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

UNITED STATES OF AMERICA, v. KRASIMIR NIKOLOV a/k/a Salvadordali	Case No. 16 838 M **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Special Agent Samantha Shelnick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed as an FBI Special Agent for five months. As an agent of the FBI, your Affiant received basic training at the FBI Academy located in Quantico, Virginia. During that time, I received training in computer crime investigations. I also received training and gained experience in interviewing and interrogation techniques, the execution of federal search and seizure warrants, and the identification and collection of computer-related evidence. I am currently assigned to the Pittsburgh Field Office, Cyber Intrusion Squad. I investigate primarily computer intrusion and computer crime cases, including those involving violations of Title 18, United States Code, Sections 371 (Criminal Conspiracy), 1030 (Computer Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), and 1349 (Fraud Conspiracy). Prior to this position, I have three years' experience analyzing cyber criminal techniques, tactics, and procedures as well as four years' experience investigating threat finance networks and financial crime in the private sector.

2. The information contained in this affidavit is based upon my personal knowledge, knowledge obtained during my participation in this investigation, knowledge obtained from other

individuals, including my conversations with other law enforcement officers, knowledge obtained from my review of documents, computer records, and other evidence related to this investigation, and knowledge gained through my training and experience. 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.

3. This Affidavit is submitted in support of an application for a criminal complaint and arrest warrant for KRASIMIR NIKOLOV (NIKOLOV) a/k/a Salvadordali. As set forth herein, there exists probable cause to believe that from in or around April 2016, the exact date being unknown, and continuing to the present, NIKOLOV and others have violated Title 18, United States Code, Sections 371 (Criminal Conspiracy), 1030(a)(2) (Obtaining Information through an Unauthorized Access of a Protected Computer), 1344 (Bank Fraud), and 1349 (Fraud Conspiracy) (hereinafter collectively the Subject Crimes).

PROBABLE CAUSE

A. Overview

4. This affidavit establishes probable cause to believe that from in or around April 2016, the exact date being unknown, and continuing to the present, NIKOLOV and others have committed the Subject Crimes. As more fully described below, NIKOLOV and his associates gained unauthorized access to victim computers infected with GozNym malware (a malware that captures confidential personal and financial information, such as online banking credentials), and then used the captured information access to the victims' online bank accounts from which funds were stolen through the initiation of unauthorized wire transfers.

B. Parties Involved

5. NIKOLOV is a citizen of Varna, Bulgaria, who uses the online moniker "Salvadordali." NIKOLOV gains unauthorized access to victim computers infected with GozNym malware and captures the victims' online banking credentials to access the victims' online bank account and steal funds through the initiation of unauthorized wire transfers.

6. NORD-LOCK, INC. is a business located in Carnegie, Pennsylvania, within the Western District of Pennsylvania.

7. PNC Bank is a financial institution insured by the Federal Deposit Insurance Corporation and headquartered in Pittsburgh, Pennsylvania. PNC Bank offers online banking services through computer servers located in the Western District of Pennsylvania.

C. GozNym Malware

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

9. GozNym is a sophisticated malware variant designed to steal online banking credentials when an unsuspecting victim attempts to access its online bank account. Those stolen credentials are then used by the criminals to access the victim's online bank account in order to steal funds through the initiation of unauthorized wire transfers. GozNym malware has been used to target private businesses in the United States since at least January 2016.

10. GozNym 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. In the event a user

clicks on a hyperlink, the user is then usually redirected to an exploit kit, which is a web based software program that scans the victim's computer and operating systems for vulnerabilities and upon discovering one, forces the download of a malicious file upon the victim. In the event the victim opens an attached file, he is then directly infected either by the GozNym malware, or by a loader program, which then downloads the Gozym payload.

D. Overview of Scheme

11. NIKOLOV and others conspired to devise and execute a scheme and artifice to defraud financial institutions that were insured by the Federal Deposit Insurance Corporation (FDIC) and to obtain money and property by means of material false and fraudulent pretenses, representations, and promises by using the unauthorized installation of GozNym malware on victim computers to steal or attempt to steal funds from bank accounts in the United States and elsewhere, and to transfer the stolen funds overseas.

12. NIKOLOV and his co-conspirators intended and foresaw that their conduct would defraud companies and banks in the Western District of Pennsylvania and elsewhere.

13. Based on information developed during this investigation, I know that NIKOLOV and his co-conspirators used the GozNym malware on infected computers to capture the user's confidential personal and financial information, such as online banking credentials. NIKOLOV and his co-conspirators then used the captured information without authorization to falsely represent to banks that they were the victim or employees of the victim with authority to access the victims' bank accounts. NIKOLOV and his co-conspirators subsequently caused or attempted to cause electronic funds transfers from the victims' bank accounts into the bank

accounts of money mules,[1] including accounts controlled by NIKOLOV's co-conspirator, Boyan Latinov.

E. Investigation Concerning Nord-Lock, Inc.

14. On April 11, 2016, the FBI-Pittsburgh Office was notified by PNC Bank that one of its corporate customers, Nord-Lock, Inc. (Nord-Lock), a company headquartered in Carnegie, Pennsylvania, had been the victim of an account takeover fraud. The fraud resulted in an unauthorized wire transfer of $378,500 (USD), from Nord-Lock's online account at PNC Bank in Pittsburgh, Pennsylvania, to D Commerce Bank, AD (account number BG83DEMI92401100167438) in Sofia, Bulgaria.

15. A Nord-Lock employee, hereinafter referred to as H.L., was interviewed by the FBI. According to H.L., on April 07, 2016, a Nord-Lock employee (hereinafter referred to as N.B.) received an email containing a Word attachment that appeared to be an invoice. Nord-Lock's antivirus logs revealed that when the suspected invoice was opened by N.B., a malware loader was installed on N.B.'s computer.

16. According to H.L., on April 11, 2016, at approximately 11:00 am, N.B. was having difficulty logging-in to Nord-Lock's PNC Bank online banking portal. Around the same time, H.L. became aware that a fraudulent and unauthorized wire transaction for $378,500 had been initiated from Nord-Lock's online PNC Bank account. H.L. immediately notified PNC who initiated a wire recall and notified the FBI in Pittsburgh. Ultimately, the wire transfer was

[1] A "mule" or "money mule" was a person who received stolen funds and subsequently transfers the stolen funds in some fashion to another account or transports the funds overseas as smuggled bulk cash.

recalled and Nord-Lock suffered no loss.

17. After the fraudulent attempt, H.L. scanned N.B.'s computer with MS Endpoint Virus protection. The antivirus (AV) program quarantined "TojanDownloader:097M." According to the AV logs, this loader was installed on H.B.'s computer on April 7, 2016, the same day H.B. opened the suspicious Word attachment that appeared to be an invoice. Based on my experience and open source research, I know that this loader has been used in the recent past to download GozNym malware. As explained above, GozNym malware is a sophisticated malware variant designed to steal online banking credentials. It has been used to target private businesses in the United States since at least January 2016.

18. Nord-Lock consented to the forensic imaging of N.B.'s computer by FBI experts. An examination revealed GozNym malware, and no other malware variant, present on the computer.

19. PNC employee, hereinafter referred to as C.H., also was interviewed by the FBI. According to C.H., in addition to the Nord-Lock attempt, PNC had at least two additional fraudulent attempts at wire transfers on accounts of other PNC corporate banking customers that were associated with the GozNym malware. In all three instances, the referring Internet protocol (IP) address (i.e., the incoming IP address accessing the PNC accounts) from which the fraud was initiated was **204.155.31.133**.

20. C.H. subsequently advised the FBI that the GozNym actors were continuing to launch account takeover attacks against PNC corporate clients, but the new referring IP address was **204.155.30.8**.

21. As explained below, both referring IP addresses (**204.155.31.133** and **204.155.30.8**) were reported by private industry security researchers as an administrative panel

for the GozNym malware actors. Additionally, multiple banks in the United States that were the victims of GozNym-related fraud identified these IP addresses as the referring IP addresses.

22. According to information provided to the FBI by a trusted private industry security expert who has previously provided credible and reliable information to the FBI, IP address **204.155.31.133** was an administrative panel utilized by unknown GozNym actors utilizing the usernames "Craft" and "Salvadordali" to initiate account takeover fraud in the United States. The expert advised that Salvadordali typically utilized a virtual private network (VPN)[2] service to log-in to the administrative panel. This had the effect of shielding Salvadordali's true IP address. However, on multiple occasions, Salvadordali did not utilize the VPN service and instead logged-in to the administrative panel from the following Bulgarian IP addresses:

September 4, 2015

IP	Date	Time (EST = GMT -4)
85.91.139.248	2015-09-04	13:11:38
85.91.139.248	2015-09-04	15:13:39
85.91.139.248	2015-09-04	15:13:30
85.91.139.248	2015-09-04	13:05:47
85.91.139.248	2015-09-04	15:17:02
85.91.139.248	2015-09-04	13:10:06
85.91.139.248	2015-09-04	15:18:47
85.91.139.248	2015-09-04	13:08:31
85.91.139.248	2015-09-04	15:15:51
85.91.139.248	2015-09-04	13:14:46
85.91.139.248	2015-09-04	13:07:02
85.91.139.248	2015-09-04	15:20:46
85.91.139.248	2015-09-04	13:05:13
85.91.139.248	2015-09-04	13:13:09
85.91.139.248	2015-09-04	13:05:25

[2] VPN is a network that is constructed by using public wires—usually the Internet—to connect to a private network, such as a company's internal network.

February 15, 2016

IP	Date	Time (EDT = GMT -5)
78.83.25.35	2016-02-15	12:37:21
78.83.25.35	2016-02-15	12:41:57
78.83.25.35	2016-02-15	12:46:27
78.83.25.35	2016-02-15	12:49:09
78.83.25.35	2016-02-15	12:49:35
78.83.25.35	2016-02-15	12:49:41
78.83.25.35	2016-02-15	12:52:57
78.83.25.35	2016-02-15	12:53:53
78.83.25.35	2016-02-15	12:57:02
78.83.25.35	2016-02-15	13:00:30
78.83.25.35	2016-02-15	13:04:02
78.83.25.35	2016-02-15	13:07:51
78.83.25.35	2016-02-15	13:12:16

February 16, 2016

IP	Date	Time (EDT = GMT -5)
78.83.25.35	2016-02-16	02:20:40
78.83.25.35	2016-02-16	02:20:53
78.83.25.35	2016-02-16	02:23:15
78.83.25.35	2016-02-16	02:25:50
78.83.25.35	2016-02-16	03:14:18
78.83.25.35	2016-02-16	03:14:54
78.83.25.35	2016-02-16	03:16:34
78.83.25.35	2016-02-16	03:17:18
78.83.25.35	2016-02-16	03:17:23
78.83.25.35	2016-02-16	03:20:33
78.83.25.35	2016-02-16	03:20:37
78.83.25.35	2016-02-16	03:27:09
78.83.25.35	2016-02-16	03:28:44
78.83.25.35	2016-02-16	03:32:10
78.83.25.35	2016-02-16	03:34:43
78.83.25.35	2016-02-16	03:38:08
78.83.25.35	2016-02-16	03:39:58
78.83.25.35	2016-02-16	03:42:51
78.83.25.35	2016-02-16	03:45:16
78.83.25.35	2016-02-16	03:47:04
78.83.25.35	2016-02-16	03:49:28
78.83.25.35	2016-02-16	03:52:26
78.83.25.35	2016-02-16	03:55:25
78.83.25.35	2016-02-16	03:58:49
78.83.25.35	2016-02-16	04:01:52

78.83.25.35	2016-02-16 04:04:42
78.83.25.35	2016-02-16 04:07:13
78.83.25.35	2016-02-16 04:09:46
78.83.25.35	2016-02-16 04:12:32
78.83.25.35	2016-02-16 04:15:44
78.83.25.35	2016-02-16 04:18:22
78.83.25.35	2016-02-16 04:21:24
78.83.25.35	2016-02-16 04:24:19
78.83.25.35	2016-02-16 04:27:16
78.83.25.35	2016-02-16 04:31:00
78.83.25.35	2016-02-16 04:34:18
78.83.25.35	2016-02-16 04:37:10
78.83.25.35	2016-02-16 04:39:38
78.83.25.35	2016-02-16 04:41:50
78.83.25.35	2016-02-16 04:44:27
78.83.25.35	2016-02-16 04:46:59

March 15, 2016

IP	Date	Time (EST = GMT -4)
78.83.221.66	2016-03-15	19:09:55
78.83.221.66	2016-03-15	19:11:40
78.83.221.66	2016-03-15	19:16:04
78.83.221.66	2016-03-15	19:21:04
78.83.221.66	2016-03-15	19:22:33
78.83.221.66	2016-03-15	19:25:45
78.83.221.66	2016-03-15	19:25:49
78.83.221.66	2016-03-15	19:29:36
78.83.221.66	2016-03-15	19:29:45
78.83.221.66	2016-03-15	19:33:34
78.83.221.66	2016-03-15	19:33:38
78.83.221.66	2016-03-15	19:37:11
78.83.221.66	2016-03-15	19:37:24

March 16, 2016

IP	Date	Time (EST = GMT -4)
78.83.221.66	2016-03-16	03:43:52
78.83.221.66	2016-03-16	03:44:18
78.83.221.66	2016-03-16	03:44:38
78.83.221.66	2016-03-16	03:44:42
78.83.221.66	2016-03-16	03:46:24
78.83.221.66	2016-03-16	03:48:11

May 24, 2016

IP	Date	Time (EST = GMT -4)
78.83.221.66	2016-05-24	10:26:27
78.83.221.66	2016-05-24	10:26:41

June 11, 2016

IP	Date	Time (EST = GMT -4)
78.83.221.66	2016-06-11	03:38:54

June 12, 2016

IP	Date	Time (EST = GMT -4)
78.83.221.66	2016-06-12	02:32:27

23. A "Whois" look up of the three IP addresses revealed that they all resolved to the Internet service provider Mobiltel EAD in Sofia, Bulgaria.

24. Through cooperation with investigative police officers from Bulgarian authorities, Mobiltel EAD subscriber information was obtained. The information revealed that, from February 15 to 16, 2016, IP address 78.83.25.35 was assigned to Krasimir Nikolov, at Varna city, Ivan Aksakov street, number: 7, entrance: A, floor: 7, apartment: 37, in Bulgaria, with a MAC identification number of f8:bf:09:bf:53:5d. A MAC ID (otherwise known as a Media Access Control Address) is a unique identifier assigned to an individual computer by the manufacturer.

25. The Mobiltel information also revealed that from March 15 to 16, 2016, IP address 78.83.221.66 was assigned to Krasimir NIKOLOV, at Varna city, Ivan Aksakov street, number: 7, entrance: A, floor: 7, apartment: 37, in Bulgaria, with the MAC ID f8:bf:09:bf:53:5d.

26. A search of open source information listed the address for NIKOLOV on Aksakov Street as the address for a "trading company" business called KM-Company, Ltd., with the phone number +359889505313. NIKOLOV was listed as the contact person for this

business. Open source information associated the phone number +359889505313 with advertisements for property and hotel rentals in Varna, Bulgaria. The advertisements were posted by the user "Lansky72" and NIKOLOV, who was born in 1972, was listed as the contact. Additionally, open source information associated the username Lansky72 with numerous posts on online forums discussing topics, such as Trojan horse malware[3] and PayPal fraud.

27. According to open source information in Bulgaria, Krasimir NIKOLOV, his wife, and their son reside at the address of Varna city, Ivan Aksakov street, number: 7, entrance: A, floor: 7, apartment: 37.

28. On September 8, 2016, investigative police officers from Bulgarian authorities, along with FBI Agents from the Pittsburgh Field Office, executed a search warrant at NIKOLOV's residence located at Varna city, Ivan Aksakov street, number: 7, entrance: A, floor: 7, apartment: 37.

29. The evidence seized during the execution of the search warrant included the following items:

a. Two laptops;

b. One desktop;

c. One external hard drive

d. One iPad;

e. Writable discs;

f. Two routers;

---

[3] Trojan horse malware is any malicious computer program that is used to hack into a computer by misleading users of its true intent.

g. Two cell phones; and

h. Miscellaneous documents.

30. During the execution of the search warrant, Agents discovered Krasimir NIKOLOV's laptop that was running a virtual machine. Agents determined the virtual machine was logged into the aforementioned current GozNym administrative panel associated with IP address **204.155.30.8**, and that the panel was currently targeting U.S. banks. As explained above, the current administrative panel associated with IP address **204.155.30.8** replaced the previous Goznym administrative panel associated with IP address **204.155.31.133** which was responsible for the attack on Nord-Lock and numerous other GozNym victims in the United States.

31. Agents also found open Jabber chats confirming that NIKOLOV is "Salvadordali," the individual seen logged into the administrative panel around the time of the Nord-Lock attack.

32. Additionally, on NIKOLOV's laptop Agents discovered chats in which he discussed with co-conspirators the GozNym administrative panel associated with IP address **204.155.31.133**, which was the panel utilized in the Nord-Lock attack.

CONCLUSION

33. Based on the above information, your Affiant believes that probable cause exists that from in or about April 2016, the exact date being unknown, and continuing to the present, Krasimir NIKOLOV violated Title 18, United States Code, Sections 371 (Criminal Conspiracy), 1030(a)(2) (Obtaining Information through an Unauthorized Access of a Protected Computer), 1344 (Bank Fraud), and 1349 (Fraud Conspiracy). Accordingly, the United States respectfully requests that a warrant be issued for the arrest of Krasimir NIKOLOV.

The above information is true and correct to the best of my knowledge, information, and belief.

Respectfully submitted,

SAMANTHA SHELNICK
Special Agent, FBI

Subscribed and sworn to before me
this 8th day of September, 2016

HONORABLE CYNTHIA REED EDDY
United States Magistrate Judge