

FILED

JUL 16 2018

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
CENTRAL DIVISION
LEXINGTON**

AT LEXINGTON
ROBERT R. CARR
CLERK U.S. DISTRICT COURT

CRIMINAL ACTION NO. 5:18-CR-73-JMH

UNITED STATES OF AMERICA

PLAINTIFF

V.

PLEA AGREEMENT

COLTON GRUBBS

DEFENDANT

* * * * *

1. Pursuant to Federal Rule of Criminal Procedure 11(c), Defendant will enter a guilty plea to Counts 1, 3, and 10 of the Indictment, charging violations of 18 U.S.C. § 371, 18 U.S.C. § 2232(a), and 18 U.S.C. § 1956(h). Pursuant to Rule 11(c)(1)(A), the United States will move at sentencing to dismiss Counts 2, 4, 5, 6, 7, 8, and 9.

2. Defendant admits the essential elements of 18 U.S.C. § 371, Conspiracy:

- (a) Two or more persons conspired, or agreed, to commit the felony crime of intentionally accessing a protected computer without authorization and obtaining information, in violation of 18 U.S.C. § 1030(a)(2)(C) and 18 U.S.C. § 1030(c)(2)(B)(ii);
- (b) Defendant knowingly and voluntarily joined the conspiracy; and
- (c) A member of the conspiracy did at least one of the overt acts described in the Indictment for the purpose of advancing or helping the conspiracy.

3. Defendant admits the essential elements of 18 U.S.C. § 2232(a), Removal of Property to Prevent Seizure:

- (a) Defendant knowingly transferred, removed, and concealed property;

- (b) Before a search and seizure of that property by persons authorized to make this search and seizure; and
- (c) The actions were done with the purpose of preventing and impairing the government's lawful authority to take this property into its custody.

4. Defendant admits the essential elements of 18 U.S.C. § 1956(h), Conspiracy:

- (a) Two or more persons conspired, or agreed, to commit the felony crime of transferring money, knowing that the transactions involved the proceeds of unlawful activity, with the intent to promote the felony crime of intentionally accessing a protected computer without authorization and obtaining information, in violation of 18 U.S.C. § 1956(a)(1)(A)(i); and
- (b) Defendant knowingly and voluntarily joined the conspiracy.

5. Defendant admits the following facts which the United States could prove

beyond a reasonable doubt to establish the elements of Counts 1, 3, and 10:

- (a) Between April 2015 and July 2017, Defendant lived in Lincoln County and Fayette County, in the Eastern District of Kentucky, where he designed the LuminosityLink software, and where he sold that software for \$39.99 apiece to over 6,000 customers, and where he knew the software would be used by some customers for computer intrusions.
- (b) Defendant marketed and sold LuminosityLink on his luminosity.link website and the public internet forum HackForums.net (within the sub-forum "Hacks, Exploits, and Various Discussions > Hacking Tools and Programs"). Defendant claimed that LuminosityLink was a legitimate tool for systems administrators, but knew that many customers were using his software to remotely access and control computers without their victims' knowledge or permission. Defendant's marketing emphasized these malicious features of LuminosityLink, including that it could be remotely installed without notification, record the keys that a victim pressed on their keyboard, surveil victims using their computer cameras and microphones, view and download the computer's files, steal names and passwords used to access websites, mine and earn virtual currency using victim computers and electricity, use victim computers to launch DDoS attacks against other computers, and prevent anti-malware software from detecting and removing LuminosityLink.

- (c) Defendant used the name “KFC Watermelon” to publicly post on HackForums.net help forums and on his luminosity.link website about other software tools his customers needed to avoid detection, such as virtual private networks and crypters. Defendant also directly sent private messages to customers, knowingly answering their questions about accessing and controlling victim computers without authorization or detection. Defendant was aware that his customers were using his software on victim computers in the United States and around the world.
- (d) Defendant used public HackForums.net posts to solicit applications and used private messages to organize a LuminosityLink “Volunteer Support Team.” This service provided free support to LuminosityLink customers, and included at least nineteen other HackForums.net users who agreed to give advice and answer customer questions, including in an official Skype group chat monitored by Defendant. Defendant knew that many of these customers wanted to use LuminosityLink for unauthorized computer intrusions, and needed this help from the Volunteer Support Team in order to do so.
- (e) Defendant recruited others to sell LuminosityLink software as affiliates. Defendant operated a software licensing system to ensure that every LuminosityLink user would have to separately buy his software. Defendant collected money through PayPal, Stripe, and bitcoin payment processors. Defendant used this money for his personal living expenses. When Defendant was banned from PayPal for selling malware, another PayPal user agreed to collect the \$39.99 LuminosityLink payments and subsequently transfer the majority of that money to Defendant.
- (f) On July 10, 2017, after learning that the Federal Bureau of Investigation was about to perform an authorized search and seizure of his apartment, Defendant called the PayPal user collecting his LuminosityLink payments and warned him to “clean your room.” Defendant gave his laptop to his roommate and asked that it be concealed in the roommate’s car. Defendant concealed a debit card associated with his bitcoin account in his kitchen cabinet. Defendant concealed a phone storing his bitcoin information in his roommate’s closet. Defendant removed the hard drives from his desktop computer and removed them from his apartment before the authorized search so that they would not be seized by the government. Three days later, Defendant transferred over 114 bitcoin from his LuminosityLink bitcoin address into six new bitcoin addresses.

6. The statutory punishment for Counts 1 and 3 is imprisonment for not more than 5 years, a fine of not more than \$250,000, and a term of supervised release of not more than 3 years. The statutory punishment for Count 10 is imprisonment for not more than 20 years, a fine of not more than \$500,000, and a term of supervised release of not more than 3 years. A special assessment of \$100 applies for each count, and Defendant will pay this assessment to the U.S. District Court Clerk at the time of the entry of the plea.

7. Pursuant to Rule 11(c)(1)(B), the United States and Defendant recommend the following minimum sentencing guidelines calculations, and they may object to or argue in favor of other calculations. This recommendation does not bind the Court.

- (a) The United States Sentencing Guidelines November 1, 2016 manual will determine Defendant's guidelines range.
- (b) Pursuant to U.S.S.G. § 2B1.1(a)(2), the base offense level is 6.
- (c) Pursuant to U.S.S.G. § 2B1.1(b)(1)(F), increase the offense level by 10 levels because Defendant's gain exceeded \$150,000.
- (d) Pursuant to U.S.S.G. § 2B1.1(b)(10)(C), increase the offense level by 2 levels because the offense involved sophisticated means and Defendant intentionally engaged in and caused the conduct constituting sophisticated means.
- (e) Pursuant to U.S.S.G. § 3B1.3, increase the offense level by 2 levels because Defendant used a special skill in a manner that significantly facilitated the commission of the offense.
- (f) Pursuant to U.S.S.G. § 3C1.1, increase the offense level by 2 for obstructing or impeding the administration of justice.
- (g) Pursuant to U.S.S.G. § 3E1.1 and unless Defendant commits another crime, obstructs justice, or violates a court order, decrease the offense level by 2 levels for Defendant's acceptance of responsibility. If the offense level determined prior to this 2-level decrease is level 16 or greater, the United

States will move at sentencing to decrease the offense level by 1 additional level based on Defendant's timely notice of intent to plead guilty.

8. No agreement exists about Defendant's criminal history category pursuant to U.S.S.G. Chapter 4.

9. Defendant will not file a motion for a decrease in the offense level based on a mitigating role pursuant to U.S.S.G. § 3B1.2 or a departure motion pursuant to U.S.S.G. Chapter 5, Parts H or K.

10. The United States will not bring additional charges against Defendant based on information known to the United States at the time of this plea agreement.

11. Defendant waives the right to appeal the guilty plea and conviction. Defendant waives the right to appeal any determination made by the Court at sentencing with the sole exception that Defendant may appeal any aspect of the sentence if the length of the term of imprisonment exceeds the advisory sentencing guidelines range as determined by the Court at sentencing. Except for claims of ineffective assistance of counsel, Defendant also waives the right to attack collaterally the guilty plea, conviction, and sentence.

12. The United States will recommend releasing Defendant on the current conditions for future court appearances if Defendant does not violate the terms of the order setting conditions of release.

13. Defendant will forfeit to the United States all interest in the property listed in the forfeiture allegation of the Indictment. Defendant agrees that this property is subject

to forfeiture because a nexus exists between the property and the offenses, as set out in the forfeiture allegation of the Indictment.

14. Defendant agrees to cooperate fully with the United States Attorney's Office by making a full and complete financial disclosure. Within 30 days of pleading guilty, Defendant agrees to complete and sign a financial disclosure statement or affidavit disclosing all assets in which Defendant has any interest or over which Defendant exercises control, directly or indirectly, including those held by a spouse, nominee, or other third party, and disclosing any transfer of assets that has taken place within three years preceding the entry of this plea agreement. Defendant will submit to an examination, which may be taken under oath and may include a polygraph examination. Defendant will not encumber, transfer, or dispose of any monies, property, or assets under Defendant's custody or control without written approval from the United States Attorney's Office. If Defendant is ever incarcerated in connection with this case, Defendant will participate in the Bureau of Prisons Inmate Financial Responsibility Program, regardless of whether the Court specifically directs participation or imposes a schedule of payments. If Defendant fails to comply with any of the provisions of this paragraph, the United States, in its discretion, may refrain from moving the Court pursuant to U.S.S.G. § 3E1.1(b) to reduce the offense level by one additional level, and may argue that Defendant should not receive a two-level reduction for acceptance of responsibility under U.S.S.G. § 3E1.1(a).

15. Defendant understands and agrees that, pursuant to 18 U.S.C. § 3613, whatever monetary penalties are imposed by the Court will be due and payable immediately and subject to immediate enforcement by the United States. If the Court imposes a schedule of payments, Defendant agrees that it is merely a minimum schedule of payments and not the only method, nor a limitation on the methods, available to the United States to enforce the judgment. Defendant waives any requirement for demand of payment on any fine, restitution, or assessment imposed by the Court and agrees that any unpaid obligations will be submitted to the United States Treasury for offset. Defendant authorizes the United States to obtain Defendant's credit reports at any time. Defendant authorizes the U.S. District Court to release funds posted as security for Defendant's appearance bond in this case, if any, to be applied to satisfy Defendant's financial obligations contained in the judgment of the Court.

16. If Defendant violates any part of this Agreement, the United States may void this Agreement and seek an indictment for any violations of federal laws, and Defendant waives any right to challenge the initiation of additional federal charges.

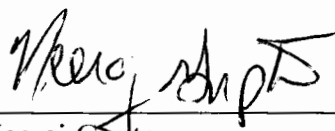
17. This document and the supplement contain the complete and only Plea Agreement between the United States Attorney for the Eastern District of Kentucky and Defendant.

18. This Agreement does not bind the United States Attorney's Offices in other districts, or any state or local prosecuting authorities.

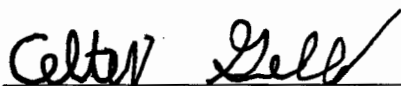
19. Defendant and Defendant's attorney acknowledge that Defendant understands this Agreement, that Defendant's attorney has fully explained this Agreement to Defendant, and that Defendant's entry into this Agreement is voluntary.

ROBERT M. DUNCAN, JR.
UNITED STATES ATTORNEY

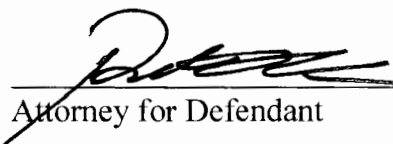
Date: 7.16.18

By: 
Neeraj Gupta
Assistant United States Attorney

Date: 7/16/18


Colton Grubbs
Defendant

Date: 7/16/18


Attorney for Defendant