IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

TAYLOR HUDDLESTON,

Defendant

Criminal No. 1:17-cr-34

STATEMENT OF FACTS

The United States and the defendant, TAYLOR HUDDLESTON ("HUDDLESTON"), agree that the following facts are true and correct, and that had this matter proceeded to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence.

Net Seal

1. From May 2012 through October 2016, in the Eastern District of Virginia and elsewhere, HUDDLESTON knowingly aided and abetted Zachary Shames and other persons who knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to protected computers, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 2.

2. In particular, HUDDLESTON made a financial profit by aiding and abetting computer intrusions, that is, by selling software that would be used by some of his customers to further illegal and unauthorized computers intrusions. At all relevant times, HUDDLESTON knew and was aware that these customers intended to use, and in fact did use, the software for illegal and unauthorized computer intrusions. At all relevant times, HUDDLESTON acted with

the purpose of furthering and aiding and abetting these illegal and unauthorized computer intrusions and causing them to occur.

3. HUDDLESTON developed licensing software called "Net Seal" and sold it to other software developers, some of whom used Net Seal to distribute their own malicious software. By developing and selling Net Seal, HUDDLESTON assisted in the distribution of that malicious software.

4. HUDDLESTON marketed Net Seal on Hackforums.net, a forum where members can obtain hacking tools and programs and chat with other members on the forum about computer intrusions.

5. HUDDLESTON accepted payment for Net Seal via PayPal. Generally, HUDDLESTON required his Net Seal customers pay for 50 licenses at a time, meaning that they would buy the right to use Net Seal to distribute 50 copies of their software (either malicious software or other software). HUDDLESTON received thousands of payments via PayPal from Net Seal customers.

6. HUDDLESTON was a member of a group on the messaging service "Skype" with approximately seven other prominent members of Hackforums.net where they could discuss the topic of computer intrusions and the products they were developing. One of the members of this Skype group was Zachary Shames, who was well-known on Hackforums.net as the developer and distributor of a popular keylogger called "Limitless." Limitless allowed users to steal information from victim computers, including sensitive information such as passwords to online banking and email accounts, as well as any keystroke typed by the owner of the victim computer.

7. HUDDLESTON provided Shames with access to his Net Seal licensing software in order to assist Shames in the distribution of his Limitless keylogger. In exchange, Shames made approximately one thousand payments via PayPal to HUDDLESTON. HUDDLESTON knew that he was assisting in the distribution of the Limitless keylogger, and that the purchasers of the keylogger intended to use it and did use it to commit unauthorized and unlawful computer intrusions.

8. HUDDLESTON set up his Net Seal licensing software to automatically send emails to purchasers of software developed by HUDDLESON's customers, including Shames. Those emails contained a license serial code and instructions for how to download and activate the software, including Shames' Limitless keylogger. The purpose of these emails was to help with the orderly, effective, and profitable distribution of software, including Shames' Limitless keylogger.

9. HUDDLESTON aided and abetted Shames' distribution of the Limitless keylogger to over 3,000 people who used it to infect, damage, and access without authorization, over 16,000 computers and who had the goal of stealing sensitive information from those computers.

10. HUDDLESTON provided Net Seal to several other customers to assist in the profitable distribution of the malicious software they developed including malware that has repeatedly been used to conduct unlawful and unauthorized computer intrusions and to damage victim computers.

11. The following acts in furtherance of and to effect the object of the above-described aiding and abetting were committed in the Eastern District of Virginia and elsewhere:

a. On or about May 8, 2012, Shames, from a computer located in Great Falls, Virginia, within the Eastern District of Virginia, paid HUDDLESTON $7.40 via PayPal in exchange for using the Net Seal licensing software to assist in the distribution of the Limitless keylogger to individuals who intended to use Limitless to commit unlawful computer intrusions.

b. On or about July 9, 2012, HUDDLESTON caused to be sent an automated email to Shames in the Eastern District of Virginia containing the code to activate Net Seal.

c. On or about November 21, 2013, HUDDLESTON caused an activation email to be sent to a customer who had purchased the Limitless keylogger, knowing that customers of the Limitless keylogger intended to use it for the purpose of committing unlawful and unauthorized computer intrusions. The email contained the license serial code and instructions for how to download and activate the keylogger.

d. HUDDLESTON agrees that the evidence would show that:

i. On or about April 23, 2013, Shames, from a computer located in Great Falls, Virginia, within the Eastern District of Virginia, exchanged emails with a customer of Limitless who complained that "the victim's keyboard after infected will no longer work properly. Victim will call the pc doctor and the logger will be compromised." In response, Shames assured him: "Trust me. I made this logger. I coded it. It doesn't change the way the words are typed."

ii. Shames also had several discussions with customers of Limitless on Hackforums.net in which he instructed them on how the Limitless keylogger could be used to steal email and social media passwords from the victim computers. For instance, on or about September 27,

2013, a customer posted: "Confirm … Outlook recovery WORKING!," referring to the Keylogger's ability to recover the victims' passwords to Microsoft's popular email service. Shames responded, "Thanks for testing and posting this. I hope you enjoy the new update!"

iii. On or about November 2, 2013, a customer asked Shames via Hackforums.net whether the Keylogger "steal[s] saved passwords of [sic] 2014 outlook." Shames responded: "Yes it should do that. It has the latest recoveries."

iv. On or about November 4, 2013, a customer asked Shames via Hackforums.net : "still waiting to know if it steals 2014 Outlook." Shames responded: "We are 100% sure it recovers 2013 passwords. If anyone wants to test 2014, feel free."

v. On or about November 21, 2013, a customer asked Shames via Hackforums.net whether "this is a worm which grabs the login data, log into a facebook/twitter account and spreads a text." Shames replied: "yes, it spreads as many posts as you want, and custom ones too!"

NanoCore

12. From January 2014 through February 2016, at which point he sold NanoCore to a third party, HUDDLESTON, knowingly and intentionally aided and abetted unlawful computer intrusions and attempted unlawful computer intrusions that occurred through October 2016, in violation of title 18 United States Code, Section 1030(a)(5)(A) and (b), that is, HUDDLESTON

knowingly caused the transmission of a program, information, code, and command, and knowingly aided and abetted others in doing the same and attempting to do the same, and as a result of such conduct, intentionally caused damage and attempted to cause damage without authorization to a protected computer, and resulting in a loss of $5,000 or more and damage affecting ten or more protected computers during a one year period, specifically from December 1, 2015 through November 30, 2016.

13. Specifically, in 2013, HUDDLESTON developed and distributed computer intrusion software known as the NanoCore Remote Access Tool ("NanoCore"). A remote access tool, or "RAT," is a program designed to allow a computer hacker to take complete control of a victim's computer for the purpose of performing various malicious activities. RATs provide hackers with a backdoor into the infected system of a victim computer so that the hacker can spy on the victim's computer, cause it to run additional malicious software, or launch attacks on other computer systems.

14. HUDDLESTON designed NanoCore to include a number of features, including the following:

a. A keylogger that allowed NanoCore users to record all keystrokes typed on the victim computer;

b. A password downloader that allowed NanoCore users to steal passwords that were saved on the victim computer;

c. A webcam feature that allowed NanoCore users to surreptitiously activate the webcam on the victim computer in order to spy on victims; and

d. A file access feature that allows NanoCore users to view, delete, download, and otherwise manipulate files stored on the victim computer.

15. In addition, the following features of which HUDDLESTON was aware were added to NanoCore by third parties through NanoCore's plug-in feature:

a. A ransomware feature that allowed NanoCore users to lock the victim computer with a password held by the user; and

b. A "booter" or "stresser" feature that allowed NanoCore users to participate in a distributed denial of service (DDOS) attack through the victim's computer.

16. HUDDLESTON advertised NanoCore on Hackforums.net, and caused it to be distributed to over 350 people, some of whom HUDDLESTON knew intended to use, and were using, this malicious software for illegal and unauthorized computer intrusions and for attempted illegal and unauthorized computer intrusions. At all relevant times, HUDDLESTON acted with the purpose of furthering these unauthorized computer intrusions and causing them to occur.

17. By developing NanoCore and distributing it to hundreds of people, some of whom he knew intended to use it for malicious purposes, HUDDLESTON knowingly and intentionally aided and abetted thousands of unlawful computer intrusions and attempted unlawful computer intrusions, including intrusions and attempted intrusions that occurred within the Eastern District of Virginia.

18. HUDDLESTON agrees the evidence would show that NanoCore was used in a massive "spear phishing" scheme designed to infect and attempt to infect thousands of victim computers, including computers within the Eastern District of Virginia. A spear phishing scheme is a scheme to trick victims into downloading malicious software onto their computer by sending them communications, typically emails, that purport to be from a friendly source and ask the victim to click on a link or open an attachment that looks benign but in fact contains a request to download malicious software.

19. HUDDLESTON agrees the evidence would show that as part of the spear phishing scheme, a hacker created a so-called "spoofed" email address, meaning an email address that appeared to come from a major oil and gas company ("Company 1") but was, in fact, controlled by the hacker. In or about August 2016, the hacker sent emails from this spoofed email address to over 6,000 targeted victim computers, including a targeted victim computer located in Norfolk, Virginia, within the Eastern District of Virginia. The spear phishing email stated that the victims owed money to Company 1 and included a PDF file attachment that purported to be an invoice from Company 1. The attachment in fact contained a link to a malicious executable that, if clicked by the victim, would send a request to download NanoCore onto the victim's computer from a remote server. The sending by the hacker of each spear phishing email constituted an attempt to transmit a program, information, code, and command that would intentionally cause damage without authorization to protected computers.

Conclusion

20. The statement of facts includes those facts necessary to support the defendant's guilty plea. It does not include each and every fact known to the defendant or to the government and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

21. The actions of the defendant, as recounted above, were in all respects knowing, voluntary, and intentional, and were not committed by mistake, accident or other innocent reason.

Dana J. Boente
United States Attorney

Date: July 19, 2017

By: _____
Kellen S. Dwyer
Assistant United States Attorney

Ryan K. Dickey, Senior Counsel
U.S. Department of Justice, Criminal Division
Computer Crime & Intellectual Property Section

Defendant's Signature: After consulting with my attorney, I hereby stipulate that the above Statement of Facts is true and accurate and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: July 17, 2017

Taylor Huddleston
Taylor Huddleston
Defendant

Defense Counsel Signature: I am Taylor Huddleston's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Date: July 17, 2017

Kenneth ~~P.~~ Troccoli, Esq.
Hayter L. Whitman, Esq.
Counsel for the Defendant