

UNITED STATES DISTRICT COURT

for the

District of Nebraska

United States of America

v.

MAKSIM VIKTOROVICH YAKUBETS
a/k/a "AQUA"*Defendant(s)***SEALED**

Case No. 4:19MJ3142

CRIMINAL COMPLAINT

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 May, 2009 to May 21, 2010, in the county of Douglas in the
District of Nebraska, and elsewhere, the defendant(s) violated:*Code Section*18 U.S.C. § 1344
18 U.S.C. § 1349*Offense Description*

Defendant MAKSIM VIKTOROVICH YAKUBETS, also known as "aqua," did knowingly and intentionally conspire with others, both known and unknown, to commit bank fraud, as more specifically described in the attached affidavit, said affidavit incorporated herein by reference.

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT OF SA JACOB M. FOILES, INCORPORATED HEREIN BY
REFERENCE.☒ Continued on the attached sheet.*Complainant's signature*

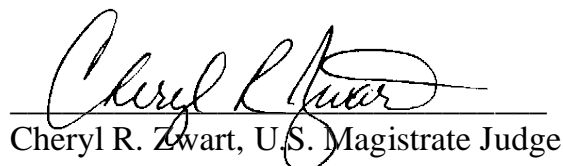
JACOB M. FOILES, SPECIAL AGENT, FBI

Printed name and title

Sworn to before me by reliable electronic means:

Date: November 14, 2019.

District of Nebraska


Cheryl R. Zwart, U.S. Magistrate Judge

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Special Agent Jacob M. Foiles, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a criminal complaint against MAKSIM VIKTOROVICH YAKUBETS, also known as “aqua” (hereinafter, the “DEFENDANT”).

2. I am presently employed as a Special Agent of the Federal Bureau of Investigation (FBI), and am assigned to the Cyber Task Force of the Omaha Field Office in the District of Nebraska. I have been employed by the FBI since November 2014, including five months of training at the FBI Academy in Quantico, Virginia. Subsequent to my initial training at the FBI academy, I have received additional training in the investigation of computer and financial related crimes. Previous to my employment with the FBI, I obtained a Bachelor’s degree in Computer Engineering, and was employed in the information technology industry for almost seven years. As a result of my training and experience, I am familiar with information technology and its use in criminal activities.

3. The information contained in this affidavit is based upon my personal knowledge, my review of documents and other evidence, my conversations with other law enforcement officers and other individuals, and my training and experience. All conversations and statements described in this affidavit are related in substance and in part unless otherwise indicated. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every detail of every aspect of the investigation. Rather, I have set forth only

those facts that I believe are necessary to establish probable cause. I have not, however, excluded any information known to me that would defeat a determination of probable cause.

PROBABLE CAUSE

A. Overview

4. This affidavit establishes probable cause to believe that DEFENDANT has been a member of a long-running conspiracy to employ widespread computer intrusions, malicious software, and fraud to steal millions of dollars from numerous bank accounts in the United States and elsewhere. As more fully described below, DEFENDANT and others (collectively, the “Jabber Zeus Crew”) have infected thousands of business computers with malicious software that captures passwords, account numbers, and other information necessary to log into online banking accounts, and have then used the captured information to steal millions of dollars from victims’ bank accounts.

B. Defendant and Co-Conspirators

5. At all times material to this affidavit:

- a. DEFENDANT was a resident of Russia. He used the online nickname “aqua.” DEFENDANT provided money mules¹ and their associated banking credentials in order to facilitate the movement of money which was withdrawn from victim accounts by fraudulent means.
- b. EVGENIY MIKHAYLOVICH BOGACHEV was a resident of Russia. He used the online nickname “lucky12345.” BOGACHEV was a coder who developed new codes to compromise banking systems and assisted

¹ “Money mules,” as detailed below, are persons in the United States who are recruited to receive stolen funds via wire and then wire the money outside the United States.

others in stealing and exploiting banking credentials.

- c. VYACHESLAV IGOREVICH PENCHUKOV was a resident of Ukraine. He used the online nickname “tank.” PENCHUKOV coordinated the exchange of stolen banking credentials and money mules. PENCHUKOV also received alert messages which provided notification once a bank account had been compromised.
- d. IVAN VIKTORVICH KLEPIKOV was a resident of Ukraine. He used the online nickname “petr0vich.” KLEPIKOV was a systems administrator who handled the technical aspects of the criminal scheme. KLEPIKOV also received alerts which provided notification once a bank account has been compromised.
- e. ALEXEY DMITRIEVICH BRON was a resident of Ukraine. He used the online nickname “thehead.” BRON was the financial manager of the criminal operations. BRON managed the transfer of money through an online money system known as Webmoney.
- f. ALEXEY TIKONOV was a resident of Russia. He used the online nickname “kusanagi.” TIKONOV was a coder or developer who assisted in the development of new codes to compromise banking systems.
- g. “MRICQ” was a resident of Ukraine. He used the online nickname “mricq.” “MRICQ” was a coder who developed new codes to compromise the banking system and passed user credentials to other conspirators.

C. Selected Victims

- 6. At all times material to this affidavit:
 - a. BANK OF ALBUQUERQUE was a subsidiary of BANK OF OKLAHOMA, a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Albuquerque, New Mexico.
 - b. BANK OF AMERICA was a financial institution insured by the Federal Deposit Insurance Corporation, was headquartered in Charlotte, North Carolina, and had offices in Nebraska.

- c. BASTRIRE EDWARDS, CPAS was a business located in Visalia, California.
- d. BULLITT COUNTY FISCAL COURT was a municipal government office in Shepherdsville, Kentucky.
- e. CALIFORNIA BANK AND TRUST was a financial institution insured by the Federal Deposit Insurance Corporation, and was headquartered in San Diego, California.
- f. DOLL DISTRIBUTING was a business located in Des Moines, Iowa.
- g. DOWNEAST ENERGY AND BUILDING SUPPLY was a business located in Brunswick, Maine.
- h. ESCROW SCOURCE was a business located in Seattle, Washington.
- i. FIRST FEDERAL SAVINGS BANK was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Elizabethtown, Kentucky.
- j. FIRST NATIONAL BANK OF OMAHA was a financial institution insured by the Federal Deposit Insurance Corporation, and was headquartered in Omaha, Nebraska. It offered online banking services through computer servers located in Nebraska.
- k. FRANCISCAN SISTERS OF CHICAGO was a religious congregation headquartered in Homewood, Illinois.
- l. GENLABS was a business located in Chino, California.
- m. HUSKER AG, LLC was a business located in Plainview, Nebraska.
- n. KEY BANK was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Sylvania, Ohio.
- o. LIEBER'S LUGGAGE was a business located in Albuquerque, New Mexico.
- p. PARAGO, INC. was a business located in Lewisville, Texas.
- q. SALISBURY BANK & TRUST was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Salisbury,

Massachusetts.

- r. TOWN OF EGREMONT was a town in Massachusetts with its own municipal government.
- s. UNION BANK AND TRUST was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Lincoln, Nebraska.
- t. UNITED DAIRY, INC. was a business located in Martins Ferry, Ohio.
- u. VISALIA COMMUNITY BANK was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Visalia, California.

D. Overview of the Scheme

7. DEFENDANT, being a person employed by and associated with the Jabber Zeus Crew, conspired with BOGACHEV, PENCHUKOV, KLEPIKOV, BRON, TIKONOV, and “MRICQ” (the “CO-CONSPIRATORS”),² and with others both known and unknown to devise and execute a scheme and artifice to defraud several depository institutions insured by the Federal Deposit Insurance Corporation.

8. It was part of the scheme that DEFENDANT AND CO-CONSPIRATORS used computer intrusions, malicious software, and fraud to steal or attempt to steal millions of dollars from several bank accounts in the United States, and elsewhere. DEFENDANT AND CO-CONSPIRATORS infected thousands of business computers with software that captured passwords, account numbers, and other information necessary to log into online banking

² DEFENDANT was previously charged by indictment in 4:11CR3074, but under his online nickname only.

accounts, and then used the captured information to steal millions of dollars from account holding victims' bank accounts. Account-holding victims included APC PROPERTIES, ARBEN GROUP, BASTRIRE EDWARDS, CPAS, BULLITT COUNTY FISCAL COURT, DOLL DISTRIBUTING, DOWNEAST ENERGY AND BUILDING SUPPLY, ESCROW SOURCE, FRANCISCAN SISTERS OF CHICAGO, GENLABS, HUSKER AG, LLC, LIEBER'S LUGGAGE, PARKINSON CONSTRICTION, PARAGO, INC., and TOWN OF EGREMONT.

9. DEFENDANT AND CO-CONSPIRATORS intended and foresaw that their conduct would defraud banks in the District of Nebraska.

10. The actions of DEFENDANT AND CO-CONSPIRATORS to execute the scheme included the following:

- a. Infecting the computers used by small businesses and non-profit organizations with malicious software;
- b. Obtaining bank account numbers, passwords, PIN numbers, RSA SecureID token codes, and similar information necessary to log into online bank accounts;
- c. Initiating electronic funds transfers from those bank accounts to the bank accounts of money mules;
- d. Transferring funds from money mules to overseas;
- e. Obtaining the use of computer servers necessary to obtain banking credentials and provide real-time communications among enterprise members; and
- f. Assigning different members the tasks of writing malicious software, administering computer servers, recruiting money mules, infecting computers, accessing bank accounts to make unauthorized transfers, and receiving transferred funds outside the United States.

E. Electronic Funds Transfer System

11. This investigation has identified numerous unauthorized Electronic Funds Transfers (EFTs) initiated from victim bank accounts. There are two primary types of EFTs: wire transfers and Automated Clearing House (ACH) payments. Both of these EFTs are performed through the Federal Reserve Bank System. The primary method used by DEFENDANT AND CO-CONSPIRATORS to steal funds was through ACH payments.

12. Wire transfers are real-time transfers of funds. After a wire transfer is initiated from a sending bank, the sending bank's Reserve Account at the Federal Reserve Bank is immediately debited and the receiving bank's Reserve Account is immediately credited. Wire transfers are typically performed when transactions are time-sensitive or are for large dollar amounts. Recipients of wire transfers have immediate access to the funds through their account at the receiving financial institution.

13. ACH Payments are made through the ACH Network, which is a batch-oriented EFT system wherein batch transfers are settled the next day. The ACH Network is governed by the National Automated Clearing House Association (NACHA) regulations. The Federal Reserve and Electronic Payments Network act as the central clearing facilities through which institutions transmit or receive funds. ACH Payments are typically used for direct deposit to payroll, direct payment for consumer bills (mortgages, loans, etc.), electronic checks, business-to-business payments, or e-commerce payments. ACH payments are either credits (also known as direct deposits) or debits (also known as direct payments). An ACH credit is always initiated by the sender whereas ACH debits are initiated by either the sender or receiver. ACH Payments

are submitted in batches from the originator (through their financial institution) to the Federal Reserve Bank. One day later, these batch payments are settled and the payment is sent to the receiving depository financial institution. At the time of settlement, funds are debited from the sending financial institution's account at the Federal Reserve Bank and credited to the receiving financial institution's account.

14. Larger financial institutions have developed their own software to conduct ACH Payments and wire transfers based on the rules governing EFTs through the Federal Reserve Bank. Smaller financial institutions that do not have their own Information Systems Departments utilize Third-Party Processor systems, which allow these banks to conduct EFTs. There are several companies which have developed systems which are utilized by these smaller financial institutions to conduct EFTs. Each of these companies must comply with same regulations that the financial institutions are required to follow. This investigation has uncovered fraudulent EFTs which were processed through several Third-Party Processors.

F. The Zeus Malware

15. Beginning in or about May 2009, the FBI began receiving numerous complaints of fraudulent ACH transfers. Through techniques described later in this affidavit, the FBI was able to determine that a large number of fraudulent transfers were being made by unauthorized users, who were gaining the one-time PINs and security questions in real-time to initiate the transfers. FBI Omaha, the FBI's Cyber Division, and several other FBI Division offices began coordinating with Internet security researchers, ACH payment processors, and financial institutions in an effort to determine how the unauthorized users were gaining the one-time PINs

and security questions in real-time and initiated an effort to determine links between incidents nationwide.

16. On or about June 1, 2009, Internet security researchers at the company iDefense, a provider of computer security intelligence to corporate clients, discovered a modified version of the “Zeus” malicious software that was capable of sending one-time passwords, such as one-time PINs, directly to the attackers in real-time, through an “instant message” protocol known as “Jabber.” Based on my training and experience, I know that Jabber is a method of sending and receiving text-based communication sent over the Internet, also referred to as “chat.”

17. Based on my training and experience and on information developed during this investigation, I know that Zeus is the name of an identified “keylogger” that was used to steal online banking information. A keylogger is a form of malicious code which are designed to capture the keystrokes of a user on the machine which the keylogger is installed.³ The primary purpose of a keylogger is to capture the keystrokes for usernames and passwords used to access websites, e-mail, and other services from the victim computer. Keyloggers are often designed to send the captured keystrokes back to the criminal who installed the keylogger on the victim machine. These captured keystrokes are typically sent over the Internet in regular time intervals

³ Malicious code is a term used to describe any software code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, trojan horses, backdoors, and malicious active content. It is often installed on a victim computer system via the Internet through spam that contains attachments or through a website where code is injected to automatically download onto a victim system when it is viewed through a web browser. When it is installed onto a victim computer system to perform malicious activity, it is often referred to as malware.

from the victim machine to a machine controlled by the criminal. An unknown criminal or group of criminals developed this keylogger as part of a toolkit to sell to other criminals.

18. FBI investigations and Internet security company researchers identified criminals advertising the Zeus toolkit for sale on various Internet forums used by criminals to exchange fraud information. Copies of the toolkit were obtained for analysis. The developers of Zeus gave the toolkit that name. However, it was often detected by anti-virus software under the name “zbot” (short for “Zeus bot”) or “wsnpoem,” based on a directory name created on the victim machine when it is installed. Zeus was referred to as a toolkit because it contained software which enabled a criminal to operate a database for storing captured data, operate a command and control server, and create new variants of the keylogger which were not detectable by anti-virus programs. Simple changes in the software code changed the signature of the keylogger, thus creating a new variant which is not recognized as a Zeus bot even though it was performing the same function as the previous variant.⁴

19. Zeus had become such a notorious toolkit that in or about January 2009, computer security researchers in Switzerland, who are well known to FBI Cyber investigators, had devoted a website to tracking command and control servers communicating with Zeus bots. Their page

⁴ A bot is a computer that has been compromised by malicious software for use in completing malicious and/or illegal tasks via remote direction. Most users that have a computer acting as a bot are not aware that their computers have been compromised. Compromised computer is synonymous with bot, and either may be used based on context. A larger number of bots, called a bot network or botnet, are typically controlled by one computer called a command and control server. The owner of the command and control server can direct the botnet to initiate a denial of service attack, send spam, operate as proxies (blindly forwarding Internet data), host phishing sites, or participate in other crime.

was hosted at the URL <https://zeustracker.abuse.ch> until on or about July 8, 2019. This site was often referred to as the “Zeustracker” site. The Zeus bots on victim computers could be configured to communicate to the command and control servers through a domain name, such as kerchon.com, and not by the command and control server’s Internet Protocol (IP) address. Therefore, a criminal could easily change the computer on which the domain resides (kerchon.com, in this example) and the infected victim computers would communicate with the criminal’s new computer system. The criminal could also send the Zeus bot a software configuration update with a new domain for the Zeus bot to communicate. It was therefore difficult to quantify how many criminals or criminal groups were operating Zeus command and control servers.

20. Zeus bots used encoded (not humanly-readable) configuration files that contained the list of banking/web targets for which that particular bot was programmed to capture information. The security researchers referenced above devoted time to decoding the configuration files in order to alert the Internet security community of the current and historical target websites. Researchers searched for the unique alpha-numeric key that would decode the configuration file. The unique alpha-numeric keys could be used to decode multiple configuration files. This indicated a relationship between the Zeus bots for which the configuration files were decoding, meaning there is reason to believe that the Zeus bots were deployed or controlled by the same criminal or criminal group. The deployment of the Zeus malware resulted in the attempted theft of an estimated \$220 million USD, with actual losses of an estimated \$70 million USD from victims’ bank accounts.

21. iDefense Security Intelligence Services (“iDefense”) (now owned by Accenture) released analysis in iDefense report #486471 on or about June 4, 2009. The analysis revealed that the modified version of Zeus was capable of sending one-time passwords, such as one-time PINs, directly to the attackers in real-time, through the Jabber instant message protocol.

22. Further analysis published by iDefense stated that stolen login credentials were sent via the Jabber instant-message protocol to the domain incomeet.com, which was hosted on the IP address 66.199.248.195 (the “INCOMEET SERVER”). Further, iDefense advised that once the Zeus keylogger was fully installed on a victim system, it would be detected as having the filename “sdra64.exe,” if the virus was not already removed by an anti-virus program.

G. Investigation and Searches of the INCOMEET SERVER

23. Investigation of the Zeus malware led FBI investigators to believe that a computer with the IP address 66.199.248.195 – i.e., the INCOMEET SERVER – was receiving Jabber instant messages containing the usernames, passwords, PIN numbers, and possibly other credentials necessary to log into victims’ bank accounts.

24. An open source address lookup of the IP address 66.199.248.195 on or about September 17, 2009, revealed that it hosted the domain incomeet.com. It also revealed that the address corresponded to EZZI.NET. EZZI.NET was at that time headquartered at 882 Third Avenue, 9th Floor, Brooklyn, NY 11232. EZZI.NET maintained server computers connected to the Internet. Their customers used those computers to operate servers on the Internet that, in turn, provide services to client computers. In general, customers configured their computers at EZZI.NET remotely.

25. On or about September 18, 2009, an FBI agent interviewed Mohammed Salim, an employee at EZZI.NET. According to Salim, the INCOMEET SERVER was built by EZZI.NET at the request of the customer, to the customer's specification. The INCOMEET SERVER had one 500 gigabyte hard drive, 2 gigabytes of RAM, and a dual-core AMD processor. It ran the CentOS 5.0 distribution of the Linux operating system. It was leased to someone who identified himself as "Alexey S." (no full last name known), who claimed to be associated with a company "IP-Server Ltd," supposedly located at Komsomolskaya St. 1, Moscow, Russian Federation.

26. Pursuant to search warrants, the FBI searched the INCOMEET SERVER on four occasions: on or about September 28, 2009, December 9, 2009, March 17, 2010, and May 21, 2010.

27. On the INCOMEET SERVER, agents found extensive logs of chat communications. These included usernames, passwords, and temporary token numbers for hundreds of bank and brokerage accounts, username and passwords for Paypal.com and other financial sites, and other information collected from infected victim computers.

28. For example, on or about March 16, 2010, alone, 16 different Jabber communications that appeared to pertain to stolen banking credentials were passed through the INCOMEET SERVER. Many of these pertained to the same victims. For example, one of those messages read as follows:

```
Panel: http://193.104.41.131/  
Template: WebCashMgmt  
Added: 2010-03-15 23:48:09  
Updated: 2010-03-15 23:48:09
```

IPv4: 76.79.206.130
BotID:
BotNet:
Country: US
Host: rrcs-76-79-206-130.west.biz.rr.com
UserAgent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; AskTB5.6)
Location: https://bob.sovereignbank.com/wcmfd/wcmpw/CustomerLogin
Status: Waitoperator
Data:
Customer/Organization ID: KUS2761
User ID: sysadmin
Password: Kunal[remainder of password redacted]

29. From my review of other messages sent through the server, I know that this message represented the transmission of compromised banking credentials. Specifically, this says that a user with user ID “KUS2761,” and a password beginning “Kunal” (the remainder of the password was in the original message but has been redacted from this affidavit) used the IP address 76.79.206.130 to attempt to access an account on Sovereign Bank, which was in the United States.

30. Additionally, the INCOMEET SERVER contained evidence that it was used by the conspirators to communicate with each other. The INCOMEET SERVER’s operators had configured it to record on its hard drive ongoing logs of every chat message sent through the server. These chat communications included discussions among conspirators made as they were in the progress of transferring money out of victim bank accounts. They also discussed the recruitment of “mules” – persons in the United States who are recruited to receive ACH payments and wire the money outside the United States. They also discussed the operation of their botnet. The conspirators communicated in Russian, using both the Cyrillic and Roman alphabets. All chats quoted in this affidavit have been translated into English, using human

translators except where indicated. In some cases, immaterial lines of chat have been omitted for brevity's sake.

31. Participants in the chat identified themselves by nicknames. With exceptions, some of which are noted below, they did not generally reveal in chat their real names or other personally identifiable information.

32. On or about July 2, 2009, a writer for the Washington Post website posted a blog entry entitled "PC Invader Costs Ky. County \$415,000," which began with the lead paragraph, "Cyber criminals based in Ukraine stole \$415,000 from the coffers of Bullitt County, Kentucky this week. The crooks were aided by more than two dozen co-conspirators in the United States, as well as a strain of malicious software capable of defeating online security measures put in place by many banks."⁵ The article generally described the theft of funds from the Bullitt County Fiscal Court in Shepherdsville, Kentucky, as described in this affidavit. The blog entry is accessible at http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html.

33. Chat logs show that the conspirators viewed this posting and recognized that it described their criminal activity. For example, on or about July 12, 2009, the user with the online name of "aqua" (i.e., DEFENDANT) said the following to user "tank" (i.e., PENCHUKOV): "But they described the entire scheme. The Bastards. They exposed the texts.

⁵ In this quotation, and hereinafter in this affidavit, all money/currency amounts are in U.S. dollars, unless otherwise indicated.

They laid out the entire scheme. ... It's necessary to give to the supporting [people?] to read.

I'm really pissed. They exposed the entire deal."

34. Also on or about July 12, 2009, DEFENDANT and PENCHUKOV had this exchange:

tank: Well, nevertheless, they were writing about us.
aqua: So because of whom did they lock Western Union for Ukraine?
aqua: Tough shit.
tank: *****Originator: BULLITT COUNTY FISCAL Company: Bullitt
County Fiscal Court
aqua: So?
aqua: This is the court system.
tank: Shit.
tank: Yes
aqua: This is why they fucked [nailed?] several drops.
tank: Yes, indeed.
aqua: Well, fuck. Hackers: It's true they stole a lot of money.

35. That same day, PENCHUKOV, while chatting with another individual, specifically referenced the URL of the Washington Post blog posting and discussed its contents:

tank: [Are you] there?
indep: Yeah.
indep: Greetings.
tank: [http://voices.washingtonpost.com/securityfix/2009/07/
an_odyssey_of_fraud_part_ii.html#more](http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html#more)
tank: This is still about me.
tank: Originator: BULLITT COUNTY FISCAL Company: Bullitt County Fiscal
Court
tank: He is the account from which we cashed.
tank: Today someone else send this news.
tank: I'm reading and thinking: Let me take a look at history. For
some reason this name is familiar.
tank: I'm on line and I'll look. Ah, here is this shit.
indep: How are you?
tank: Did you get my announcements?
indep: Well, I congratulate [you].
indep: This is just fuck when they write about you in the news.
tank: Whose [What]?

tank: :D
 indep: Too much publicity is not needed.
 tank: Well, so nobody knows who they are talking about.

36. At roughly the same time that PENCHUKOV was having this above chat conversation, he was also having the following chat conversation with user “lucky12345” (i.e., BOGACHEV):

tank: Are you [it] there?
 tank: This is what they damn wrote about me.
 tank: http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html#more
 tank: I'll take a quick look at history
 tank: Originator: BULLITT COUNTY FISCAL Company: Bullitt County Fiscal Court
 tank: Well, you got [it] from that cash-in.
 lucky12345: From 200K?
 tank: Well, they are not the right amounts and the cash out from that account was shitty.
 tank: Levak was written there.
 tank: Because now the entire USA knows about Zeus.
 tank: :D
 lucky12345: It's fucked.

37. On or about July 29, 2009, DOLL DISTRIBUTING, a company that banks with FIRST NATIONAL BANK OF OMAHA, reported that it experienced two fraudulent ACH payments totaling \$59,222. In a chat message sent on or about July 28, 2009, from user “777” to user “hrd” on the INCOMEET SERVER, it was reported that \$29,383 was transmitted from Doll to KODASH CONSULTING, LLC, and that \$29,839 was transmitted to PANDORA SERVICES, LLC.

38. On or about July 31, 2009, an FBI agent interviewed Renee Michelli, the proprietor of PANDORA SERVICES, LLC. Michelli stated that she had been looking for a job

and had posted her resume on Internet job seeker sites. She was supposedly “hired” as a United States representative for a Russian software company, “1C.” She was told to establish an LLC with a bank account. She was told her job would involve receiving payments and wiring them outside the United States. On or about October 2, 2009, Heidi Nelson, the proprietor of KODASH CONSULTING, LLC, was interviewed by another FBI agent. Nelson stated that she lost her job in early 2009, and put her resume on Internet job seeker sites. She was contacted by an individual claiming to be an assistant human resources manager for a Russian company. Her job would be to work with clients in the United States, and on occasion to receive payments from them, which she would transmit to Russia. Based on my training and experience and information developed during this investigation, I believe that Michelli and Nelson were money mules hired by the DEFENDANT AND CO-CONSPIRATORS to facilitate the transfer of stolen funds.

39. Through the execution of the four search warrants, FBI agents found chat communications on the INCOMEET SERVER describing the transfer of money from a large number of bank accounts, including those held by BASTRIRE EDWARDS, CPAS, BULLITT COUNTY FISCAL COURT, DOLL DISTRIBUTING, DOWNEAST ENERGY AND BUILDING SUPPLY, ESCROW SOURCE, FRANCISCAN SISTERS OF CHICAGO, GENLABS, HUSKER AG, LLC, LIEBER’S LUGGAGE, PARAGO, INC., TOWN OF EGREMONT, and UNITED DAIRY, INC. These chats usually occurred within hours of the transfers in question. Among other things, the chats were used to transmit log-in credentials for victims, report the transfer of funds to mules, and/or request bank account information for mules.

DEFENDANT AND CO-CONSPIRATORS referenced herein participated in one or more chats relating to or facilitating thefts of log-in credentials or fraudulent transfers of funds from victims. Some of those chats are referenced in Overt Acts, below.

40. The chat communications on the INCOMEET SERVER also establish that the primary role of DEFENDANT in the conspiracy was to provide money mules and their associated banking credentials in order to facilitate the movement of money which was withdrawn from victim accounts by fraudulent means.

41. One example of this conduct occurred on or about August 12, 2009, in an incident victimizing the FRANCISCAN SISTERS OF CHICAGO of Homewood, Illinois, that involved two batch transactions totaling at least fourteen fraudulent ACH transfer attempts. Sister Helene Galuska of the FRANCISCAN SISTERS OF CHICAGO reported that she received what appeared to be an email from her bank. Upon opening it, she saw that it was blank. After opening the email, she saw several unauthorized ACH transfers. Transfers totaling approximately \$130,261 were attempted, and the FRANCISCAN SISTERS OF CHICAGO suffered an actual loss of approximately \$24,141.

42. Chat logs concerning the incident show that on or about August 13, 2009, user “tank” sent DEFENDANT a chat message containing a list of ACH transfer recipients and the amounts of funds they received. This list matched the actual mule recipients and the amounts they received.

43. Chat logs also demonstrate that email address aquamo@mail.ru was controlled by DEFENDANT. Specifically, on or about August 11, 2009, DEFENDANT and PENCHUKOV

had this exchange:

aqua: If something comes up I'll text you.
tank: I don't have a work phone, because I don't talk on the telephone from work.
tank: I can give you my personal phone number.
aqua: Then send it to aquamo@mail.ru.
tank: Did you receive?
aqua: I'll check now.

THE CONSPIRACY

44. From in or about May 2009, the exact date being unknown, and continuing to on or about September 29, 2010, in the District of Nebraska and elsewhere, DEFENDANT, being a person employed by and associated with the Jabber Zeus Crew, did unlawfully, voluntarily, intentionally and knowingly conspire, combine, confederate, and agree with each other, with CO-CONSPIRATORS, and with others both known and unknown to the Grand Jury to devise and execute a scheme and artifice to defraud BANK OF ALBUQUERQUE, BANK OF AMERICA, CALIFORNIA BANK AND TRUST, FIRST FEDERAL SAVINGS BANK, FIRST NATIONAL BANK OF OMAHA, KEY BANK, SALISBURY BANK & TRUST, UNION BANK AND TRUST, and VISALIA COMMUNITY BANK, all of which were depository institutions insured by the Federal Deposit Insurance Corporation.

A. Manner and Means of the Conspiracy

45. It was part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS used computer intrusion, malicious software, and fraud to steal or attempt to steal millions of dollars from several bank accounts in the United States, and elsewhere.

46. It was further part of the conspiracy that DEFENDANT AND CO-

CONSPIRATORS installed, without authorization, malicious software known as “Zeus” or “Zbot” on Internet-connected computers without those computers’ owners’ authorization, thereby causing damage to those computers.

47. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS used that malicious software to capture bank account numbers, passwords, and other information necessary to log into online banking accounts.

48. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS used that captured information without authorization to falsely represent to banks that DEFENDANT AND CO-CONSPIRATORS were employees of the victims authorized to make transfers of funds from the victims’ bank accounts.

49. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS used that captured information to cause banks to make unauthorized transfers of funds from the victims’ bank accounts.

50. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS used as money mules residents of the United States who received funds transferred over the ACH network or through other interstate wire systems from victims’ bank accounts into the money mules’ own bank accounts, and then withdrew some of those funds and wired the funds overseas to conspirators.

51. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS maintained Internet-connected computer servers, in the United States and elsewhere, to facilitate communication.

52. It was further part of the conspiracy that DEFENDANT AND CO-CONSPIRATORS knowingly falsely registered a domain name and knowingly used that domain name in the course of the offense, in violation of 18 U.S.C. § 3559(g)(1).

B. Overt Acts

53. In furtherance of the conspiracy and to achieve the objectives thereof, at least one of the conspirators performed or caused to be performed at least one of the following overt acts,⁶ among others, in the District of Nebraska and elsewhere:⁷

- a. On or about June 22, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by BULLITT COUNTY FISCAL COURT.
- b. On or about June 22, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause FIRST FEDERAL SAVINGS BANK to transfer funds out of a bank account belonging to BULLITT COUNTY FISCAL COURT and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- c. On or about July 8, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by TOWN OF EGREMONT.
- d. On or about July 12 and 13, 2009, DEFENDANT, BOGACHEV, PENCHUKOV, and other individuals exchanged chat messages about unauthorized withdrawals they had made from accounts owned by BULLITT COUNTY FISCAL COURT.

⁶ I note that 18 U.S.C. § 1349 does not require proof of an overt act in furtherance of the conspiracy.

⁷ In the description of the overt acts as set forth below, DEFENDANT is specifically identified as an actor. Evidence concerning the attribution of the nickname used by DEFENDANT on the INCOMEET SERVER, “aqua,” is set forth below under “ATTRIBUTION.”

- e. On or about July 28, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by DOLL DISTRIBUTING.
- f. On or about July 28, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to attempt to cause FIRST NATIONAL BANK OF OMAHA to transfer funds out of a bank account belonging to DOLL DISTRIBUTING and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- g. On or about July 29, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause SALISBURY BANK & TRUST to transfer funds out of a bank account belonging to TOWN OF EGREMONT and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- h. On or about July 30, 2009, "MRICQ" sent DEFENDANT a chat message about the TOWN OF EGREMONT bank account.
- i. On or about July 30, 2009, DEFENDANT sent another individual a chat message about the TOWN OF EGREMONT bank account.
- j. On or about August 12, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by FRANCISCAN SISTERS OF CHICAGO.
- k. On or about August 12, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause BANK OF AMERICA to transfer funds out of a bank account belonging to FRANCISCAN SISTERS OF CHICAGO and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- l. On or about August 13, 2009, PENCHUKOV sent a chat message to DEFENDANT listing recipients and amounts of funds transferred from a bank account belonging to FRANCISCAN SISTERS OF CHICAGO.
- m. On or about August 13, 2009, DEFENDANT sent a chat message to another individual listing recipients and amounts of funds transferred from a bank account belonging to FRANCISCAN SISTERS OF CHICAGO.

- n. On or about August 25, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by UNITED DAIRY, INC.
- o. On or about August 26, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause KEY BANK to transfer funds out of a bank account belonging to UNITED DAIRY, INC. and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- p. On or about August 27, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by DOWNEAST ENERGY AND BUILDING SUPPLY.
- q. On or about September 1, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause KEY BANK to transfer funds out of a bank account belonging to DOWNEAST ENERGY AND BUILDING SUPPLY and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- r. On or about September 1, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by ESCROW SOURCE.
- s. On or about September 1, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause KEY BANK to transfer funds out of a bank account belonging to ESCROW SOURCE and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- t. On or about September 16, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by GENLABS.
- u. On or about September 16, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause CALIFORNIA BANK AND TRUST to transfer funds out of a bank account belonging to GENLABS and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.

- v. On or about September 18, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by LIEBER'S LUGGAGE.
- w. On or about September 18, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause BANK OF ALBUQUERQUE to transfer funds out of a bank account belonging to LIEBER'S LUGGAGE and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- x. On or about September 28, 2009, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by PARAGO, INC.
- y. On or about September 28, 2009, DEFENDANT AND CO-CONSPIRATORS used stolen access information to attempt to cause FIRST NATIONAL BANK OF OMAHA to transfer funds out of a bank account belonging to PARAGO, INC. and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- z. On or about February 10, 2010, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by BASTRIRE EDWARDS, CPAS.
- aa. On or about February 10, 2010, DEFENDANT AND CO-CONSPIRATORS used stolen access information to cause VISALIA COMMUNITY BANK to transfer funds out of a bank account belonging to BASTRIRE EDWARDS, CPAS and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.
- bb. On or about March 3, 2010, DEFENDANT AND CO-CONSPIRATORS caused malicious software to be installed, without authorization, on a computer used by HUSKER AG, LLC.
- cc. On or about March 3, 2010, DEFENDANT AND CO-CONSPIRATORS used stolen access information to attempt to cause UNION BANK AND TRUST to transfer funds out of a bank account belonging to HUSKER AG, LLC and into one or more bank accounts designated by DEFENDANT AND CO-CONSPIRATORS.

ATTRIBUTION

54. As indicated above, participants in the chat on the INCOMEET SERVER identified themselves by nicknames. As set forth below, the nickname “aqua” is associated with DEFENDANT, and was used in chat communications discussing the overt acts set forth above that involved DEFENDANT.

55. On or about July 9, 2010, U.S. authorities transmitted a mutual legal assistance request to Russian authorities concerning “aqua.” Russian authorities produced a response that, in pertinent part, attributed the moniker to DEFENDANT. The response included numerous affidavits from Russian law enforcement officials concerning their investigation, which was initiated to effectuate the mutual legal assistance request.

56. These affidavits included submissions summarizing the investigation taken by Russian authorities concerning email address aquamo@mail.ru.⁸ In pertinent part, Russian law enforcement officials determined that: (1) the email account contained incoming electronic messages addressed to “aqua” (for example, an offer to write a malicious computer program), as well as to someone named “Maksim Yakubets;” (2) “Yakubets Maksim Viktorovich” had made travel arrangements through a travel agency using the account; and, (3) the user of the account

⁸ I believe, based on my training and experience, as well as the review of evidence obtained in this investigation, that the Russian response to the mutual legal assistance request was reliable. Russian authorities did not produce the actual records and information they had obtained, as had been requested; instead, they summarized the records and information in affidavits. The United States would not be able to compel the testimony of the affiants at trial using a trial subpoena. However, I have gathered additional evidence that would clearly be admissible at trial, discussed below, which further demonstrates that the nickname “aqua” is associated with DEFENDANT.

had arranged for a delivery of a baby carriage to a specific address in Moscow, Russia (the “Moscow Address”), listing a specific Russian telephone number as the contact number.

57. Other pertinent findings from Russian authorities were also summarized by affidavit in the response. In obtaining login information for email address aquamo@mail.ru, Russian law enforcement officials found that the account was accessed from a specific Russian IP address on two occasions. After obtaining records from the provider associated with this IP address, they determined that the service address for the IP address was the Moscow Address. Russian law enforcement officials also monitored the Russian telephone number associated with the baby carriage delivery, and determined that the number was used by Yakubets.

58. Affidavits from the Russian response also indicated that on or about November 24, 2010, Russian authorities executed a residential search warrant at the Moscow Address. According to the affidavits produced by Russian authorities, individuals present or with belongings at the residence included Maksim Yakubets and a specific female individual (“Female 1”).

59. On March 19, 2018, this Court issued an Order to Microsoft Corporation (“Microsoft”) under 18 U.S.C. § 2703(d). In response, Microsoft produced records showing, in pertinent part, that the email address associated with Skype telecommunications account “maksim.ya” is aquamo@mail.ru. This Court then issued a search warrant for the “maksim.ya” Skype account on May 23, 2018. The return from that warrant revealed the existence of a contacts list associated with the account, including a specific Skype contact (“Skype Contact 1”).

60. On July 17, 2018, this Court issued another Order to Microsoft under 18 U.S.C. § 2703(d). In response, Microsoft produced records showing, in pertinent part, that a specific email address hosted at domain mail.ru (the “Female 1 Mail.ru Email Address”) was associated with Skype Contact 1.

61. On or about December 25, 2012, Female 1, a Russian national, applied for a visa to visit the United States. On her visa application, Female 1 listed her marital status as “married,” “Maksim Viktorovich Yakubets” as her spouse (with a specific date of birth in 1987), and “[redacted] Yakubets” in the “Alias Surname” field. Female 1 also listed her home address as the Moscow Address, and the Female 1 Mail.ru Email Address as her email address. She also listed a male child (“Child 1”) who would be traveling with her. Child 1’s middle name was a patronymic name consistent with DEFENDANT’s first name.⁹ Child 1’s last name matched Female 1’s, except for the omission of an “a” at the end.¹⁰

62. On or about December 25, 2012, Child 1, a Russian national, also applied for a visa to visit the United States. On the application, Female 1 was listed as assisting the child with its preparation. A specific date of birth in 2009 was provided for Child 1 on the application. Female 1 was listed on the application as the child’s mother, and “Maksim Viktorovich

⁹ Russian middle names, or patronymics, are taken from the father’s first name. The patronymic is formed by the father’s first name and different suffixes depending on gender. Males have patronymics that end in -ovich or -evich.

¹⁰ Russian last names are similar to last names in English, but there are male forms and female forms of Russian last names, with female forms generally adding an “a.”

Yakubets” as his father (with the same specific date of birth in 1987). The home address listed for Child 1 was the Moscow Address, and the email address associated with the application was the Female 1 Mail.ru Email Address.

63. On or about August 12, 2018, Female 1 again applied for a visa to visit the United States. On her visa application, Female 1 listed her marital status as “divorced,” “Maksim Yakubets” as her former spouse (with the same specific date of birth in 1987), and “[redacted] Yakubets” in the “Alias Surname” field. Female 1 also listed her home address as the Moscow Address, but listed a different email address as her email address. She again listed Child 1 (with his middle name omitted) as who would be traveling with her. Child 1’s last name again matched Female 1’s, except for the omission of an “a” at the end.

64. On or about August 12, 2018, Child 1 again applied for a visa to visit the United States. The same specific date of birth in 2009 was provided for Child 1 on the application. Female 1 was again listed on the application as the child’s mother, and “Maksim Yakubets” as his father (with the same specific date of birth in 1987). The home address listed for Child 1 was again the Moscow Address, and the email address associated with the application matched the email address used on Female 1’s August 12, 2018, visa application.

65. On the date of Child 1’s birth in 2009, chat logs show that DEFENDANT and PENCHUKOV had this exchange:

```
tank:      So what's going on over there? =)))
aqua:      She's giving birth!!!
aqua:      I will write later.
tank:      =) - =) OK new dad.  =)
aqua:      He was born.
aqua:      She gave birth.
tank:      Yayyyyyy.
```

Aqua: He's already crying.

66. In a chat message sent earlier the same day (i.e., prior to the above-quoted exchange), DEFENDANT told PENCHUKOV the planned name for the child that was about to be born. This name matches the first and middle names of Child 1.

67. Based on the information set forth above, and my training and experience, and the information set forth above, I believe that DEFENDANT controlled the online nickname "aqua" used, in pertinent part, in the communications of the Jabber Zeus Crew found on the INCOMEET SERVER.

CONCLUSION

68. Based on the foregoing, I submit there is probable cause to believe that from in or about May 2009, and continuing to on or about September 29, 2010, in the District of Nebraska and elsewhere, MAKSIM YAKUBETS, also known as "aqua," together with others known and unknown, did knowingly and intentionally conspire to violate 18 U.S.C. §§ 1344 and 1349, that is, devised and executed a scheme and artifice to defraud BANK OF ALBUQUERQUE, BANK OF AMERICA, CALIFORNIA BANK AND TRUST, FIRST FEDERAL SAVINGS BANK, FIRST NATIONAL BANK OF OMAHA, KEY BANK, SALISBURY BANK & TRUST, UNION BANK AND TRUST, and VISALIA COMMUNITY BANK, all of which were depository institutions insured by the Federal Deposit Insurance Corporation.

REQUEST FOR SEALING

69. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and complaint. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits via the Internet, and disseminate them to other online criminals as they deem appropriate, e.g., by posting them publicly online. The crimes discussed in this affidavit have already been the subject of media attention, and there is a danger that the information in this affidavit could be further disseminated by journalists. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

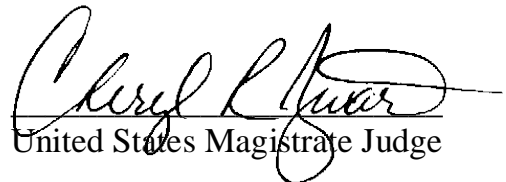
Respectfully submitted,



Jacob M. Foiles, Special Agent
Federal Bureau of Investigation

Sworn to before me by reliable electronic means:

Dated: November 14, 2019.



United States Magistrate Judge