

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA)	
)	Criminal No. 15-148
v.)	
)	(18 U.S.C. §§ 371, 2;
JOHAN ANDERS GUDMUNDS)	1349, 1956(h))
a/k/a "Mafi")	
a/k/a "Crim")	[UNDER SEAL]
a/k/a "Synthet!c")	

INDICTMENT

INTRODUCTION

At all times relevant to the Indictment:

1. DARKODE was an Internet forum where individuals convened online to buy, sell, trade, and discuss intrusions on computers and electronic devices belonging to others. One could only become a member of DARKODE by declaring to existing members what type of relevant ability or product he or she could bring to the forum and then being approved for membership by the other members.

2. Defendant JOHAN ANDERS GUDMUNDS resided in Sweden and used the Internet nicknames "Mafi," "Crim" and "Synthet!c." JOHAN ANDERS GUDMUNDS was a member and administrator of the Internet forum known as DARKODE.

3. A "protected computer" is as defined at 18 U.S.C. § 1030(e)(2)(B).

COUNT ONE

The grand jury charges:

THE CONSPIRACY AND ITS OBJECTS

4. From in and around September 2008, and continuing thereafter until on or about January 23, 2015, in the Western District of Pennsylvania and elsewhere, the defendant, JOHAN ANDERS GUDMUNDS, a/k/a "Mafi," a/k/a "Crim," a/k/a "Synthet!c", knowingly and willfully did aid and abet and conspire, combine, confederate and agree together with other persons, known and unknown to the grand jury, to commit offenses against the United States, that is:

a) to intentionally access a computer without authorization and exceed authorized access to a protected computer, and thereby obtain information from a protected computer, and the offense was committed for purposes of commercial advantage and private financial gain and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States and of any state, including the Commonwealth of Pennsylvania, and the value of the information obtained exceeded \$5,000, in violation of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(i)-(iii) (unauthorized access and exceeding authorized access to a protected computer).

b) to knowingly and with intent to defraud access a protected computer without authorization and exceeding authorized access and by means of such conduct further the intended fraud and

obtain something of value, in violation of 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A).

c) knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and the offense caused damage affecting 10 or more protected computers during a 1-year period, in violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B).

d) knowingly and with intent to defraud traffic in a password and similar information through which a computer may be accessed without authorization, and such trafficking affected interstate and foreign commerce, in violation of 18 U.S.C. §§ 1030(a)(6)(A) and (c)(2)(A).

MANNER AND MEANS OF THE CONSPIRACY

5. It was a part of the conspiracy that the conspirators would participate in the online, password-protected, hacker forum known as Darkode and that they would share information, ideas, and tools with each other to support each other's unlawful activities.

6. It was further part of the conspiracy that Darkode would be available to all of its members, including any within the Western District of Pennsylvania, over the Internet.

7. It was further part of the conspiracy that members of Darkode would carefully vet prospective members through a two-step process in which a prospective member would first be invited to the forum by an existing member, and then the prospective member would

introduce him/herself on the Darkode forum, typically by listing the criminal skills that the prospective user could bring to the group and describing the criminal activities in which he or she engaged. Only if existing members vouched for the new member would the prospective member be allowed access to the Darkode forum.

8. It was further part of the conspiracy that the members of Darkode would use the tools and experience gained on Darkode to infect the computers of victims around the world, including victims within the Western District of Pennsylvania, with malware and thereby access those computers without authorization and in excess of authorization of their owners.

OVERT ACTS

9. In furtherance of the conspiracy, and to effect the objects of the conspiracy, the defendant, JOHAN ANDERS GUDMUNDS, a/k/a "Mafi," a/k/a "Crim," a/k/a "Synthet!c," together with others both known and unknown to the grand jury, did commit and cause to be committed, the following overt acts, among others, in the Western District of Pennsylvania and elsewhere:

10. Sometime in 2007, M.S., using the moniker "Iserdo," and an unindicted coconspirator known to the Grand Jury, using the monikers "nocen" and "Loki," created the online hacker forum Darkode.com for the purpose of bringing together the most talented computer hackers and cyber-criminals on the Internet in one virtual location.

11. On or about September 30, 2008, JOHAN ANDERS GUDMUNDS joined the Darkode forum using the monikers "Mafi" and "Crim."

12. In or around January 2009, JOHAN ANDERS GUDMUNDS posted on Darkode that he was selling access to a botnet for \$80 per 1,000 compromised computers.

13. In or around July 2009, a coconspirator posted on Darkode forum that "Mafi" had coded the malicious software known as "Blazebot."

14. Later in or around July 2009, JOHAN ANDERS GUDMUNDS, using the moniker Mafi, responded to the posting by stating that Blazebot had the following capabilities: "it uses http protocol...it has fud usb spreader conficker style, im spreaders, ring0 rootkit, various p2p spreads that retrieves the 10 latest win32 app files from rlslog, account stealers."

15. On or about August 3, 2009, JOHAN ANDERS GUDMUNDS posted on Darkode that he was selling root access to hacked servers located at the University of Erlangen-Nurnberg (located in Germany) and University of Pisa (located in Italy) for \$50 each.

16. On or about August 5, 2009, JOHAN ANDERS GUDMUNDS posted on Darkode that he was selling access to approximately 200 hacked servers located in various countries for \$10 to \$50 each.

17. On or about August 6, 2009, JOHAN ANDERS GUDMUNDS controlled a "Zeus" botnet that infected approximately 60,000 computers and that had stolen data from the users of those computers approximately 200,000,000 times, allowing GUDMUNDS and his customers

to gather unique credentials that gave them access to bank accounts and other information.

18. In or around September 2009, JOHAN ANDERS GUDMUNDS created and marketed on Darkode a computer malware exploit package called "Crimepack" that had the "highest rates [of infection] for the lowest price."

19. On or about February 2, 2010, JOHAN ANDERS GUDMUNDS posted on Darkode that he was selling malicious software, which he coded, that spreads itself via MSN Messenger. GUDMUNDS posted:

...it will only send to each contact once (reset when msn is restarted) and will be totally invisible to the user sending it I'll also include a not-so-tested version of my link replacer that replace links sent from the user with your own spread link... I'm selling the source which is coded in C++ for \$300 and will explain usage and how to implement it in your bot."

20. On or about March 2, 2010, JOHAN ANDERS GUDMUNDS claimed that Crimepack had an infection rate of thirty percent and that it was programmed to be undetectable by anti-virus programs, blacklists, and other mechanisms that protect computers against malware.

21. On or about April 20, 2010, JOHAN ANDERS GUDMUNDS engaged in an online chat with an undercover FBI Agent (the "UCA") in which GUDMUNDS offered to sell root access to servers that he had hacked to the UCA.

22. On or about April 21, 2010, JOHAN ANDERS GUDMUNDS sold to the UCA root access to three hacked servers in exchange for a negotiated price.

23. On or about the same date, JOHAN ANDERS GUDMUNDS provided the UCA with the user name and password to the three hacked servers located within the United States and Europe, along with his banking information, including a WebMoney account number.

24. Beginning in or about May 2010, JOHAN ANDERS GUDMUNDS took over the management of Darkode from unindicted coconspirator M.S., also known as "Iserdo," by becoming the administrator of the site responsible for governing the forum and its members, managing technical details of the forum, settling disputes among members, managing the identity and function of forum monitors, and exercising the final say over who would be granted membership to the forum.

25. On or about October 31, 2010, JOHAN ANDERS GUDMUNDS offered for sale on Darkode a sophisticated malware package that he himself coded called "Antiklus," and posted several specific features of the malware.

26. On December 1, 2010, JOHAN ANDERS GUDMUNDS posted that he was selling root access to compromised servers for \$10 each with a minimum of five.

27. On or about January 20, 2011, JOHAN ANDERS GUDMUNDS posted on Darkode that he was selling root access to ten compromised Linux servers for \$60.

28. On or about April 7, 2011, JOHAN ANDERS GUDMUNDS posted on Darkode that he was looking for a partner in order to send spam email messages, and offered to provide the mailer software program and the bots that work along with the mail to facilitate the spamming.

29. On or about May 16, 2011, JOHAN ANDERS GUDMUNDS posted on the Darkode forum that there was a vulnerability on a particular website and encouraged other members of Darkode to "try to pull something off."

30. On or about January 28, 2012, JOHAN ANDERS GUDMUNDS changed his online moniker on Darkode to Synthet!c.

31. On or about November 28, 2012, JOHAN ANDERS GUDMUNDS, using the account "mafi@thesecure.biz," discussed the status of the Darkode forum with another individual known as Sp3ciall1st who was interested in becoming a moderator or administrator and asked the individual for help recruiting new members and improving participation of current members to "make it the best forum."

32. During the same conversation on or about November 28, 2012, JOHAN ANDERS GUDMUNDS stated that he would like to bring in guys from "other niches . . . instead of the every day script kiddies," and that he would demote those who are not participating in the forum or limit their access to the site to encourage more discussions on "technical topics" and to "share ideas."

33. During the same conversation on or about November 28, 2012, JOHAN ANDERS GUDMUNDS directed Sp3ciall1st to send out invitations to new potential members of Darkode, including an "offshore hosting

provider," an "off the books exchanger for" WebMoney and Liberty Reserve "who wont care if names dont match," and "private exploit kit" authors.

34. On about January 16, 2013, in an effort to protect the security of the Darkode forum from a computer security reporter who recently had published an article describing a Darkode posting, JOHAN ANDERS GUDMUNDS, using the account mafioso@xmpp.jb, advised Sp3ciall1st that he was reviewing the logs and developing a plan to identify the person leaking information to the reporter.

35. On or about January 20, 2013, JOHAN ANDERS GUDMUNDS, using the jabber account mafioso@xmpp.jb, engaged in a discussion with another individual in which GUDMUNDS reviewed the status of multiple members of Darkode, discussed their reliability and skills to the forum, and determined their level of access to Darkode.

36. On or about January 23, 2014, JOHAN ANDERS GUDMUNDS, using the moniker synthet!c, offered for sale on Darkode the malicious software known as "Pandemiya 2014 [injection, proxy, grabber]" which he described as having the following powerful infection and information stealing capabilities:

core features:

- injects for chrome, ie, ff
- grabbers for chrome, ie, ff
- tasks
- file grabber
- digital signature on files to load

additional features:

- reverse proxy
- iframer/ftp stealer
- pe infector (for startup)...

for pricing, details, questions contact me on pm or by jabber

37. On or about January 27, 2015, JOHAN ANDERS GUDMUNDS, using the moniker synthet!c and the account mafioso@xmpp.jp, contacted Sp3cial1st and advised that the darkode.com domain was in danger of being terminated due to a complaint about invalid contact information.

All in violation of Title 18, United States Code, Sections 371 and 2.

advertising revenue, and to dupe victims into fraudulently advertised goods that were falsely advertised.

45. It was further part of the scheme and artifice for members of the conspiracy to trick victims into unwittingly downloading and installing malicious software on their computers that allowed members of the conspiracy to unlawfully access and obtain money from the accounts of the victims, including bank accounts, lines of credit and credit cards.

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

COUNT THREE

The grand jury further charges:

46. Paragraphs 1 through 3, 5 through 37, and 40 through 45 are incorporated herein and re-alleged as if set forth in full.

47. From in and around September 2008, and continuing thereafter until on or about January 23, 2015, in the Western District of Pennsylvania and elsewhere, the defendant, JOHAN ANDERS GUDMUNDS, a/k/a "Mafi," a/k/a "Crim," a/k/a "Synthet!c," knowingly and willfully did conspire, combine, confederate and agree together and with other persons, known and unknown to the grand jury, to commit offenses against the United States in violation of Title 18, United States Code, Section 1956, to wit:

- a. to knowingly conduct and attempt to conduct a financial transaction affecting interstate and foreign commerce, which involved the proceeds of a specified unlawful activity, that is, proceeds of violations of 18 U.S.C. §§ 1030 and 1343, with the intent to promote the carrying on of specified unlawful activity, that is, violations of 18 U.S.C. §§ 1030 and 1343, and that while conducting and attempting to conduct such financial transaction knew that the property involved in the financial transaction represented the proceeds of some form of unlawful activity in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i); and

- b. to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, proceeds of violations of 18 U.S.C. §§ 1030 and 1343, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and
- c. to transport, transmit and transfer and attempt to transport, transmit and transfer a monetary instrument and funds to a place in the United States from and through a place outside the United States and from a place in the United States to and through a place outside the United States with the intent to promote the carrying on of specified unlawful activity, that is violations of 18 U.S.C. §§ 1030 and 1343, in violation of Title 18, United States Code, Section 1956(a)(2)(A).

All in violation of Title 18, United States Code, Section 1956(h).

The Grand Jury further finds that there is probable cause to believe the following property is forfeitable to the United States as a result of the violations alleged in Counts One through Three.

FORFEITURE ALLEGATION I

48. The allegations contained in Count One of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

49. Upon conviction of the conspiracy offense in violation of Title 18, United States Code, Section 371, set forth in Count One of this Indictment, defendant JOHAN ANDERS GUDMUNDS, a/k/a "Mafi", a/k/a "Crim", a/k/a "Synthet!c", shall forfeit to the United States of America:

- a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense, such property includes but is not limited to a money judgment for a sum of money equal to the proceeds obtained as a result of the offense; and
- b. pursuant to Title 18, United States Code, Section 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of such offense. The property

to be forfeited includes, but is not limited to the domain name **darkode.com**.

50. If any of the property described above, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot

be divided without difficulty, the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b) and 1030(i).

All pursuant to Title 18, United States Code, Sections 982(a)(2)(B), 982(b) and 1030(i), Title 21, United States Code, Section 853, and Title 28 U.S.C. § 2461(c).

FORFEITURE ALLEGATION II

51. The allegations contained in Count Two of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c).

52. Upon conviction of the offense in violation of Title 18, United States Code, Section 1343 and 1349 set forth in Count Two of this Indictment, the defendant, JOHAN ANDERS GUDMUNDS, a/k/a "Mafi", a/k/a "Crim", a/k/a "Synthet!c", shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to a violation constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violation or a conspiracy to commit such violation. The property to be forfeited includes, but is not limited to, the following: the domain **darkode.com** and a money judgment for a sum of money equal to the proceeds obtained as a result of the offense.

53. If any of the property described above, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty, the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

All pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).

FORFEITURE ALLEGATION III

1. The allegations contained in Count Three of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 982(a)(1).

2. Pursuant to Title 18, United States Code, Section 982(a)(1), upon conviction of an offense in violation of Title 18, United States Code, Section 1956, the defendant, JOHAN ANDERS GUDMUNDS, a/k/a "Mafi", a/k/a "Crim", a/k/a "Synthet!c", shall forfeit to the United States of America any property, real or personal, involved in such offense, and any property traceable to such property. The property to be forfeited includes, but is not limited to, the following: the domain darkode.com.

3. If any of the property described above, as a result of any act or omission of the defendant[s]:


- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty, the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18,

United States Code, Section 982(b)(1) and Title 28, United States Code, Section 2461(c).

All pursuant to Title 18, United States Code, Section 982(a)(1) and 28 U.S.C. § 2461(c).

A True Bill,


FOREPERSON


DAVID J. HICKTON
United States Attorney
PA ID No. 34524