

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

FILED

DEC 8 2015

Judge Gary Feinerman
United States District Court

UNITED STATES OF AMERICA)	
)	No. 14 CR 318
v.)	
)	Honorable Gary Feinerman
TIMOTHY JUSTEN FRENCH)	

PLEA DECLARATION

The defendant, TIMOTHY JUSTEN FRENCH, after extensive consultation with his attorney, CANDACE R. JACKSON of the Federal Defender Program, acknowledges and states the following:

1. The indictment in this case charges Timothy Justen French with conspiracy to commit an offense against the United States (the offense of intentionally damaging a protected computer without authorization, which violates Title 18, United States Code, Section 1030(a)(5)(A)), in violation of Title 18, United States Code, Section 371 (Count One); conspiracy to intentionally damage a protected computer without authorization, in violation of Title 18, United States Code, Section 1030(b) (Count Two); and intentionally damaging a protected computer without authorization, in violation of Title 18, United States Code, Section 1030(a)(5)(A) (Count Three).

2. Mr. French has read the charges against him contained in the indictment, and those charges have been fully explained to him by his attorney.

3. Mr. French fully understands the nature and elements of the crimes with which he has been charged. Specifically, he understands the elements are as follows:

Conspiracy (Count One) – 18 U.S.C. § 371

(a) There was a conspiracy, meaning an express or implied agreement between the defendant and one or more person(s) to commit the crime described in Count One;

(b) The defendant knowingly became a member of the conspiracy with an intent to advance the conspiracy; and

(c) One of the conspirators committed an overt act in an effort to advance the goals of the conspiracy.

Conspiracy (Count Two) – 18 U.S.C. § 1030(b)

(a) There was a conspiracy, meaning an express or implied agreement between the defendant and one or more person(s) to commit the crime described in Count One; and

(b) The defendant knowingly became a member of the conspiracy with

an intent to advance the conspiracy.

Computer fraud (Count Three) - 18 U.S.C. § 1030(a)(5)(A)

(a) The defendant knowingly caused the transmission of a program, information, code, or command; and

(b) By doing so, the defendant intentionally caused damage to a protected computer without authorization.

4. Mr. French will enter a voluntary plea of guilty to Count Three of the indictment.

Factual Basis

5. Mr. French will plead guilty because he is in fact guilty of intentionally damaging a protected computer without authorization. In pleading guilty, Mr. French acknowledges the following:

From December 10, 2013, to February 1, 2014, in the Northern District of Illinois, Eastern Division, and elsewhere, Timothy Justen French, also known as "Orbit," "orbit.girl," "@Orbit_g1rl," "crysis," "rootcrysis," and "c0rps3," knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, namely, a computer server belonging to

Company A, 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, Section 1030(a)(5)(A).

More specifically, Mr. French was a member of NullCrew, a group of computer hackers who carried out a series of cyber-attacks against businesses, universities, and government entities in the United States and abroad. Through the cyber-attacks, the group intentionally caused damage to the computer systems of the victim businesses, universities, and government entities.

To do so, Mr. French, Individual A, and other members of NullCrew identified vulnerabilities in victims' computer systems for the purpose of gaining unauthorized access to those systems. They shared those vulnerabilities with each other and, thereafter, coordinated their efforts to exploit those vulnerabilities to obtain unauthorized access and steal confidential information, including encrypted and unencrypted sensitive personal information for thousands of individuals.

To publicize their cyber-attacks, Mr. French, Individual A, and other members of NullCrew maintained Twitter accounts, including @NullCrew_FTS and @OfficialNull, which they used to announce their cyber-attacks, ridicule

their victims, and publicly disclose confidential information they had stolen through their cyber-attacks. Mr. French, Individual A, and other members of NullCrew hid their true identities by using aliases when communicating with the public and with each other. Mr. French used the aliases "Orbit," "@Orbit_g1rl," "crysis," "rootcrysis," and "c0rps3." Members of NullCrew, including Mr. French, also hid their identity by launching cyber-attacks from intermediary computer servers, either a virtual private network or a compromised computer server. One of the intermediary computer servers the Mr. French used was located in Naperville, Illinois.

In late January 2014, Mr. French and Individual A used the computer server in Naperville from which to launch a cyber-attack against Company A, a large Canadian telecommunications company. In particular, Individual A gave Mr. French a vulnerability to access databases owned by Company A. Mr. French and Individual A used those vulnerabilities to attack Company A, with the assistance of a syntax provided by a confidential witness who was working with the FBI. Mr. French and Individual A stole from Company A's databases the usernames and passwords for over 12,000 of Company A's customers, intentionally causing damage to Company A's computer servers. Mr. French and

Individual A stored the stolen information on the Naperville computer server.

On February 1, 2014, Mr. French, through the Twitter account @NullCrew_FTS, announced on behalf of NullCrew their computer attack against Company A. In particular, the message stated: "Whelp, let's start things off properly - nullcrew.org/[Company A].txt . . . hacked by #NullCrew." On February 2, 2014, the Twitter account provided a link to a website where Mr. French had published copies of database tables and credentials for a computer server Company A rented from a third party. The materials on that website included a section marked "tblCredentials," containing a list of Company A customer credentials in the form of 12,000 account username and password pairs.

Mr. French, Individual A, and others, acting on behalf of NullCrew, launched a number of similar cyber-attacks against other victims, including:

- On October 23, 2012, Mr. French and others participated in a cyber-attack on, and gained unauthorized access to, computer systems belonging to U.S. State A;
- Between July 19, 2013, and May 28, 2014, Mr. French and Individual A participated in a cyber-attack on, and gained unauthorized access to, computer systems belonging to University

A;

- Between January 17, 2014, and April 15, 2014, Individual A gained unauthorized access to computer systems belonging to Company B and Mr. French compiled the data stolen from Company B;
- Between January 23, 2014, and February 5, 2014, Mr. French and Individual A participated in a cyber-attack on, and gained unauthorized access to, computer systems belonging to Company C;
- Between January 23, 2014, and April 15, 2014, Mr. French and Individual A participated in a cyber-attack on, and gained unauthorized access to, computer systems belonging to University B; and
- Between April 2, 2014, and April 4, 2014, Mr. French and Individual A participated in a cyber-attack on, and gained unauthorized access to, computer systems belonging to Company D.

Mr. French acknowledges that his cyber-attacks caused damage. He acknowledges that his cyber-attacks caused loss of at least \$5,000 to one or more persons during a one-year period. The loss includes the cost to the victim

companies, universities, and government entities of responding to the computer intrusion, conducting damage assessments, and restoring the computer systems. Mr. French further acknowledges that it is the government's position that his cyber-attacks caused in aggregate at least \$792,000 in loss to the victim companies, universities, and government entities.

Potential Penalties

6. Mr. French understands that the charge carries a maximum penalty of 10 years' imprisonment; a maximum fine of \$250,000, or twice the gross gain or gross loss, whichever is greater, as well as any restitution ordered by the Court; and a term of supervised release of not more than three years.

7. Mr. French understands that pursuant to Title 18, United States Code, Section 3013, he will be assessed \$100, in addition to any other penalty imposed.

8. Mr. French understands that the Court will be guided by the United States Sentencing Guidelines. He understands that the Sentencing Guidelines are advisory only and merely one of several factors the Court must consider, pursuant to Title 18, United State Code, Section 3553(a), to determine a reasonable sentence. Mr. French has reviewed the Sentencing Guidelines with his attorney.

9. Mr. French understands that the United States Probation Office will conduct its own investigation, that the Court ultimately determines the facts and law relevant to sentencing, and that the Court's determinations govern the final advisory guideline calculation.

Trial Rights and Appellate Rights

10. Mr. French understands that by pleading guilty he surrenders certain rights, including the following:

(a) If he persisted in a plea of not guilty to the charges against him, he would have the right to a public and speedy trial. The trial could be either a jury trial or a trial by the judge sitting without a jury. Defendant has a right to a jury trial. However, in order that the trial be conducted by the judge sitting without a jury, the defendant, the government and the judge all must agree that the trial be conducted by the judge without a jury.

(b) If the trial is a jury trial, the jury would be composed of twelve laypersons selected at random. The defendant and his attorney would have a say in who the jurors would be by removing prospective jurors for cause where actual bias or other disqualification is shown, or without cause by exercising so-called peremptory challenges. The jury would have to agree unanimously before

it could return a verdict of either guilty or not guilty. The jury would be instructed that defendant is presumed innocent, and that it could not convict him unless, after hearing all the evidence, it was persuaded of defendant's guilt beyond a reasonable doubt, and that it was to consider each count of the indictment separately.

(c) If the trial is held by the judge without a jury, the judge would find the facts and determine, after hearing all the evidence, and considering each count separately, whether or not the judge was persuaded of defendant's guilt beyond a reasonable doubt.

(d) At a trial, whether by a jury or a judge, the government would be required to present its witnesses and other evidence against defendant. Defendant would be able to confront those government witnesses and his attorney would be able to cross-examine them. In turn, defendant could present witnesses and other evidence on his own behalf. He would be under no obligation to do so, however, because he is presumed to be innocent and, therefore, need not prove his innocence. If the witnesses for defendant would not appear voluntarily, he could require their attendance through the subpoena power of the court.

(e) At a trial, defendant would have a privilege against self-incrimination so that he could decline to testify, and no inference of guilt could be drawn from his refusal to testify. If defendant desired to do so, he could testify on his own behalf.

11. Mr. French understands that by pleading guilty he is waiving all the rights set forth in the prior paragraph. By pleading guilty, Mr. French admits he is guilty and agrees that he should be found guilty. Mr. French's attorney has explained those rights to him, and the consequences of his waiver of those rights. Mr. French further understands that he is waiving all appellate issues that might have been available if he had exercised his right to trial, and only may appeal the validity of his plea of guilty or the sentence.

Limitations and Consequences of this Plea Declaration

12. Mr. French understands that the United States Attorney's Office will fully apprise the Court and the Probation Office of the nature, scope and extent of his conduct regarding the charges against him, and related matters, including matters in aggravation and mitigation relevant to the issue of sentencing. Mr. French further understands that he will be able to present evidence in mitigation at the time of sentencing.

13. Mr. French understands that at the time of sentencing, the government and Mr. French will be free to make their respective recommendations to the Court.

14. Should this Court refuse to accept Mr. French's plea of guilty, this Plea Declaration shall become null and void and he will not be bound hereto. It is the defense's position that, should the Court reject his plea, Mr. French withdraws his plea of guilty pursuant to Rule 11 of the Federal Rules of Criminal Procedure. Additionally, pursuant to Rule 11(f) and Federal Rule of Evidence 410, this Plea Declaration and the ensuing court proceedings are inadmissible in later court proceedings.

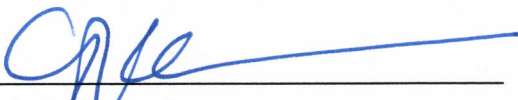
15. Mr. French agrees that this Plea Declaration, if accepted, shall be filed and become part of the record of his case.

16. Mr. French and his attorney acknowledge that no threats, promises, or representations have been made, nor agreements reached, to induce him to plead guilty. Mr. French further acknowledges that he has read this Plea Declaration and carefully reviewed each provision with his attorney.

Signed this 8 day of Dec., 2015

Timothy Justen French
Timothy Justen French, Defendant

FEDERAL DEFENDER PROGRAM
Carol A. Brook, Executive Director

By: 
Candace R. Jackson
Attorney for Timothy Justen French

55 East Monroe Street, Suite 2800
Chicago, Illinois 60603
(312) 621-8300