IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 19-342
	)	
MAKSIM V. YAKUBETS	)	(18 U.S.C. §§ 371, 1349, 1344, 1343,
a/k/a Aqua	)	1030(a)(5)(A) and 1030(c)(4)(B)(i))
a/k/a Aquamo	)	
a/k/a Carlos	)	**(UNDER SEAL)**
a/k/a Shluhnet	)	
a/k/a 388888	)	
IGOR TURASHEV	)	
a/k/a Igor Tueashev	)	
a/k/a Enki	)	
a/k/a Parasurama	)	
a/k/a Nintutu	)	
a/k/a Vzalupkin	)	
a/k/a Vasya Zaluplin	)	
a/k/a Diananbeauty	)	
a/k/a domain.access	)	
a/k/a Tigrr	)	
a/k/a Tigrruz	)	

INDICTMENT

The grand jury charges:

INTRODUCTION

At all times material to this Indictment, unless otherwise alleged:

1) Malicious software ("malware") is a software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, or do other unauthorized action on a computer system. Common examples of malware include viruses, worms, Trojan horses, rootkits, keyloggers, spyware, and others.

2) Keystroke logging is the action of recording (or logging) the keys struck on a keyboard. This action is usually done surreptitiously by a computer program (i.e., keylogger) to capture the keys typed on a computer without the typist's knowledge. Malware that uses keystroke

logging often will provide the captured keystrokes to the individual who caused the malware to be installed or to a place designated by the individual. Through keystroke logging, individuals are able to obtain online banking credentials as soon as the user of the infected computer logs into their account. After obtaining this information, these individuals can access the victim's online bank account and execute unauthorized electronic funds transfers ("EFT"), such as Automated Clearing House ("ACH") payments or wire transfers,[1] to accounts that they control.

3) Web injects introduce (or inject) malicious computer code into a victim's web browser while the victim browses the Internet and "hijacks" the victim's Internet session. Different injects are used for different purposes. Some web injects are used to display false online banking pages into the victim's web browser to trick the victim into entering online banking information, which is then captured by the individual employing the web inject.

4) "Bot," which is short for "robot," is a computer that has been infected by malware and does tasks at the malware's direction.

5) A "botnet" is a network of bots. It is a collection of bots that can communicate with a computer controlling the botnet or with each other through some network architecture.

6) Bugat is a multifunction malware package designed to automate the theft of confidential personal and financial information, such as online banking credentials, from infected

[1] Electronic funds transfers ("EFT") are the exchange and transfer of money through computer-based systems using the Internet. ACH payments allow the electronic transferring of funds from one bank account to another bank account within the ACH network without any paper money changing hands. The ACH network is a network of participating depository financial institutions across the United States, and the network provides for interbank clearing of electronic payments. Because ACH payments require the network to clear the transaction, the funds are not immediately available. Wire transfers also allow electronic transferring of funds from one bank account to another bank account without any paper money changing hands; however, unlike ACH payments, wire transferred funds are immediately available.

computers through the use of keystroke logging and web injects. Later versions of the malware were designed with the added function of assisting in the installation of ransomware.[2]

7) Bugat is a malware specifically crafted to defeat antivirus and other protective measures employed by victims. As the individuals behind Bugat improved the malware and added functionality, the name of the malware changed, at one point being called "Cridex," and later "Dridex." However, each version was based upon the same original code. Hereinafter a reference in this Indictment to Bugat is meant to refer to Cridex and Dridex as well.

8) Bugat malware is generally distributed through a process known as "phishing," where spam emails are distributed to victims. The emails appear legitimate and are carefully crafted to entice the victim to click on a hyperlink or to open an attached file. By clicking on the hyperlink or opening the attached file, the victim causes the installation of malware without the victim's consent or knowledge

9) A "mule" or "money mule" is a person who received stolen funds into their bank account, and then moved the money to other accounts, or withdrew the funds and transported the funds overseas as smuggled bulk cash.

10) First National Bank was a financial institution insured by the Federal Deposit Insurance Corporation, and was headquartered in Pittsburgh, Pennsylvania. It offered online banking services through computer servers located in the Western District of Pennsylvania.

11) First Commonwealth Bank was a financial institution insured by the Federal Deposit Insurance Corporation, and was headquartered in Indiana, Pennsylvania. It offered online banking services through computer servers located in the Western District of Pennsylvania.

---

[2] Ransomware is a type of malware designed to deny access to a victim's computer and/or computer files until the payment of a ransom.

12) The Sharon City School District was a public school district located in Sharon, Pennsylvania in the Western District of Pennsylvania.

13) Penneco Oil Company, Inc., Penneco Pipeline Corporation and Pennquest Oil Corporation (collectively Penneco Oil) were petroleum businesses located in Delmont, Pennsylvania in the Western District of Pennsylvania.

14) Remington Outdoor Company ("Remington") was a firearm manufacturing company located in Madison, North Carolina.

15) 84 Lumber was a building materials supply company located in Eighty Four, Pennsylvania in the Western District of Pennsylvania.

16) Kurt J. Lesker Company was a vacuum and thin film deposition technology company located in Jefferson Hills, Pennsylvania in the Western District of Pennsylvania.

17) JWF Industries was a metal manufacturing company located in Johnstown, Pennsylvania in the Western District of Pennsylvania.

18) The defendant, MAKSIM V. YAKUBETS, was a resident of Russia. He was the leader of the group of conspirators involved with the Bugat malware and botnet. As the leader, YAKUBETS oversaw and managed the development, maintenance, distribution, and infection of Bugat as well as the financial theft and the use of money mules. At times material to this Indictment and prior to this Indictment, YAKUBETS used the online nicknames "Aqua," "Aquamo," "Carlos," and "Shluhnet," as well as the ICQ number 388888.

19) The defendant, IGOR TURASHEV, was a resident of Russia. He was a close associate of MAKSIM V. YAKUBETS and handled a variety of functions for the Bugat conspiracy, including system administration, management of the internal control panel, and oversight of botnet operations. At times material to this Indictment and prior to this Indictment, TURASHEV used the online nicknames "Enki," "Parasurama," "Nintutu," "Vzalupkin," "Vasya

Zaluplin," "Diananbeauty," "domain.access," "Tigrr," and "Tigrruz," as well as the name Igor Tueashev.

MANNER AND MEANS OF THE CONSPIRACY

20) From in and around November 2011, the exact date being unknown to the grand jury, and continuing to the present, in the Western District of Pennsylvania and elsewhere, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators, known and unknown to the grand jury, did devise, and intend to devise, a scheme and artifice to defraud and to obtain money and property through the unauthorized installation of the Bugat malware on victim computers.

21) It was a part of the scheme and artifice that the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, sent phishing emails that contained material false and fraudulent pretenses, representations, and promises, and that omitted material information, to employees of victim companies.

22) It was further a part of the scheme and artifice that the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, sent, through the Internet, these phishing emails that falsely represented to be legitimate emails from legitimate companies, associations, and organizations.

23) It was further a part of the scheme and artifice that the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, created the phishing emails to fraudulently induce recipients to click on a hyperlink or open an attachment that falsely represented itself to be a legitimate link or attachment containing business or personal information, when in truth and fact, it installed and caused the installation of the Bugat malware on Internet-connected victim computers without the email recipients' consent, knowledge, or authorization.

24) It was further a part of the scheme and artifice that the Bugat malware was designed to automate the theft of confidential personal and financial information, such as online banking credentials. The Bugat malware facilitated the theft of confidential personal and financial information by a number of methods. For example, the Bugat malware obtained such information through keystroke logging. Alternatively, the Bugat malware allowed computer intruders to hijack a computer session and use web injects to present a fake online banking webpage to trick a user into entering personal and financial information.

25) It was further a part of the scheme and artifice that the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, used the Bugat malware on infected computers to capture the user's confidential personal and financial information, such as online banking credentials, by keystroke logging or by hijacking the computer session and presenting a web inject, i.e., fake online banking webpages.

26) It was further a part of the scheme and artifice that the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, used the captured information, without authorization, to falsely represent to banks that the defendants and co-conspirators were victims or employees of victims who had authorization to access the victims' bank accounts and to make electronic funds transfers from the victims' bank accounts.

27) It was further a part of the scheme and artifice that the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, used the captured banking credentials to cause banks to make unauthorized wire transfers, ACH payments, or other electronic funds transfers from the victims' bank accounts, without the knowledge or consent of the account holders.

28) It was further a part of the scheme and artifice that the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, used money mules to receive the wire transfers, the ACH payments, or other electronic funds transfers from the victims' bank accounts.

29) It was further a part of the scheme and artifice that the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, used the money mules to further transfer the stolen funds to reach the control of other members of the conspiracy.

30) It was further a part of the scheme and artifice that, on or about November 8, 2011, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, engaged in interstate and foreign wire communications over the Internet by sending to an employee of the Sharon City School District, which was located in the Western District of Pennsylvania, a phishing email to fraudulently induce the employee to click on a graphic falsely represented to be a legitimate graphic.

31) It was further a part of the scheme and artifice that, on or about November 10, 2011, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, caused the employee to click on the fraudulent graphic and, in so doing, resulted in the unauthorized installation of the Bugat malware on an Internet-connected computer used by the Sharon City School District and located in the Western District of Pennsylvania.

32) It was further a part of the scheme and artifice that, on or about December 16, 2011, in the Western District of Pennsylvania, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, fraudulently attempted to cause the electronic transfer of $999,000.00 from Sharon City School District's

account at First National Bank to an account in the name of S.M. at PJSC Bank Forum, Kiev, Ukraine.

33) It was further a part of the scheme and artifice that, on or about August 31, 2012, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, caused the Bugat malware to be installed, without authorization, on an Internet-connected computer used by Penneco Oil and located in the Western District of Pennsylvania.

34) It was further a part of the scheme and artifice that, on or about August 31, 2012, through on or about September 4, 2012, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, used the Bugat malware to fraudulently obtain the banking credentials of Penneco Oil and to cause the transfer of funds out of Penneco Oil's bank accounts maintained with First Commonwealth Bank.

35) It was further a part of the scheme and artifice that, on or about August 31, 2012, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, used the fraudulently obtained online banking credentials to falsely represent to First Commonwealth bank that the defendants and co-conspirators were persons authorized to access the online banking accounts of Penneco Oil and to cause, or attempt to cause, the transfer of funds out of Penneco Oil's bank accounts maintained with First Commonwealth Bank.

36) It was further a part of the scheme and artifice that, on or about August 31, 2012, in the Western District of Pennsylvania, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, fraudulently caused the international electronic transfer of $2,158,600.00 from Penneco Oil's bank account x2948 at First Commonwealth Bank to an account in the name of G.S. at Krajinvestbank in

Krasnodar, Russia. The transaction was processed through Citibank, New York City, New York, as the correspondent bank for Krajinvestbank.

37) It was further a part of the scheme and artifice that, on or about September 4, 2012, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, used the fraudulently obtained online banking credentials to falsely represent to First Commonwealth Bank that the defendant and co-conspirators were persons authorized to access the online banking accounts of Penneco Oil and to cause, or attempt to cause, the transfer of funds out of Penneco Oil's bank accounts maintained with First Commonwealth Bank.

38) It was further a part of the scheme and artifice that, on or about September 4, 2012, in the Western District of Pennsylvania, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, fraudulently attempted to cause the electronic transfer of $76,520.00 from Penneco Oil's bank account x0464 at First Commonwealth Bank to a bank account at Trumark Financial Credit Union in Philadelphia, Pennsylvania.

39) It was further a part of the scheme and artifice that, on or about September 4, 2012, in the Western District of Pennsylvania, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, fraudulently caused the international electronic transfer of $1,350,000.00 from Penneco Oil's bank account x1858 at First Commonwealth Bank to a bank account at CJSC VTB Bank in Minsk, Belarus. The transaction was processed through Citibank, New York City, New York, as the correspondent bank for CJSC VTB Bank.

40) It was further a part of the scheme and artifice that the defendant, MAKSIM V. YAKUBETS, electronically communicated with Aleskey Yaroschevich a/k/a/

"morgan.zaebiz," who is located in Minsk, Belarus, to arrange money mule services for the receipt of fraudulent electronic funds transfers. On or about September 4, 2012, the defendant, MAKSIM V. YAKUBETS, provided Aleskey Yaroschevich a/k/a/ "morgan.zaebiz" with Penneco Oil's First Commonwealth Bank account information, and Aleskey Yaroschevich a/k/a/ "morgan.zaebiz" provided the defendant, MAKSIM V. YAKUBETS, with the CJSC VTB Bank account information to receive the fraudulent electronic funds transfers. On September 4, 2012, the defendant, MAKSIM V. YAKUBETS, provided confirmation that $1,350,000.00 from Penneco Oil's First Commonwealth Bank account was transferred to the CJSC VTB Bank account provided by Aleskey Yaroschevich.[3]

41) It was further a part of the scheme and artifice that the defendant, MAKSIM V. YAKUBETS, electronically communicated with an individual, who resides in the United Kingdom and who is known to the grand jury, concerning money mule services for the receipt of fraudulent electronic funds transfers. On or about August 10, 2015, this U.K. resident explained that, although he successfully cashed out approximately $25,000 on behalf of the defendant and co-conspirators known and unknown to the grand jury, he was unable to cash out more money because banks were freezing accounts and not releasing monies until after investigating the legitimacy of the wire transfers. In response, the defendant, MAKSIM V. YAKUBETS, explained that he works on the malware and botnet while another co-conspirator is "in charge of tranches."

42) On or about August 31, 2015, in electronic communications with the U.K. resident, the defendant, MAKSIM V. YAKUBETS, stated that he has two teams who worked with his malware and botnets and that each team has their own spammers (i.e., individuals who sent out phishing email campaigns) and so on.

---

[3] The Belarussian authorities arrested Aleskey Yaroschevich and three of his associates who were involved in the receipt of the fraudulent $1,350,000.00 electronic funds transfer. All four were convicted and sentenced in Belarus.

43) In subsequent conversations, the defendant, MAKSIM V. YAKUBETS, agreed, for $100,000 initial fee and 50% of all revenues with a minimum of $50,000 a week, to allow the U.K. resident to join the conspiracy, to infect computers with his malware, and to make fraudulent electronic funds transfers from funds associated with the victims of the infected computers.

44) It was further a part of the scheme and artifice that, from on or about April 20, 2016 to on or about March 17, 2017, the defendant, IGOR TURASHEV, also electronically communicated with this U.K. resident. The defendant, IGOR TURASHEV, supplied the U.K. resident with executable files for the Bugat malware so that the U.K. resident could conduct phishing email campaigns and infect computers with the malware. The defendant, IGOR TURASHEV, further provided the U.K. resident with technical assistance concerning the internal control panel used by the conspirators and concerning the botnet created by the U.K. resident's malware infections. [4]

45) It was further a part of the scheme and artifice that, subsequently, the exact date being unknown to the grand jury, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, used the Bugat malware to cause the installation of ransomware onto the victims' computers.

46) It was further a part of the scheme and artifice that, on or about September 11, 2018, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, caused the Bugat malware to be installed, without authorization, on an Internet-connected computer used by Remington.

47) It was further a part of the scheme and artifice that, on or about February 18, 2019, in the Western District of Pennsylvania, the defendants, MAKSIM V. YAKUBETS and

[4] U.K. authorities prosecuted and sentenced this U.K. resident.

IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, caused the Bugat malware to be installed, without authorization, on an Internet-connected computer used by 84 Lumber.

48) It was further a part of the scheme and artifice that, on or about March 4, 2019, in the Western District of Pennsylvania, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, caused the Bugat malware to be installed, without authorization, on an Internet-connected computer used by Kurt J. Lesker Company.

49) It was further a part of the scheme and artifice that, on or about March 19, 2019, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, engaged in interstate and foreign wire communications over the Internet by sending to an employee of JWF Industries, which was located in the Western District of Pennsylvania, a phishing email to fraudulently induce the employee to open an attached zip file.

50) It was further a part of the scheme and artifice that, on or about March 19, 2019, in the Western District of Pennsylvania, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators known and unknown to the grand jury, caused the employee to open an attached zip file and, in so doing, resulted in the Bugat malware being installed, without authorization, on an Internet-connected computer used by JWF Industries.

COUNT ONE
(Conspiracy)

The grand jury further charges:

51) Paragraphs 1 through 50 above are hereby realleged and incorporated by reference herein, as if fully stated.

52) From in and around November 2011, the exact date being unknown to the grand jury, and continuing to the present, in the Western District of Pennsylvania and elsewhere, the defendants, MAKSIM V. YAKUBETS, a/k/a Aqua, a/k/a Aquamo, a/k/a Carlos, a/k/a Shluhnet, a/k/a 388888, and IGOR TURASHEV, a/k/a Igor Tueashev, a/k/a Enki, a/k/a/ Parasurama, a/k/a/ Nintutu, a/k/a/ Vzalupkin, a/k/a Vasya Zaluplin, a/k/a Diananbeauty, a/k/a domain.access, a/k/a Tigrr, a/k/a Tigrruz, knowingly and willfully did conspire, combine, confederate, and agree together and with each other and with other persons both known and unknown to the grand jury, to commit the following offenses against the United States:

(a) to intentionally access a computer without authorization and thereby obtain information from a protected computer, which offense was committed for the purpose of private financial gain, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B);

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

(c) to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage, and attempt to cause damage, without authorization, to a protected computer, and the offense did cause and, if completed, caused loss to one or more persons during any one-year period aggregating at least

$5,000.00, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B); and

(d) to devise, and intend to devise, a scheme and artifice to defraud businesses and individuals, and to obtain money and property from these businesses and individuals, by means of material false and fraudulent pretenses, representations, and promises, and for purpose of executing such scheme and artifice, to transmit, and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, and pictures, in violation of Title 18, United States Code, Section 1343.

OVERT ACTS

53) In furtherance of the conspiracy, and to effect the objects of the conspiracy, the defendants, MAKSIM V. YAKUBETS and IGOR TURASHEV, and co-conspirators both known and unknown to the grand jury, did commit and cause to be committed, the following overt acts, among others, in the Western District of Pennsylvania and elsewhere:

(a) On or about November 8, 2011, co-conspirators sent a phishing email to an employee at the Sharon City School District.

(b) On or about November 10, 2011, co-conspirators caused the Bugat malware to be installed, without authorization, on a Sharon City School District's Internet-connected computer.

(c) On or about December 16, 2011, co-conspirators attempted to cause the electronic transfer of $999,000.00 from Sharon City School District's account at First National Bank to an account in the name of S.M. at PJSC Bank Forum, Kiev, Ukraine.

(d) On or about August 31, 2012, co-conspirators caused the Bugat malware to be installed, without authorization, on a Penneco Oil's Internet-connected computer.

(e) On or about August 31, 2012, co-conspirators caused the international electronic transfer of $2,158,600.00 from Penneco Oil's account x2948 at First Commonwealth Bank to an account in the name of G.S. at Krajinvestbank in Krasnodar, Russia.

(f) On or about September 4, 2012, co-conspirators attempted to cause the electronic transfer of $76,520.00 from Penneco Oil's bank account x0464 at First Commonwealth Bank to a bank account at Trumark Financial Credit Union in Philadelphia, Pennsylvania.

(g) On or about September 4, 2012, co-conspirators caused the international electronic transfer of $1,350,000.00 from Penneco Oil's account x1858 at First Commonwealth Bank to an account in the name of B. at CJSC VTB Bank in Minsk, Belarus.

(h) On or about September 4, 2012, outside the Western District of Pennsylvania, the defendant, MAKSIM V. YAKUBETS, provided Aleskey Yaroschevich a/k/a/ "morgan.zaebiz" with confirmation that $1,350,000.00 from Penneco Oil's First Commonwealth Bank account was transferred to a CJSC VTB Bank account.

(i) On or about September 11, 2018, outside the Western District of Pennsylvania, co-conspirators caused the Bugat malware to be installed, without authorization, on an Internet-connected computer used by Remington.

(j) On or about February 18, 2019, co-conspirators caused the Bugat malware to be installed, without authorization, on an Internet-connected computer used by 84 Lumber.

(k) On or about March 4, 2019, co-conspirators caused the Bugat malware to be installed, without authorization, on an Internet-connected computer used by Kurt J. Lesker Company.

(l) On or about March 19, 2019, co-conspirators sent a phishing email to an employee at JWF Industries.

(m) On or about March 19, 2019, co-conspirators caused the Bugat malware to be installed, without authorization, on an Internet-connected computer used by JWF Industries.

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

COUNT TWO
(Fraud Conspiracy)

The grand jury further charges:

54) Paragraphs 1 through 44 above are hereby realleged and incorporated by reference herein, as if fully stated.

55) From in and around November 2011, the exact date being unknown to the grand jury, and continuing to in and around March 2017, the exact date being unknown to the grand jury, in the Western District of Pennsylvania and elsewhere, the defendants, MAKSIM V. YAKUBETS, a/k/a Aqua, a/k/a Aquamo, a/k/a Carlos, a/k/a Shluhnet, a/k/a 388888, and IGOR TURASHEV, a/k/a Igor Tueashev, a/k/a Enki, a/k/a/ Parasurama, a/k/a/ Nintutu, a/k/a/ Vzalupkin, a/k/a Vasya Zaluplin, a/k/a Diananbeauty, a/k/a domain.access, a/k/a Tigrr, a/k/a Tigrruz, knowingly and willfully did conspire, combine, confederate, and agree together and with each other and with other persons both known and unknown to the grand jury, to commit the following fraud offense against the United States:

(a) to knowingly execute, and attempt to execute, a scheme and artifice to defraud a financial institution and to obtain any of the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, a financial institution by means of material false or fraudulent pretenses, representation, and promises, in violation of Title 18, United States Code, Section 1344.

In violation of Title 18, United States Code, Section 1349.

COUNTS THREE THROUGH FIVE
(Bank Fraud)

The grand jury further charges:

56) Paragraphs 1 through 44 above are hereby realleged and incorporated by reference herein, as if fully stated.

57) On or about the dates set forth below, in the Western District of Pennsylvania and elsewhere, the defendants, MAKSIM V. YAKUBETS, a/k/a Aqua, a/k/a Aquamo, a/k/a Carlos, a/k/a Shluhnet, a/k/a 388888, and IGOR TURASHEV, a/k/a Igor Tueashev, a/k/a Enki, a/k/a/ Parasurama, a/k/a/ Nintutu, a/k/a/ Vzalupkin, a/k/a Vasya Zaluplin, a/k/a Diananbeauty, a/k/a domain.access, a/k/a Tigrr, a/k/a Tigrruz, having devised and intended to devise a scheme and artifice to defraud First Commonwealth Bank and First National Bank to obtain monies and funds owned by and under the custody and control of First Commonwealth Bank and First National Bank by means of material false and fraudulent pretenses, representations and promises, well knowing at the time that the pretenses, representations and promises would be and were false and fraudulent when made, did knowingly execute and attempt to execute the foregoing scheme and artifice, by causing, and attempting to cause, the transfer of funds, with each transfer, and attempted transfer, being a separate count of this indictment as described below:

Count	On or About Date	Description
3	December 16, 2011	The attempted wire transfer of $999,000.00 from Sharon City School District's account at First National Bank to an account in the name of S.M. at PJSC Bank Forum, Kiev, Ukraine.
4	August 31, 2012	The wire transfer of $2,158,600.00 out of First Commonwealth Bank account x2948 belonging to Penneco Oil to an account in the name of G.S. at Krajinvestbank in Krasnodar, Russia. The transaction was processed through Citibank, New York City, New York, as the correspondent bank for Krajinvestbank.

5	September 4, 2012	The wire transfer of $1,350,000.00 out of First Commonwealth Bank account x1858 belonging to Penneco Oil to an account in the name of B. at CJSC VTB Bank in Minsk, Belarus. The transaction was processed through Citibank, New York City, New York, as the correspondent bank for CJSC VTB Bank.

In violation of Title 18, United States Code, Section 1344 and Section 2.

COUNT SIX
(Wire Fraud)

The grand jury further charges:

58) Paragraphs 1 through 50 above are hereby realleged and incorporated by reference herein, as if fully stated.

59) On or about November 8, 2011, in the Western District of Pennsylvania and elsewhere, the defendants, MAKSIM V. YAKUBETS, a/k/a Aqua, a/k/a Aquamo, a/k/a Carlos, a/k/a Shluhnet, a/k/a 388888, and IGOR TURASHEV, a/k/a Igor Tueashev, a/k/a Enki, a/k/a/ Parasurama, a/k/a/ Nintutu, a/k/a/ Vzalupkin, a/k/a Vasya Zaluplin, a/k/a Diananbeauty, a/k/a domain.access, a/k/a Tigrr, a/k/a Tigrruz, for the purpose of executing, and attempting to execute, a scheme and artifice to defraud the Sharon City School District, and to obtain money and property from the Sharon City School District, and to affect a financial instruction, that is, to obtain control of a Sharon City School District's computer and to obtain Sharon City School District's First National Bank online banking credentials in order to gain online access to funds maintained with a financial institution, by means of material false and fraudulent pretenses, representations, and promises, well knowing at the time that the pretenses, representations, and promises were false and fraudulent when made, knowingly did transmit, and cause to be transmitted, in interstate and foreign commerce, by means of wire communication, from an IP address then located in the Republic of Korea, to a computer located in Sharon, Pennsylvania, certain writing, signs, signals, and pictures, that is, an electronic phishing email that falsely represented that a graphic within the email was a legitimate graphic.

In violation of Title 18, United States Code, Section 1343.

COUNT SEVEN
(Wire Fraud)

The grand jury further charges:

60) Paragraphs 1 through 50 above are hereby realleged and incorporated by reference herein, as if fully stated.

61) On or about March 19, 2019, in the Western District of Pennsylvania and elsewhere, the defendants, MAKSIM V. YAKUBETS, a/k/a Aqua, a/k/a Aquamo, a/k/a Carlos, a/k/a Shluhnet, a/k/a 388888, and IGOR TURASHEV, a/k/a Igor Tueashev, a/k/a Enki, a/k/a/ Parasurama, a/k/a/ Nintutu, a/k/a/ Vzalupkin, a/k/a Vasya Zaluplin, a/k/a Diananbeauty, a/k/a domain.access, a/k/a Tigrr, a/k/a Tigrruz, for the purpose of executing, and attempting to execute, a scheme and artifice to defraud JWF Industries, and to obtain money and property from JWF Industries, that is, to obtain control of a JWF Industry computer and to cause the installation of ransomware on JWF Industry's systems, by means of material false and fraudulent pretenses, representations, and promises, well knowing at the time that the pretenses, representations, and promises were false and fraudulent when made, knowingly did transmit, and cause to be transmitted, in interstate and foreign commerce, by means of wire communication, from an IP address then located in Taiwan, to a computer located in Johnstown, Pennsylvania, certain writing, signs, signals, and pictures, that is, an electronic phishing email that falsely represented that an attached zip file contained a document.

In violation of Title 18, United States Code, Section 1343.

COUNT EIGHT TO TEN
(Intentional Damage to a Computer)

The grand jury further charges:

62) Paragraphs 1 through 50 above are hereby realleged and incorporated by reference herein, as if fully stated.

63) On or about the dates set forth below, in the Western District of Pennsylvania and elsewhere, the defendants, MAKSIM V. YAKUBETS, a/k/a Aqua, a/k/a Aquamo, a/k/a Carlos, a/k/a Shluhnet, a/k/a 388888, and IGOR TURASHEV, a/k/a Igor Tueashev, a/k/a Enki, a/k/a/ Parasurama, a/k/a/ Nintutu, a/k/a/ Vzalupkin, a/k/a Vasya Zaluplin, a/k/a Diananbeauty, a/k/a domain.access, a/k/a Tigrr, a/k/a Tigrruz, did knowingly caused the transmission of a program, information, code, and command, that is, caused the installation of the Bugat malware, and, as a result of such conduct, intentionally caused damage, without authorization, to a protected computer belonging to the persons set forth below, an offense which, if completed, would have caused a loss aggregating at least than $5,000 to a person during a one-year period.

Count	On or About Date	Persons
8	February 18, 2019	84 Lumber
9	March 4, 2019	Kurt J. Lesker Company
10	March 19, 2019	JWF Industries

In violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i), and Section 2.

FORFEITURE ALLEGATIONS

64) The grand jury realleges and incorporates by reference the allegations contained in Counts One through Ten of this Indictment for the purpose of alleging criminal forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(A), 982(a)(2)(B), 981(a)(1)(C), 1030(i), 1030(j), Title 28, United States Code, Section 2461(c), and Title 21, United States Code, Section 853(p).

65) The United States hereby gives notice to the defendants charged in Counts One, Eight, Nine, and Ten that, upon his conviction of any such offense, the government, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(B), 1030(i), and 1030(j), will seek forfeiture of (a) any property, real or personal, constituting or derived from, proceeds obtained, directly or indirectly, as a result of such offense, such property includes, but is not limited to, a money judgment for a sum of money equal to the proceeds obtained as a result of the offense; and (b) any personal property that was used or intended to be used to commit or to facilitate the commission of the offense.

66) The United States hereby gives notice to the defendants charged in Counts Two through Seven that, upon his conviction of any such offense, the government, pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2)(A), and Title 28, United States Code, Section 2461(c), will seek forfeiture of any property, real or personal, constituting or derived from, proceeds obtained, directly or indirectly, as a result of such offense, such property includes, but is not limited to, a money judgment for a sum of money equal to the proceeds obtained as a result of the offense.

67) If through any acts or omission by the defendant(s), any or all of the property described in paragraphs 64 to 66 above (hereinafter the "Subject Properties")

(a) Cannot be located upon the exercise of due diligence;

(b) Has been transferred, sold to, or deposited with a third person;

(c) Has been placed beyond the jurisdiction of the Court;

(d) Has been substantially diminished in value; or

(e) Has been commingled with other property which cannot be subdivided without difficulty,

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of such defendant(s) up to the value of the forfeitable property described in this forfeiture allegation.

A True Bill,

FOREPERSON

SCOTT W. BRADY
United States Attorney
PA ID NO. 88352