



IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

JURIJS MARTISEVS,

Defendant

Criminal No. 1:16-CR-228

Hon. Liam O'Grady

STATEMENT OF FACTS

The United States and the defendant, JURIJS MARTISEVS ("MARTISEVS"), agree that the following facts are true and correct, and that had this matter proceeded to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence.

1. From at least 2009, and continuing until May 2017, in the Eastern District of Virginia and elsewhere, MARTISEVS knowingly and intentionally conspired and agreed with Ruslans Bondars ("Bondars") and others, to commit offenses against the United States, that is:

a. to intentionally access a computer without authorization and exceed authorized access, and thereby obtain information from any protected computer, for purposes of commercial advantage and private financial gain, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(i);

b. to knowingly and with intent to defraud access a protected computer without authorization and exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value, in violation of Title 18, United States Code, Section 1030(a)(4); and

c. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to 10 or more protected computers during any one year period, in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(A)(i)(VI).

2. In addition, and as explained in more detail in paragraphs 20 through 28, from on or about October 15, 2012 through on or about December 2014, within the Eastern District of Virginia and elsewhere, MARTISEVS knowingly and intentionally aided and abetted computer intrusions with the intent to cause damage, and did cause damage to more than 10 protected computers within the one-year period of January 1, 2013 through December 31, 2013, in violation of 18 U.S.C. § 1030(a)(5)(A).

The Counter Antivirus Service

3. From at least 2009, and continuing until May 2017, MARTISEVS and Bondars agreed, combined, and worked together with each other and others to operate a counter antivirus service (hereinafter, the “SERVICE”). Bondars was a non-citizen of Latvia who resided in Riga, Latvia, while MARTISEVS was a citizen of Russia who resided in Moscow, Russia.

4. The SERVICE was a counter antivirus service that provides information that computer hackers used to determine whether the computer viruses and other malicious software (“malware”) they created would be detected by antivirus software, including and especially by antivirus software used to protect major United States retailers, financial institutions, and government agencies from computer intrusions. The SERVICE operated as an antivirus clearinghouse, making it possible for users to check their files against the databases of dozens of widely used brands of antivirus software. Users submitting files to the SERVICE were essentially checking their files against the “signatures,” or information about the characteristics

of known malware, to determine if their files contained characteristics that antivirus companies would flag as a virus or malware.

5. The purpose of the SERVICE, and MARTISEVS and Bondars' intent in operating the SERVICE, was to aid and abet the development of malware and the resulting unauthorized computer intrusions. In particular, MARTISEVS and Bondars intentionally ran the SERVICE in a manner that allowed malware developers to learn whether their malware would be detected by antivirus software and, if their malware was detectable, make changes to their malware so as to reduce the chances that the malware would be detected by the antivirus systems of the companies and institutions they targeted. At all relevant times, MARTISEVS knew and understood that the malware that the SERVICE was assisting in developing was designed to be used, and was in fact being used, to commit illegal and unauthorized computer intrusions against computers in the United States and elsewhere. At all relevant times, MARTISEVS acted with the intent and goal of aiding, abetting, and furthering these illegal computer intrusions and causing them to occur.

6. MARTISEVS was the co-owner and co-administrator of the SERVICE along with his partner, Bondars. MARTISEVS' responsibilities in the conspiracy included, among other things, providing customer support to the SERVICE's customers, typically via email, ICQ, Jabber, and Skype. MARTISEVS also advertised the SERVICE on underground online cybercrime forums, which are support networks used by cybercriminals worldwide to buy, sell, and rent malware kits, botnets, and stolen personal identifying information (PII). Bondars was aware that MARTISEVS was intentionally marketing the SERVICE to computer hackers because MARTISEVS showed Bondars some of MARTISEVS' communications on at least one of the online cybercrime forums on which MARTISEVS had posted an advertisement for The SERVICE. While MARTISEVS was primarily responsible for the advertising of the SERVICE

and customer support, Bondars primarily designed and maintained the technical aspects of the the SERVICE service. Because customers' inquiries often required technical support, MARTISEVS worked closely with Bondars and asked Bondars to look into and solve technical problems brought to light by customers.

7. MARTISEVS and Bondars intentionally marketed The SERVICE to computer hackers using the website the SERVICE.net and a hidden service accessible via The Onion Router (TOR), an online network for enabling anonymity.

8. The SERVICE differed from legitimate services in multiple ways. For example, there are legitimate services designed to protect computers from viruses by allowing customers to scan suspicious files against databases of known malware. These services, however, share data with antivirus companies about files that are determined to be malicious in order to help the antivirus companies better protect consumers in the future. By contrast, the SERVICE informed its users that they could upload their malware anonymously and that data about uploaded files would not be shared with antivirus communities. MARTISEVS knew that Bondars had designed the SERVICE so that the SERVICE members could scan their malicious files against the databases maintained by the antivirus companies without the antivirus companies receiving automated reports about those malicious files. MARTISEVS knew that the SERVICE was designed not to report the detection of malicious files to antivirus companies because the SERVICE's customer base consisted of individuals who were developing or using malicious files and for that reason did not want their malicious files shared with antivirus companies. MARTISEVS understood that the SERVICE customers would have lower odds of successfully committing computer intrusions if antivirus companies were provided information about their malicious files and thereby detecting new threats.

9. Up until MARTISEVS' and Bondars' arrest in May 2017, the SERVICE was the largest service of its kind. Throughout its lifetime, the SERVICE has had thousands of users and has received and scanned millions of malicious files.

10. The malware submitted to the SERVICE includes, but is not limited to, the following:

- a. **"Crypters"**: software used to hide malicious files from antivirus software so that the software cannot detect and quarantine the malicious files;
- b. **"Remote Access Trojans"**: software that allows a remote "operator" to control a system as if he or she has physical access to that system, including the possibility of administrator-level privileges;
- c. **"Keyloggers"**: surveillance software that has the capability to record keystrokes entered on the victim computer and send that information to the user of the keylogger. A keylogger can record and steal any information typed on a keyboard, including sensitive information such as emails, instant messages, and passwords to email, social media, and financial accounts; and
- d. **"Malware Tool Kits"**: toolkits specifically designed for users to create customized malicious files with functions of user preference. Some of the toolkits have embedded the SERVICE's Application Program Interface (API) in order to determine if the created malicious files were detected by antivirus software. Typically, if the malicious files were detected by antivirus software, users would change the digital signature of the malicious files and rescan the malicious files using the SERVICE with the goal of making the malicious files fully undetectable by antivirus software.

11. In addition to running the SERVICE service themselves, MARTISEVS and Bondars also entered into something akin to franchise agreements with co-conspirators in other countries. These co-conspirators operated the same service as the SERVICE, using largely the same technical infrastructure created by Bondars, but marketed the service under different names and in different languages. As the customer support contact for the SERVICE, MARTISEVS fielded inquiries from the SERVICE's customers who wanted to become franchisees, or resellers, of the SERVICE and referred these customers to Bondars to provide them with technical support. At all relevant times, MARTISEVS and Bondars understood that these individuals intended to use their version of the SERVICE to assist with the development of malware and ultimately to assist in illegal computer intrusions.

12. In addition, MARTISEVS referred the SERVICE customers to Bondars when they requested an application programming interface (API) tool, which MARTISEVS and Bondars both understood would allow users the flexibility to scan malicious files, IPs, and URLs without the need to directly submit the malicious files, IPs, and URLs on the SERVICE's website or on The SERVICE's site on TOR's hidden service. Bondars created APIs for the SERVICE's customers, and the purpose and effect of the API tool was to allow malware developers to integrate the SERVICE directly into the malware toolkits they designed and sold. Integrating the SERVICE into a malware toolkit made it easier for users of the malware toolkit to scan the malicious executable files they created with the toolkit through the SERVICE in order to determine whether those executables would be detected by antivirus software. As explained in paragraphs 24-28 below, several of the world's most prolific malware toolkits did in fact integrate the SERVICE using the API that Bondars created.

13. As the SERVICE's customer support contact, MARTISEVS received and responded to emails from a variety of cybercriminals who made little effort to disguise the malicious nature of their activities from MARTISEVS or Bondars. On many occasions, the SERVICE's customers communicated with MARTISEVS using email addresses containing words plainly associated with illegal activities, such as, "crypter," "hack," or "hacker." Some of the SERVICE's users discussed their cybercrime explicitly in their emails to MARTISEVS. For example, in an email dated June 3, 2014, one user of the SERVICE wrote, "Hi I'm building a crypter and wish to use your api, is there a different contract for this sort of thing?"

14. Bondars created and maintained a sophisticated technical infrastructure to support the the SERVICE website and service, which included virtual private servers and TOR. In addition, as noted in paragraph 8 above, Bondars disabled automated reports to antivirus companies so as to prevent the antivirus companies from learning about the millions of malicious files that was scanned through the SERVICE.

15. Both MARTISEVS and Bondars received copies of antivirus scan reports generated by the SERVICE after users had submitted and scanned their files through the SERVICE. These reports indicated, on their face, which antivirus software detected the files as malware. The reports revealed that numerous scanned files were detected as malware. Moreover, users repeatedly submitted files with the same names but with different hash values and received reports corresponding to the submitted files. The early reports would show that multiple antivirus software detected the files as being malicious and later reports would show a decrease in detection to no detection by antivirus software.

Overt Acts

16. In furtherance of the conspiracy and its objects, the following overt acts, among others, were committed in the Eastern District of Virginia and elsewhere by members of the conspiracy.

17. In approximately 2011, MARTISEVS added the business name of the SERVICE to his PayPal account.

18. On or about November 18, 2012, Z.S., a co-conspirator malware developer, described in more detail in paragraphs 24-26 below, using a computer in Great Falls, Virginia, within the Eastern District of Virginia, caused a payment to be made to an account controlled by Bondars and MARTISEVS, in exchange for access to the SERVICE and the SERVICE's API tool.

19. On or about November 18, 2012 through on or about November 23, 2012, Z.S., using a computer located in Great Falls, Virginia, within the Eastern District of Virginia, and MARTISEVS exchanged emails regarding Z.S.'s access to the SERVICE.

Computer Intrusions Aided and Abetted By the SERVICE

20. Malware that was developed by MARTISEVS'S co-conspirators, who were members of the SERVICE located in the Eastern District of Virginia and elsewhere, with the assistance of MARTISEVS, Bondars, and the SERVICE, were used to perpetrate hundreds of thousands of computer intrusions against victim computers in the United States and elsewhere, including multiple computers within the Eastern District of Virginia. The purpose of these computer intrusions was to steal information, including financial and personal identifying information, which could be used to commit fraud.

(a) Computer Intrusions Against Major U.S. Retailer

21. For instance, beginning in at least early 2012, a computer hacker became a member and user of the SERVICE and a co-conspirator of MARTISEVS and Bondars. Like the other members of the SERVICE, MARTISEVS and Bondars provided this co-conspirator with access to the SERVICE knowing that the co-conspirator would use the SERVICE to develop malicious software to be used for illegal computer intrusions. On or about November 14, 18, 24, and 25, 2013, the co-conspirator described in this paragraph scanned credit and debit card stealing malware (bearing unique hash signatures) through the SERVICE to determine whether that malware would be detected by the antivirus systems that were then being used to protect major American retail stores.

22. Beginning on or about November 30, 2013, the same co-conspirator and his accomplices caused the malware described in the above paragraph (with identical hash signatures) to be sent (illegally and without authorization) to computers connected to the payment processing systems of over a thousand branches of a major retail store located in the United States.

23. Using this malware, the co-conspirator and his accomplices stole credit and debit card numbers, addresses, phone numbers, and other pieces of personal identifying information belonging to customers of the retailer located throughout the United States, including from within the Eastern District of Virginia.

(b) Computer Intrusions Committed Using the Limitless Logger and Syndicate Stealer

24. Another one of MARTISEVS' co-conspirators was Z.S., the SERVICE member described in paragraphs 18-19 above, who operated, in part, from Great Falls, Virginia, within

the Eastern District of Virginia. Z.S. designed two keyloggers called the “Limitless Logger” and the “Syndicate Stealer.” These keyloggers were designed and marketed for purpose of recording, without the computer owner’s knowledge or consent, all key strokes typed into a victim computer, for stealing passwords (including financial account, email, and social media passwords) saved on a victim computer, and for other malicious purposes.

25. On or about November 18, 2012, MARTISEVS and Bondars provided Z.S. with access to The SERVICE and allowed Z.S. to integrate the SERVICE’s API tool that Bondars created directly into Z.S.’s keyloggers’ toolkits. The integration of the SERVICE’s API into Z.S.’s keyloggers’ toolkits allowed the users of Z.S.’s keyloggers to scan the malicious executable files they created using the SERVICE’s API to determine if the executable files would be detected by the antivirus systems of the victim computers they targeted. If the executables were detected, the keylogger user could change the file’s digital signature and rescan the executable, with the goal of making the malware fully undetectable by antivirus software.

26. With the aid of the SERVICE, Z.S. sold his keyloggers to over 3,000 customers who in turn accessed over 16,000 computers without authorization and thereby intentionally damaged those computers by changing their functioning such that those computers recorded sensitive information such as account passwords and sent that information to the users of Z.S.’s keyloggers without the authorization of the owners of the victim computers. The keyloggers sold by Z.S. with the integrated API of the SERVICE caused damage to more than 10 protected computers within the one-year period of January 1, 2013 through December 31, 2013. At all relevant times, MARTISEVS and Bondars understood that Z.S. and other users of the SERVICE’s API tool intended to use the tool to cause unauthorized computer intrusions. At all

relevant times, MARTISEVS and Bondars acted with the intent of aiding and abetting these unauthorized intrusions and causing them to occur.

(c) Computer Intrusions Committed Using the Citadel Banking Trojan

27. The SERVICE was used to assist the development of a widely-used banking trojan called "Citadel," which was sold on underground cybercrime forums, and designed to steal online banking credentials, credit card information, and personal identifying information from victim computers. Citadel was used to infect hundreds of thousands of computers worldwide, including in the United States, resulting in the theft of banking information and ultimately in fraud-related losses. The developer of Citadel, who was a member of the SERVICE and a co-conspirator of MARTISEVS and Bondars, integrated the SERVICE into certain later versions of the Citadel malware toolkit using the API tool created by Bondars.

28. MARTISEVS and Bondars intentionally allowed the developers of Citadel to integrate The SERVICE's API into certain later versions of Citadel. As intended by MARTISEVS and Bondars, The SERVICE's integrated API allowed users of Citadel to check the malicious executable files created using Citadel to determine whether they would be detected by antivirus services. The Citadel manual described the function of the SERVICE's integrated tool as follows (emphasis added):

In the admin panel there is a new section "Efficiency and Security", we tested the integration into [**the SERVICE**], and now you can click and check the detectability of all of your exe-build directly from the Citadel admin. You can also install a once-a-day automatic file check and if one of your files is detected by more than 3 AV, you will immediately receive a notification in Jabber, so you can immediately substitute the exe. Now the mechanism will work for you automatically, you can be as lazy as you want!

Conclusion

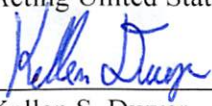
29. The Statement of Facts includes those facts necessary to support the defendant's guilty plea. It does not include each and every fact known to the defendant or to the

government and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

30. The actions of the defendant, as recounted above, were in all respects knowing, voluntary, and intentional, and were not committed by mistake, accident or other innocent reason.

Tracy Doherty-McCormick
Acting United States Attorney


Date: March 2, 2018

By: 
Kellen S. Dwyer
Laura Fong
Assistant United States Attorneys

Catherine Alden Pelker, Trial Attorney
U.S. Department of Justice, Criminal Division
Computer Crime & Intellectual Property Section

Defendant's Signature: After consulting with my attorney, I hereby stipulate that the above Statement of Facts is true and accurate and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

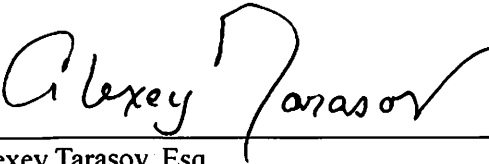
Date: 3/2/18, 2018



Jurijs Martisevs
Defendant

Defense Counsel Signature: I am Jurijs Martisevs' attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Date: 3/2/2018, 2018



Alexey Tarasov, Esq.
Counsel for the Defendant