

Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington

March 18, 2021

WILLIAM M. McCOOL, Clerk

By [Signature] Deputy

UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff

NO. CR21-048 RAJ

INDICTMENT

v.

TILL KOTTMANN, a/k/a, "deletescape," a/k/a, "tillie crimew," a/k/a, Tillie Kottmann, Defendant.

The Grand Jury charges that:

COUNT 1

(Conspiracy to Commit Computer Fraud and Abuse)

A. Overview

1. The defendant, TILL KOTTMANN, known by the monikers "deletescape" and "tillie crimew," among others, is a Swiss national who resides in or around Lucerne, Switzerland.

2. KOTTMANN is a member of a group of cybercriminal actors engaged in the hacking of protected computers of corporate and government entities and the theft

1 and public dissemination of confidential and proprietary information, including source
2 code and internal user data.

3 3. KOTTMANN conducted intrusion activity, using a variety of techniques,
4 and predominantly has targeted “git” and other source code repositories belonging to
5 private companies and public sector entities in the United States and elsewhere. “Git”
6 refers to a distributed version-control system for tracking changes in source code during
7 software development in containers called repositories. It is designed for coordinating
8 work among programmers, but it can be used to track changes in any set of files.

9 KOTTMANN copied or cloned source code, files, and other confidential and proprietary
10 information, which at times included administrative credentials, access keys, and other
11 means of further system or network access. KOTTMANN then used such means of
12 access to further infiltrate the internal infrastructure of victims and copy additional files,
13 records and information.

14 4. KOTTMANN further published, or “leaked,” victim data obtained through
15 KOTTMANN’s and other actors’ hacking conduct. Since at least 2019, KOTTMANN
16 operated the website <http://git.rip> (“git.rip website”), which promotes, supports, and
17 facilitates data leaks by publishing databases of “Confidential & Proprietary” files and
18 information of corporate and government entities. KOTTMANN similarly promoted and
19 disseminated hacked material through the messaging service Telegram, specifically, in an
20 associated channel called “ExConfidential,” and through a foreign-based file-sharing
21 service. Through such various means, as of March 2021, KOTTMANN has hacked
22 dozens of companies and government agencies and purportedly has published internal
23 files and records of more than 100 entities for public review and download.

24 5. In order to solicit and recruit the assistance, participation, and collaboration
25 of others, to drive traffic to the actors’ data leak sites, and to promote an anti-intellectual-
26 property ideology, KOTTMANN has utilized various online platforms and services.
27 KOTTMANN also has invited contact from journalists and provided interviews to media
28 outlets to promote hacking conduct, data leaks, and ultimately KOTTMANN.

1 | **B. Offense**

2 | 6. Beginning at a time unknown, but no later than November 2019, and
3 | continuing to March 2021, in King County, within the Western District of Washington,
4 | and elsewhere, the defendant, TILL KOTTMANN, and others known and unknown to
5 | the Grand Jury, did knowingly and willfully combine, conspire, confederate and agree
6 | together to commit offenses against the United States, to wit: to intentionally access
7 | computers without authorization, and thereby obtain information from protected
8 | computers, and to commit the offense in furtherance of a criminal and tortious act in
9 | violation of the Constitution and the laws of the United States and the laws of a state,
10 | including the State of Washington, and to obtain information with a value exceeding
11 | \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and
12 | (c)(2)(B)(ii) and (iii).

13 | **C. Objects of the Conspiracy**

14 | 7. The objects of the conspiracy included, through use of deceptive and
15 | fraudulent means, gaining access to protected computers without authorization and
16 | stealing confidential and proprietary files and information stored thereon. The objects of
17 | the conspiracy further included sharing and disseminating stolen confidential and
18 | proprietary files and information, all with the purpose and intent to deprive victims of the
19 | exclusive control and ownership of their property.

20 | **D. Manner and Means of the Conspiracy**

21 | 8. The manner and means used to accomplish the conspiracy included the
22 | following:

23 | a. KOTTMANN, and others, accessed protected computers, including
24 | “git” and source code repositories as well as internal infrastructure, through use of stolen
25 | access keys, credentials and exploits allowing expansive permissions to new users. In
26 | doing so, the conspirators falsely and fraudulently represented that they had authorization
27 | to access the protected computers, to access the data stored thereon, and to use legitimate
28 | access keys and credentials, when in fact they were not authorized to do so.

1 b. KOTTMANN, and others, accessed, without authorization,
2 repositories and other accounts to survey the content and to copy and clone databases to
3 servers under the custody or control of the conspiracy. The servers used by the
4 conspiracy to store stolen data were located in one or more foreign countries and were
5 hosted by KOTTMANN and by foreign-based service providers.

6 c. KOTTMANN, and others, solicited others for access to stolen and
7 hacked data, including confidential and proprietary source code, files, and information.

8 d. KOTTMANN, and others, in order to perpetuate, advance, and
9 facilitate the scheme, shared with one another and publicly posted, or leaked, copies of
10 the stolen data, databases, and other records and information through a variety of
11 channels, including the git.rip website, the “ExConfidential” Telegram channel, and a
12 foreign-based file-sharing service, which data and other information were distributed to
13 and in fact were accessed from the Western District of Washington, and elsewhere.

14 e. KOTTMANN, and others, in order to perpetuate, advance, and
15 facilitate the scheme, promoted the git.rip website and their associated hacking and data
16 leak efforts and recruited others into their exploits through use of multiple online
17 accounts, including Twitter and other social media and messaging platforms, and through
18 interviews and information provided to media outlets.

19 f. KOTTMANN, and others, further promoted their conduct, and
20 obtained financial benefit, by designing and selling clothing and paraphernalia related to
21 computer hacking activity and anti-intellectual-property ideology.

22 **E. Overt Acts**

23 9. In furtherance of the conspiracy, and to achieve the objects thereof, the
24 defendant, and others known and unknown, did commit and cause to be committed the
25 following overt acts, among others, in the Western District of Washington and elsewhere:

26 a. On about November 18, 2019, KOTTMANN registered the git.rip
27 domain at a U.S.-based domain registrar.

28 b. On about December 20, 2019, KOTTMANN accessed an account at

1 a U.S.-based cloud infrastructure provider, which KOTTMANN used to host the git.rip
2 website.

3 c. On about February 14, 2020, KOTTMANN accessed one or more
4 protected computers, without authorization, and copied files of a manufacturer of security
5 devices based in the Western District of Washington (“Victim-1”). On or about the same
6 date, KOTTMANN posted Victim-1’s data, which included confidential and proprietary
7 source code, on the git.rip website.

8 d. On about April 15, 2020, KOTTMANN accessed one or more
9 protected computers, without authorization, and copied files of a manufacturer of tactical
10 equipment (“Victim-2”). On or about the same date, KOTTMANN posted Victim-2’s
11 data, which included confidential and proprietary source code, on the git.rip website.

12 c. On about April 28, 2020, as on numerous other occasions,
13 KOTTMANN accessed the administrative account related to the git.rip website at the
14 U.S.-based cloud infrastructure provider.

15 f. On about May 17, 2020, KOTTMANN sent a message (“tweeted”)
16 from the Twitter account with the username @deletescape, “i love helping companies
17 open source their code.”

18 g. On about July 22, 2020, KOTTMANN tweeted from the
19 @deletescape Twitter account a message soliciting others with “access to any confidential
20 info, documents, binaries or source code” to contact KOTTMANN using an encrypted
21 messaging service. On the same date, KOTTMANN sent a similar solicitation, using an
22 online messaging application.

23 h. On about August 6, 2020, KOTTMANN published technical
24 material, code, and documents related to a microchip and processor manufacturer
25 (“Victim-3”). KOTTMANN later tweeted from the @deletescape Twitter account about
26 the leak of Victim-3’s files, which he claimed to have obtained through “an anonymous
27 source who breached them this year.”

28 i. On about August 10, 2020, KOTTMANN registered an account at

1 | Twitter, with username @antiproprietary, after Twitter suspended the @deletescape
2 | account for violations of user terms of service. On or about the same date, KOTTMANN
3 | tweeted from the @antiproprietary Twitter account soliciting access to confidential
4 | information, including source code, for public dissemination without authorization.

5 | j. On about August 15, 2020, KOTTMANN accessed a protected
6 | computer, located in the State of Washington, without authorization, and copied source
7 | code repositories related to the Washington State Department of Transportation (“Victim-
8 | 4”). On the same date, KOTTMANN sent a message, using an online messaging
9 | application, regarding the hack of Victim-4 and a description of the data obtained, which
10 | included source code for web applications.

11 | k. On about August 15, 2020, KOTTMANN accessed a protected
12 | computer, without authorization, of a government contractor and copied files related to a
13 | U.S. government agency (“Victim-5”). On the same date, KOTTMANN sent a message,
14 | using an online messaging application, regarding the hack and a description of Victim-5
15 | and the data obtained.

16 | l. On about August 15, 2020, KOTTMANN, directly or indirectly,
17 | published additional victim data to the git.rip website, including source code related to
18 | Victim-4 and Victim-5.

19 | m. On about October 21, 2020, KOTTMANN tweeted from the
20 | @antiproprietary Twitter account that “stealing and releasing” corporate data and “using
21 | up corporate resources,” including “by means of ransom,” was “the morally correct thing
22 | to do.”

23 | n. On about November 8, 2020, KOTTMANN accessed a protected
24 | computer, without authorization, and copied source code repositories related to an
25 | information technology services company based in the State of Washington (“Victim-6”).
26 | On or about the same date, KOTTMANN sent a message, using an online messaging
27 | application, regarding the hack of Victim-6 and a description of the data obtained. On or
28 | about the same date, KOTTMANN, directly or indirectly, posted Victim-6’s data, which

1 included confidential and proprietary source code, on the git.rip website.

2 o. On about December 7, 2020, KOTTMANN tweeted from the
3 @antiproprietary Twitter account images of hacking-inspired clothing KOTTMANN had
4 designed for sale and a link to an online store.

5 p. On about January 4, 2021, KOTTMANN accessed a protected
6 computer, without authorization, and copied source code repositories related to an
7 automobile manufacturer (“Victim-7”). On or about the same date, KOTTMANN sent a
8 message, using an online messaging application, regarding the hack of Victim-7 and a
9 description of the data obtained, including multiple git repositories.

10 q. On about January 7, 2021, KOTTMANN sent a message, using an
11 online messaging application, regarding the hack of an investment platform (“Victim-8”)
12 and a description of the data obtained, including source code, transaction records, and
13 access keys to Victim-8’s cloud-storage infrastructure.

14 r. On about January 15, 2021, KOTTMANN provided a presentation
15 distributed by livestream over online platforms, in which KOTTMANN promoted the
16 scheme by offering details related to computer hacking activity KOTTMANN conducted,
17 including the methodology and results of the hacks of Victim-7 and Victim-8.

18 s. On about February 19, 2021, KOTTMANN registered an account at
19 Twitter, with username @nyancrimew, after Twitter suspended the @antiproprietary
20 account for violations of user terms of service.

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

22 **COUNT 2**

23 **(Conspiracy to Commit Wire Fraud)**

24 10. The allegations set forth in Paragraphs 1 through 9 of this Indictment are
25 re-alleged and incorporated as if fully set forth herein.

26 **A. Offense**

27 11. Beginning at a time unknown, but no later than November 2019, and
28 continuing to March 2021, in King County, within the Western District of Washington,

1 and elsewhere, the defendant, TILL KOTTMANN, and others known and unknown to
2 the Grand Jury, did knowingly and willfully combine, conspire, confederate and agree
3 together to commit an offense against the United States, to wit: to knowingly and
4 willfully devise and execute and attempt to execute, a scheme and artifice to defraud, and
5 for obtaining money and property by means of materially false and fraudulent pretenses,
6 representations, and promises; and in executing and attempting to execute this scheme
7 and artifice, to knowingly cause to be transmitted in interstate and foreign commerce, by
8 means of wire communication, certain signs, signals and sounds as further described
9 below, in violation of Title 18, United States Code, Section 1343.

10 **B. Objects of the Conspiracy**

11 12. The objects of the conspiracy are set forth in Paragraph 7 of this Indictment
12 and are re-alleged and incorporated as if fully set forth herein. The objects of the
13 conspiracy further involved obtaining intellectual property, including proprietary source
14 code and information, and depriving public and private entities of the confidentiality and
15 exclusive use of information stored on their protected computer networks.

16 **C. Manner and Means of the Conspiracy**

17 13. The manner and means used to accomplish the conspiracy are forth in
18 Paragraph 8 of this Indictment and are re-alleged and incorporated as if fully set forth
19 herein.

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

21 **COUNTS 3 - 7**

22 **(Wire Fraud)**

23 14. The allegations set forth in Paragraphs 1 through 13 of this Indictment are
24 re-alleged and incorporated as if fully set forth herein.

25 **A. Scheme and Artifice to Defraud**

26 15. Beginning at a time unknown, but no later than November 2019, and
27 continuing to March 2021, in King County, within the Western District of Washington,
28 and elsewhere, the defendant, TILL KOTTMANN, and others known and unknown to

1 the Grand Jury, devised and intended to devise a scheme and artifice to defraud and to
 2 obtain money and property by means of materially false and fraudulent pretenses,
 3 representations and promises.

4 **B. Manner and Means**

5 16. The manner and means of the scheme and artifice to defraud are set forth in
 6 Paragraph 8 of this Indictment and are re-alleged and incorporated as if fully set forth
 7 herein.

8 **C. Execution of the Scheme and Artifice to Defraud**

9 17. On or about the dates set forth below, in King County, within the Western
 10 District of Washington, and elsewhere, the defendant, and others known and unknown to
 11 the Grand Jury, having devised a scheme and artifice to defraud, and to obtain money and
 12 property by means of materially false and fraudulent pretenses, representations, and
 13 promises, did knowingly transmit and cause to be transmitted writings, signs, signals,
 14 pictures, and sounds, for the purpose of executing such scheme, by means of wire
 15 communication in interstate and foreign commerce, including the following
 16 transmissions, each of which constitutes a separate count of this Indictment:

Count	Date(s)	Wire Transmission
3	7/22/2020	Message sent by KOTTMANN, from outside the State of Washington, soliciting access to confidential information, including source code, for public dissemination, received in the State of Washington
4	8/15/2020	Access by KOTTMANN, from outside the State of Washington, to data of Victim-4, in the State of Washington
5	8/15/2020	Message sent by KOTTMANN, from outside the State of Washington, about data hacked from Victim-4, received in the State of Washington
6	1/4/2021	Message sent by KOTTMANN, from outside the State of Washington, about data hacked from Victim-7, received in the State of Washington
7	1/15/2021	Presentation by KOTTMANN, from outside the State of Washington, streamed online to devices located in the State of Washington

1 All in violation of Title 18, United States Code, Sections 1343 and 2.

2 **COUNT 8**

3 **(Aggravated Identity Theft)**

4 18. The allegations set forth in Paragraphs 1 through 17 of this Indictment are
5 re-alleged and incorporated as if fully set forth herein.

6 19. On or about April 15, 2020, in King County, within the Western District of
7 Washington, and elsewhere, the defendant, TILL KOTTMANN, did knowingly transfer,
8 possess, and use, without lawful authority, a means of identification of another person, to
9 wit: the login credentials of an employee of Victim-2, initials R.D., a real person, during
10 and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is,
11 conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349, as charged in Count 2,
12 knowing that the means of identification belonged to another actual person.

13 20. The grand jury alleges that this crime was committed during, and in
14 furtherance of, the Conspiracy charged in Count 2.

15 All in violation of Title 18, United States Code, Sections 1028A(a) and 2.

16 **FORFEITURE ALLEGATION**

17 21. All of the allegations contained in this Indictment are hereby realleged and
18 incorporated by reference for the purpose of alleging forfeiture.

19 22. Upon conviction of the offense charged in Count 1, the defendant shall
20 forfeit to the United States any property that constitutes or is traceable to proceeds the
21 defendant obtained from the commission of the offense, including but not limited to a
22 sum of money reflecting the proceeds the relevant defendant obtained from the offense,
23 as well as any personal property that facilitated the offense. All such property is
24 forfeitable pursuant to Title 18, United States Code, Section 982(a)(2)(B), and Title 18,
25 United States Code, Section 1030(i).

26 23. Upon conviction of any of the offenses charged in Counts 2 through 8, the
27 defendant shall forfeit to the United States any property, real or personal, which
28 constitutes or is derived from proceeds traceable to such offenses, including but not

1 | limited to a judgment for a sum of money representing the property described in this
2 | section. All such property is forfeitable pursuant to pursuant to Title 18, United States
3 | Code, Section 981(a)(1)(C) (by way of Title 28, United States Code, Section 2461(c)).

4 | ***(Substitute Assets)***

5 | 24. If any of the property described above, as a result of any act or omission of
6 | the defendant:

- 7 | a. cannot be located upon the exercise of due diligencc;
- 8 | b. has been transferred or sold to, or deposited with, a 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 divided
12 | without difficulty,

13 | //

14 | //

15 |

16 |

17 |

18 |

19 |

20 |

21 |

22 |

23 |

24 |

25 |

26 |

27 |

28 |

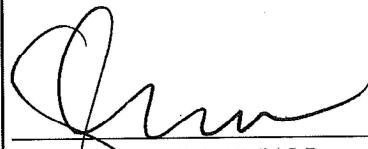
1 the United States of America shall be entitled to forfeiture of substitute property pursuant
2 to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States
3 Code, Section 2461(c).

4 A TRUE BILL:


5
6 DATED: 3/18/21

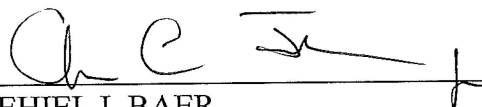
7 *Signature of Foreperson redacted pursuant*
8 *to the policy of the Judicial Conference of*
9 *the United States.*

10 _____
11 FOREPERSON

12 
13 _____
14 TESSA M. GORMAN
15 Acting United States Attorney

16 
17 _____
18 ANDREW C. FRIEDMAN
19 Assistant United States Attorney

20 
21 _____
22 STEVEN T. MASADA
23 Assistant United States Attorney

24 
25 _____
26 JEHIEL I. BAER
27 Assistant United States Attorney
28