UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

UNITED STATES OF AMERICA

2018 DEC 21 P 3:59

v.

No. 1:18-cr-214-SM-1

WAYNE KENNEY, JR

INFORMATION

BACKGROUND

The United States Attorney Charges:

1. At all times relevant to this information, defendant WAYNE KENNEY, JR. ("KENNEY") resided and worked in the District of New Hampshire. KENNEY has a background in computer programming.
2. At all times relevant to this information, a person whose identity is known to the government and known to the defendant, but is identified herein as "John Doe 1," was a law enforcement officer who worked for the Auburn Police Department in the District of New Hampshire.
3. At all times relevant to this information, a person whose identity is known to the government and known to the defendant, but is identified herein as "John Doe 2," was a law enforcement officer who worked for the Auburn Police Department in the District of New Hampshire.
4. At all times relevant to this information, a person whose identity is known to the government and known to the defendant, but is identified herein as "Jane Doe 1," was an officer manager who worked for the Auburn Police Department in the District of New Hampshire.

5. At all times relevant to this information, a person whose identity is known to the government and known to the defendant, but is identified herein as "Jane Doe 2," was an administrative assistant who worked for the Town of Auburn in the District of New Hampshire.

6. At all times relevant to this information, the Farnum Center was a drug and alcohol treatment facility located in the District of New Hampshire. The Farnum Center operated a website, www.estreatment.org/farnumcenter.org, that provided information, guidance, and other assistance to those seeking alcohol and drug treatment. The landing page of the website contained hyperlinks that directed website visitors to additional information. It also contained phone numbers that connected callers to Farnum Center personnel.

7. The computer servers for the Auburn Police, the Town of Auburn, and the Farnum Center were located in the District of New Hampshire.

8. On or about January 23, 2015, John Doe 1 arrested KENNEY in the District of New Hampshire for possession of heroin. KENNEY was later charged with and convicted of possession of heroin. As part of his sentence, KENNEY was ordered to undergo drug treatment at the Farnum Center.

9. As set forth below, from in or about February 2015 through July 2015, KENNEY intentionally gained unauthorized access to ("hacked") a variety of computer systems, online accounts, and websites belonging to the Auburn Police Department, the Town of Auburn, the Farnum Center, and their respective employees. He obtained information from these compromised computers, which he used in furtherance of his criminal activities. He also sent commands to these compromised computers, which in turn

damaged them in a variety of ways, including by defacing them, deleting files from them, and otherwise impairing the integrity of data.

Hacking into Police Department and Town of Auburn Computers, Deploying Keystroke Logger, Stealing Employee Log-In Credentials, and Defacing Social Media Accounts

10. At a date uncertain but in or before February 2015, KENNEY devised a customized keystroke logger ("KSL"), which is a type of malicious software program that surreptitiously tracks (or logs) the keys that a computer user strikes on a keyboard and then transmits (or "uploads") the logged information electronically, usually through the Internet, to a remote storage location. KENNEY programmed his KSL to transfer the recorded keystrokes (including the computer user's usernames and passwords for various accounts) to e-mail accounts under his control.

11. On or about February 17, 2015, KENNEY hacked into, and installed his KSL on, numerous computers belonging to employees of the Auburn Police Department and the Town of Auburn. These included Jane Doe 1 and Jane Doe 2, among others.

12. From in or about February 17, 2015, through April 2015, using his KSL, KENNEY obtained information from his victims' compromised computers, including his victims' log in credentials for their personal e-mail and Facebook accounts, as well as for the Police Department's Facebook account.

13. From in or about February through in or about March 2015, KENNEY then used the employees' stolen log in credentials to hack into their various online accounts. Once KENNEY had hacked into those accounts, KENNEY took control of the accounts. He typically re-set the passwords, in turn locking the victims out of their accounts. He defaced some of the accounts, for example, by posting pornographic or other

embarrassing content on employees' Facebook pages, including on the Facebook profile page for Jane Doe 1. He also sent embarrassing e-mail messages from his victims' accounts, including from the email account of Jane Doe 1.

Hacking Into E-Mail Network of Town of Auburn, Deploying Virus, and Damaging Police Department and Town of Auburn Computers

14. At a date uncertain, but in or before February 2015, KENNEY developed a virus that, once installed on a compromised computer, would cause files on those computers to be deleted and would cause pop up messages to be displayed on the monitors, stating "I pray for the death of [John Doe 1]."

15. On or about March 4, 2015, KENNEY hacked into the Town of Auburn's e-mail network and took over multiple employee e-mail accounts, including the account belonging to the former Town Administrator. KENNEY then posed as the former Town Administrator and sent fraudulent "urgent" "phishing" email messages to numerous employees of the Town of Auburn and the Auburn Police. KENNEY's "phishing" e-mail messages contained a disguised link that, when clicked by the email recipient, would cause KENNEY's virus to be installed on the recipient's computer.

16. On or about March 26, 2015, KENNEY hacked into the Town of Auburn's e-mail network and took over multiple employee e-mail accounts, including the account of Jane Doe 1, the office manager for the Police Department and the account of the Captain of the Auburn Police Department. He then posed as the office manager and the police captain and sent fraudulent "urgent" "phishing" email messages to numerous employees of the Town of Auburn and the Auburn Police. KENNEY's email warned that a virus was infecting the Police Department and urged recipients to click on an embedded link to install a supposed security patch. KENNEY's "phishing" e-mail messages contained a

disguised link that, when clicked by the email recipient, would cause KENNEY's virus to be installed on the recipient's computer.

17. Between in or about March 2015 through in or about April 2015 KENNEY hacked into, and installed his virus on, numerous computers belonging to police officers and other employees of the Auburn Police Department and the Town of Auburn. These included John Doe 1, John Doe 2, and Jane Doe 1, among others. KENNEY caused files to be deleted from these compromised computers and caused the "I pray for the death of [John Doe 1]" message to be displayed on their monitors.

18. As a result of KENNEY's conduct, the Auburn Police Department and the Town of Auburn spent a significant amount of time and more than five thousand dollars responding to KENNEY's conduct, and its functions were temporarily impaired.

Hacking Into and Damaging the Farnum Center's Website

19. On or about July 1, 2015, KENNEY hacked into the website for the Farnum Center and took control of the site.

20. KENNEY disabled a link that would have provided website visitors access to information about alcohol and drug treatment assistance. KENNEY embedded a link to a video that played when a viewer clicked on it. The video was a video depicting "safer heroin injecting."

21. KENNEY deleted phone numbers on the website that would have provided website visitors access to alcohol and drug treatment assistance. KENNEY changed those phone numbers to phone numbers associated with adult entertainment services.

COUNT ONE
Unauthorized Access to a Protected Computer
(18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(ii)

22. The United States Attorney re-alleges and incorporates by reference paragraphs 1-21 of this Information and further charges that:

Between a date uncertain, but at least as early as on or about February 17, 2015, and at least as late as April, 2015, in the District of New Hampshire and elsewhere, defendant,

WAYNE KENNEY, JR.,

did intentionally access a computer, namely, the workplace computers of Jane Doe 1 and Jane Doe 2 at the Auburn Police Department and the Town of Auburn, respectively, without authorization and exceeding authorized access, and thereby obtained information from a protected computer, namely, (A) log in credentials to online accounts and (B) a roster of employee e-mail accounts, and the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution and laws of the United States and of any State, namely in furtherance of a fraudulent phishing campaign to further distribute malicious software and damage protected computers.

All in violation of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii).

COUNT TWO
Damage to a Protected Computer
(18 U.S.C. § 1030(a)(5)(A) and 1030(c)(4)(B)(i)(I), (II) and (IV))

23. The United States Attorney re-alleges and incorporates by reference paragraphs 1-21 of this Information and further charges that:

From a date uncertain, but at least as early as on or about March 4, 2015, through on or about July 1, 2015, in the District of New Hampshire and elsewhere, defendant,

WAYNE KENNEY, JR.,

did knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, and as a result of such conduct, intentionally caused damage, without authorization, to protected computers, namely (A) to workplace computers at the Auburn Police Department belonging to John Doe 1, John Doe 2, and Jane Doe 1, and the offense caused loss to one or more persons during any one-year period aggregating at least $5,000 in value during one year, and (B) the web server belonging to the Farnum Center, and the offense caused (1) the modification and impairment, and potential modification and impairment, of the medical examination, diagnosis, treatment, and care of one or more individuals, and (2) a threat to public health and safety.

All in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B)(i)(I), (II) and (IV).

December 21, 2018

Scott W. Murray
United States Attorney

By: _____
Arnold H. Huftalen
Assistant United States Attorney

BY: FOR _____
Mona Sedky
Senior Trial Attorney, USDOJ
Computer Crime & Intellectual
Property Section