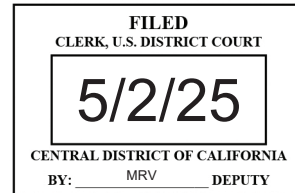




U.S. Department of JUSTICE

The Department of Justice is posting this court document as a courtesy to the public. An official copy of this court document can be obtained (irrespective of any markings that may indicate that the document was filed under seal or otherwise marked as not available for public dissemination) on the Public Access to Court Electronic Records website at <https://pacer.uscourts.gov>. In some cases, the Department may have edited the document to redact personally identifiable information (PII) such as addresses, phone numbers, bank account numbers, or similar information, and to make the document accessible under Section 508 of the Rehabilitation Act of 1973, which requires federal agencies to make electronic information accessible to people with disabilities.



UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

January 2025 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

RUSTAM RAFAILEVICH GALLYAMOV,
aka "Cortes,"
aka "Tomperz,"
aka "Chuck,"

Defendant.

CR 2:25-cr-00340-SB

I N D I C T M E N T

[18 U.S.C. § 371: Conspiracy; 18
U.S.C. § 1349: Conspiracy to
Commit Wire Fraud; 18 U.S.C. §§
981(a)(1)(C), 982, and 28 U.S.C. §
2461(c): Criminal Forfeiture]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS AND DEFINITIONS

At all times relevant to this Indictment:

A. THE DEFENDANT & THE CONSPIRACY

1. Defendant RUSTAM RAFAILEVICH GALLYAMOV, also known as ("aka") "Cortes," aka "Tomperz," aka "Chuck," ("GALLYAMOV") whose photograph is attached as Exhibit A, was a resident of Russia.

2. Qakbot (or Qbot) was malicious computer software developed, deployed, and controlled since 2008 by members of a cybercriminal conspiracy led by defendant GALLYAMOV. From at least 2019, defendant GALLYAMOV and his coconspirators infected hundreds of thousands of

1 victim computers around the world with the Qakbot malware, thereby
2 gaining unauthorized access to and control of those computers. Using
3 this access, defendant GALLYAMOV and his coconspirators further
4 infected victim computers with ransomware, including Prolock,
5 Doppelpaymer, Egregor, REvil, Conti, Name Locker, Black Basta, and
6 Cactus. Sometimes, defendant GALLYAMOV and his coconspirators gained
7 access to victim computers by means other than the Qakbot malware.
8 In those instances, victim computers were also infected with
9 ransomware. Ransomware victims were then extorted by defendant
10 GALLYAMOV and his coconspirators to pay ransoms to regain access to
11 and/or prevent the dissemination of their private data. Defendant
12 GALLYAMOV and his coconspirators received a portion of any ransom
13 paid.

14 B. QAKBOT'S VICTIMS

15 3. The "Los Angeles Dental Office" was located in the Central
16 District of California.

17 4. The "Nebraska Technology Company" was located in Nebraska.

18 5. The "Wisconsin Manufacturer" was located in Wisconsin.

19 6. The "Canadian Real Estate Company" was located in Canada.

20 7. The "Wisconsin Marketing Company" was located in Wisconsin.

21 8. The "Tennessee Music Company" was located in Tennessee.

22 9. The "Colorado Communications Company" was located in
23 Colorado.

24 10. The "Pennsylvania Technology Company" was located in
25 Pennsylvania.

26 11. The "Maryland Insurance Company" was located in Maryland.

1 C. DEFINITIONS

2 12. "Malware" is malicious computer software intended to cause
3 a victim computer to behave in a manner inconsistent with the
4 intention of the owner or user of the victim computer, usually
5 unbeknownst to that person. Qakbot was malware developed, deployed,
6 and controlled by defendant GALLYAMOV and his coconspirators.

7 13. "Command and control" or "C2" devices are computers which
8 communicate with infected victim computers to send and receive data
9 and commands.

10 14. A "botnet" is a network of computers (each a "bot") that
11 have been infected with malware and are being controlled as a group.
12 Botnets are typically controlled through several tiers of C2 devices.
13 Computers infected with the Qakbot malware became part of the Qakbot
14 botnet and were controlled by defendant GALLYAMOV and his
15 coconspirators.

16 15. "Ransomware" is a type of malware that infects a victim
17 computer and encrypts some or all of the data or files on the
18 computer. Ransomware is typically deployed by cybercriminals who
19 then demand that the victim pay a ransom in order to decrypt and
20 recover the files, or in order to prevent further disclosure of files
21 that the cybercriminals stole before encrypting them. Defendant
22 GALLYAMOV and his coconspirators partnered with groups to deploy
23 ransomware, including Prolock, Doppelpaymer, Egregor, REvil, Conti,
24 Name Locker, Black Basta, and Cactus on compromised computers.

25 16. A "spam bomb attack" is a type of cyber attack that floods
26 a victim's inbox by using automated techniques to sign the victim up
27 for a large number of email subscriptions.

1 17. "Cryptocurrency" or "virtual currency" is a digital asset
2 designed to work as a medium of exchange that uses cryptography to
3 secure financial transactions, control the creation of additional
4 units of the currency, and verify and transfer assets. Bitcoin
5 ("BTC") is a popular type of virtual currency.

COUNT ONE

[18 U.S.C. § 371]

18. The Grand Jury re-alleges and incorporates paragraphs 1 through 17 of the Introductory Allegations and Definitions of this Indictment.

A. OBJECTS OF THE CONSPIRACY

19. Beginning on a date unknown to the Grand Jury, but no later than 2019, and continuing through at least May 2, 2025, in Los Angeles and Orange Counties, within the Central District of California, and elsewhere, defendant GALLYAMOV, together with others known and unknown to the Grand Jury, knowingly conspired:

a. to intentionally access computers without authorization and obtain information from protected computers, in violation of Title 18, United States Code, Section 1030(a)(2)(C), (c)(2)(B)(i)-(iii);

b. to knowingly and with intent to defraud access protected computers without authorization, and by means of such conduct further the intended fraud and obtain a thing of value, in violation of Title 18, United States Code, Section 1030(a)(4), (c)(3)(A);

c. to knowingly cause the transmission of programs, information, codes, and commands, and as a result of such conduct intentionally cause damage without authorization to protected computers, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI); and

d. to transmit in interstate and foreign commerce, with the intent to extort money and other things of value, a communication

1 containing (i) a threat to cause damage to a protected computer,
2 (ii) a threat to impair the confidentiality of information obtained
3 from a protected computer without authorization, and (iii) a demand
4 and request for money and other things of value in relation to damage
5 to a protected computer, where such damage was caused to facilitate
6 the extortion, in violation of Title 18, United States Code,
7 Section 1030(a)(7)(A)-(C), (c)(3)(A).

8 B. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE
9 ACCOMPLISHED

10 20. The objects of the conspiracy were to be accomplished, in
11 substance, as follows:

12 Qakbot Compromises

13 a. Defendant GALLYAMOV and coconspirators would develop
14 malware that could be transmitted to potential victims in order to
15 gain unauthorized access to the computers of the victims. Such
16 malware included the Qakbot malware.

17 b. Defendant GALLYAMOV and coconspirators would conceal
18 the malware within seemingly legitimate documents or links that they
19 distributed to victim computers primarily through malicious spam
20 email campaigns.

21 c. Through the Qakbot malware, defendant GALLYAMOV and
22 coconspirators would gain unauthorized access to victim computers and
23 make them part of the Qakbot botnet.

24 Spam Bombing Compromises

25 d. Defendant GALLYAMOV and coconspirators would research
26 potential ransomware victim companies and identify information
27 technology and administrative employees at those companies.

1 e. Defendant GALLYAMOV and coconspirators would launch
2 targeted spam bomb attacks at employees of victim companies and then
3 contact those employees, posing as information technology workers
4 tasked with remediating the spam bomb attacks.

5 f. Defendant GALLYAMOV and coconspirators would trick
6 employees of victim companies into executing malicious code or
7 otherwise providing access to company computers.

8 g. Defendant GALLYAMOV and coconspirators would gain
9 unauthorized access to victim computers.

10 Ransomware Deployment

11 h. After gaining unauthorized access to victim computers,
12 defendant GALLYAMOV and coconspirators would sell or provide access
13 to the compromised computers to coconspirator ransomware groups,
14 including Prolock, Doppelpaymer, Egregor, REvil, Conti, Name Locker,
15 Black Basta, and Cactus.

16 i. Coconspirator ransomware groups would deploy
17 ransomware on the victim computers, encrypting data on those
18 computers. They would also often steal data from those computers
19 before encrypting them.

20 j. Coconspirator ransomware groups would threaten victims
21 with destruction or release of data stolen from their computers and
22 would demand payment of a ransom by the victim to (i) unlock their
23 encrypted systems; and/or (ii) prevent dissemination of stolen data
24 from those systems.

25 k. When a victim paid a ransom, a percentage of that
26 ransom would be paid to defendant GALLYAMOV. The percentage paid
27 would vary, depending on the arrangement between defendant GALLYAMOV
28 and the particular ransomware group.

1 1. During the course of the conspiracy, defendant
2 GALLYAMOV and his coconspirators caused ransomware infections on
3 hundreds of victims in the United States and around the world.

4 C. OVERT ACTS

5 21. In furtherance of the conspiracy, and to accomplish its
6 objects, defendant GALLYAMOV, together with others known and unknown
7 to the Grand Jury, on or about the dates set forth below, committed
8 and caused to be committed various overt acts, in the Central
9 District of California and elsewhere, including but not limited to
10 the following:

11 Overt Act No. 1: On May 5, 2020, defendant GALLYAMOV caused a
12 Qakbot infection on a computer of the Los Angeles Dental Office.

13 Overt Act No. 2: On October 1, 2021, defendant GALLYAMOV
14 caused a Qakbot infection on a computer of the Nebraska Technology
15 Company that was thereafter the victim of a ransomware attack by
16 Conti.

17 Overt Act No. 3: On October 4, 2021, defendant GALLYAMOV
18 received 15.251732 BTC that represented his share of the ransom paid
19 by the Nebraska Technology Company for the Conti ransomware attack.

20 Overt Act No. 4: On December 7, 2021, defendant GALLYAMOV
21 caused a Qakbot infection on a computer of the Wisconsin Manufacturer
22 that was thereafter the victim of a ransomware attack by Conti.

23 Overt Act No. 5: On December 16, 2021, defendant GALLYAMOV
24 received 5.066 BTC that represented his share of the ransom paid by
25 the Wisconsin Manufacturer for the Conti ransomware attack.

26 Overt Act No. 6: On December 22, 2021, defendant GALLYAMOV
27 caused a Qakbot infection on a computer of the Canadian Real Estate
28

1 Company that was thereafter the victim of a ransomware attack by
2 Conti.

3 Overt Act No. 7: On January 25, 2022, defendant GALLYAMOV
4 received 2.277034 BTC that represented his share of the ransom paid
5 by the Canadian Real Estate Company for the Conti ransomware attack.

6 Overt Act No. 8: On April 27, 2022, defendant GALLYAMOV
7 caused a Qakbot infection on a computer of the Wisconsin Marketing
8 Company that was thereafter the victim of a ransomware attack by
9 Black Basta.

10 Overt Act No. 9: On May 12, 2022, defendant GALLYAMOV
11 received 3.9999865 BTC that represented his share of the ransom paid
12 by the Wisconsin Marketing Company for the Black Basta ransomware
13 attack.

14 Overt Act No. 10: On November 14, 2022, defendant GALLYAMOV
15 caused a Qakbot infection on a computer of the Tennessee Music
16 Company that was thereafter the victim of a ransomware attack by
17 Black Basta.

18 Overt Act No. 11: On December 20, 2022, defendant GALLYAMOV
19 received 19.1543 BTC that represented his share of the ransom paid by
20 the Tennessee Music Company for the Black Basta ransomware attack.

21 Overt Act No. 12: On February 22, 2023, defendant GALLYAMOV
22 caused a Qakbot infection on a computer of the Colorado
23 Communications Company that was thereafter the victim of a ransomware
24 attack by Black Basta.

25 Overt Act No. 13: On March 20, 2023, defendant GALLYAMOV
26 received 17.976 BTC that represented his share of the ransom paid by
27 the Colorado Communications Company for the Black Basta ransomware
28 attack.

1 Overt Act No. 14: On January 17, 2025, defendant GALLYAMOV
2 received 19.8142 BTC that represented his share of the ransom paid by
3 the Pennsylvania Technology Company for a Black Basta ransomware
4 attack.

5 Overt Act No. 15: On January 24, 2025, defendant GALLYAMOV
6 received a 9.417 BTC ransom payment from the Maryland Insurance
7 Company for a Cactus ransomware attack.

COUNT TWO

[18 U.S.C. § 1349]

22. The Grand Jury re-alleges and incorporates paragraphs 1 through 17 of the Introductory Allegations and Definitions of this Indictment.

A. OBJECT OF THE CONSPIRACY

23. Beginning on a date unknown to the Grand Jury, but no later than 2019, and continuing through at least May 2, 2025, in Los Angeles and Orange Counties, within the Central District of California, and elsewhere, defendant GALLYAMOV, together with others known and unknown to the Grand Jury, knowingly conspired to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

B. THE MANNER AND MEANS OF THE CONSPIRACY

24. The object of the conspiracy was to be accomplished, in substance, as follows:

a. The Grand Jury re-alleges and incorporates paragraphs 20.a through 20.1 of Section B of Count One of this Indictment.

C. OVERT ACTS

25. In furtherance of the conspiracy, and to accomplish its object, defendant GALLYAMOV, together with others known and unknown to the Grand Jury, on or about the dates set forth below, committed and caused to be committed various overt acts, in the Central District of California and elsewhere, including, but not limited to, the following:

Overt Act Nos. 1-15: The Grand Jury re-alleges and incorporates Overt Act Number 1 through Overt Act Number 15 of Section C of Count One of this Indictment here.

1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8

[18 U.S.C. § 981 (a) (1) (C) and 28 U.S.C. § 2461 (c)]

1. Pursuant to Rule 32.2 of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), in the event of the defendant's conviction of the offenses set forth in Count One of this Indictment.

2. The defendant, if so convicted, shall forfeit to the United States of America the following:

(a) all right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds traceable to the offenses; and

(b) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), the defendant, if so convicted, shall forfeit substitute property, up to the value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph or any portion thereof (a) cannot be located upon the exercise of due diligence; (b) has been transferred, 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 that cannot be divided without difficulty.

1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8

2

3
4
5
6
7
8

9.0

- 1
- 2
- 3

4
5
6

7
8
9
0
1
2
3
4
5
6

7


8

1 substantially diminished in value; or (e) has been commingled with
2 other property that cannot be divided without difficulty.

3
4 A TRUE BILL

5
6 /s/
7 Foreperson

8 BILAL A. ESSAYLI
9 United States Attorney

10 
11 DAVID T. RYAN
12 Assistant United States Attorney
Chief, National Security Division

13 KHALDOUN SHOBAKI
14 Assistant United States Attorney
Chief, Cyber & Intellectual
15 Property Crimes Section

16 LAUREN RESTREPO
Assistant United States Attorney
17 Deputy Chief, Cyber &
Intellectual Property Crimes
18 Section

19 JESSICA PECK
Senior Counsel
20 Computer Crime & Intellectual
Property Section

Exhibit A

RUSTAM RAFAILEVICH GALLYAMOV

aka "Cortes"

aka "Tomperz"

aka "Chuck"

