

Unsealed on 9/25/22
SSB
SEALED **FILED**
2019 NOV 20 P 4:46

CLERK OF DISTRICT COURT
DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
CLERK OF DISTRICT COURT
DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
January 2019 Grand Jury

19CR4748W

1 UNITED STATES OF AMERICA,
2
3
4
5
6
7
8 Plaintiff,

9 v.

10 DENIS ALEKSANDROVICH EMELYANTSEV,
11 aka "Denis Kloster,"
12 aka "Stanx,"
13 Defendant.

Case No. _____

I N D I C T M E N T

Title 18, U.S.C., Secs. 371,
1030(a)(5)(A), 1030(c)(4)(B)(i)
and 1030(c)(4)(A)(i)(I) and (VI) -
Conspiracy to Damage Protected
Computers; Title 18, U.S.C.,
Secs. 1030(a)(5)(A) and
1030(c)(4)(B) - Damage Protected
Computers; Title 18, U.S.C.,
Sec. 3559(g)(1) - False
Registration of Domain Name;
Title 18, U.S.C.,
Secs. 982(a)(2)(B) and 982(b)(1),
and 1030(i) and (j) - Criminal
Forfeiture

17 The grand jury charges:

18 Count 1

19 Object of the Conspiracy

20 1. From a date unknown to the grand jury, but no later than
21 June 27, 2015, up to and including November 20, 2019, within the Southern
22 District of California, and elsewhere, defendant DENIS ALEKSANDROVICH
23 EMELYANTSEV, aka "Denis Kloster," aka "Stanx," did knowingly and
24 intentionally conspire with other persons known and unknown to the grand
25 jury to commit an offense against the United States, that is, to
26 knowingly cause the transmission of a program, information, code, and
27 command, and, as a result of such conduct, intentionally cause damage
28 without authorization to a protected computer, and the offense caused

duf

1 damage affecting 10 or more protected computers during a one-year period
2 and loss to at least one person during a one-year period resulting from
3 a related course of conduct affecting one or more other protected
4 computers aggregating at least \$5,000 in value, in violation of Title 18,
5 United States Code, Sections 371, 1030(a)(5)(A), 1030(c)(4)(B)(i), and
6 1030(c)(4)(A)(i)(I) and (VI).

7 **Manner and Means**

8 2. Members of the conspiracy used the following manner and means,
9 among others, to accomplish the objects of the conspiracy:

10 i. Conspirators created and operated a botnet (the Rsocks
11 botnet), which was a group of compromised computers
12 connected in a coordinated fashion and typically used
13 for malicious purposes.

14 ii. In order to create the Rsocks botnet, conspirators
15 targeted Internet of Things (IoT) devices. IoT devices
16 included a broad range of devices - including smart
17 garage door openers, biometric time clocks, and audio-
18 video transcoding devices - that were connected to and
19 could communicate over the Internet. Because they were
20 connected to the Internet, these devices were assigned
21 Internet Protocol (IP) addresses. An IP address is the
22 unique series of numbers assigned to all computing
23 devices connected to the Internet.

24 iii. Conspirators developed and used computer code to
25 (a) identify IoT devices; (b) gain unauthorized access
26 to those devices by guessing the login information
27 (known as "brute forcing" or "bruting"); and
28 (c) maintain a persistent connection to the

1 7. On December 16, 2016, defendant DENIS ALEKSANDROVICH
2 EMELYANTSEV sent an email to an online forum to inquire about advertising
3 the botnet. Defendant DENIS ALEKSANDROVICH EMELYANTSEV agreed to pay
4 \$500 per month to advertise the botnet.

5 8. On October 14, 2017, having gained unauthorized access to a
6 digital audio server (IoT device) located in San Diego, California, and
7 belonging to Victim A (an educational institution located in San Diego,
8 California), defendant DENIS ALEKSANDROVICH EMELYANTSEV and conspirators
9 maintained unauthorized access to that device.

10 9. On October 23, 2017, defendant DENIS ALEKSANDROVICH
11 EMELYANTSEV and conspirators sent a program, information, code, or
12 command and thereby gained unauthorized access and caused damage to a
13 computer in San Diego, California.

14 **Special Allegation**

15 10. In furtherance of the Conspiracy, and as set forth in
16 paragraphs 1 through 13, the conspirators knowingly falsely registered
17 a domain name and knowingly used that domain name in the course of
18 committing an offense, namely, the conspirators registered the domain
19 rsocks.net with false names and addresses, and used that domain in the
20 course of committing the felony offense charged in Count One.

21 All in violation of Title 18, United States Code, Sections 371
22 and 3559(g)(1).

23 **Count 2**

24 11. From a date unknown to the grand jury, but no later than
25 June 27, 2015, up to and including November 20, 2019, within the Southern
26 District of California, and elsewhere, defendant DENIS ALEKSANDROVICH
27 EMELYANTSEV, aka "Denis Kloster," aka "Stanx," knowingly caused the
28 transmission of a program, information, code, and command, and, as a

1 result of such conduct, intentionally caused damage without
2 authorization to a protected computer, and the offense caused damage
3 affecting 10 or more protected computers during a one-year period and
4 loss to at least one person during a one-year period resulting from a
5 related course of conduct affecting one or more protected computers
6 aggregating at least \$5,000 in value, to wit, within a one-year period,
7 EMELYANTSEV accessed without authorization 10 or more computers in the
8 Southern District of California, and elsewhere and sold access to those
9 computers without authorization as part of a botnet and thereby caused
10 a loss of at least \$5,000, in violation of Title 18, United States Code,
11 Section 1030(a)(5)(A), (c)(4)(B)(i), and (c)(4)(A)(i)(I) and (VI).

12 12. In furtherance of this offense, defendant DENIS ALEKSANDROVICH
13 EMELYANTSEV, aka "Denis Kloster," aka "Stanx," knowingly falsely
14 registered a domain name and knowingly used that domain name in the
15 course of committing the offense, namely, EMELYANTSEV registered the
16 domain rsocks.net with false names and addresses, and used that domain
17 in the course of committing the felony offense charged in Count Two, in
18 violation of Title 18, United States Code, Section 3559(g)(1).

19 Criminal Forfeiture

20 13. Upon conviction of one or more of the offenses alleged in this
21 indictment, defendant DENIS ALEKSANDROVICH EMELYANTSEV, aka "Denis
22 Kloster," aka "Stanx," shall forfeit to the United States of America,
23 pursuant to Title 18, United States Code, Section 982(a)(2)(B), any
24 property constituting or derived from proceeds the defendants obtained
25 directly or indirectly as a result of the offenses, and, pursuant to
26 Title 18, United States Code, Section 1030(i) and (j), defendants'
27 interest in any personal property that was used or intended to be used
28 to commit or to facilitate the commission of such violations and any

1 property, real or personal, constituting or derived from, any proceeds
2 that such person obtained, directly or indirectly, as a result of such
3 violations.

4 14. In the event that any of the property described above, as a
5 result of any act or omission of the defendant:

- 6 a. cannot be located upon the exercise of due diligence;
7 b. has been transferred or sold to, or deposited with, a
8 third party;
9 c. has been placed beyond the jurisdiction of the court;
10 d. has been substantially diminished in value; or
11 e. has been commingled with other property which cannot be
12 divided without difficulty,

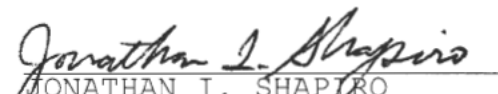
13 the United States of America shall be entitled to forfeit substitute
14 property pursuant to Title 21, United States Code, Section 853(p), as
15 incorporated by Title 18, United States Code, Sections 982(b)(1)
16 and 1030(i)(2).

17 All in violation of Title 18, United States Code, Sections 982(a)(2)(B),
18 982(b)(1), and 1030(i) and (j).

19 DATED: November 20, 2019.

20
21
22 ROBERT S. BREWER, JR.
23 United States Attorney

24 By:


25 JONATHAN I. SHAPIRO
Assistant U.S. Attorney

26 RYAN K. DICKEY
27 Senior Counsel
Computer Crime & Intellectual Property Section
28 United States Department of Justice