

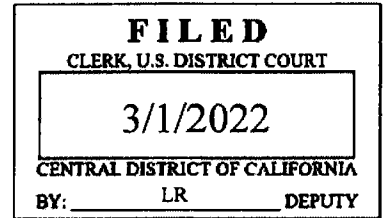
AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20)

☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California



United States of America

v.

ARTEM ALEKSANDROVICH KALINKIN,

Defendant

Case No. 2:22-MJ-00829

**CRIMINAL COMPLAINT BY TELEPHONE
OR OTHER RELIABLE ELECTRONIC MEANS**

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

Beginning on an unknown date but no later than March 2019, in the county of Los Angeles, in the Central District of California, and elsewhere, the defendant violated:

Code Section

18 U.S.C. § 371

Offense Description

Conspiracy to violate 18 U.S.C. §§ 1030(a)(2)(C);
1030(a)(4); and 1030(a)(5)(A)

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

Complainant's signature

ELLIOTT PETERSON, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: March 1, 2022

Judge's signature

City and state: Los Angeles, California

Hon. Steve Kim, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Elliott Peterson, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation and have been so employed since 2011. I am currently assigned within the Anchorage Field Office to the Cyber Squad. I perform and have performed a variety of investigative tasks, including functioning as a case agent on computer crime cases. Since becoming a Special Agent of the FBI, I have received many hours of specialized cyber training, including on the topic of computer networking, online attribution techniques, and malware analysis. I have also received training and gained experience in interviewing and interrogation techniques, the execution of federal search warrants and seizures, and the identification and collection of computer-related evidence. I specialize in the investigation of botnets, Distributed Denial of Service ("DDoS") attacks, and crimes involving embedded devices, also known as the "Internet of Things." I have previously investigated complex botnets designed to facilitate account takeover fraud, such as Gameover Zeus, Dridex, and Dyre. Those botnets functioned similarly to the DanaBot systems described within this affidavit.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a criminal complaint against and arrest warrant for ARTEM ALEKSANDROVICH KALINKIN ("KALINKIN") for a violation of 18 U.S.C. § 371

(Conspiracy to Gain Unauthorized Access to a Computer to Obtain Information, in violation of 18 U.S.C. § 1030(a)(2)(C); to Gain Unauthorized Access to a Computer to Defraud, in violation of 18 U.S.C. § 1030(a)(4); and to Commit Unauthorized Impairment of a Protected Computer, in violation of 18 U.S.C. § 1030(a)(5)(A)).

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and other witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and arrest warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only and all dates and times are approximate.

III. BACKGROUND OF INVESTIGATION AND SUMMARY OF PROBABLE CAUSE

4. As described in detail below, since at least March 2019, KALINKIN has been a principal member of a criminal group responsible for the distribution of a malicious computer software, or "malware," known as "DanaBot." DanaBot is a "Trojan" and credential stealer, meaning that it is designed to bypass a computer's malware detection capabilities in order to infect it, after which it can steal a variety of data, including information associated with online accounts, such as bank accounts, in order to facilitate fraud against those accounts. Like most malware of its type, DanaBot has the capability of performing additional criminal actions on the computers it

infects. DanaBot is an incredibly invasive malware and has the ability to hijack victim banking sessions and to record videos of user activity directly from the victim devices. Any information stored on a victim device - and many actions taken on a victim device - are vulnerable to discovery, interception, and theft by DanaBot actors.

5. As part of this investigation, I have obtained, via federal warrant or legal assistance requests to foreign authorities, copies of (1) servers which facilitated the distribution of the malware, (2) servers which served as repositories for stolen victim information and access points for criminal affiliates ("back-end" servers), (3) servers which issued instructions to victim computers ("command-and-control" or "C2" servers), and (4) relay or proxy servers which obfuscated the group's activities. By reviewing these servers, I was able to see how the malware was communicating and what information it was stealing, among other things. I was also able to identify instances in which DanaBot actors configured these servers by examining connection and activity logs contained on the servers. In addition, I have obtained copies of several computers that were infected with the DanaBot malware, which also confirmed aspects of its operation. Based on review of logs collected from DanaBot servers and examination of actual infected devices, I identified victim computers infected with the DanaBot malware in many different countries, and in numerous judicial districts within the United States, including many victims in the Central District of California.

These victims include small businesses that have suffered extensive financial fraud, U.S. and foreign governments from whom sensitive information was stolen, and large financial institutions which suffered millions of dollars in losses. To date, I am aware of hundreds of thousands of computers that appear to have been infected by DanaBot, several hundred of which appear to belong to victims located within the Central District of California.

6. Data obtained from servers that are part of the DanaBot infrastructure, as well as information provided in reports by Internet security researchers, have shown that DanaBot is organized into an "affiliate," or subscription-type, system. There is a core group of individuals - including KALINKIN, as described herein - who develop and maintain the malware and associated architecture and make it available to the criminal "affiliates," or subscribers, to use on a pay-per-month basis. The criminal affiliates pay for the right to deploy the DanaBot malware, and to use the architecture and interfaces developed by the administrators to collect and store data, with the goal of compromising victim computers and using information stolen from these computers to facilitate other illegal activity. Based upon my training and experience, I know that this is a common method through which criminals procure access to malware: they buy or lease the malware from third parties who specialize in its maintenance and development. This model is often referred to as "Crime as a Service" (CaaS) or "Malware as a Service" (Maas). Previous research performed by Internet

security companies, including negotiations for purchase of the malware, has indicated that the price per month to be a DanaBot affiliate is \$3,000 to \$4,000. That is, an affiliate would pay the DanaBot actors \$3,000 to \$4,000 each month for access to the malware, support, and infrastructure. Access would include malware configured specifically for the criminal affiliate and access to servers where the stolen data would be stored for that affiliate, including a user interface for the affiliate to access and manipulate the stolen data. It follows that the criminal affiliates would expect to realize criminal gains in an amount greater than the subscription price - that is, an affiliate would expect to make more in profit than the affiliate would pay for the right to lease DanaBot, i.e. more than \$3,000 to \$4,000 per month. Based on my review of the DanaBot servers, I have identified approximately 40 different criminal affiliates that were active between 2018 and 2021.

7. The server data also show numerous instances in which DanaBot actors - including KALINKIN - infected themselves with the DanaBot malware, thereby allowing me to view data from their own computers that was collected by the malware and stored on the DanaBot servers. In some cases, such self-infections appeared to be deliberately done in order to test, analyze, or improve the malware. In other cases, the infections seemed to be inadvertent - one of the hazards of committing cybercrime is that criminals will sometimes infect themselves with their own malware by mistake. The inadvertent infections often resulted in sensitive and compromising data being stolen from the actor's

computer by the malware and stored on the DanaBot servers, including data that helped identify members of the DanaBot organization.

8. Evidence obtained from online forums, DanaBot servers, and accounts used by KALINKIN show that he was one of the DanaBot administrators, apparently responsible for sales and support. As outlined below, KALINKIN used the online handles "Grandmaster" and "Onix" (also appearing in the variations "O*nix" and "Onx") in connection with distribution of the DanaBot malware. My identification of KALINKIN was based on online advertisements for, and discussions of, the DanaBot malware that were posted on well-known criminal forums, data on the DanaBot servers tied to KALINKIN, and records I obtained from his online accounts through the execution of federal search warrants. As described herein, these sources contained photographs, documents, and other information that revealed KALINKIN's true identity and confirmed his participation in the DanaBot conspiracy.

IV. STATEMENT OF PROBABLE CAUSE

A. DanaBot Malware Discovery and Functionality

9. DanaBot is a newer Trojan, first publicly reported in May 2018 by Proofpoint, a leading cyber-security company. I have been investigating DanaBot since approximately January 2019. As part of my investigation, I have reviewed many publications and reports on DanaBot, including Proofpoint's published reports. I have compared these reports to other publications by prominent cyber-security companies, including

ESET, Arbor, Crowdstrike, and Intel-471. In many cases, I was able to interview the authors of these reports and, in so doing, was able to learn about how the DanaBot malware was configured and what capabilities the malware possessed.

10. Proofpoint's initial report, dated May 31, 2018, indicated that its researchers had first observed the DanaBot malware on May 6, 2018, as the payload of a malicious email campaign targeted at Australia, but noted that they found even earlier indications of the malware in repositories that dated from the middle of April 2018, although those had not been seen in use targeting Proofpoint's customers. The report further documented Proofpoint's findings that the DanaBot malware contained several capabilities designed to facilitate online fraud schemes. These capabilities included the ability to "sniff" selected traffic and use banking "web injects."

"Sniffing" is a term used to denote the ability to monitor and steal certain network traffic. Commonly, this can include stealing usernames and passwords when a victim initiates an authenticated session with a given web application, such as online banking. Similarly, "web injects" is a term used to denote behavior of advanced malware that recognizes specified patterns in a user's web browsing, such as going to a bank website, and interrupts the user's legitimate session in order to inject the malware user's own traffic. In this way, cyber-criminals can choose to present to the victim a seemingly authentic online banking session in which the user is asked for a password, two-factor authentication, and security questions.

However, these questions are being "injected" into the victim's web browser by the malware, and not by the bank itself. Once the criminals have obtained this information, they can then initiate their own banking session, using the victim's stolen credentials, and attempt to steal funds from the user's bank account.

11. Proofpoint's initial report also documented its findings that the DanaBot malware had the capability to steal cryptocurrency information contained on a victim computer. Based upon my training and experience, I know that it is increasingly common for malware to search for and steal information relating to cryptocurrency accounts, passwords, keys, and wallets.

12. Finally, the Proofpoint report noted that the DanaBot malware appeared to possess the capability to take a screen-capture of a given victim's computer desktop, and that it also contained a module designed to steal email and other credentials from a victim computer. Such credentials would allow criminals to illegally access a victim's email accounts. Based upon my training and experience, I am familiar with this behavior and know that these email and account credentials are often used to facilitate further types of fraud, including bank fraud, or are resold to other criminal groups. I know of multiple instances where the compromise of such email credentials has resulted in the later theft of millions of dollars.

13. The data I obtained from both the DanaBot servers and victim computers infected by DanaBot confirmed that the malware

does indeed operate as described above. For example, according to data I was able to view from seized servers used in DanaBot architecture, at least one criminal affiliate used the DanaBot malware to target Australian banks and their customers, resulting in millions of dollars of losses. This affiliate would infect computers of victims located in Australia with the DanaBot malware and, upon infection, would use the malware to steal the victims' banking credentials. The affiliate used the stolen credentials to initiate fraudulent transfers from the victims' bank accounts. The affiliate also used web injects to hijack victims' online banking sessions.

14. Evidence uncovered during my investigation also shows that the fraud perpetrated using the DanaBot malware was not limited to banking accounts. For example, one criminal affiliate used the malware to target e-commerce third-party sellers, primarily located in the United States, including in the Central District of California; this scheme also resulted in millions of dollars of losses. The affiliate would use the malware to steal credentials for the victims' e-commerce storefront accounts. The affiliate would then purchase items from the storefront, initiate a "return" of the items, and use the stolen credentials to issue refunds in amounts greater than the original purchase price (often two to three times greater). In one specific instance of this scheme, which unfolded in 2019, a company headquartered in the Northern District of California, but that conducts business and has facilities in the Central District of California, noticed an unusual number of product

returns and refunds in its online sales logs. In most cases, the amount returned was several times higher than the purchase price. The sales logs indicated that the company itself had authorized these refunds, but a representative for the company told me that no employee at the company had actually done so. The company believed that its primary customer service computer may have become infected, based on the credentials used in the fraud scheme. I later examined that computer, and discovered that it was indeed infected with the DanaBot malware. According to sales logs, the stolen credentials were used to authorize the fraudulent refunds, causing a loss to the company of almost \$100,000. Data from DanaBot servers, e-commerce records, and other investigation showed that several companies located within the Central District of California similarly fell victim to compromise by DanaBot malware and this "return fraud" scheme, including a sanitation supply company and a clothing manufacturer.

15. The seized DanaBot servers contained evidence of over 100,000 similar intrusions and victimizations performed by approximately 40 different criminal DanaBot affiliates. These infections targeted various geographic regions around the world, including the United States, Australia, Italy, and Poland. Based upon an analysis of victim IP address, or other identifying information such as the name of a victim's business name or a listed location or address, I determined that several hundred victims appeared to be located within the Central District of California. I observed the theft of many forms of

sensitive data, from credit card numbers, to passwords, to computer browsing history and bank account information. This information was then used in a multitude of fraudulent schemes. Some victims related to me that their balances from online payment services such as PayPal were emptied out. Other victims told me that their bank accounts were drained. One victim showed me how the victim's Facebook advertiser account had been compromised and thousands of dollars had been fraudulently directed to an advertisement for malicious software. Many victims were online retailers and saw extensive fraud conducted on their sales platforms, resulting in losses that I estimate to be in the millions of dollars. Some victims had their mail servers compromised, due to credential theft by DanaBot malware, resulting in the compromise of internal and external communications, the contents of which were used to facilitate additional fraud schemes against the victims. Finally, I also uncovered extensive and deliberate targeting of a number of government computer systems, where the malware was used to steal a variety of types of sensitive data.

B. Criminal Forum Posts Advertising DanaBot

16. From posts dating back to at least 2015 on well-known online criminal forums that cater to Russian-speaking cyber criminals, I identified an individual using the nickname "JimmBee" who was inviting partners to work with him on a malicious software project, and later offering it to customers. As time went on, another individual appeared in the posts, using the nicknames/handles "Onix"/"O*nix" and "Grandmaster," who

appeared to be specifically responsible for support and sales. An internet security company later purchased and analyzed the software offered by "JimmBee" and "O*nix" and confirmed that it was DanaBot.

17. One of the main examples of these communications is a thread that originated in 2015 on Exploit.im, a Russian-language criminal forum. In the first post, dated September 19, 2015, "JimmBee" said that he was seeking investors or partners for updating a malicious software he referred to as "FormGrabber" (transliterated from English to Russian as "ФормГраббер"). "JimmBee" described the software as a "multipurpose private form-grabber,"¹ which I understand to mean a malware designed to steal, or "grab," data from forms, or web pages. A picture of the initial Russian post, along with a translation, is attached hereto as Exhibit A. In another post the next day, "JimmBee" elaborated that his project was a "Form grabber, keylogger, injector, and lots of nice VNC and other features... Tricks, nuances, diligence, and high-quality code."² In the original post, "JimmBee" provided the jabber³ contact

¹ The forum communications were in Russian. Translations of Russian text herein and in the attached exhibits were provided by Russian-language speakers who are familiar with cybercrime terminology, but should be considered draft translations.

² Based on my training and experience, I understand these terms to describe malicious computer activity, designed to steal information from, and compromise the integrity of, computer systems, as well as to advertise the quality of service users could expect to receive for their paid subscription.

³ Jabber is a communication protocol that is commonly used for exchanging instant messages; although used for many purposes, it is favored by cybercriminals because it functions
(footnote cont'd on next page)

"main.villain@xmpp.ru." The signature line appended to "JimmBee's" posts throughout the ensuing thread included contact information for the FormGrabber "creator" as jabber IDs "sportbetter@jabbim.cz" and "unfeelingmonster@exploit.im," and for "support" as jabber IDs "grandmaster@verified.pm" and "grandmaster@laba.im."⁴

18. After a few follow-up posts from "JimmBee" directing any interested parties to contact him via jabber, this thread went dormant for more than two years. On April 16, 2018,⁵ "JimmBee" reappeared in the thread, and posted a specific description of the functionality of the malware he and his partners had been developing, including the computer systems it would run on, its ability to remain invisible to the computers it infected, its inclusion of a keylogger, its ability to record video of the victim's screen and to perform various other

as a decentralized platform, and allows for private, anonymous communication. Every user on the network has a unique address, called a jabber ID (or JID), that is structured like an email address - e.g. username@example.net. The first part of the address is generally considered the handle of the user - e.g. "main villain," "sportbetter," or "unfeelingmonster"; users will sometimes use the same names across platforms, and it is not uncommon for the same user to have several different handles.

⁴ Due to the ability of users to modify the signature lines of their postings, and based on review of subsequent posts, these jabber IDs were likely added at some point after the thread was initiated in 2015. For example, in April 2018, after "JimmBee" reappeared after extended silence, he stated in a post that his "new" jabber ID was "unfeelingmonster@exploit.im," so this address was likely added to the signature at or after that point. Similarly, on June 18, 2018, he posted that he had another new jabber ID, "sportbetter@jabbim.cz."

⁵ Notably, this timing is consistent with the observations of the DanaBot malware by Proofpoint, described above: the first samples were observed in repositories in mid-April 2018, with the first phishing email campaigns (targeting Australia) showing up in May 2018.

illegal operations, as well as descriptions of the server and control modules available to customers. Further exchanges over the next few weeks within this thread included discussions of the ability of the malware to avoid detection by numerous antivirus and computer security systems, messages with potential customers, and messages from users vouching for the functionality of the malware. "JimmBee" made clear in posts that he would not work with people that did not have "good" reputations or could not confirm their reputations on "subject-specific forums." He further indicated that he would not work with people who could not speak Russian, noting "If you can pay for the work of software then I think you will not have problems to hire a translator...so I don't work with people without reputation."⁶ On May 27, 2018, "JimmBee" posted that he and his partners had made several improvements in the malware, and they were "ready to hire one or two partners," and indicated that interested persons should contact him via jabber. On June 14, 2018, "JimmBee" posted that "One more partner [was] required." He added, "We also need a person to deal with cryptocurrency-

⁶ I know, based on my training and experience, that it is common for Russian cyber criminals to be skeptical of persons they are not familiar with and who have not developed longstanding reputations on criminal forums, like Exploit.im. This is often a way of ensuring both that the person is not connected to law enforcement or internet security companies, and also that they will not scam the cyber criminal. In addition, I know that it is common for Russian cyber criminals to be wary of persons who do not speak Russian, for similar reasons.

related schemes (it is preferable to have experience in dealing with ATS,⁷ web-injects, etc.)."

19. On July 29, 2018, "JimmBee" posted: "My offer is available for movers and shakers. Contact me via Jabber. We are looking forward to cooperating with you." On September 11, 2018, a user named "Margus" posted a review of the malware in the thread. "Margus" described all of the features as functioning properly, noting that s/he had been using the product for several weeks. "Margus" also commented, "They provide a proper support service, modify and refine some small things according to my, of course, reasonable requests. :) It's the best software I have ever used. You just need good installs to work profitably." Between September and December 2018, users posted that they could not get in touch with the malware sellers. Then, on February 26, 2019, "JimmBee" reappeared and posted, "The offer is valid. We're looking for partners."

20. Shortly thereafter, in March 2019, the user "O*nix" began posting within this same thread and responding to customer questions. On March 4, 2019, a customer using the name "Fixxx" asked about the build size and runtime detection rate of the malware, and said that he had been waiting for a reply on jabber. "O*nix" responded on March 17, 2019, writing that there were various options available with the malware, and that it

⁷ I know, based on my training and experience, that ATS stands for Automatic Transfer Script (or System), which is a tool to automate online banking fraud.

would depend also on whether the customer used "our crypting"⁸ services or those offered by third parties." "O*nix" added, "If you use third-party services, we can't say how much rubbish they will add to the build. If we crypt it, the size of each file will change dynamically within the limits." A copy of this post, along with a translation, is attached hereto as Exhibit B. "Fixxx" complained that s/he still hadn't received a reply on jabber, and the following day, "JimmBee" joined the discussion to provide his jabber IDs as "sportbetter@jabbim.cz" and "unfeelingmoster@exploit.im," and indicated that the "Support Jabber" (i.e. the account to contact for support) was "grandmaster@verified.pm." "JimmBee" asked where "Fixxx" had sent messages, and "Fixxx" indicated it was not the first two addresses (presumably indicating he had contacted "grandmaster" instead). On April 5, 2019, "O*nix" posted a message that the jabber ID in the signature line for the thread (i.e. "grandmaster@verified.pm") was temporarily unavailable, and told customers to use the jabber ID "grandmaster@laba.im" to communicate further. Then, on May 13, 2019, "O*nix" responded to his own post and said, "All our Jabber IDs are available. We are open for business." (Copies of these posts are also attached in Exhibit B hereto.) On June 25, 2019, in response to a customer asking how much they wanted for the malware, "O*nix" responded, "Write using the contact in the signatures" (i.e. the

⁸ "Crypting" refers to encrypting/obfuscating malware to make it harder to detect by antivirus or other security programs. It is used by cybercriminals to create malware that can bypass security programs by presenting itself as a harmless program until it gets installed.

jabber IDs in the signature lines of the posts). On August 28, 2019, "O*nix" noted to anyone who was interested in "working together" that he could refuse to partner up at any time, and, similar to "JimmBee's" prior statements, that he was not interested in "people who don't have a good reputation score and are unable to prove their reputation on specialized forums."

21. After a few months of no further posts on this thread, on January 19, 2020, "JimmBee" posted again and said, "We're looking for partners. Contact us on Jabber." On March 31, 2020, a user named "cybercartel" wrote, "Been using software for a month now, good software, great support! Thank you." Finally, in March 2020, "O*nix" posted again, claiming, "Most bot modules have been updated. A few additional slots for customers have been added"; he then provided additional information about a new tool (a "VBS Dropper") the team had made available, which, as he described, allowed the malware to be loaded (or "dropped") onto victim computers and remain undetected for a considerable period of time. He added, "As usual, bot owners get a discount :)" - which I believe to mean that current customers of the DanaBot subscription would receive a discount on the VBS dropper tool.

C. Direct Contact with "JimmBee" and "O*nix" Regarding Danabot

22. I spoke with members of a U.S.-based threat intelligence company,⁹ who told me that in 2018, they contacted

⁹ A threat intelligence company is an Internet security company that specializes in investigating people and their communications in the context of computer crime. Such companies will often have employees who can communicate in different languages and are familiar with the websites and terminology common in cyber-crime underground communities.

"JimmBee," via one of the accounts listed in the posts described above, and negotiated a purchase of the "FormGrabber" software. Subsequent analysis performed by the same company of the software purchased from "JimmBee" found that what he called "FormGrabber" was, in fact, the malware that later came to be named DanaBot by internet security researchers.¹⁰

23. In August 2019, an FBI Confidential Human Source ("CHS")¹¹ had an online conversation about purchasing the malware by contacting the "grandmaster@verified.pm" jabber ID listed in the thread described above. During this conversation, "grandmaster" detailed the capabilities of the DanaBot malware and offered it for sale to the CHS.

a. During the exchanges with the CHS, "grandmaster" also provided a copy of a document with the filename "help" for the DanaBot malware (called "Windows RAT"¹² in the document

¹⁰ There are many ways that malware comes to be named. Sometimes criminal groups choose a name for their malware and use it in marketing. Other times, a product will gain a name from a specific, unique fragment of code discovered during analysis. In this case, the malware was named after an employee of one of the first security companies to discover it. The name was thereafter adopted by the rest of the security community, and eventually, the criminals themselves.

¹¹ This CHS is a Russian-language speaker who is cooperating as a result of criminal charges pending in a separate district; I am unaware of any criminal convictions for this person. The CHS was not directed to communicate with DanaBot members, but rather to have incidental contact with members of various online criminal services. I have not interviewed the CHS myself, but I have reviewed the communications between the CHS and "Grandmaster" and found them to be accurate and consistent with other information gathered in this investigation.

¹² A RAT is a "remote-access trojan," a type of malware that disguises itself while loading, but once installed, allows a criminal to control the victim computer, often in a largely invisible fashion.

itself), which included a written description of its functionality, and appeared to be an instruction manual for new customers. A copy of the first page of the file, along with an English translation, is attached hereto as Exhibit C. Copies of this same document were also obtained independently by security researchers, and I recovered a copy of it from one of the DanaBot servers I searched as well. The file describes in very plain terms the criminal functionality of the malware, including, among other things, its ability to operate invisibly on the entire line of Windows systems starting from XP; its ability to log keystrokes; its ability to record video from the infected user's screen; its supportive architecture which allows the criminal affiliate to work offline or online with victim computer files; its ability to perform web injects; its ability to load additional files onto victim computers - which can be targeted at certain countries, IPs, etc.; and its inclusion of a stealer (transliterated from English as "stiller") module which was designed to collect data stored by web browsers, email programs, messaging systems, and more.

24. Similarly, the prominent Internet threat intelligence company Intel-471 published a report in 2019 about engagement with O*nix, which I have reviewed. The researchers reported seeing posts on an online forum in which the user "O*nix" offered a private bot.¹³ The researchers reported that a

¹³ I know from my training and experience that in this context, criminals often use the term "bot" to refer to malware that allows the remote control and compromise of victim computers, at scale.

reliable source with whom they work engaged with O*nix and relayed the following information: "O*nix" was a long-standing member of the Russian-language cybercrime forum "Exploit," and used two jabber ID's: "grandmaster@verified.pm" (i.e. the same jabber ID contacted by the CHS and listed for DanaBot support in the thread described above) and "onix@exploit.im." In exchanges with the source, "O*nix" offered to rent a private banking bot for US \$3,500 per month, or a week-long test for US \$500. According to the source, O*nix described the various criminal features of the bot, which accorded with the descriptions in the "help" file described above, including its ability to install a malware loader on an infected system, an included keylogger, and the ability to take videos and screenshots of the infected user's screen, download files, and steal certain information from the infected device, among other things. "O*nix" also provided a video of how the bot operated.

D. Further Research Into "O*nix"/"Grandmaster"

25. As described above, in the posts about the DanaBot malware on the Exploit.im forum, the user posting as "O*nix" on that forum used "grandmaster" as the name for his jabber IDs, indicating that he used both handles. Similarly, security researchers investigating the DanaBot malware found that this actor used several online handles, including "grandmaster," "O*nix," "EoGeneo," and "MafiozI" (or variations thereof).

26. For example, as indicated in the Intel-471 report described above, research into "O*nix's" activity on the Exploit forum showed that he had previously offered to sell

root/administrative access to servers controlled by mail.ru, a large email provider in Russia, and had provided the ICQ number 4633355.¹⁴ The researchers conducted searches relating to that ICQ number, and found it to be used by the persona "EoGeneo" on another forum; the "EoGeneo" user ID in turn was set up using the email address "artem-korp@mail.ru," with a listed date of birth of July 13, 1990. Further review of posts by the "EoGeneo" persona showed that he also used the alternative handle "MaffiozI," and had a VKontakte¹⁵ account registered under the name "Арте́м Сиби́ряк" ("Artem Siberian").

27. Additional evidence regarding these handles on Russian-language cyber criminal forums confirmed these assessments. For example, I found that accounts using both the "grandmaster" and "O*nix"/"Onix" handles used the same ICQ account identified by the security researchers, 4633355.¹⁶

¹⁴ ICQ is an instant messaging service that uses numerically based account numbers, somewhat similar to phone numbers. ICQ is a popular service among cyber criminals. Many criminals retain their account numbers for long periods of time, and since smaller ICQ numbers can be a sign of prestige (because they indicate the user was an early adopter of the platform), some members retain their account numbers indefinitely.

¹⁵ VKontakte, or VK, is a Russian social media platform similar to Facebook.

¹⁶ The security researchers also found one reference to this ICQ number on a forum relating to Toyota Prius owners. The forum user was "alexandr43," and he had provided a date of birth of [REDACTED] 9 and a location of Novosibirsk, Russia. Notably, upon searching KALINKIN's social media accounts, as described herein, I found documents indicating that KALINKIN's father was named [REDACTED] and had a date of birth of [REDACTED] 1. I do not believe this post relates to KALINKIN's criminal activity, but could indicate KALINKIN's father borrowing KALINKIN's ICQ account, particularly given the Novosibirsk location.

E. Identification of KALINKIN as "Grandmaster"/"O*nix"

28. As described above, evidence had begun to provide indications that the "Grandmaster"/"O*nix"/"Onix" persona was an individual named Artem, likely in Siberia, and with a possible date of birth of July 13, 1990. I conducted substantial additional research, detailed below, that confirmed this actor's identity as Artem Aleksandrovich KALINKIN, a resident of Novosibirsk, Russia, who had that same date of birth. The evidence I found shows KALINKIN's extensive and pivotal involvement in the DanaBot conspiracy.

1. Review of data from "Onix's" infected computer leads to discovery of his online accounts

29. First, as described above, I obtained copies of several servers used by the DanaBot malware infrastructure, either by federal search warrant or via legal assistance requests to foreign authorities. These servers served as repositories for the majority of information stolen from DanaBot victims.

30. From my review of these servers, I discovered that a computer with the active user ID of "onx" (which appears to be a variation of the handles "O*nix" and "Onix") had been infected with the DanaBot malware, thereby allowing me to view data from this computer that was stored on the DanaBot servers. System information about the computer captured by the DanaBot software showed that the infected computer was located in Russia, and was set to use the Russian language. Based on my training, experience, and knowledge of this investigation, the computer's

location indicated to me that this was a "self-infection," meaning that the user of the computer had installed DanaBot malware on the computer either inadvertently or for the purpose of testing the malware. Specifically, of the hundreds of thousands of computers infected by DanaBot that have been identified, only a tiny number were in Russia; the server data shows that nearly all of those Russian computers appeared to be used to test or develop the DanaBot malware, rather than reflecting the type of activity seen among actual victims, indicating that they were used by DanaBot actors rather than victims.

31. This choice of apparently designing or deploying malware so as to not target computers within Russia is consistent with other sophisticated cyber criminal groups that I have investigated. What is more, the core DanaBot members, including KALINKIN, seem particularly tied to Russia and Russian themes. For example, they appear to have adopted as an informal trademark for the malware the former Soviet symbol of a hammer and sickle. This logo appeared both on the client application given to criminal affiliates as well as on the instructional "help" document described above (see Exhibit C). I also found within communication accounts the exchange of what appeared to be many Russian patriotic memes. It was therefore consistent with my experience with and knowledge of other Russian cyber criminal groups that I did not see a large number of "victim" computers located within Russia, and, in fact, the majority of the Russian-based computers infected with DanaBot that I

examined appeared to be computers connected to the administrators themselves, or to their customers, and likely reflected either accidental or testing and development infections.

32. Also relevant to the "onx" infection, the "onx" computer appears to have become infected multiple times. That is, I have discovered infections tied to different DanaBot affiliate IDs, for different time periods, but which infected the same computer. In my investigation, I have not observed any apparently true victim whose computer was infected by DanaBot more than once, strengthening my belief that the infections of the "onx" computer were self-infections either associated with deliberate testing of the malware, or with careless handling of the live malware samples.

33. Further, the DanaBot malware, as it was designed to do, captured the "onx" computer's browsing history, which revealed frequent use of DynCheck.com. DynCheck.com is a tool that allows users to submit copies of malicious files in order to determine if the files are recognized by commercial anti-virus products (and thus are not as likely to successfully infect their intended victims). I am unaware of the commercial use of DynCheck by non-criminal entities. Based on my training and experience, I believe that the "onx" computer likely became infected with DanaBot while handling the malware, such as would be required to submit the DanaBot malware to a service like DynCheck. In fact, DynCheck figured prominently in the advertising of DanaBot malware. At several times within the

previously referenced thread on the Exploit forum, "JimmBee" posted the results of anti-virus checks, including results that he represented as being from a scan using DynCheck.¹⁷ Thus, this use of DynCheck is consistent with the browsing history on the "onx" computer, and its possible source of self-infection.

34. Finally, as the malware was also designed to do, it recorded the user of the "onx" computer accessing various accounts, including cryptocurrency accounts, using the credentials "artemsiberian@icloud.com" and "maffiozmobile@gmail.com," among others. As noted above, the handles "Artem Siberian" and "MaffiozI" were observed by researchers investigating the identity of "O*nix"; thus, these account names corroborated the connections between these handles and the person known as "Grandmaster"/"Onix"/"O*nix." The malware also simultaneously recorded the IP address¹⁸ assigned to the infected computer, which then connected to further investigation, described below.

¹⁷ These results show that very few of the world's leading anti-virus products were detecting DanaBot - so few that the posts spawned conversations between "JimmBee" and prospective customers who believed that the low anti-virus detection rates were too good to be true. Ultimately, "JimmBee" conceded that his assistant, who I believe to be "O*nix," may have run the queries improperly, leading to an exaggeration of how effective DanaBot was at evading malware detection (and also possibly leading to "O*nix's" self-infection). However, JimmBee appears to have run the check again and still found a very successful rate of evasion, as he reported only 6 out of 23 services detected the malware. My investigation has confirmed that DanaBot was very effective at evading many of the prominent anti-virus products, especially early in its development.

¹⁸ An "Internet Protocol" (IP) address is the globally unique address of a computer or other device connected to a network, such as the Internet, and is used to route Internet communications to and from that computer or device.

2. Review of "Onix's" accounts confirms his DanaBot activity and use of the "Grandmaster" and "Onix" handles

35. I obtained data from Apple and Google for the "artemsiberian@icloud.com" and "maffiozimobile@gmail.com" accounts. The data confirmed that the accounts were used by the same individual as the infected "onx" computer, that this individual also used the "grandmaster@verified.pm" account, and that the user was a DanaBot administrator.

36. For example, in the access logs for both the "maffiozimobile@gmail.com" and the "artemsiberian@icloud.com" accounts, I observed access by the same IP address that was recorded by the DanaBot malware as being used by the "onx" computer. Based on my training and experience, this indicates that the computer and the accounts were controlled and accessed by the same individual.

37. Further, a record of online searches within the "maffiozimobile@gmail.com" account revealed that the user had performed multiple searches related to DanaBot. For example, in January 2019, the user conducted a search for the terms "DanaBot Avira" and then viewed a webpage which displayed research by Avira, an Internet security company, about the DanaBot malware. Similarly, in July 2018, the user conducted a search for the term "DanaBot" and then viewed two reports published by Proofpoint that discussed the DanaBot malware. Examination of browser data associated with the "artemsiberian@icloud.com" account showed that the user had conducted similar searches related to the analysis of the DanaBot malware.

38. Also in the "artemsiberian@icloud.com" account, I found hundreds of photographs of computer screens reflecting various activities and communications, many of which related to online criminal activity. Many of these photographs showed the user's involvement with the DanaBot malware and/or with the "grandmaster" and "onix" handles.

a. For example, I found photographs of a computer screen that reflected a conversation between "grandmaster@verified.pm" and "chopin@exploit.im," in which "grandmaster" and "chopin" talked about a problem with the crypting of the malware loader, and "chopin" pasted a chat he had had with the "technician" about the issue (the image of the conversation is attached as Exhibit D). Notably, I previously identified "chopin" as a DanaBot criminal affiliate by analyzing a user table found on the DanaBot back-end server, which was used to authenticate users of the server. The table depicted active affiliates by their affiliate number and jabber ID. The entry for Affiliate 14 listed the jabber ID "chopin@exploit.im." The table also contained a user named "Root" (which I know, based on my training and experience, to be a common title for administrator accounts), which listed the jabber ID "grandmaster@verified.pm," providing further evidence that "grandmaster" was one of the DanaBot administrators.

b. Another photograph seized from the "artemsiberian@icloud.com" account (attached hereto as Exhibit E) depicted an instant messaging client in which the user was simultaneously logged into three instant messaging accounts:

"onix_onx@jabber.ru," "spam@185.199.80.103," and "grandmaster@verified.pm." This photograph thus further indicates that the user of the "artemsiberian@icloud.com" account is also the user of the nicknames "Onix"/"O*nix"/"Onx" and "Grandmaster," and specifically, the account provided as the contact for DanaBot support in the Exploit post, "grandmaster@verified.pm." The photograph also displays portions of the account holder's list of "buddies," which included the usernames "benzz@exploit.im," "chopin@exploit.im," "diveragent@exploit.im," and "flawless." I recognize each of these users to be DanaBot criminal affiliates based on my review of data from the DanaBot servers, including the authorized user table described above, which included both "chopin@exploit.im" and "benzz@exploit.im." I recognize "diveragent@exploit.com" and "flawless" as DanaBot affiliates from other data on these servers.

c. I also found a photograph that depicted a "root" login to the DanaBot software, a copy of which is attached hereto as Exhibit F. I know this to be the DanaBot software because I have seen several examples of the DanaBot client software throughout this investigation, and it has a very distinct appearance. As described above, based on my training and experience, I know that "root" logins are typically administrative logins, indicating that the user of this account was logging in to the DanaBot software as an administrator. The photograph also showed an IP address to which the client appeared to be making a connection. I recognized that IP

address to be assigned to a DanaBot server that I had previously searched and analyzed. Thus, this photograph corroborates this account user's role as a DanaBot "root" level administrator, with access to DanaBot's back-end infrastructure where victim data was maintained, and from which commands to victims were issued.

39. Finally, in the data associated with the "artemsiberian@icloud.com" account, I discovered a file that actually contained the DanaBot client software itself. This software allows an individual with the proper login credentials to review each device infected by DanaBot, examine stolen data, and issue additional commands such as the downloading of files from a victim computer. The possession of this file by this user indicates that the user is either a criminal affiliate or an administrator of the DanaBot malware; all of the above information signifies that the user of the "artemsiberian@icloud.com" account is, in fact, the latter.

3. KALINKIN is identified as the user of
"artemsiberian.icloud.com" and
"maffiozmobile@gmail.com"

40. Both of the above-listed accounts also contained many indications of the user's real identity. For example, in the "artemsiberian@icloud.com" account, I observed photographs of work emails and financial invoices containing the name Artem Aleksandrovich Kalinkin (Артём Александрович Калинин) and the name of a large Russian corporation which I understand to be his employer. An image of one such email is attached in redacted form as Exhibit G.

41. Also in the "artemsiberian@icloud.com" account, I found photographs of a Russian driver's license and passport¹⁹ in the same name, showing a date of birth of July 13, 1990 (i.e. the same date of birth identified for "O*nix" by the Intel471 researchers), along with thousands of photographs that depict the same individual, his family, and his friends. The photograph of the passport is attached as Exhibit H. Based on these documents, I believe the user of this account is KALINKIN, and thus that KALINKIN is "Grandmaster" and "O*nix"/"Onix."

42. Similarly, in the "maffiozimobile@gmail.com" account, I found additional corporate emails bearing KALINKIN's true name. I examined email header information associated with these emails and was able to determine that they originated on a mail exchange server registered to the same Russian corporation. Several of these emails included photographs which depicted KALINKIN at corporate events. One such email is attached hereto as Exhibit I. The photographs associated with these emails depict the same individual who appears in "artemsiberian@icloud.com" account. Thus, I was able to confirm that the "artemsiberian@icloud.com" account, the "maffiozimobile@gmail.com," and the corporate email account were all used by KALINKIN, and therefore that he is the actual person behind the "Grandmaster" and "Onix" handles.

¹⁹ I also found photographs of passports of other people, including individuals who appear to be KALINKIN's girlfriend, family, and/or friends, who appear to have traveled with KALINKIN on international trips, based on the photographs I have seen. However, all of the other evidence in the accounts discussed above confirms that KALINKIN is the actual user.

V. CONCLUSION

10. For all the reasons described above, there is probable cause to believe that KALINKIN has committed a violation of 18 U.S.C. § 371 (Conspiracy to Gain Unauthorized Access to a Computer to Obtain Information, in violation of 18 U.S.C. § 1030(a)(2)(C); to Gain Unauthorized Access to a Computer to Defraud, in violation of 18 U.S.C. § 1030(a)(4); and to Commit Unauthorized Impairment of a Protected Computer, in violation of 18 U.S.C. § 1030(a)(5)(A)).

/s/

ELLIOTT PETERSON, Special Agent
Federal Bureau of Investigation

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on this 1st day of
March, 2022.



HONORABLE STEVE KIM
UNITED STATES MAGISTRATE JUDGE