

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO

UNITED STATES OF AMERICA

v.

CASE NO. 1:23-MJ-00978

DENISS ZOLOTARJOVS,
a/k/a “Sforza_cesarini”

Defendant.

AFFIDAVIT

I, Megan Gaffney Painter, being duly sworn, hereby depose and state:

1. I am a citizen of the United States of America and a resident of the State of Ohio. From March 2013 to the present, I have been employed as an Assistant United States Attorney (“AUSA”), first in the United States Attorney’s Office for the Southern District of New York and now in the United States Attorney’s Office for the Southern District of Ohio. As an Assistant United States Attorney, my duties are to prosecute persons charged with criminal violations of the laws of the United States. During my practice as an Assistant United States Attorney, I have become knowledgeable about the criminal laws and procedures of the United States.

2. In the course of my official duties, I have become familiar with the charges and evidence in the case against DENISS ZOLOTARJOVS, also known as “Sforza_cesarini,” entitled *United States v. Deniss Zolotarjovs*, Case Number 1:23-MJ-00978, which arose out of an investigation by the Federal Bureau of Investigation

("FBI").

THE CHARGES AND RELEVANT UNITED STATES LAW

3. Under the laws of the United States, a criminal prosecution may be commenced by a criminal complaint, which is a charging document that alleges violations of the criminal laws of the United States. A criminal complaint is usually written by a law enforcement officer and must be made under oath before a federal Magistrate Judge. If the Magistrate Judge determines there is probable cause to believe that a federal crime was committed and the person accused committed it, the Magistrate Judge authorizes and signs an arrest warrant.

4. If Zolotarjovs's extradition to the United States is granted, another charging document, called an indictment, will be sought from a federal grand jury sitting in the Southern District of Ohio, unless Zolotarjovs waives indictment. If Zolotarjovs waives indictment, the United States Attorney for the Southern District of Ohio will issue a charging document called an information. The indictment or information, which would supersede the criminal complaint would only include the offenses as alleged in the criminal complaint and as set forth above.

5. On November 28, 2023, a Magistrate Judge in the Southern District of Ohio approved a complaint for Zolotarjovs, charging him with the crimes listed below:

Count	Crime	Statutory Citation	Maximum Penalty
One	Money Laundering Conspiracy	18 U.S.C. § 1956(h) ¹	20 years' imprisonment, \$500,000 fine or twice the value of the monetary instrument or funds involved, 3 years supervised release, \$100 special assessment
Two	Wire Fraud Conspiracy	18 U.S.C. § 1349	20 years' imprisonment, \$250,000 fine or twice the gross gain or loss, 3 years supervised release, \$100 special assessment
Three	Extortion Conspiracy	18 U.S.C. § 1951	20 years' imprisonment, \$250,000 fine or twice the gross gain or loss, 3 years supervised release, \$100 special assessment
Four	Extortion	18 U.S.C. § 1951	20 years' imprisonment, \$250,000 fine or twice the gross gain or loss, 3 years supervised release, \$100 special assessment

6. Based on the charges in the complaint, on November 28, 2023, the United States District Court for the Southern District of Ohio issued an arrest warrant for Zolotarjovs. I have obtained certified true and accurate copies of the November 28, 2023, complaint and arrest warrant from the Clerk of the Court and have attached them to this affidavit as **Exhibit A** and **Exhibit B**, respectively.

¹ As referenced throughout the document, 18 U.S.C § is Title 18, United States Code, Section.

7. The relevant portions of the statutes cited above are attached to this affidavit as **Exhibit C**. Each of these statutes was duly enacted and in force at the time the offenses were committed and at the time the complaint was authorized, and they remain in full force and effect. A violation of Counts One through Four constitute a felony under the laws of the United States.

8. Regarding Money Laundering Conspiracy, as charged in Count One of the complaint (18 U.S.C. § 1956(h)), the United States must prove: (1) two or more persons, in some way or manner, agreed to try to accomplish a common and unlawful plan to commit money laundering; and (2) Zolotarjovs knowingly became a member of the conspiracy with an intent to advance the conspiracy. A person may be a conspirator without knowing all the details of the unlawful plan or the names and identities of all the other alleged conspirators. If Zolotarjovs played only a minor part in the plan but had a general understanding of the unlawful purpose of the plan and willfully joined in the plan on at least one occasion, that's sufficient to find him guilty. But simply being present at the scene of an event or merely associating with certain people and discussing common goals and interests does not establish proof of a conspiracy. A person who doesn't know about a conspiracy but happens to act in a way that advances some purpose of one does not automatically become a conspirator.

9. Regarding Wire Fraud Conspiracy, as charged in Count Two of the complaint (18 U.S.C. § 1349), the United States must prove: (1) two or more persons,

in some way or manner, agreed to try to accomplish a common and unlawful plan to commit a wire fraud; and (2) Zolotarjovs knew the unlawful purpose of the plan and willfully joined it. A person may be a conspirator without knowing all the details of the unlawful plan or the names and identities of all the other alleged conspirators. If Zolotarjovs played only a minor part in the plan but had a general understanding of the unlawful purpose of the plan and willfully joined in the plan on at least one occasion, that's sufficient to find him guilty. But simply being present at the scene of an event or merely associating with certain people and discussing common goals and interests does not establish proof of a conspiracy. A person who doesn't know about a conspiracy but happens to act in a way that advances some purpose of one does not automatically become a conspirator.

10. Regarding Extortion Conspiracy, as charged in Count Three of the complaint (18 U.S.C. § 1951), the United States must prove: (1) two or more persons agreed to commit the substantive crime of extortion; and (2) Zolotarjovs knowingly and voluntarily joined the conspiracy. A person may be a conspirator without knowing all the details of the unlawful plan or the names and identities of all the other alleged conspirators. If Zolotarjovs played only a minor part in the plan but had a general understanding of the unlawful purpose of the plan and willfully joined in the plan on at least one occasion, that's sufficient to find him guilty. But simply being present at the scene of an event or merely associating with certain people and

discussing common goals and interests does not establish proof of a conspiracy. A person who doesn't know about a conspiracy but happens to act in a way that advances some purpose of one does not automatically become a conspirator.

11. Regarding Extortion, as charged in Count Four of the complaint (18 U.S.C. § 1951), the United States must prove: (1) Zolotarjovs knowingly obtained money or property from a victim; (2) Zolotarjovs did so by means of extortion by fear; (3) The victim consented to part with the money or property because of the extortion; (4) Zolotarjovs believed that the victim parted with the money or property because of the extortion; and (5) Zolotarjovs's conduct affected interstate commerce. Extortion means the wrongful use of fear to obtain money or property. Fear includes fear of economic loss, which includes fear of direct loss of money, fear of harm to future business operations, or fear of some loss of ability to compete in the marketplace in the future if the victim did not pay Zolotarjovs. The government must prove that the victim's fear was reasonable under the circumstances, but the government need not prove that Zolotarjovs actually intended to cause the harm threatened.

12. I have also included as part of **Exhibit C** the true and accurate text of 18 U.S.C. § 3282, which is the statute of limitations for the crimes charged in Count One through Four of the complaint. The statute of limitations requires that a defendant be formally charged within five years of the date on which the offense or offenses were

committed. Once an indictment has been filed in a federal district court, as with the charges against Pankov, the statute of limitations is tolled and no longer runs.

13. I have thoroughly reviewed the applicable statute of limitations for the crimes charged in Count One through Four of the complaint, and the prosecution of the charges in this case are not barred by the statute of limitations. Because the applicable statute of limitations is five years and the indictment, which charges criminal violations from August of 2021 through November of 2023, was filed on November 28, 2023, Zolotarjovs was formally charged within the prescribed five-year time period.

14. The United States will prove its case against Zolotarjovs through witness testimony and documentary evidence.

15. Zolotarjovs has not been tried or convicted of any offense charged in the complaint, nor has he been ordered to serve any sentence in connection with this case.

SUMMARY OF THE INVESTIGATION AND FACTS OF THE CASE

16. The FBI has been investigating a Russian-based cybercrime group known as “Karakurt,” among other names. Karakurt uses a variety of computer intrusion techniques to infiltrate victim computer systems, and steal data or encrypt computer systems. Karakurt then demands ransom payments from the victims, threatening to publish the victims’ data.

17. The FBI has identified Deniss Zolotarjovs as a member of Karakurt, through IP addresses, cryptocurrency accounts, and internal Karakurt chats, among other evidence. I have also attached to this affidavit as **Exhibit D** the original affidavit of Special Agent Connor Lentz. In his affidavit, Special Agent Lentz summarizes some of the evidence identifying Deniss Zolotarjovs as a member of Karakurt.

IDENTIFICATION

18. Zolotarjovs is a citizen of Latvia, born on August 27, 1990. A photograph of him is attached to the affidavit of Special Agent Lentz and is incorporated as part of this request.

CONCLUSION

19. I request that any items relevant to the charged offenses found in the Zolotarjovs's possession at the time of his arrest be delivered to the United States, if the extradition is granted.

20. Should Georgian authorities require supplementary information in order to grant the extradition, I ask for a reasonable time to provide such information.

21. This affidavit and the affidavit of Special Agent Lentz each were sworn to before a Magistrate Judge of the United States District Court for the Southern District of Ohio who is duly empowered to administer an oath for this purpose.


Megan Gaffney Painter
Assistant United States Attorney

Sworn to before me in Cincinnati, Ohio this 18th day of December, 2023.



HONORABLE KAREN L. LITKOVITZ
United States Magistrate Judge

EXHIBIT LIST

- | | |
|------------------|---|
| EXHIBIT A | Certified Copy of Complaint |
| EXHIBIT B | Certified Copy of Arrest Warrant |
| EXHIBIT C | Relevant Legal Provisions |
| EXHIBIT D | Affidavit of FBI Special Agent Connor Lentz |

AO 91 (Rev. 11/11) Criminal Complaint (modified by USAO for telephone or other reliable electronic means)

UNITED STATES DISTRICT COURT

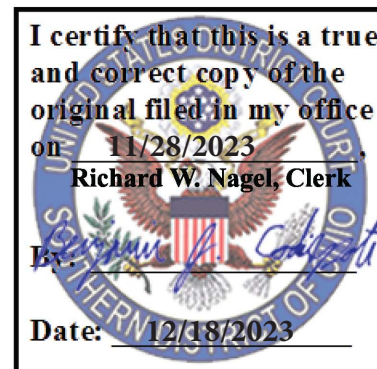
for the

Southern District of Ohio

United States of America)
v.)
DENISS ZOLOTARJOVS)
a/k/a "Sforza_cesarini")

Case No. 1:23-MJ-00978

Defendant(s)



CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of Aug. of 2021 through Nov. 2023 in the county of Ham'lt., Montg., Butler, Frank. in the Southern District of Ohio, the defendant(s) violated:

Table with 2 columns: Code Section and Offense Description. Rows include 18 U.S.C. Section 1956(h) Money Laundering Conspiracy, 18 U.S.C. Section 1349 Wire Fraud Conspiracy, 18 U.S.C. Section 1951 Hobbs Act Extortion Conspiracy, and 18 U.S.C. Section 1951 Hobbs Act Extortion.

This criminal complaint is based on these facts:

See affidavit

[X] Continued on the attached sheet.

Connor James Lentz
Complainant's signature
Special Agent Connor Lentz, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by FaceTime video conference (specify reliable electronic means).

Date: Nov 28, 2023

Stephanie K. Bowman
Judge's signature

City and state: Cincinnati, OH

Hon. Stephanie K. Bowman, U.S. Magistrate Judge
Printed name and title



**AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Connor J. Lentz, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since January of 2020. I am presently assigned to the Cincinnati Division Cyber Squad, which investigates, among other things, matters related to computer crimes. I am a certified FBI Digital Evidence Extraction Technician, I maintain a current cyber security certification from the Global Information Assurance Certification body, and have received additional FBI and commercial training from the SANS Institute regarding investigative skills as they relate to cybersecurity, information security, and examining the use of computers, computer networks, the internet, and digital communications. I am a Federal Law Enforcement officer who is engaged in enforcing criminal laws, including the offenses outlined here, and I am authorized by law to request a criminal complaint and arrest warrant.

2. This affidavit is made in support of an application for the issuance of a criminal complaint and arrest warrant charging DENISS ZOLOTARJOVS in violation of 18 U.S.C. § 1349 (Wire Fraud Conspiracy); 18 U.S.C. § 1956(h) (Money Laundering Conspiracy); and 18 U.S.C. § 1951 (Hobbs Act Extortion and Conspiracy). This affidavit is intended to show merely that there is sufficient probable cause for the requested arrest warrant and does not set forth all of my knowledge about this matter.

DETAILS OF THE INVESTIGATION

3. I have spoken with employees and representatives of a company located in Fairfield, Ohio (“Company-1”), as well as reviewed records provided by Company-1, and from those conversations and that review, I have learned, among other things, the following:

- a. On or about August 11, 2021, two employees of Company-1 received an email from the Google account Karakurtlair@gmail.com. The email stated, in substance and in part, that “Karakurt” had breached Company-1’s internal computer network and taken a large volume of private client data. The email instructed Company-1 to contact Karakurt by accessing a chat application via a Tor browser link listed in the email.
- b. Between on or about August 14, 2021 and September 10, 2021, representatives of Company-1 used the chat application via a Tor browser to communicate and negotiate with Karakurt. Over 100 messages were exchanged between Karakurt and Company-1 representatives, including messages from Karakurt containing samples of stolen Company-1 documents. Many of the documents contained large amounts of personally identifiable information and medical records of Company-1 clients, including Social Security numbers matched with names, addresses, dates of birth, home addresses, and lab results. Karakurt demanded a ransom payment of approximately \$650,000.00 and threatened to post publicly private victim data if the ransom was not paid. On or about September 10, 2021, Company-1 representatives negotiated the ransom payment down to \$250,000. Company-1 made the payment of 5.18 Bitcoin (BTC) to a cryptocurrency address provided by Karakurt.
- c. Company-1 and its representatives identified evidence that indicated unauthorized intrusion into Company-1’s internal computer network using known remote access protocol exploits, network device enumeration tools, executable tools permitting the intruders to persist in the network without being detected, and

various other known programs the intruders used to move throughout the network to discover, obtain, and exfiltrate protected files to external networks.

4. I have spoken with employees and representatives of a company located in Wichita, Kansas (“Company-2”), as well as reviewed records provided by Company-2, and from those conversations and that review, I have learned, among other things, the following:

- a. On or about November 21, 2021, employees of Company-2 received communications from Karakurt, including images of Company-2’s employees’ personally identifiable information, including passports, Social Security numbers, addresses, and financial information. Karakurt threatened to sell or publicly release the information if Company-2 refused to pay ransom.

5. I have spoken with employees and representatives of a company located in Boston, Massachusetts (“Company-3”), as well as reviewed records provided by Company-3, and from those conversations and that review, I have learned, among other things, the following:

- a. On or about April 1, 2022, employees of Company-3 received communications from Karakurt, including demands to contact Karakurt via the same Tor link provided to previous victims to prevent employee data from Company-3 from being published online. Company-3 informed the FBI it did not plan to pay any ransom demand.
- b. On or about July 1, 2022, employees of Company-3 received additional email communications from Karakurt stating Karakurt planned to release the data in a public auction by July 10, 2022 if Company-3 did not pay.

- c. On or about July 20, 2022, employees of Company-3 reported to FBI Cincinnati that Karakurt had published Company-3's stolen data on the Karakurt leaks website. Company-3 provided screenshots of the data and confirmed it was indeed Company-3 data believed to have been stolen by Karakurt during the initial incident in April of 2022.

6. On or about July 13, 2022, I reviewed the publicly-accessible website on which Karakurt published private data purportedly stolen from victim companies that refused to pay ransom. The website was found by visiting a Tor URL ("Tor URL-1"). Tor URL-1 resolved to the home webpage of the Karakurt public leaks website. On the home page, among other items, were four headings, "Auction," "Prereleasing," "Releasing," and "Released." "Auction" appeared to pertain to instructions for participating in auctions to purchase victims' stolen data prior to the data being posted publicly on the website. "Prereleasing" appeared to be a *name and shame*² listing of companies that had fallen victim to Karakurt and had not yet paid ransom demands. Publications under "Releasing" and "Released" headings appeared to be online repositories where the public could download data stolen from victims. Representatives of multiple Karakurt victims have reported to the FBI as having discovered their stolen data posted on the website.

7. I have spoken with employees and representatives of a company located in Beaumont, Texas ("Company-4"), as well as reviewed records provided by Company-4, and from those conversations and that review, I have learned, among other things, the following:

- a. On or about October 31, 2022, Company-4 reported to the FBI they had received communications from a threat actor called TommyLeaks indicating Company-4 had been hacked, and they had should negotiate with TommyLeaks to pay a

ransom to prevent sensitive data belonging to Company-4 from being published online.

- b. Based on my previous experience investigating Karakurt, this activity aligned closely with Karakurt's known tactics, techniques, and procedures.
- c. Company-4 also found login credentials to a file transfer protocol ("FTP") server in a software configuration file on one of Company-4's compromised devices. Analysis of the compromised device by an independent forensics firm determined unauthorized outgoing file transfers were made to the FTP server on or about October 24, 2022 between 2:30 PM and 9:30 PM UTC.
- d. On or about November 22, 2022, representatives of Company-4, of their own volition and without the advice, consent, or prior knowledge of the FBI, used the login credentials to login to the FTP server. Upon logging in, representatives of Company-4 viewed files they recognized as belonging to Company-4, as well as folders with names that appeared to belong to other unknown victim companies. Company-4 downloaded several of the files and verified they were indeed files that had been stolen from Company-4's computer network.

8. I have spoken with employees and representatives of a privately-held company headquartered in Springfield, Missouri with numerous locations throughout the Southern District of Ohio ("Company-5"), as well as reviewed records provided by Company-5, and from those conversations and that review, I have learned, among other things, the following:

- a. Company-5 suffered a Karakurt attack on or about November 18, 2021, during which employees of Company-5 received extortion demands from representatives of Karakurt to pay ransom in exchange for not publishing private company data.

- b. Company-5 paid a ransom of approximately \$1.37 million to a bitcoin wallet provided by Karakurt on or about January 7, 2022.
- c. Company-5 received notification from Karakurt that their data would be deleted upon receipt of the ransom payment, and would not be posted to Karakurt's public leaks website.
- d. Company-5 received certain promises from Karakurt that the matter would remain confidential between Company-5 and Karakurt following payment of ransom.

9. I have spoken with employees and representatives of a company located in Ft. Washington, Pennsylvania ("Company-6"), as well as reviewed records provided by Company-6, and from those conversation and that review, I have learned, among other things, the following:

- a. Company-6 received communications from TommyLeaks on or about September 8, 2022, in which TommyLeaks claimed to have breached Company-6's internal network and stolen approximately four terabytes of private data. TommyLeaks provided a Tor URL and an access code to negotiate terms of ransom payment.
- b. Over the following weeks, down-stream clients of Company-6, including a medical office in Springdale, Ohio, received email communications from representatives of TommyLeaks, in which the recipients of the email were informed their data was also taken during the attack, and that they should pressure representatives of Company-6 to negotiate for the deletion of data.

10. On or about October 26, 2022, a source who has provided accurate and reliable information to the FBI in the past provided a copy of communications from a private Rocket.Chat server located at a Tor URL ("Rocket.Chat Tor URL") previously unknown to

the FBI. The source also provided login credentials to the Rocket.Chat server. Review of the messages indicated the Rocket.Chat server hosted discussions conducted by members of the Karakurt group regarding Karakurt victims, some known to the FBI previously, and some previously unknown to the FBI.

11. On or about March 26, May 16, and August 28, 2023, the FBI's Technical Operations Unit ("TOU") executed search warrants signed by Magistrate Judges in the Northern District of Texas and Southern District of Ohio to search the servers accessible at the Rocket.Chat Tor URL believed to be hosting the Rocket.Chat used by Karakurt to discuss cybercriminal activity. The execution of those search warrants resulted in the collection of approximately 18,500 Rocket.Chat messages from a private Rocket.Chat server, with messages dating from as early as in or about April of 2022 through on or about August 28, 2023. The messages were primarily in the Russian Cyrillic language, and the FBI used a commercial machine translating service to review them in English.

12. I combined the messages provided by the CHS with the messages collected via the search warrants, and I have reviewed those messages, and from that review, I have learned the following:

- a. The user accounts, message contents, and configuration of the Rocket.Chat messages provided by the CHS matched those collected by the search warrants, except some of the messages in the earlier collections appeared to have been deleted in the later collections, and additional users appeared to have been added in later collections as well. Additionally, the contents of the "trash" folder appeared to have been emptied between collections.

- b. Virtually all of the conversations between participants of the private Rocket.Chat server related to the Karakurt ransomware group's cybercriminal activities.
- c. In late July and early August of 2022, the users discussed concerns regarding decreased returns on victimizations due to Karakurt's association with the Conti ransomware organization name, which had been sanctioned by the United States in the spring of 2022 due to Conti's close ties to Russian government activities. The users suggested the Karakurt group needed to further distance itself from Conti by again changing their group's name to TommyLeaks, Schoolboys Ransomware Gang, and Blockbit. Additionally, the users expressed disappointment that recent attacks using the TommyLeaks and Schoolboys Ransomware Gang names had already been publicly associated back to Karakurt and Conti.
- d. During on or about August 30, 2022 through October 29, 2022, users discussed Company-6. On or about September 22, 2022, user "dixie" messaged:

@sforza_cesarini I give you carte blanche for this case

Over the next four weeks, the user called Sforza_cesarini ("Sforza") discussed in depth to the Rocket.Chat participants the kind of data that was stolen from Company-6, and on numerous occasions shared what appeared to be medical records of Company-6 clients to the Rocket.Chat participants, as well as discussed how the group could leverage the cyberattack remediation company contracted by Company-6 to further extort Company-6. Additionally, on or about October 3, 2022, Sforza wrote the following message, in substance and in part, to the

Rocket.Chat, which appeared to be an extortion note addressed to patients of Company-6:

“Dear Sirs & Madams, On behalf of [Company-6], we are glad to inform you that their data has been breached. As a result you are getting this message containing your personal sensitive data. This is just a small proof that your personal data was obtained by third party members. We are strongly recommending you to contact [Company-6] nearest branches and resolve this matter as soon as possible. Otherwise your data may be sold in the dark market which results in more difficult consequences. Below you can find exactly your specific data. Once again, this is not a joke. You need to act ASAP.”

- e. On or about November 8, 2022, users discussed Company-5. Sforza referenced Company-5 when they sent a message, “Maybe heard about Company-5 on Karakurt... my handiwork”. Sforza again referenced Company-5 on or about November 10, 2022, in which they suggested to another user, “maybe we take Company-5 for a ride again”.
- f. Further analysis of Sforza’s communications indicated Sforza appeared to be responsible for conducting negotiations on Karakurt victim cold case extortions, as well as open-source research to identify phone numbers, emails, or other accounts at which victims could be contacted and pressured to either pay a ransom or re-enter a chat with the ransomware group. Some of the chats indicated Sforza’s efforts to revive cold cases were successful in extracting ransom payments. Sforza also discussed efforts to recruit paid journalists to publish news articles about victims in order to convince the victims to take Karakurt’s extortion

demands seriously. Sforza also sent a message with an encrypted communications instant messaging account ID (“IM ID-1”) to another user after discussing with the other user plans to communicate over Tox.

13. I conducted cryptocurrency analysis on the ransom payment made by Victim Company-1 and learned the following:

- a. The ransom payment of approximately 5.18 BTC was made on or about September 16, 2021 to a cryptocurrency cluster identified by commercial cryptocurrency tracing software as “Karakurt 1PLpQH3ntG”. Approximately 0.52 BTC, or approximately 10% of the initial ransom payment, was laundered across 12 cryptocurrency transactions between, on or about September 16, 2021 and September 28, 2021. Among the transactions was a September 27, 2023 0.52 BTC deposit made to a cryptocurrency tumbling service.¹ A commercial cryptocurrency tracing firm contracted by the FBI successfully traced the 0.52 BTC through the tumbling service, which revealed the 0.52 BTC reemerged from the tumbling service on or about September 28, 2021 via seven deposits of approximately 0.1 BTC or less into a never previously-used Bitcoin address cluster (“BTC Cluster-1”). BTC Cluster-1 received one additional deposit of 1.39 BTC from a U.S. cryptocurrency firm on September 29, 2021 at 4:17 PM UTC in the Bitcoin transaction block 702741.
- b. On September 29, 2021 at 4:17 PM UTC, in the same bitcoin transaction block, 702741, BTC Cluster-1 sent the combined .52 BTC of Karakurt laundered

¹ I know from my training and experience that a cryptocurrency tumbling service is a service that mixes identifiable cryptocurrency funds with others to make those funds harder to trace.

proceeds and the 1.39 BTC from the U.S. cryptocurrency firm to a cryptocurrency address associated with Garantex, a Russian cryptocurrency exchange sanctioned on or about April 5, 2022 by the U.S. Department of Treasury for laundering criminal proceeds. In my training and experience, the instantaneous timing of Cluster-1 receiving the 1.39 BTC from the U.S. cryptocurrency firm and sending the combined 1.91 BTC containing both Karakurt laundered proceeds and funds from the U.S. cryptocurrency firm to Garantex indicated it was likely that the same individual maintained control of both the U.S. cryptocurrency firm account and BTC Cluster-1.

- c. I reviewed records provided to the FBI by the U.S. cryptocurrency firm regarding BTC Cluster-1 and learned the deposit account that sent 1.39 BTC to BTC Cluster-1 belonged to an individual named Deniss Zolotarjovs (“ZOLOTARJOVS”), a Latvian national living in Moscow, Russia, date of birth August 27, 1990, with mobile telephone phone number +79257006567, email address dennis.zolotaryov@icloud.com, Russian driver’s license 9916268972, and Latvian passport number LV4626616.

14. I conducted additional cryptocurrency analysis of cryptocurrency cluster Karakurt 1PLpQH3ntG and learned, among other things, the following:

- a. Karakurt 1PLpQH3ntG contained numerous addresses that received numerous reported Karakurt and Conti victim ransom payments, and has engaged in hundreds of transactions consistent with money laundering of cryptocurrency. Furthermore, the first transaction associated with the cluster, a deposit to the cluster’s root address, abbreviated 1PLpQH3ntG, was previously identified as

having received half of the first known Conti victim ransom payment on or about June 4, 2020. Thus, the cluster has been associated with illegal activity since the very first transaction conducted with the cluster.

- b. Bitcoin addresses reported by Karakurt victims as the ransom payment addresses, and associated by commercial cryptocurrency tracing software with Karakurt 1PLpQH3ntG, received six deposits in value between 1.25 BTC and 32 BTC, between on or about January 5, 2022 and January 7, 2022. Five of the six deposits were associated with previously reported Karakurt ransom payments, and the sixth, on January 7, 2022 for 22.7 BTC, was of unknown original.

15. I investigated the January 7, 2022 deposit of 22.7 BTC to Karakurt 1PLpQH3ntG, worth approximately \$930,000 at the time, and found the following:

- a. The deposit was sent via a foreign cryptocurrency exchange in a single large payment. Based on my training and experience in investigating Karakurt and Conti's ransomware laundering practices, and how the deposit was rapidly divided shortly after receipt, it is my belief the 22.7 BTC deposit on January 7, 2022 was an unreported victim ransom payment.
- b. Of the 22.7 BTC, approximately 5.68 of the BTC was laundered through multiple addresses before arriving at a deposit address associated with Garantex, on or about January 25, 2022.
- c. I searched a Garantex dataset provided by the United States Secret Service, which was obtained by the United States Secret Service via a search warrant issued by a U.S. Magistrate Judge in the Eastern District of Virginia on April 5, 2022, for information related to the above referenced transaction to Garantex, and found the

5.68 BTC was deposited to an account associated with Bitcoin24.pro, a nested exchange within Garantex known for exchanging bitcoin for Russian rubles. The Bitcoin24.pro account records revealed the 5.68 BTC deposited into the Bitcoin24.pro account were associated with a Bitcoin24.pro account registered to email address dennis.zolotaryov@icloud.com.

16. On or about September 5, 2023, I served a search warrant issued by a U.S. Magistrate Judge in the Southern District of Ohio to Apple, Inc. for records associated with an account registered to dennis.zolotaryov@icloud.com. Apple, Inc. provided records responsive to the warrant, and I have reviewed those records. From that review, I have learned the following:

- a. The account was registered to Deniss Zolotarjovs with telephone number +79257006567. The records showed the account was accessed by numerous IP addresses in Russia and Latvia over the previous three years.

17. On or about September 6, 2023, I spoke again with representatives of Company-5, who reported having received email communications on or about September 6, 2023 from an anonymous individual claiming to have knowledge of the November 2021 attack against Company-5, and to have access to the data taken during that incident, which Karakurt had claimed to have been deleted after Company-5 sent the ransom payment. The unknown individual threatened to publish the stolen data if Company-5 did not respond to the email. The individual provided an encrypted communications instant messaging account ID (“IM ID-2”) in the email.

18. On or about November 8, 2023, I spoke with an editor of an online cybersecurity news blog who contacted the FBI after having been in communications with an anonymous

person with knowledge of the Karakurt hacking group. The editor said the anonymous person reported they had been contacting previous Karakurt victims and asking them for money in exchange for deleting their private data they found while privately investigating the Karakurt ransomware group. The anonymous person said they wanted the editor's help in convincing the victims that the individual was serious, and asked the editor to either contact the victims or publish victim information. The editor refused to provide the requested assistance to the anonymous person, but offered to connect the person with the FBI because those with important information on cybercriminals can receive financial rewards. I asked the editor to pass the anonymous person's contact information to me, and to relay to the anonymous person a message to expect an email from the FBI. The editor provided an email address, anonymoux@proton.me, and an encrypted communications instant messaging account ("IM ID-3").

19. The FBI requested investigative assistance from Swiss law enforcement for records associated with anonymoux@proton.me, and in response, Swiss law enforcement provided records indicating the email address was registered on October 17, 2023 at approximately 11:28 AM UTC from an IP address ("IP-1").

20. I conducted link analysis of IM ID-1, IM ID-2, IM ID-3, anonymoux@proton.me, and dennis.zolotaryov@icloud.com. From that link analysis, I learned the following:

- a. IM ID-1, associated with Karakurt Rocket.Chat user Sforza, was accessed by the same IP addresses at or about the same times, on multiple occasions, as those used to access dennis.zolotarjov@icloud.com.
- b. IM ID-1 was accessed by the same IP addresses at the same times, on multiple occasions, as those used to access IM ID-2.

- c. IM ID-2 was accessed by the same IP addresses at the same times, on multiple occasions, as those used to accessed IM ID-3.
- d. On at least one occasion, the same IP address was used to access IM ID-1, IM ID-2, and IM ID-3 on the same day.
- e. IP-1, which was used to register anonymoux@proton.me on October 17, 2023 at approximately 11:28 UTC, was used to access both IM ID-2 and IM ID-3 on October 17, 2023 at approximately 11:30 UTC.

21. I communicated with the individual using email address anonymoux@proton.me numerous times between on or about November 8, 2023 and November 22, 2023. In those communications, the individual claimed to be an independent cybersecurity researcher with information to share on Karakurt, including their knowledge that Karakurt was the successor to Conti ransomware group, and also operated the Akira ransomware encryptor, as well as used the names TommyLeaks and SchoolBoys Ransomware Group in the past. The individual claimed to not be a criminal, and to not have spoken with any members of the group, but claimed to have access to their internal communications and their stolen victim data storage servers. Based on my knowledge and experience in investigating Karakurt, I believe it is unlikely anyone could have simply come across credentials to both the Rocket.Chat server as well as the victim data storage servers because Karakurt is known to be strict about not sharing user credentials openly, but rather only through direct, self-destructing private messaging services, such as privnote and onetimesecret.² The individual

²I know from my training and experience that private temporary messaging services such as privnote and onetimesecret allow individuals to create an encrypted communications message that can only be accessed via a unique URL and a password, and that they typically self-destruct after the intended recipient views the message.

provided screenshots of the Karakurt Rocket.Chat panel the FBI previously seized in the above-referenced search warrants located at the Rocket.Chat Tor URL. The screenshot of the Rocket.Chat panel provided by the individual showed the individual was logged in as a username with an avatar represented by a large, uppercase, white font “S” in a brown box. Only one user on the seized Rocket.Chat had the same avatar, Sforza_cesarini, indicating the individual was almost certainly logged in as Sforza_cesarini at the time of taking the screenshot. The individual requested approximately \$365,000 in Bitcoin from the FBI in exchange for sharing additional information on the group.

22. Based on the above, and my knowledge, training, and experience, it is reasonable to believe the same individual, Deniss Zolotarjovs, operated the Karakurt Rocket.Chat user ID Sforza_cesarini, email address anonymoux@proton.me, Apple iCloud account dennis.zolotarjov@icloud.com, IM ID-1, IM ID-2, IM ID-3, Bitcoin24.pro account dennis.zolotarjov@icloud.com, and the U.S. cryptocurrency firm account associated with dennis.zolotarjov@icloud.com.

23. Based on the above, and my knowledge, training, and experience, it is reasonable to believe Deniss Zolotarjovs received and laundered funds associated with a ransomware attack against Company-1 on or about August 10, 2021.

24. Based on the above, and my knowledge, training, and experience, it is reasonable to believe Deniss Zolotarjovs received and laundered funds associated with ransomware activity on or about January 7, 2022.


25. Based on the above, and my knowledge, training, and experience, it is reasonable to believe Deniss Zolotarjovs conspired to extort against Company-5, among other reported victim companies, with unnamed conspirators, and engaged in communications with said

conspirators via interstate communications on a private Rocket.Chat server hosted at the above-referenced Rocket.Chat Tor URL.

26. Based on the above, and my knowledge, training, and experience, it is reasonable to believe Deniss Zolotarjovs committed extortion, whereupon Deniss Zolotarjovs, while negotiating with Company-5 in or about December of 2021 and January of 2022, promised to delete all stolen data upon Karakurt receiving the ransom payment, and whereupon, on or about September 6, 2023, Deniss Zolotarjovs extorted Company-5 again.

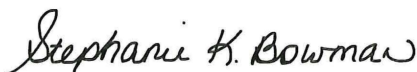
CONCLUSION

24. Based on my knowledge, training, and experience, the experience of other agents with whom I have conferred, and the facts set forth herein, probable cause exists to believe that DENISS ZOLOTARJOVS has committed violations of 18 U.S.C. § 1349 (Wire Fraud Conspiracy); 18 U.S.C. § 1956(h) (Money Laundering Conspiracy); and 18 U.S.C. § 1951 (Hobbs Act Extortion and Conspiracy). Thus, I respectfully request that this Court authorize a criminal complaint and arrest warrant for ZOLOTARJOVS.



Connor Lentz
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me by reliable electronic means, specifically, FaceTime video conference this 28 day of November, 2023.



HONORABLE STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE



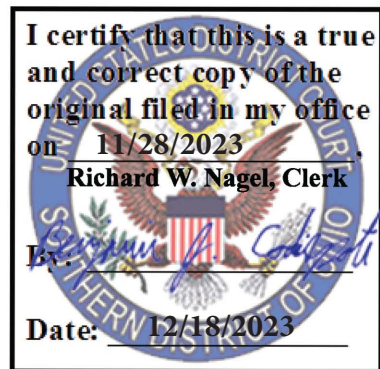
AO 442 (Rev. 11/11) Arrest Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

United States of America
v.
DENISS ZOLOTARJOVS
a/k/a "Sforza_cesarini"

Case No. 1:23-MJ-00978



Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay
(name of person to be arrested) DENISS ZOLOTARJOVS,
who is accused of an offense or violation based on the following document filed with the court:

- Indictment Superseding Indictment Information Superseding Information Complaint
- Probation Violation Petition Supervised Release Violation Petition Violation Notice Order of the Court

This offense is briefly described as follows:

- Money Laundering Conspiracy (18 U.S.C. Section 1956(h))
- Wire Fraud Conspiracy (18 U.S.C. Section 1349)
- Hobbs Act Extortion Conspiracy (18 U.S.C. Section 1951)
- Hobbs Act Extortion (18 U.S.C. Section 1951)

Date: Nov 28, 2023

Stephanie K. Bowman
Issuing officer's signature



City and state: Cincinnati, Ohio

Honorable Stephanie K. Bowman, U.S. Magistrate Judge
Printed name and title

Return

This warrant was received on (date) _____, and the person was arrested on (date) _____
at (city and state) _____.

Date: _____
Arresting officer's signature

Special Agent Connor Lentz, FBI
Printed name and title

AO 442 (Rev. 11/11) Arrest Warrant (Page 2)

**This second page contains personal identifiers provided for law-enforcement use only
and therefore should not be filed in court with the executed warrant unless under seal.**

(Not for Public Disclosure)

Name of defendant/offender: _____

Known aliases: _____

Last known residence: _____

Prior addresses to which defendant/offender may still have ties: _____

Last known employment: _____

Last known telephone numbers: _____

Place of birth: _____

Date of birth: _____

Social Security number: _____

Height: _____ Weight: _____

Sex: _____ Race: _____

Hair: _____ Eyes: _____

Scars, tattoos, other distinguishing marks: _____

History of violence, weapons, drug use: _____

Known family, friends, and other associates (*name, relation, address, phone number*): _____

FBI number: _____

Complete description of auto: _____

Investigative agency and address: _____

Name and telephone numbers (office and cell) of pretrial services or probation officer (*if applicable*): _____

Date of last contact with pretrial services or probation officer (*if applicable*): _____

RELEVANT LEGAL PROVISIONS

Exhibit C contains the applicable portions of statutes describing the offenses with which DENISS ZOLOTARJOVS, also known as “Sforza_cesarini,” is charged, the penalties that he faces if convicted, and the applicable statutes of limitations. Ellipses are used to indicate the omission of portions of the statutes and asterisks are used to indicate the omission of paragraphs or sub-paragraphs of the statutes because those portions and paragraphs or sub-paragraphs do not apply to the case against ZOLOTARJOVS.

Title 18, United States Code, Section 1956(h)
Money Laundering Conspiracy

* * *

(a)(2) Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States—

(A) with the intent to promote the carrying on or specified unlawful activity; or

(B) knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity;

* * *

Shall be sentenced to a fine of not more than \$500,000 or twice the value of the monetary instrument or funds involved in the transportation, transmission, or transfer, whichever is greater, or imprisonment of not more than twenty years, or both.

* * *

(h) Any person who conspires to commit any offense defined in this section . . . shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

* * *

Title 18, United States Code, Section 1343

Wire Fraud

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire . . . in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years or both.

Title 18, United States Code, Section 1349
Wire Fraud Conspiracy

Any person who attempts or conspires to commit any offense under this chapter [including wire fraud] shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

Title 18, United States Code, Section 1951

Extortion

(a) Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery or extortion or attempts or conspires so to do, or commits or threatens physical violence to any person or property in furtherance of a plan or purpose to do anything in violation of this section shall be fined under this title or imprisoned not more than twenty years, or both.

* * *

Title 18, United States Code, Section 3282

Offenses not capital

(a) In General.—

Except as otherwise expressly provided by law, no person shall be prosecuted, tried, or punished for any offense, not capital, unless the indictment is found or the information is instituted within five years next after such offense shall have been committed.

* * *

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO

UNITED STATES OF AMERICA

v.

CASE NO. 1:23-MJ-0978

DENISS ZOLOTARJOVS,
a/k/a “Sforza_cesarini”

Defendant.

AFFIDAVIT

I, Connor J. Lentz, being duly sworn, hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of the request of the United States of America to the Republic of Georgia for the extradition of DENISS ZOLOTARJOVS, also known as “Sforza_cesarini.” Because this affidavit is being submitted for the limited purpose of securing the extradition of Zolotarjovs, it does not contain every fact known to me about this investigation.

2. I am employed as a Special Agent with the Federal Bureau of Investigation (“FBI”), and have been employed in this capacity since January of 2020. I am currently assigned to the Cyber Squad, Cincinnati, Ohio Division. My responsibilities include the investigation of criminal violations of the United States Code, and related offenses. In my capacity as a Special Agent with FBI, I have conducted a variety of cybercrime investigations.

3. I received a Bachelor of Arts degree in Political Science from Indiana University. I received a certification from the FBI as a Digital Evidence Extraction Technician, I received a cyber security certification from the Global Information Assurance Certification body, and I received additional training from the FBI and the SANS Institute regarding various investigative skills as they relate to cybersecurity, information security, and examining the use of computers, computer networks, the internet, and digital communications as they pertain to the investigation of criminal activities. In my capacity as an FBI Special Agent, I am assigned to, and responsible for, the investigation which resulted in the complaint and arrest warrant for *Zolotarjovs* in the case of *United States v. Deniss Zolotarjovs*, which is pending in the United States District Court for the Southern District of Ohio, under Case Number 1:23-MJ-0978. I have participated in this investigation and am familiar with the facts and evidence in the case.

4. The information contained in this affidavit is based, in part, on my personal knowledge and observations during the course of this investigation, as well as information provided to me by other law enforcement agents, and is based on a review of various documents and records. Additionally, this affidavit is based on my training and experience as well as that of other law enforcement agents working with me in this investigation. The dates listed in this affidavit should be read as approximate dates. This affidavit is intended to show that

there is sufficient evidence for extradition and does not purport to set forth all of the information about which I, or collectively, the other law enforcement agents involved in this investigation, have knowledge of regarding this investigation and criminal case.

SUMMARY OF FACTS

5. The criminal complaint affidavit details some of the facts of the case and the charges.

IDENTIFICATION

6. One of the cryptocurrency accounts at a U.S.-registered cryptocurrency exchange involved in the money laundering conspiracy charged belongs to Deniss Zolotarjovs, and was registered to dennis.zolotaryov@icloud.com and telephone number +79257006567. In order to open the account, Zolotarjovs provided identification documents, including his passport, and took a photograph of himself. The photograph matched the image on the passport in his name.

7. Another cryptocurrency account at a global cryptocurrency exchange was also registered to Deniss Zolotarjovs, using the same telephone number, +79257006567. In order to open the account, Zolotarjovs provided identification documents, including his passport, and took a photograph of himself. The photograph matched the image on the passport in his name.

8. Another cryptocurrency account at a Russian-registered cryptocurrency exchange involved in the money laundering conspiracy was registered to Deniss Zolotarjovs's email account, dennis.zolotaryov@icloud.com.

9. According to records provided by Apple, Inc., the telephone number +79257006567 was also registered to the email address dennis.zolotaryov@icloud.com. We obtained records from that iCloud account and found many self-taken photographs of Zolotarjovs, as well as photographs of a Russian foreign resident identification document with the name Deniss Zolotarjovs, date of birth August 27, 1990, and a photo matching the image on Zolotarjovs's Latvian passport. Additionally, the records contained email messages from the above-referenced cryptocurrency exchanges, with transaction receipts matching transactions contained within the records associated with the cryptocurrency exchange accounts registered to Zolotarjovs, as well as transaction receipts matching transactions involved in the money laundering conspiracy.

10. Two encrypted communications accounts associated with ransomware and extortion attacks against victim companies in the United States, and also associated with the cybercriminal moniker "Sforza_cesarini," as well as an email account Zolotarjovs used to communicate with me,

xanonymoux@proton.me, shared significant IP address activity with a WhatsApp account registered to +79257006567.

11. Zolotarjovs is a Latvian citizen born on August 27, 1990. He is the holder of a Latvian passport in the name of "Deniss Zolotarjovs," number LV4626616, with date of birth August 27, 1990. I have attached to this affidavit as Exhibit D-1 photographs of Zolotarjovs received from the U.S. cryptocurrency platform where Zolotarjovs has the cryptocurrency account. Latvian authorities also provided information indicating Zolotarjovs received a new passport in his name on or about September 2, 2022, number LV6596613.

12. I DECLARE UNDER PENALTY OF PERJURY THAT THE FOREGOING IS TRUE AND CORRECT.



Connor J. Lentz
FBI Special Agent

Sworn to before me in Cincinnati, Ohio this 18th day of December, 2023.



HONORABLE KAREN L. LITKOVITZ
United States Magistrate Judge