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

Alexandria Division

UNITED STATES OF AMERICA v. ALEKSANDR BROVKO, *Defendant*.	Case No. 1:18-CR-407 The Honorable T.S. Ellis, III

POSITION OF THE UNITED STATES ON SENTENCING

For at least twelve years, the defendant, Aleksandr Brovko, played an important role in international cybercrime schemes targeting U.S. victims. Brovko was a member of elite, online forums designed for Russian-speaking cybercriminals to gather and exchange tools and services for crime, and he was consistently hired by other cybercriminals to perform two roles that enabled the success of fraudulent schemes targeting U.S. victims.

First, he wrote computer code that extracted easily monetized information – such as personally identifiable information (PII) and online banking credentials – from vast troves of stolen data gathered from botnets, or networks of infected computers. Where his computer code could not effectively parse the data, Brovko supplemented his computer-automated efforts with manual searches of the data.

Brovko's second role was to perform quality checks on the victim information he had identified. He did this, for example, by attempting to log in to victims' online banking accounts using the stolen usernames and passwords he had identified. If he was able to log in, he would know that the username-and-password combination was still valid. Once he was signed into a

victim's account, Brovko also could determine whether the account possessed a balance high enough to make the account a worthwhile target of fraudulent activity. Once Brovko had performed his quality checks, Brovko relayed the information to his co-conspirators and worked with them to initiate fraudulent transactions using the information, or to repackage and sell the victims' information to other criminals.

Brovko earned a comfortable living for more than a decade predominately from the criminal work that other cybercriminals contracted him to perform. He was actively engaged in cybercrime up until his arrest in his home in the Czech Republic in 2019. While he was not the mastermind of the criminal schemes he supported, he nonetheless played a significant role. Without his services, much of the stolen data held by the botnet operators he worked with would have remained too unwieldy to use, which would have greatly curtailed the pervasiveness of fraud targeting U.S. victims. For these reasons, and the reasons stated below, the Government respectfully requests a significant sentence to reflect the seriousness of his crimes and to deter international cybercrime schemes targeting U.S. victims.[1]

[1] [redacted]

I. Offense of Conviction

The defendant became a member of elite cybercrime forums catering to Russian speakers beginning in or around 2007. Membership to these forums is lucrative: it gives a cybercriminal access to other highly skilled cybercriminals with whom he or she can exchange advice and services in the furtherance of schemes more complex and far-reaching than ones many cybercriminals could undertake alone. The forums also serve as a marketplace for cybercriminals to sell stolen payment card information and PII, and to recruit others to help them "cash out," or extract money using the stolen financial and personal information.

The cybercrime forums to which the defendant belonged allowed him to do exactly that. With the criminal connections he gained using the forums, Brovko formed business partnerships with like-minded cybercriminals, specifically entering into agreements with botnet operators to access botnet logs – the information stolen from infected computers. *See* Presentence Investigation Report (PSR) ¶¶ 16-18. As part of the agreements, Brovko wrote software to parse the voluminous data, and where that was not feasible, manually reviewed the stolen information. *Id.* ¶ 25. His objective was to identify sensitive victim data, such as victims' online banking credentials, from the stolen data, and use the sensitive information to commit fraud. *Id.* Once he had identified this information, Brovko passed the usernames and passwords of victims' online bank accounts to others to coordinate fraudulent transfers of money from victims' accounts to those he or his co-conspirators controlled. *Id.* At other times, he sold this information to other criminals. *Id.* To perform quality checks on the sensitive information he had extracted from the botnet logs, Brovko typically attempted to log in to victims' accounts using the credentials he had identified. He was then also able to check financial account balances before initiating fraudulent transfers of money, collaborating with his co-conspirators to do the same, or repackaging the information for sale to others. *See, e.g., id.* ¶ 18 (discussing instances in which

Brovko coordinated with a co-conspirator to verify account balances and determine how to use the information).

While Brovko did not himself install malicious software on victims' computers, or use exploits to gain unauthorized access to victims' computers, he partnered with those who did. By doing so, he enabled the collective success of their crimes. Without Brovko's services, the stolen data held by botnet operators would have largely remained indecipherable and unusable. That is because most of the raw data siphoned from infected computers contains a jumble of sensitive information entered by users – for example, online banking credentials – and information that is not – for example, computer code representing system processes running on victims' machines. In other words, Brovko's software served the function of separating the proverbial wheat from the chaff.

In addition, even if the average criminal *could* extract PII and other sensitive victim information through manual review of botnet logs, the process would have been herculean since botnet operators were in possession of high volumes of stolen data. Brovko designed software to automate, and thereby expedite, this process. Furthermore, his quality checks of the extracted victim information enhanced the collective success of his fraudulent schemes and that of other criminals by allowing them to focus on information that was usable and likely to generate significant criminal proceeds.

II. Guidelines Range

The Probation Officer correctly calculated the defendant's offense level as follows:

Guideline	Offense Level
Base Offense Level (Section 2B1.1(a)(1))	7
Loss amount between $65 Million but less than $150 Million (Section 2B1.1(b)(1)(M))	+24
Offense involved 10 or more victims (Section 2B1.1(b)(2))	+2

Offense involved receiving stolen property and the defendant was in the business of receiving and selling stolen property (Section 2B1.1(b)(4))	+2
Substantial part of offense committed abroad (Section 2B1.1(b)(10))	+2
Offense involved the production or trafficking of an unauthorized access device or counterfeit access device, or authentication feature (Section 2B1.1(b)(11))	+2
Offense involved use of a special skill (Section 3B.1.3)	+2
Acceptance of responsibility (Section 3E1.1)[2]	-3
TOTAL	**38**

PSR ¶¶ 28-42. Based on the defendant's Category I Criminal History, the resulting Guidelines Range is **235-293 months' imprisonment**. *Id.* ¶¶ 64-65.

In the plea agreement, the Government and defendant agreed to all but one of the sentencing guidelines calculations assessed by the Probation Office – the 2-level enhancement for use of a special skill under Section 3B1.3 of the U.S. Sentencing Guidelines. Application Note 4 accompanying Section 3B1.3 of the U.S. Sentencing Guidelines provides that an enhancement for use of a special skill is warranted where the skill in question is one "not possessed by members of the general public and usually require[es] substantial education, training or licensing." Here, Brovko used his considerable computer programming skills to automate the extraction of sensitive victim information from vast pools of stolen data. He gained these computer programming skills from a university education centering on systems engineering – in particular, the automation of technical processes – and more than a decade of practical experience writing computer code. *See* PSR ¶ 9, 59-60. The Probation Officer, therefore, correctly applied the enhancement for use of a special skill because the computer skills

[2] The Government hereby moves, under U.S.S.G. § 3E1.1(b), for a third point to be reduced from the defendant's offense level, based on the defendant's timely acceptance of responsibility.

Brovko employed in furtherance of his criminal offense are not possessed by members of the general public and required substantial education and training to develop.

III. Sentencing Recommendation

As the Court is well aware, the Sentencing Guidelines are advisory, and just one factor that must be considered along with the other factors set forth in 18 U.S.C. § 3553(a).[3] Here, due consideration should be given to the seriousness of the offense and the need to adequately deter others from participating in international, organized cybercrime.

A. The Sentence Should Reflect the Harm Caused to Individuals, the Banking Industry, and Society.

The full harm caused by the defendant's crimes is difficult to calculate. The parties have stipulated to a provable loss amount of between $65 million to $150 million based on the Government's discovery of at least 202,543 files found within one folder in Brovko's computer, each containing at least one access device consisting of either of personally identifying information or financial account details. *See* PSR ¶ 21-22. The Application Notes to Section 2B1.1 of the U.S. Sentencing Guidelines provide that, "[i]n a case involving any counterfeit access device or unauthorized access device, loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device and *shall be not less than $500 per*

[3] The § 3553(a) factors include: the nature and circumstances of the offense and the history and characteristics of the defendant; the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, to provide just punishment for the offense, to afford adequate deterrence to criminal conduct, to protect the public from further crimes of the defendant, and to provide the defendant with needed training, medical care, or other treatment; the kinds of sentences available; the kinds of sentence and the sentencing range established for the type of offense committed; any pertinent policy statement; the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and the need to provide restitution to any victims of the offense.

access device" (emphasis added).[4] Accordingly, the loss associated with 202,543 stolen access devices is approximately $101 million: the result of 202,543 multiplied by $500. *See* PSR ¶¶ 10, 21-22.

Because of the high volume of stolen information trafficked by Brovko and his co-conspirators over the span of the offense conduct, it is difficult to identify specific harms that may have befallen those whose information was stolen and traded. Yet, it is likely that Brovko's criminal work directly or indirectly caused PII or other sensitive victim information to be used in the commission of fraud. Indeed, it was the objective of Brovko's criminal partnerships that money would either be transferred from victims' accounts into those that Brovko or his co-conspirators controlled or otherwise sold or provided to other criminals for their use in the commission of fraud. *See* PSR ¶¶ 11-12, 18. It also likely that victims whose information was trafficked bore the cost of rectifying fraudulent charges or wire transfers, or that the U.S. financial institutions maintaining those victims' accounts incurred those losses.

Beyond the individual victims or financial institutions impacted by Brovko's criminal activities, society, as a whole, bears the cost of Brovko's hand his co-conspirators' crimes. That is because when banks and businesses sustain fraud-related losses or expenses, they generally

---

[4] "Access device" is defined at 18 U.S.C. § 1029(e)(1) as any "card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds . . . ."

"Counterfeit access device" is defined at 18 U.S.C. § 1029(e)(2) as "any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device."

"Unauthorized access device" is defined at 18 U.S.C. § 1029(e)(3) as "any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud."

pass these costs on to the average American in the form of higher prices, fees and other indirect charges. *See* Lydia Segal, *Credit Card Fraud: A New Perspective on Tackling an Intransigent Problem*, 16 FORDHAM J. CORP. & FIN. L. 743, 754, 775 (2011) (banks and credit card companies pass on costs of fraud to consumers in the form of higher prices, banking costs, and other charges); *see also* Ronald Mann, *Credit Cards and Debit Cards in the United States and Japan*, 55 VAND. L. REV. 1055, 1093-94 (2002) (credit card companies pass on costs of fraud to cardholders and merchants).

Finally, it is hard to overstate the impact of cybercrime's disruption to the nation's banking industry and the erosion of consumer confidence in online transactions caused by sophisticated criminal operations such as the defendant's. The defendant's sentence should reflect the seriousness of these harms.

B. The Sentence Should Reflect the Defendant's Role and Be Sufficient to Deter Others from Engaging in International Organized Cybercrime.

Financially motivated cybercrime targeting U.S. victims is increasingly carried out as a result of highly organized activity among individuals located overseas. Cybercriminals like Brovko are able to earn a comfortable living by contributing their considerable computer skills toward complex fraud schemes. Like Brovko, many cybercriminals cannot claim to be the mastermind of such schemes, but nonetheless play an integral part in the success of these crimes. And, like Brovko, many cybercriminals based overseas exploit the anonymity afforded them by the internet to carry out crimes against U.S. victims, secure in the belief they will never face criminal punishment in the United States.

Unfortunately, high rewards and a relatively low risk of detection are basic features of cybercrime. The only way to affect the cost-benefit analysis of these crimes is to impose meaningful sentences on those who are caught. If the Court does so, there is every reason to

believe that many would-be criminals will get the message. Computer hackers are among the most sophisticated criminals in the world and are known to closely monitor U.S. authorities' response to cybercrime and plan accordingly. Achieving general deterrence in this area therefore appears particularly promising. *See United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (because "economic and fraud-based crime are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence").

III. Conclusion

The Government respectfully recommends a serious sentence to account for the harm caused by the defendant and to provide general deterrence of international, organized cybercrime.

G. Zachary Terwilliger
United States Attorney

By: /s/
Laura Fong
Senior Trial Attorney
Computer Crime & Intellectual Property Section
U.S. Department of Justice

October 16, 2020

Alexander P. Berrang
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700

Certificate of Service

I hereby certify that on or around October 16, 2020, I filed the foregoing with the Clerk of Court.

I also certify that on or around October 16, 2020, I will send a true and correct copy of the foregoing by e-mail to the following:

William Byerley
United States Probation Officer
William_Byerley@vaep.uscourts.gov

By: /s/
Laura Fong
Senior Trial Attorney
Computer Crime & Intellectual Property Section
Department of Justice