U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

November 7, 2019

BY ECF

The Honorable Valerie E. Caproni
United States District Judge
Southern District of New York
Thurgood Marshall U.S. Courthouse
40 Foley Square
New York, New York 10007

Re: ***United States v. Stanislav Vitaliyevich Lisov*, 17 Cr. 48 (VEC)**

Dear Judge Caproni:

The Government respectfully submits this letter in advance of sentencing of defendant Stanislav Vitaliyevich Lisov ("Lisov" or the "defendant"), which is scheduled for November 21, 2019 at 10:00 a.m. Earlier this year, the defendant pled guilty to one count of conspiracy to commit computer intrusion, pursuant to a plea agreement between the parties (the "Plea Agreement"). As set forth in the Plea Agreement, the applicable range under the United States Sentencing Guidelines ("U.S.S.G." or "Guidelines") would be 108 to 135 months' imprisonment, except that by operation of the statutory maximum punishment (5 years), the stipulated Guidelines sentence becomes 60 months' imprisonment (the "Stipulated Guidelines Sentence"). For the reasons set forth below, the Government respectfully submits that the Stipulated Guidelines Sentence of 60 months' imprisonment would be fair and appropriate in this case.

A. Offense Conduct

Summary: From at least June 2012 until January 2015, Lisov and his co-conspirators used a type of malicious software, or malware, known as NeverQuest, to infect the computers of unwitting victims in order to, among other things, steal victims' login information for financial institution accounts. Lisov and his co-conspirators subsequently used the illegally acquired information to steal money from those victims via various means, including wire transfers, ATM withdrawals, and online purchases of expensive items. In total, Lisov and his co-conspirators attempted to steal at least approximately $4.4 million using NeverQuest, and in fact stole at least approximately $855,000 from their victims' online financial accounts. Lisov was responsible for key aspects of the creation and administration of a network of computers, or botnet, infected by NeverQuest. Lisov maintained infrastructure to further the scheme, including leasing computer servers used to administer the NeverQuest botnet. He also deployed and used NeverQuest for his own personal enrichment, including by selling victims' login information and other personal identifying information on the criminal black market. (*See* U.S. Probation Office's Final Presentence Investigation Report ("PSR"), dated October 4, 2019 (Dkt. 17), ¶¶ 9–11).

NeverQuest Malware: NeverQuest is a type of malware known as a banking Trojan.[1] NeverQuest was initially detected on computer networks and infected computers in or around late 2013. NeverQuest can be introduced to victims' computers through social media websites, phishing emails, or file transfers. Once surreptitiously installed on a victim's computer, NeverQuest is able to (1) identify when a victim attempted to log onto an online banking website, and (2) capture and transfer the victim's login credentials—including his or her username and password—back to a computer server used to administer the NeverQuest malware. Specifically, if a user visited a financial institution website that NeverQuest already had in its database, NeverQuest would surreptitiously insert computer code into the webpage through a "webpage injection," so that any data entered by a user into the webpage would be communicated back to a computer server (a command and control server) used to administer the NeverQuest malware. NeverQuest also had the functionality to identify new banking and financial websites that were not previously in the NeverQuest database, and to update the server with that information; NeverQuest administrators would then be able to create webpage injections for those new websites and send an update to all computers infected with NeverQuest. (*Id.* ¶¶ 12–14).

Once surreptitiously installed, NeverQuest enables its administrators remotely to control a victim's computer and log into the victim's online banking or financial accounts, transfer money to other accounts, change login credentials, write online checks, and purchase goods from online vendors. NeverQuest was ranked the number two global financial malware in 2015 and the number one global financial malware in 2016, according to a leading private sector cloud-based threat intelligence platform. (*Id.* ¶¶ 14–15 & n.2).

Lisov's Roles: Between approximately June 2012 and January 2015, Lisov was responsible for key aspects of the creation and administration of a network of victim computers (a botnet) that was infected with NeverQuest. Among other things, Lisov maintained computer network infrastructure for this criminal enterprise, including by renting and paying for computer servers used to manage the botnet that had been compromised by NeverQuest. Those computer servers contained lists with approximately 1.7 million stolen login credentials—including usernames, passwords, and security questions and answers—for victims' accounts on banking and financial websites. Lisov had administrative-level access to those computer servers. (*Id.* ¶¶ 10, 20(a), 21).

Lisov also deployed and used NeverQuest. He personally harvested login information from unwitting victims of NeverQuest, including usernames, passwords, and security questions and answers. (*Id.* ¶ 21).

As noted in detail in the PSR, Lisov's communications in furtherance of this hacking conspiracy covered a range of topics, including (among other things):

1. The operation of the malware, including "injects"—*i.e.*, software code to insert into a webpage, so that the malware would function as intended ("*I am looking*

[1] A Trojan is malware that appears, prior to installation, to perform a desirable function for the user, but once installed, it instead facilitates unauthorized access to the victim's computer. (PSR ¶ 12 n.1).

for injects"; *"do you have injects for the US? I'd like to poke around there"*) (*id.* ¶¶ 33, 35);

2. The types of stolen account information available for sale (*e.g.*, *"US bank accounts"*) (*id.* ¶ 24);

3. The types of stolen account information desired by purchasers (*"which banks?"; "are you still interested in logs' info?"; "what should be the minimum balance?"*) (*id.* ¶¶ 24, 28, 29);

4. The prices he charged for victim information (*e.g.*, *"25 bucks"*) (*id.* ¶ 26);

5. Mules—*i.e.*, individuals who can cash out stolen money in the United States (*id.* ¶¶ 26, 37); and

6. The details of monetary transfers out of victim accounts (*id.* ¶ 37).

For instance, in one conversation in January 2013, Lisov exchanged messages with a co-conspirator (CC-1), during which they discussed writing computer code to check whether stolen account information was valid. During their conversation, they discussed the following, in substance and in part:

LISOV:	well, while I was talking to you 400 accounts got checked
CC-1:	anything good?
[* * *]	
LISOV:	1200 [] 5000 [] 6000 [] 5000 [] 1100
LISOV:	only 2 or three accounts for 5000 each
LISOV:	yes 2 accounts for 5000 and one for 600..
LISOV:	I'm checking them on Thank You
[* * *]	
CC-1:	this is the fucking greatest [data] base – that time I could not download it normally from the server where it was stored
[* * *]	
CC-1:	-(I swear to God it's an ideal one
LISOV:	stop hurting my heart)

LISOV: I sent it to you, go to bed, I don't wanna hear from you any more today)))

CC-1: I gave out citi cards from there for about 2 thousand for 20 bucks each

(Compl. ¶ 26(q)). In this conversation, Lisov advised CC-1 that during the course of their messaging, Lisov had validated stolen login information for 400 financial institution accounts ("*400 accounts got checked*"), and then reported on account balances for some of those accounts ("*1200 [] 5000 [] 6000 [] 5000 [] 1100*"). CC-1 compliments the quality of the database of stolen accounts, and Lisov acknowledges that he is the source of the database ("*I sent it to you, go to bed*"). CC-1 responds that CC-1 sold Citibank account information for $20 per account ("*I gave out citi cards from there for about 2 thousand for 20 bucks each*").

B. Procedural History

Lisov was originally charged in a two-count criminal Complaint in 2016. (Dkt. 1). In January 2017, a Grand Jury in this District returned a two-count Indictment charging Lisov with conspiracy to commit computer intrusion and conspiracy to commit wire fraud. (Dkt. 3). Lisov, a Russian national, was arrested in Spain on or about January 13, 2017 and has been detained since that time. He was extradited from Spain to the United States on or about January 19, 2018. In February 2019, Lisov pleaded guilty before Your Honor to conspiracy to commit computer intrusion, in violation of 18 U.S.C. § 371. Pursuant to the Plea Agreement, the applicable range under the Guidelines would be 108 to 135 months' imprisonment, but the stipulated Guidelines sentence becomes 60 months' imprisonment because the statutory maximum punishment is 5 years. (PSR ¶ 100). In the final PSR, Probation agrees with the Guidelines calculation in the Plea Agreement. Probation recommends a sentence of 48 months' imprisonment. (*Id.* pp. 23–24).

C. Applicable Law

As the Court is well aware, although the Sentencing Guidelines are no longer mandatory, they provide strong guidance to courts following *United States v. Booker*, 543 U.S. 220 (2005), and *United States v. Crosby*, 397 F.3d 103 (2d Cir. 2005). Because the Guidelines are "the product of careful study based on extensive empirical evidence derived from the review of thousands of individual sentencing decisions," *Gall v. United States*, 552 U.S. 38, 46 (2007), district courts must treat the Guidelines as the "starting point and the initial benchmark" in sentencing proceedings. *Id.* at 49. The Guidelines' relevance stems in part from the fact that, while they are advisory, "the sentencing statutes envision both the sentencing judge and the Commission as carrying out the same basic § 3553(a) objectives." *Rita v. United States*, 551 U.S. 338, 348 (2007). After making that calculation, the Court must consider the seven factors outlined in 18 U.S.C. § 3553(a), which include the nature and circumstances of the offense, the history and characteristics of the defendant, the need to deter criminal conduct and promote respect for the law, the need to protect the public from further crimes of the defendant, and the need to avoid unwarranted sentencing disparities. *Gall*, 552 U.S. at 50 & n.6. If the judge "decides that an outside-Guidelines sentence is warranted, [s]he must consider the extent of the deviation and ensure that the justification is sufficiently compelling to support the degree of the variance." *Id.* at 50.

D. Discussion

The Government respectfully submits that the Stipulated Guidelines Sentence would be appropriate in this case in light of the nature, duration, and seriousness of the offense; the need for just punishment; and the need for deterrence.

As to the nature and circumstances of the offense, this computer hacking offense is extremely serious. For several years, the defendant and his co-conspirators deployed and used malware to infect the computers of unwitting victims, steal their login information for online banking accounts, and use that information to steal money out of the victims' accounts. This conspiracy's malware was highly sophisticated. NeverQuest was installed surreptitiously and was able to identify banking and financial websites visited by a victim user's web browser. NeverQuest also enabled its administrators remotely to control a victim's computer and log into the victim's financial accounts. Furthermore, NeverQuest was deployed across the globe and was highly successful. Log files (on a server registered to Lisov) contained lists of approximately 1.7 million stolen login credentials—including usernames, passwords, and security questions and answers—for victims' accounts on banking and financial websites.

This offense was also highly profitable; the defendant and his co-conspirators used NeverQuest to steal at least approximately $855,000 from their victims' online financial accounts and attempted to steal more than $4 million. Such losses are borne by victim banks which not only had their network systems compromised by the offense, but also absorbed pecuniary losses from unauthorized cash withdrawals, transfers, and purchases made from their customers' bank and credit card accounts. Presumably, such losses are ultimately borne, at least to a large extent, by the average consumer. In addition to banks, the other victims of this crime are those whose computers were infected by NeverQuest, leading to the obtainment and misappropriation of their personal identifying and/or financial information. The harm to these individual victims includes the anxiety and concern that hackers cause, as well as presumably the hassle, inconvenience, and lost time required by victims (and/or their financial institutions) to remedy the intrusion.

This defendant also occupied a central, pivotal role. As noted above, he maintained infrastructure for the scheme, including leasing computer servers; he received victims' login information and other PII, without their knowledge, which he sold on the black market; he personally deployed and used NeverQuest; and he discussed a wide range of topics relating to NeverQuest and trafficking in stolen login information and PII of victims. He also displayed an apparent eagerness to cater to his clientele and to profit off his crime; for instance, when an individual indicated a willingness to pay for victim PII (stolen credit card numbers, social security numbers, etc.), Lisov replied, "great I was looking for somebody who needs this info." (PSR ¶ 29).

In sum, the nature, duration, harmfulness, profitability, sophistication, and seriousness of the offense, as well as the defendant's roles therein, weigh heavily in favor of the Stipulated Guidelines Sentence. The same considerations point to the need for a Guidelines sentence to ensure a just punishment.

Deterrence considerations also support the Stipulated Guidelines Sentence. As for specific deterrence, it is important to personally deter the defendant from again choosing to use his considerable technological skills for nefarious purposes. Indeed, as noted in the PSR, a suspected co-conspirator advised Lisov (1) to evade detection by using particular servers not associated with Lisov, and (2) to ensure that his Internet browser was cleared of "cookies" that might enable a financial institution to detect information about Lisov's location. (PSR ¶¶ 29–30).

As for general deterrence, computer hacking is a significant and growing problem, one which costs the U.S. economy dearly every year. *See, e.g.*, THE COUNCIL OF ECONOMIC ADVISERS, *The Cost of Malicious Cyber Activity to the U.S. Economy*, at 2, 36 (Feb. 2018) (estimating that computer hacking cost the U.S. economy between $57 and 109 billion in 2016); Tom Risen, *Study: Hackers Cost More Than $445 Billion Annually*, U.S. NEWS & WORLD REPORT (June 9, 2014). Hackers, particularly foreign cybercriminals, may reason that the likelihood of even being identified—not to mention located, arrested, and extradited—is small. But the financial benefits of cybercrime can, unfortunately, be considerable and immediate, especially when (as here) the crime involves access to bank account information on a wide scale. Given this calculus, it is important to send a clear message to other hackers—domestic and foreign alike—that the costs of cybercrime far outweigh the potential financial benefits.

E. Conclusion

For the reasons set forth above, the Government respectfully submits that the Stipulated Guidelines Sentence (60 months' imprisonment) would be fair and appropriate in this case.

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York

By: Michael D. Neff
Michael D. Neff
Assistant United States Attorney
(212) 637-2107

cc: Arkady Bukh, Esq. (via ECF)