

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

U.S. DISTRICT COURT
EASTERN DISTRICT-WI
FILED

2018 JUN -5 P-3: 48

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 17-CR-124

STEPHEN C. DRIES
CLERK

v.

MARCUS HUTCHINS,
aka "Malwaretech,"
aka "irp@jabber.se"

[Title 18, United States Code, Sections
371, 1001(a)(2), 1030(a)(5)(A),
(a)(2)(C) and (b), 2511(a)(1),
2512(1)(c)(i) and (ii); and 1349]

Defendant.

FIRST SUPERSEDING INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES:

1. At times material to this indictment:

RELEVANT ENTITIES

a. Defendant MARCUS HUTCHINS developed malware. HUTCHINS used various aliases, including "Malwaretech" and "irp@jabber.se."

b. Individual A, also known as "Vinny," "VinnyK," "Gone with the Wind," "Cocaine," "Jack of All Trades," and "Aurora123" advertised, promoted, and distributed malware developed by defendant MARCUS HUTCHINS.

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 communications of the United States.

d. "Malware" was a term used to describe malicious computer code intended to damage a computer. Malware deletes, creates, and modifies files on a computer and allows unauthorized access to a 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." Kronos utilized a key logger, a form grabber, and web injects to intercept and collect personal information from a protected computer. During the installation process, Kronos was concealed in a legitimate program already running on the victim computer.

f. "UPAS Kit" was the name given to a particular type of malware that was advertised as a "modular HTTP bot." UPAS Kit was marketed to "install silently and not alert antivirus engines." UPAS Kit allowed for the unauthorized exfiltration of information from protected computers. UPAS Kit used a form grabber and web injects to intercept and collect personal information from a protected computer.

g. A "form grabber" was the process of intercepting certain data being sent from a computer's internet browser to a website.

h. "Web injects" work by intercepting data being sent from a website to a computer's internet browser. The data is intercepted before it is displayed by the browser, allowing the malware to modify the data before it is displayed by the browser. Typically, the modifications cause false and fraudulent representations to be displayed by the browser, prompting the user to provide additional personal and account related information like PIN numbers, credit and debit card numbers, or a social security number, among other information.

i. “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 2012 and September 2015, in the state and Eastern District of Wisconsin and elsewhere,

MARCUS HUTCHINS, aka “Malwaretech,” aka “irp@jabber.se”

knowingly conspired and agreed with Individual A, aka “Vinny,” aka “VinnyK,” aka “Gone with the Wind,” aka “Cocaine,” aka “Jack of All Trades,” aka “Aurora123,” and others unknown to the Grand Jury, to commit an offense against the United States, namely, to:

(a) knowingly cause and aid and abet 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) and 2;

(b) intentionally access and aid and abet another to intentionally access a computer without authorization, and obtain information from a protected computer for the purpose of private financial gain, in violation of Title 18 United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i) and 2; and

(c) intentionally intercept, endeavor to intercept, and procure any other person to intercept and endeavor to intercept, any electronic communication in violation of Title 18, United States Code, Section 2511(1)(a).

Manner and Means of the Conspiracy

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

- a. Advertising, promoting, and marketing the availability of the UPAS Kit and Kronos;
- b. Selling and distributing the UPAS Kit and Kronos;
- c. Receiving and distributing the proceeds obtained from selling malware; and
- d. Concealing acts done in furtherance of the conspiracy.

Overt Acts in Furtherance of the Conspiracy

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

- a. Defendant MARCUS HUTCHINS developed UPAS Kit and provided it to Individual A, who was using alias "Aurora123" at the time.
- b. On or about July 3, 2012, Individual A, using the alias "Aurora123," sold and distributed UPAS Kit to an individual located in the Eastern District of Wisconsin in exchange for \$1,500 in digital currency.
- c. On or about July 20, 2012, Individual A, using the alias "Aurora123," distributed an updated version of UPAS Kit to an individual located in the Eastern District of Wisconsin.
- d. Prior to July 2014, defendant MARCUS HUTCHINS developed Kronos and provided it to Individual A. HUTCHINS intended Individual A to advertise, promote, sell, and distribute Kronos.
- e. On or about July 13, 2014, a video showing the functionality of the "Kronos Banking trojan" was posted to YouTube. Individual A and defendant MARCUS HUTCHINS used the video to demonstrate how Kronos worked and to promote the sale of Kronos.

f. In or around August 2014, Individual A, using the alias “Vinny,” offered to sell the “Kronos Banking trojan” for \$3,000 on the forum exploit.in.

g. On or about September 7, 2014, Individual A, using the alias “VinnyK,” marketed Kronos to members of the Darkode forum.

h. On or about December 23, 2014, defendant MARCUS HUTCHINS hacked control panels associated with Phase Bot, malware HUTCHINS perceived to be competing with Kronos. In a chat with Individual B, HUTCHINS stated, “well we found exploit (sic) in his panel just hacked all his customers and posted it on my blog sucks that these [] idiots who cant (sic) code make money off this :|” HUTCHINS then published an article on his Malwaretech blog titled “Phase Bot – Exploiting C&C Panel” describing the vulnerability.

i. In or around February 2015, defendant MARCUS HUTCHINS and Individual A, updated Kronos. On February 9, 2015, in a chat with Individual B, HUTCHINS described the update. Individual B asked, “[D]id you guys just happen to make a (sic) update?” HUTCHINS responded, “[W]e made a few fixes to both the panel and bot.” Individual B replied, “ah okay yeah read something that vinny posted was curious on what it was exactly.”

j. In or around February 2015, defendant MARCUS HUTCHINS distributed Kronos to Individual B, who was located in the State of California. At that time, HUTCHINS knew Individual B was involved in the various cyber-based criminal enterprises including the unauthorized access of point-of-sale systems and the unauthorized access of ATMs.

k. On or about April 29, 2015, Individual A, using the alias “VinnyK,” advertised the availability of the Kronos on the AlphaBay market forum.

1. On or about June 11, 2015, Individual A, using the alias "Vinny" sold a version of Kronos in exchange for approximately \$2,000 in digital currency to an individual located in the Eastern District of Wisconsin.

m. On or about July 17, 2015, Individual A, using the alias "VinnyK," offered crypting services for Kronos.

n. Defendant MARCUS HUTCHINS referred customers interested in buying Kronos to Individual A.

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

MARCUS HUTCHINS, aka "Malwaretech," aka "irp@jabber.se,"

intentionally disseminated and aided and abetted the dissemination by electronic means any 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:

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

MARCUS HUTCHINS, aka "Malwaretech," aka "irp@jabber.se,"

intentionally disseminated and aided and abetted the dissemination by electronic means any advertisement of any other electronic, mechanical, or other device, where such advertisement promotes the use of such device 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)(ii), 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,

MARCUS HUTCHINS, aka "Malwaretech," aka "irp@jabber.se,"

aided and abetted Individual A, who 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 FIVE

THE GRAND JURY FURTHER CHARGES:

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

MARCUS HUTCHINS, aka "Malwaretech," aka "irp@jabber.se,"

aided and abetted Individual A, who 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 SIX

THE GRAND JURY FURTHER CHARGES:

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

MARCUS HUTCHINS, aka "Malwaretech," aka "irp@jabber.se,"

knowingly and intentionally endeavored to intercept and procure any other person to intercept and endeavor 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 SEVEN

THE GRAND JURY FURTHER CHARGES:

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

MARCUS HUTCHINS, aka "Malwaretech," aka "irp@jabber.se,"

knowingly caused and aided and abetted 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.

COUNT EIGHT

THE GRAND JURY FURTHER CHARGES:

Between in or around June 2014 and on or about June 11, 2015, in the state and Eastern District of Wisconsin and elsewhere,

MARCUS HUTCHINS, aka "Malwaretech," aka "irp@jabber.se"

knowingly aided and abetted another to intentionally access a computer without authorization and thereby obtain and attempt to obtain information from a protected computer for the purpose of private financial gain.

In violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), 1030(b), and 2.

COUNT NINE

THE GRAND JURY FURTHER CHARGES:

1. On or about August 2, 2017, defendant MARCUS HUTCHINS was advised that it was a crime to make a materially false statement in a matter within the jurisdiction of the executive branch of the Government of the United States.

2. The Federal Bureau of Investigation is an agency within the executive branch of the Government of the United States.

3. On August 2, 2017, the Federal Bureau of Investigation was conducting an investigation related to Kronos, which was a matter within the jurisdiction of the Federal Bureau of Investigation.

4. On or about August 2, 2017, in the state and Eastern District of Wisconsin and elsewhere,

MARCUS HUTCHINS, aka "Malwaretech," aka "irp@jabber.se,"

knowingly and willfully made a materially false, fictitious, and fraudulent statement and representation in a matter within the jurisdiction of the Federal Bureau of Investigation when he stated in sum and substance that he did not know his computer code was part of Kronos until he reverse engineered the malware sometime in 2016, when in truth and fact, as HUTCHINS then knew, this statement was false because as early as November 2014, HUTCHINS made multiple statements to Individual B in which HUTCHINS acknowledged his role in developing Kronos and his partnership with Individual A.

In violation of Title 18, United States Code, Section 1001(a)(2).

COUNT TEN

THE GRAND JURY FURTHER CHARGES:

1. The allegations in paragraph 1 of Count One of this Superseding Indictment are realleged and incorporated into this count by reference as if they were fully set forth here.

2. Between in or around July 2012 and September 2015, in the state and Eastern District of Wisconsin and elsewhere,

MARCUS HUTCHINS, aka "Malwaretech," aka "irp@jabber.se"

knowingly conspired and agreed with Individual A and others unknown to the Grand Jury, to devise and participate in a scheme to defraud and obtain money by means of false and fraudulent pretenses, and representations and transmit by wire in interstate and foreign commerce any writing, signs, and signals for the purpose of executing the scheme, in violation of Title 18, United States Code, Section 1343.

3. The object of the conspiracy was to use interstate and foreign wire communications to obtain money by advertizing, promoting, selling, and distributing Kronos and UPAS Kit.

4. The manner and means to accomplish the object of conspiracy are described in paragraph 3 of Count One.

5. Overt acts committed in furtherance of the conspiracy are described in paragraph 4 of Count One.

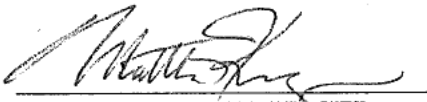
All in violation of Title 18, United States Code, Section 1349.

A TRUE BILL:



FOREPERSON

Dated: 6/5/18


MATTHEW D. KRUEGER
United States Attorney

**NATIONAL
SECURITY
ARCHIVE**

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu