internet, which enables access to a shared network between those resources. A common example is an individual who purchases access to a VPN service from a VPN service provider. A VPN service provider may also be a server hosting provider or may be a customer of a server hosting provider that is using servers hosted by the server hosting provider for the VPN service. The individual would connect from the individual's computer to the VPN service at the VPN service provider over the Internet. Once connected to the VPN, the individual's subsequent computer network communications, including access to websites, would be routed through the

VPN connection from the individual's computer to the VPN service at the VPN service provider, and then from the VPN service provider on to the destination website. The response from the destination website is sent back to the VPN service at the VPN service provider and then finally routed via the VPN connection to the individual's computer. In this scenario, the IP address which accesses the third party website is actually associated with the VPN service and is not the actual IP address of the individual's computer.

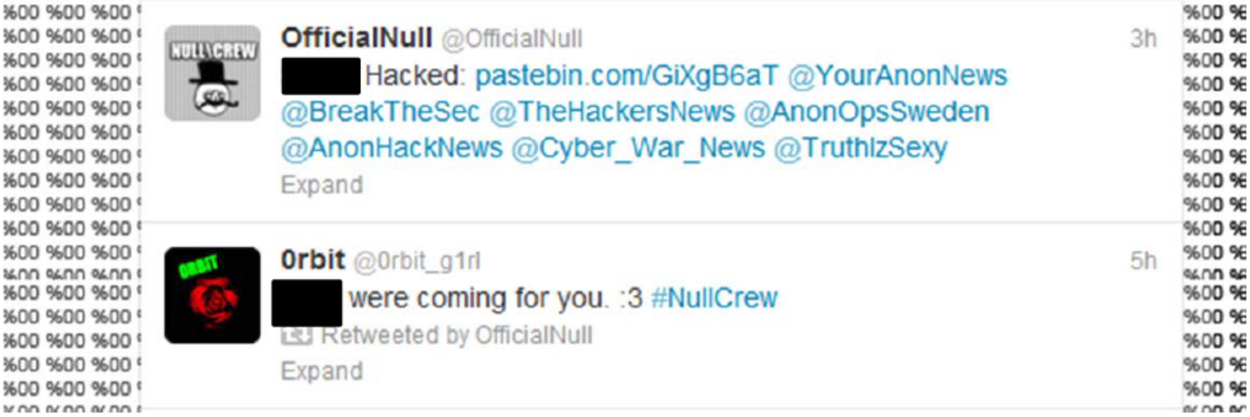
Overview

5. The FBI has been investigating "NullCrew," a collection of individuals who have claimed responsibility for many high-profile computer attacks against corporations, educational institutions, and government agencies. Individuals associated with NullCrew include "Orbit," whom the FBI has identified as Timothy Justin French (who also uses the aliases "@Orbit_g1rl," "crysis," "rootcrysis," and "c0rps3"), and "Null," whom the FBI has identified as Individual A.

6. One of the ways that NullCrew publicizes its attacks is through the online social networking and microblogging service Twitter, including via the accounts @OfficialNull and @NullCrew_FTS. Since mid-2012, NullCrew has announced dozens of attacks against various victims. For example:

a. On or about July 13, 2012, NullCrew, through the account @OfficialNull, reported hacking websites of two organizations. That announcement included a link to a Pastebin[1] post containing over a thousand usernames and passwords, purportedly for individuals associated with those organizations. The announcements stated: "We are not LulzSec, UGNazi, TeaMp0isoN, or even Anonymous.[2] This is the start of something big, and it's only just the beginning."

b. On or about September 2, 2012, NullCrew, through the account @OfficialNull, claimed it seized control of eight computer servers belonging to a large company. The Pastebin release reflected a list of hundreds of usernames and passwords, which were reportedly taken from the company's computer servers. Approximately two hours before this release, the account @Orbit_g1rl tweeted, "[the name of the company] were coming for you. :3," as reflected in this screen capture:



OfficialNull @OfficialNull 3h
[redacted] Hacked: pastebin.com/GiXgB6aT @YourAnonNews @BreakTheSec @TheHackersNews @AnonOpsSweden @AnonHackNews @Cyber_War_News @TruthIzSexy
Expand

Orbit @0rbit_g1rl 5h
[redacted] were coming for you. :3 #NullCrew
Retweeted by OfficialNull
Expand

[1] "Pastebin" is an Internet website that allows any party to upload text files for others to view.

[2] I understand these names to be references to other groups engaged in hacking.

c. On or about November 5, 2012, NullCrew, through the account @OfficialNull, announced an attack on a foreign government's ministry of defense, releasing over 3,000 usernames, email addresses, and passwords purportedly belonging to members of the ministry of defense.

7. As part of the investigation, the FBI has been working with a confidential witness ("CW"),[3] who was invited to join online chats with members of NullCrew. During those chats, NullCrew members discussed past, present, and future computer hacks; shared current computer vulnerabilities and planned targets; and discussed releases of their victim's information. These chats occurred through Skype, Twitter, and CryptoCat.[4]

8. On many occasions during these chats, NullCrew members discussed tactics for avoiding law enforcement. One of those tactics was to launch its computer attacks through an intermediary computer server, either a VPN or a compromised server, *i.e.*, a computer server to which an outsider has obtained unauthorized access. As further described below, during part of the investigation, members of NullCrew used a computer server in Chicago from which to launch computer attacks (the "Chicago computer server"). As

[3] This CW has experience in information security and has assisted with the investigation primarily in an effort to help the FBI.

[4] CryptoCat is communications software program that allows for real-time online chat. CryptoCat advertises itself as encrypted and unreadable by third parties. A user creates a new username each time the user logs into the program, which exists only for the particular session.

further described below, the FBI has obtained records from the Chicago computer server relating to NullCrew's hacking activities.

9. For reasons discussed in ¶¶32-39, the investigation has identified Timothy Justin French as "Orbit," who also operates under the usernames "@Orbit_g1rl," "crysis," "rootcrysis," and "c0rps3."[5]

Summary of the Evidence

Cyber Attack Against University A

10. On or about July 19, 2013, "0rbit" chatted with the CW via Skype about an attack on University A, a large public university. During that conversation, 0rbit wrote: "Working on rooting[6] [University A].edu." When the CW offered assistance, 0rbit replied, "Yeah, I already got a shell[7] up; I'm just rooting it" and sent the CW a link to a file called "gny.php" on a server at ifa.[University A].edu.

11. On or about July 19, 2013, FBI communicated with a system administrator from University A, who reported that one of its computer servers had been compromised, meaning someone had gained unauthorized

[5] As reflected in this affidavit, French sometimes spells the username name "Orbit" with a "0," *i.e.*, "0rbit."

[6] "Rooting" describes an attack on a computer server that is intended to result in full administrative, or "root" privileges. Such privileges allow the user to access all commands and files.

[7] A "shell" is command-line level access to a computer, meaning an individual is given direct access to run commands on the system. When used as a verb in this context, "to shell" means to get the computer to give you a shell through unauthorized means.

access to the server. That system administrator further recovered the "gny.php" file. The administrator reviewed the file, determined that it had not been installed by University A, and advised that it was likely malicious software, *i.e.*, software that could be used to obtain unauthorized access to University A's computer systems. The FBI received log files[8] from University A for the compromised computer server. An analysis of the log files showed multiple connections to the program gny.php between June 18, 2013, to June 21, 2013, consistent with the chat described above. During that time period, the attacker appeared to view different directories (*i.e.*, folders on the server) and attempted to run commands on the local database.

Cyber Attack Against Company A

12. On or about January 28, 2014, the CW engaged in an online chat with "crisis" via CryptoCat regarding Company A, a large Canadian telecommunications company. During this chat, crysis wrote "We've also been working on that [Company A] server again.. but, the problem is: If theres as much data as Null says, in that server.. then, how I've been doing it manually would take forever." Later, crysis wrote, "I tried running [Company A

[8] A log file (or simply log) for a computer server is a record of activity on that server, such as requests from information, including the source IP address, date and time, and information requested.

website] through SQLMap,[9] for quicker rates; it kept erroring me, we couldn't figure out why.. especially when I was using all flags correctly, with the right parameters."

13. On or about February 1, 2014, NullCrew, through the Twitter account @NullCrew_FTS, announced a computer attack on Company A. In particular, the message stated: "Whelp, let's start things off properly - nullcrew.org/[Company A].txt . . . hacked by #NullCrew." On or about February 2, 2014, the Twitter account provided a link to a post on Cryptobin.[10] I have reviewed the documents that were linked in these messages and they appear to be copies of database tables and credentials for one of Company A's computer servers. The materials on Cryptobin included a section marked "tblCredentials," containing a series of 12,000 username and password pairs, which appeared to be a list of Company A customer credentials.

14. On or about February 2, 2014, the CW chatted with "rootcrysis" via CryptoCat. The CW praised rootcrysis about the Company A data breach, to which rootcrysis replied "Yup LOL. Gained ALOTTTTTTT of attention.

[9] "SQLMap" is a program used to probe SQL database servers for vulnerabilities. "SQL," which stands for "Structured Query Language," refers to a special-purpose programming language designed for managing data held in certain types of databases.

[10] "Cryptobin" is an Internet website that allows any party to upload text files for others to view.

I've done like four interviews." As rootcrysis continued, "I released it like two days ago, it would've been released sooner if manual wasn't a bitch and had to wait for you and null to help me with the sqlmap response." The CW asked, "Why did we even target [Company A] to being with?" In response, rootcrysis wrote, "Good question, Null just gave me the exploit since he lost the data; told me to go to town, that it was for NC [NullCrew]."

15. On or about February 2, 2014, a blog that provides news online about data breaches (databreaches.net) posted a story about the Company A data breach. As part of that story, a purported NullCrew member was interviewed and provided a screenshot of a chat that the purported member had with a Company A employee. The screenshot showed a conversation in which the employee of Company A was warned of an attack against the company's server. During the February 2, 2014 chat referenced above, the CW inquired about this interview, asking if "Null" did "the screen shot." Rootcrysis responded, "Nah, I did rofl [rolling on the floor laughing]. I got on chat after ripping [copying] data, told them [Company A], and screened [took a screen shot of] their response."

16. I have reviewed records from the Chicago computer server referenced above. According to those records, on or about January 26, 2014, a folder was created titled "protectionmanagement.[Company A]." This folder contained a log file indicating that the program "SQLMap" was run against a

SQL installation on protectionmanagement.[Company A]. The log file indicated that SQLMap located five separate SQL injection points.[11] These records further indicate that multiple executions of the SQLMap program were made against protectionmanagement.[Company A], beginning on or about January 22, 2014. The Chicago computer server also contained a set of data from a database that appears to be associated with Company A, which is nearly identical to the usernames and passwords released on February 1, 2014.

Cyber Attack Against University B

17. On or about January 30, 2014, during an online chat with the CW via CryptoCat, crysis discussed University B, a large public university, and asked "have you taken a look at the system() backdoor[12] on [University B]?" The CW asked crysis for further information; crysis provided the CW with a link and instructions about how to access the vulnerability. As crysis explained, "I've been looking around in it for a while, theres some interesting

[11] "SQL Injection" or "sqli" refers to an attack launched on a database server in which a user attempts to send SQL commands in an area in which they are not normally allowed.

[12] "Backdoor" refers to gaining access to a system through a normal, but hidden, authentication mechanism. Unlike a vulnerability (or "vuln"), which is an error, a backdoor is an intentional entry which gets misused.

shit." The CW was also told by crysis to try running the command "cmd=whoami"[13] on the system.

18. On or about April 15, 2014, an FBI undercover employee ("UCE"), using the CW's username with the CW's permission, had online communications with rootcrysis. During those communications, rootcrysis provided a copy of information NullCrew planned to release on April 20, 2014. In this document, data from University B was presented for release.

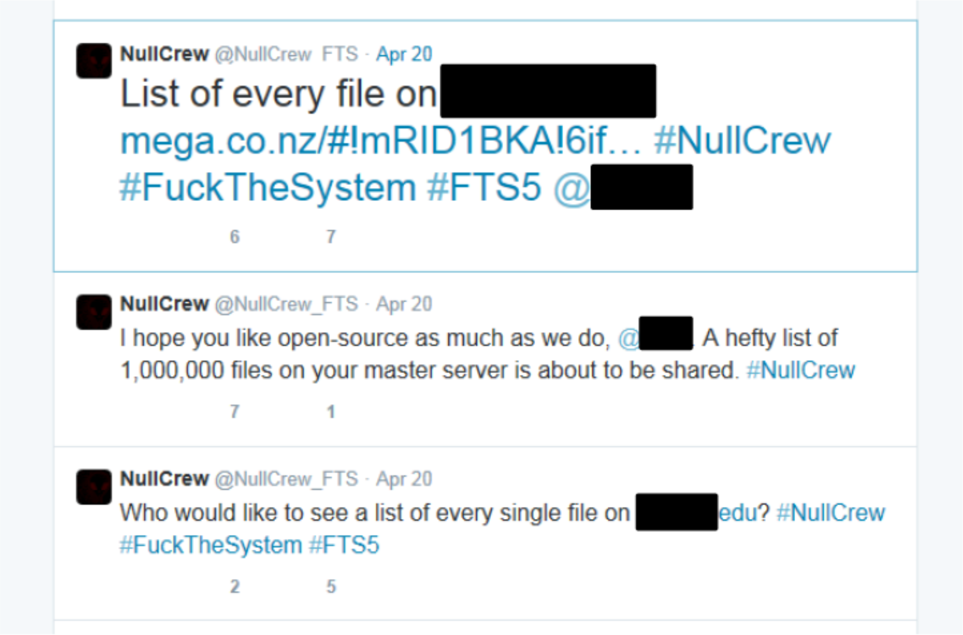
19. On or about April 20, 2014, the UCE engaged in an online chat with rootcrysis and Individual A. During the chat, Individual A stated he had a "code-execution vuln[14]" and provided the link, which is associated with the University B systems. Individual A then provided rootcrysis a command that could be used to find all files in existence on a server in a specified directory. Individual A further requested that the results be uploaded to a place where it could be accessed. In response, rootcrysis wrote, "Doing so now. Taking a while lol." Later in the conversation, rootcrysis stated, "Welcome back, and I'mma up [upload] that file now. I'll put it on mega and send it to you." Individual A asked about the size of the file, to which rootcrysis responded,

[13] A successful execution of this command would indicate that the user has the ability to run system commands on the server.

[14] "Vuln," short for "vulnerabilities," refers to errors in computer software that allow an attacker to gain unauthorized access.

"It's 76 mb [megabytes] lol." Rootcrysis then provided two links to files at mega.co.nz.[15]

20. On or about April 20, 2014, NullCrew, through its Twitter account @NullCrew_FTS, announced the hacking of a series of educational institutions and companies, including University B and Company B. This announcement included a link to a file on mega.co.nz titled "FTS5-DATA.RAR." Based on my review of this file, it appears to contain tens of thousands of emails, several SQL databases, and password files, among other items relating to University B. In reference to University B, the @NullCrew_FTS account stated:



NullCrew @NullCrew_FTS · Apr 20
List of every file on [redacted]
mega.co.nz/#!mRID1BKA!6if… #NullCrew
#FuckTheSystem #FTS5 @[redacted]
6 7

NullCrew @NullCrew_FTS · Apr 20
I hope you like open-source as much as we do, @[redacted] A hefty list of 1,000,000 files on your master server is about to be shared. #NullCrew
7 1

NullCrew @NullCrew_FTS · Apr 20
Who would like to see a list of every single file on [redacted]edu? #NullCrew #FuckTheSystem #FTS5
2 5

21. As part of this investigation, the FBI received log files from the University B, which I have reviewed. Those logs reflect access from on or

[15] This website is a New Zealand-based cloud storage and file hosting service.

about January 30, 2014, to on or about February 2, 2014, from an IP address belonging to the Chicago computer server. Those logs further reflect that on January 30, 2014, an individual attempted twice to run the same command referenced by "crisis" on January 30, 2014, in the chat with the CW described above in ¶17. That command was executed from the IP address 24.151.249.146.

22. I have reviewed files and logs stored on the Chicago computer server. Those files reflect that on or about February 5, 2014, a user operating under the name "Orbit" created a directory entitled "[University B]" on the Chicago computer server. Within this directory were several files detailing configurations and directories on server computers in the University B domain. On April 20, 2014, at approximately 1:39 pm, a file named "[University B]_files.txt" was created, in the home directory for Orbit's account. That file, based on my review, is substantially the same as the file posted to mega.co.nz, referenced above. A review of the logs of the Chicago computer server during that time period reflects that Orbit logged into the server from IP address 24.151.249.146.

Cyber Attack Against Company B

23. On or about April 15, 2014, the UCE had an online chat with rootcrysis via CryptoCat. During that discussion, rootcrysis provided the UCE a link to information NullCrew planned to release on April 20, 2014.

That release contained hardware data, WordPress configuration data, and user information for Company B, a company based in California.

24. FBI later interviewed an IT employee at Company B, who confirmed that there was unauthorized access to the company's computer servers. The IT employee also provided logs for Company B. Those logs reflected that, between January 17, 2014, and January 21, 2014, the IP address 24.151.249.146 accessed Company B's servers approximately 209 times, approximately 123 of which were to a file entitled "test.php." Based on my analysis of the usage of this file, it appears to be a malicious PHP[16] file that allows an attacker shell-type access to the system.

25. During an online chat with the UCE on or about April 20, 2014, rootcrysis stated "I'mma laugh when we've caused that web-developer of [Company B] to lose his job LOL."

26. A review of the Chicago computer server reflects that on or about February 5, 2014, a folder entitled "Targets/[Company B]" was created in Orbit's home directory on the Chicago computer server. In that folder was a file entitled "Exfil.txt,"[17] modified on or about January 21, 2014. That file contained the information that was released by NullCrew on or about April

[16] PHP is a programming language, commonly used to provide functionality on websites.

[17] "Exfil" or "exfiltration" is used in data security to refer to "data theft" or information acquired through the unauthorized access of a computer system or network.

20, 2014. An analysis of login records for the Chicago computer server for that day show that user "Orbit" logged in on multiple occasions from the IP address 24.151.249.146.

Cyber Attack Against Company C

27. On or about February 5, 2014, rootcrysis chatted with the CW via CryptoCat about Company C, a large mass media communications company. During the chat, rootcrysis provided a URL[18] to a server at Company C, stating that it was the "Current target" and that the vulnerability was "LFI[19] in Zimbra."[20] The CW asked what the goal was and rootcrysis responded, "Pretty much, get anything interesting we can; goal is to get a shell [*i.e.*, shell access]." Later, rootcrysis and the CW discussed the fact that they had exploited the LFI vulnerability and, as a result, had obtained data from the server that included credentials for other system services. According to rootcrysis, he had uploaded the material onto a computer server (later identified as the Chicago computer server). Also, during the chat, rootcrysis provided the CW a certain command to run, which was designed to exploit a second vulnerability in Zimbra.

[18] A "URL," or uniform resource locator, is a specific character string that constitutes a reference to a resource, which is commonly used for webpages.

[19] "LFI," or local file inclusion, refers to a vulnerability in webservers.

[20] Zimbra is a collaboration program, installed in a client-server model, intended to allow people to share data.

28. On or about February 5, 2014, NullCrew, through its Twitter account @NullCrew_FTS, announced an attack on Company C, and posted a link to a document located on Pastebin. The document, which I have reviewed, listed thirty-three Company C servers, and stated that they all run a software package called "Zimbra." One of the servers was the same as the one mentioned by rootcrysis in the chat with the CW and the vulnerable URL was the same as the one rootcrysis provided to the CW, as referenced above. The document also states that Zimbra is vulnerable to a technique known as LFI, and posts several critical files from the server as proof. The files include credentials for several system services.

29. A review of records on the Chicago server shows logins to user "Orbit" on February 5, 2014, from IP address 24.151.249.146. During these logins, a directory entitled "Targets/[Company C]" was created in the home directory for user Orbit. This directory contained a file named "vuln.txt," which contained the same URL sent to CW above. Additionally, a file named "subdomains.txt" contained a list of Company C servers, which included the list of vulnerable servers from the release. Finally, a series of files in the "Exfil" subdirectory contained username and password combinations that were duplicated in the release.

30. A review of records on the Chicago server for user Orbit shows that on or about February 5, 2014, the user ran two commands that are

substantially similar to the ones discussed in the chat above. These commands targeted the same server discussed in the chat above.

31. Based on my training and experience, and based on my knowledge of the investigation and conversations with employees of the victim companies and universities in this case, I believe that the victims in incurred costs that, in aggregate, exceed $5,000, including costs responding to the computer intrusion, conducting a damage assessment, and restoring the computer systems.

Identification of "Orbit," "Orbit_g1rl," "Rootcrysis," and "Crysis" as Timothy Justin French

32. During group chats on Skype among NullCrew members in early 2013, which the CW provided to the FBI, another NullCrew member stated that "Orbit" also uses the nickname "c0rps3," which Orbit confirmed in that chat.

33. During a group Skype chat on or about January 29, 2013, NullCrew members were discussing a "dox"[21] that was posted about 0rbit. 0rbit responded stating, "my name is Timothy, I've told everyone that." Later in that same chat, 0rbit stated, "My location in TN is different then what they thought" and also "Timothy Story = Not even a real name, I set that up."

[21] "Dox" or "doxxing" refers to the acquisition and release of personal information about an individual. These terms are often used in reference to identifying someone previously only know by a pseudonym.

34. On or about December 22, 2011, a search warrant was executed by FBI agents at a residence in Talbott, Tennessee, in relation to an attack on computers at a community college.[22] Agents believed that Timothy Justin French was responsible for the attack. Following the search, French was located and interviewed at a residence in Morristown, Tennessee, owned by one of French's family members ("the Morristown address"). That is the residence which is listed on French's driver's license, as of on or about March 25, 2014. During the interview, French admitted using the online nickname "c0rps3." French also stated that he used the name "Timothy Story" on the Internet.

35. During a Skype chat with the CW on or about February 8, 2013, 0rbit wrote "four hours ago I was in a bad car wreck." When the CW asked what 0rbit was driving, 0rbit responded "It's a 1996 camaro, automatic; v6 305 engine." A search of public records reflects under French's name a vehicle accident on February 7, 2013, involving a 1996 Chevrolet Camaro/RS. According to driving records, French was cited for "Failure to Yield Right of Way" and "Violation of Seat Belt Law as Driver" on February 7, 2013.

[22] The residence in Talbott, Tennessee, is owned by French's father.

36. During multiple conversations via Skype, 0rbit used the Skype username “orbit.girl.”[23] Records from Skype reflect that username orbit.girl was registered on October 23, 2012, from the IP address 75.136.47.7. Records from Charter Communications reflect that this IP address was assigned to an individual at the Morristown address between June 8, 2012, and October 24, 2012.

37. On or about February 3, 2014, the CW participated in a chat with “rootcrysis” via CryptoCat. During that chat, rootcrysis provided a password “to the nc [NullCrew] twitter.” The CW was able to use that password to log into the Twitter account @NullCrew_FTS. Records from Twitter regarding the account @NullCrew_FTS reflect that the IP address 24.151.249.146 logged into this account between February 3, 2014, and February 5, 2014. Records from Comcast reflect that the IP address was assigned to the Morristown address during that time period.

38. During each of the attacks involving the Chicago computer server, described above, a user was logged into the Chicago computer server under the name “Orbit” from the IP address 24.151.249.146. Records obtained from Charter Communications reflect that, during this time period, the IP address 24.151.249.146 was assigned to the Morristown address.

[23] Though the account username was “orbit.girl,” during the investigation, the “display name” to the CW and UCE was “0rbit.”

39. As described above, on multiple occasions, an individual accessed victim servers directly from IP addresses that resolve to the Morristown address or accessed the Chicago computer server in connection with this activity from an IP address that resolves to the Morristown address. For example:

a. Records obtained from University A regarding the attack on their servers (described above in ¶¶10-11) show connections to the file gny.php by IP address 75.136.44.71 on multiple occasions between June 18, 2013, and June 21, 2013. Additionally, multiple accesses were seen from IP address 24.151.251.118 on July 19, 2013, at or around the same time that "0rbit" was discussing an attack with CW. Records obtained from Charter Communications show that 75.136.44.71 and 24.151.251.118 were both assigned to the Morristown address during their respective time periods.

b. Records obtained from University B regarding the attack on their servers (described above in ¶¶17-22) show accesses to the vulnerable link described in ¶19 from IP address 24.151.249.146 on January 30, 2014. Additionally, those records show access to the posted vulnerable link, and another vulnerable link, from the Chicago computer server on January 30, 2014, and February 2, 2014. During this time, user "Orbit" was logged into the Chicago server from IP address 24.151.249.146. Additionally, as referenced above, University B files were uploaded to the Chicago server on

April 20, 2014, also from IP address 24.151.249.146. Records obtained from Charter Communications show that IP address 24.151.249.146 was assigned to the Morristown address during that entire time period.

c. Records obtained from Company B regarding the attack on its servers (described in ¶¶23-26) show 209 accesses to a file called "test.php," which Company B deemed malicious. These accesses, from IP address 24.151.249.146, all occurred between January 17, 2014, and January 21, 2014. Additionally, on or about February 5, 2014, a file was created on the Chicago computer server, containing Company B information. During the creation of this file, user "Orbit" was logged in from IP address 24.151.249.146. Records obtained from Charter Communications show that IP address 24.151.249.146 was assigned to the Morristown address at all times during that period.

Conclusion

40. Based on the above information, I respectfully submit that there is probable cause that beginning no later than in or around July 2013, and continuing until at least in or about May 2014, Timothy Justin French and others have conspired to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer, which offense caused a loss aggregating at least $5,000 in value to one or more persons during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), and 1030(c)(4)(B)(i).

FURTHER AFFIANT SAYETH NOT.

____
Patrick M. Geahan
Special Agent, FBI

SUBSCRIBED AND SWORN to before me on June 3, 2014.

____
Daniel G. Martin
United States Magistrate Judge