SEALED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. 17-CR-124

[redacted] and
MARCUS HUTCHINS,
aka "Malwaretech,"

Defendants.

[Title 18, United States Code, Sections 371, 1030(a)(5)(A), 2511(a)(1), and 2512(1)(a), (b), and (c)(i)]

INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES:

1. At times material to this indictment:

DEFENDANTS

a. Defendant [redacted] used the online aliases [redacted]

b. Defendant MARCUS HUTCHINS was a citizen and resident of the United Kingdom. HUTCHINS used various online aliases, including "Malwaretech."

RELEVANT TERMS

c. A "protected computer" was a computer in or affecting interstate or foreign commerce or communications, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communions of the United States.

d. "Malware" was a term used to describe malicious computer code installed on protected computers without authorization that allowed unauthorized access to the protected computer.

e. "Kronos" was the name given to a particular type of malware that recorded and exfiltrated user credentials and personal identifying information from protected computers. Kronos malware was commonly referred to as a "banking Trojan."

f. "Crypting" was a term used to describe computer code used to conceal the existence of malware from anti-virus software.

The Conspiracy

2. Between in or around July 2014 and July 2015, in the state and Eastern District of Wisconsin and elsewhere,

[redacted] **and**

MARCUS HUTCHINS, aka "Malwaretech"

knowingly conspired and agreed with each other to commit an offense against the United States, namely, to knowingly cause the transmission of a program, information, code, and command and as a result of such conduct, intentionally cause damage without authorization, to 10 or more protected computers during a 1-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B)(i) and (c)(4)(A)(i)(VI).

Manner and Means of Conspiracy

3. The manner and means sought to accomplish the object and purpose of the conspiracy included:

a. Advertising the availability of the Kronos malware on internet forums;

b. Selling the Kronos malware;

c. Receiving and distributing the proceeds obtained from selling the Kronos malware; and

d. Acts done in furtherance of the conspiracy were concealed and hidden, and caused to be concealed and hidden.

Overt Acts in Furtherance of the Conspiracy

4. In furtherance of the conspiracy, and to accomplish the object and purpose of the conspiracy, the following overt acts, among others, were committed and were caused to be committed:

a. Defendant MARCUS HUTCHINS created the Kronos malware.

b. On or about July 13, 2014, a video showing the functionality of the "Kronos Banking trojan" was posted to a publically available website. Defendant [redacted] used the video to demonstrate how Kronos worked.

c. In or around August 2014, on an internet forum, defendant [redacted] offered to sell the "Kronos Banking trojan" for $3,000.

d. In or around February 2015, defendants MARCUS HUTCHINS and [redacted] updated the Kronos malware.

e. On or about April 29, 2015, defendant [redacted], using the name [redacted] advertised the availability of the Kronos malware on the AlphaBay market forum.

f. On or about June 11, 2015, defendant [redacted] sold a version of the Kronos malware in exchange for approximately $2,000 in digital currency.

g. On or about July 17, 2015, defendant [redacted] offered cryptying services for Kronos.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO

THE GRAND JURY FURTHER CHARGES:

Between in or around July 2014 and August 2014, in the state and Eastern District of Wisconsin and elsewhere,

[redacted] **and**
MARCUS HUTCHINS, aka "Malwaretech"

knowingly disseminated by electronic means an advertisement of any electronic, mechanical, or other device, knowing and having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of electronic communications, knowing the content of the advertisement and having reason to know that such advertisement will be transported in interstate and foreign commerce.

In violation of Title 18, United States Code, Sections 2512(1)(c)(i), and 2.

COUNT THREE

THE GRAND JURY FURTHER CHARGES:

On or about June 11, 2015, in the state and Eastern District of Wisconsin and elsewhere,

[redacted] **and**
MARCUS HUTCHINS, aka "Malwaretech"

intentionally sent any electronic, mechanical, or other device, in interstate and foreign commerce, knowing and having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of electronic communications.

In violation of Title 18, United States Code, Sections 2512(1)(a), and 2.

COUNT FOUR

THE GRAND JURY FURTHER CHARGES:

On or about June 11, 2015, in the state and Eastern District of Wisconsin and elsewhere,

[redacted] **and**
MARCUS HUTCHINS, aka "Malwaretech"

intentionally sold any electronic, mechanical, or other device, knowing and having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of electronic communications and that such device and any component thereof was transported in interstate and foreign commerce.

In violation of Title 18, United States Code, Sections 2512(1)(b), and 2.

COUNT FIVE

THE GRAND JURY FURTHER CHARGES:

On or about June 11, 2015, in the state and Eastern District of Wisconsin and elsewhere,

[redacted] **and**

MARCUS HUTCHINS, aka "Malwaretech"

knowingly and intentionally endeavored to intercept and procure any other person to intercept certain electronic communications, namely computer keystrokes of others without the knowledge or consent of said others.

In violation of Title 18, United States Code, Sections 2511(1)(a), (4)(a), and 2.

COUNT SIX

THE GRAND JURY FURTHER CHARGES:

On or about June 11, 2015, in the state and Eastern District of Wisconsin and elsewhere,

[redacted] **and**
MARCUS HUTCHINS, aka "Malwaretech"

knowingly caused the transmission of a program, information, code, and command and as a result of such conduct, attempted to cause damage without authorization, to 10 or more protected computers during a 1-year period.

In violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B)(i) and (ii), (c)(4)(A)(i)(VI), 1030(b), and 2.

A TRUE BILL:

[redacted]
FOREPERSON

Dated: 07/11/2017

GREGORY J. HAANSTAD
United States Attorney