

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

MIHAI IONUT PAUNESCU,

Defendant.

13 Cr. 41 (LGS)

THE GOVERNMENT'S SENTENCING MEMORANDUM

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

Sarah Lai
Assistant United States Attorney
Of Counsel



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*

May 25, 2023

BY EMAIL AND HAND DELIVERY

Honorable Lorna G. Schofield
United States District Judge
Southern District of New York
40 Foley Square
New York, New York 10007

Re: *United States v. Mihai Ionut Paunescu*, 13 Cr. 41 (LGS)

Dear Judge Schofield:

The Government respectfully submits this letter in advance of the sentencing of defendant Mihai Ionut Paunescu (“Paunescu” or the “defendant”), scheduled for June 12, 2023, at 11:00 a.m. A proposed Order of Restitution will be submitted separately before sentencing. As explained by separate letter, the Government further requests that a redacted version of this sentencing memorandum be filed.

Paunescu pleaded guilty to one count of conspiracy to commit computer intrusion with intent to defraud, in violation of 18 U.S.C. §§ 1030(b) and 1030(a)(4), pursuant to a plea agreement with the Government (the “Plea Agreement”) that stipulates an applicable sentencing range of 108 to 135 months’ imprisonment, and a Stipulated Guidelines Sentence of five years’ imprisonment based on the statutory maximum sentence for the crime to which he pled guilty, forfeiture in the amount of \$3,510,000, and restitution in the amount of \$56,627. The U.S. Probation Office calculated the same sentencing range and recommended a sentence of five years’ imprisonment. (PSR at 18). For the reasons that follow, the Government submits that a sentence of five years’ imprisonment is warranted, to reflect the seriousness of Paunescu’s role as the facilitator of multiple major cybercrime schemes, to impart just punishment and promote respect for the law, and to provide a measure of deterrence.

I. The Offense Conduct

Paunescu, a Romanian national who resided in Bucharest, was a “bulletproof hoster.” A bulletproof hoster is an individual who knowingly provides critical online infrastructure, such as servers, Internet protocol (“IP”) addresses and domains, that enables cybercriminals throughout the world to distribute viruses and other malicious software (“malware”); to control and receive information from computers infected with such malware; to launch distributed denial of service (“DDoS”) attacks that cripple computer networks; and to distribute massive quantities of spam emails, which are a common delivery mechanism for malware or links to websites that

surreptitiously download malware to visitors' computers. Through his bulletproof hosting service, Paunescu facilitated the deployment of destructive viruses and other malware, including the Gozi Virus, the Zeus Trojan, SpyEye, and BlackEnergy. In total, the cybercrime schemes that Paunescu supported with his online infrastructure have caused tens of millions of dollars in losses and affected well over one million computers in countries throughout the world. (PSR ¶ 11).

Examples of Cybercrime Schemes Supported by Paunescu's Bulletproof Hosting Service

The Gozi Virus, the Zeus Trojan, and SpyEye were all designed to gain unauthorized access to victims' computers in order to collect confidential financial information. Such malware was typically spread by being concealed within apparently benign document files or websites. When a victim opened the document or visited the website, the malware was secretly installed onto the victim's computer, where it remained virtually undetectable by antivirus software. Once installed on a victim's computer, the malware collected the victim's account number, account address, username, password, personal identification number (PIN), and answers to challenge questions by capturing the victim's keystrokes or other means. The malware sent the stolen data to computers controlled by Paunescu's co-conspirators, who would then either sell the data to other criminals or use the data to transfer funds fraudulently out of the victim's account. (PSR ¶¶ 12-14).

From approximately 2007 to 2009, Paunescu's co-conspirators used the Gozi Virus primarily to target accounts at European banks. (PSR ¶ 12). Beginning in or about 2010, they began using the Gozi Virus to attack U.S. bank accounts. Since its inception, the Gozi Virus has infected, at a minimum, over a million computers around the world, including at least 40,000 in the United States, and has caused at least millions of dollars in losses. (PSR ¶ 12).

BlackEnergy was malware that was used primarily to launch DDoS attack. A DDoS attack occurs when a large constellation of infected computers is ordered by a remote command-and-control server to overwhelm a targeted website or computer system with requests, causing the targeted website or computer system to crash under the volume of requests. Hackers have used BlackEnergy-infected computers to target political entities, financial institutions, and e-commerce websites. (PSR ¶ 15).

Examples of Servers That Were Part of Paunescu's Bulletproof Hosting Service

One of the servers that Paunescu controlled contained a domain named "Adminpanel.ro." Adminpanel.ro contained several data tables. One data table contained a list of approximately 130 servers that were part of Paunescu's bulletproof hosting service and described how each server was being used by Paunescu's customer. (PSR ¶¶ 25, 27). Below is a screenshot of some of the entries in that data table:

method	mac	buyprice	for
vmz	52:54:00:34:58:A7	0	0 50%SBL
VMZ182194613367	52:54:00:96:5a:e7	0	0 illegal
cash	52:54:00:25:6D:D9	0	0 botnet
wmz		0 0	0 100%SBL
wmz		0 0	0 spam 100%sbl
vmz	52:54:00:57:15:DC	0 0EU	0 100%SBL
VMZ182194613367	52:54:00:24:24:92	0	0 zeus 30%SBL
	52:54:00:92:b6:ec	0	0 garena bots 0%SBL
VMZ163768491315	52:54:00:02:63:05	0 undefined	0 spam dns 100%SBL
VMZ163768491315	52:54:00:C0:DE:85	0	0 facebook spam 0%SBL
cash	52:54:00:D8:8F:AD	0	0 cash
cash	52:54:00:0B:61:65	0	0 cash
VMZ	52:54:00:F7:9F:C1	0	0 spyeye
	52:54:00:B8:CC:EE	0 undefined	0 legal shit
VMZ	52:54:00:C0:B7:0A	0	0 100%SBL
vmz	52:54:00:A2:18:21	0 0EU	0 spam fb 0% SBL
VMZ	52:54:00:CB:82:0D	0	0 100%SBL
	52:54:00:5F:F0:77	0	0 0% SBL
VMZ	00:1E:67:19:EC:0B	0 200USD	0 100%SBL
wmz	52:54:00:27:14:06	0	0 100%SBL
wmz		0 0	0 100%SBL
	52:54:00:B8:1A:1F	0 undefined	0 NON SBL - exploit seo trafic
VMZ163768491315	12:92:84:DB:41:48	0 525EU	0 facebook spam 0%SBL
VMZ125724159357	1C:6F:65:93:A4:F9	0 83EU	0 spyeye 100% SBL
VMZ	1C:6F:65:93:89:F0	0 92EU	0 0%SBL
VMZ	1C:6F:65:93:86:68	0 83EU	0 50%SBL
VMZ182194613367	1C:6F:65:90:C9:68	0 83EU	0 zeus 100%SBL

As the descriptions in the fourth column, titled “for,” shows, some servers were being used in connection with SpyEye and Zeus. Other servers were simply identified as “illegal,” “semi-illegal,” or “100% SBL.” (SBL stands for Spamhaus Block List. Spamhaus is a not-for-profit organization that tracks and publishes IP addresses found to be used for distributing spam or malware so that network administrators can block such IP addresses.) According to the descriptions in the “for” column, approximately half of the servers in this data table contained malware, was on the Spamhaus Block List, and/or were being monitored by Paunescu to determine if they were added to the Spamhaus Block List.

The servers that Paunescu operated included the following:

- At least three servers that were part of Gozi’s online infrastructure. One of them was a proxy server for Gozi located in California (the “Gozi Proxy Server”).¹ A proxy server typically acts as an intermediary between the victim’s server and a server controlled by a cybercriminal. The proxy server protects the cybercriminal because an investigator examining the compromised computer would see only the

¹ Images of the other two servers were produced in discovery as “SC2” and “SC28.”

IP address of the proxy server, not the IP address of the cybercriminal's computer, which could reveal the cybercriminal's physical location. The Gozi Proxy Server that Paunescu provided to co-conspirators received communications from more than 25,000 unique IP addresses—representing as many computers infected with the Gozi Virus—of which approximately 20,000 were located in the United States. The compromised computers included ones that belonged to the National Aeronautics and Space Administration (“NASA”) and businesses in Manhattan. (PSR ¶ 33). Data exfiltrated from those computers included login credentials for NASA and eBay accounts, details of websites visited, and content of Google chat messages. (PSR ¶ 30).

- A command-and-control server for BlackEnergy located in Romania. The defendant registered the IP addresses assigned to this server using his mother's address, thereby exposing her to criminal investigation. (PSR ¶ 34).
- A server that Paunescu used to store, among other things, the data table discussed above as well as a large database of pilfered financial account data, which is further described in Section V.A below.²
- A server rented to or hosted for a co-conspirator who appeared to be a prolific supplier of stolen credit/debit card data, based on the cache of such data on the server and his messages with Paunescu and other co-conspirators.³

II. The Relevant Procedural History

A. The Charges

On November 19, 2012, Paunescu was charged by Complaint with conspiracy to commit computer intrusion, in violation of 18 U.S.C. § 1030(b), with multiple objects (Count One), conspiracy to commit bank fraud, in violation of 18 U.S.C. § 1349 (Count Two), and conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349 (Count Three). On January 17, 2013, the defendant was indicted on the same three counts.

B. The Defendant's Arrest In Romania In November 2012 And Subsequent Outreach to U.S. Law Enforcement

On November 27, 2012, Paunescu was arrested in Romania, pursuant to a provisional arrest request from the United States. At the time of the defendant's arrest, Romanian law enforcement seized approximately 55 physical computers,⁴ along with \$300,000 in US currency and approximately \$25,000's worth of Romanian Leus. After his arrest in Romania, and while represented by his father, who was a lawyer, Paunescu consented to a voluntary interview.

² An image of this server was produced in discovery as “SC1.”

³ An image of this server was produced in discovery as “SC33.”

⁴ Multiple virtual machines, which are software-created simulations of a physical computer, can be stored within a physical computer. Each virtual machine can be assigned a separate IP address.

However, he changed his mind before the interview began. Thereafter, the United States requested the defendant's extradition for years, but without success.

Based on information provided by Romanian authorities, the defendant was detained from November 27, 2012, to January 29, 2013, pursuant to the United States' provisional arrest request.⁵ In or about January 2014, Paunescu reached out to U.S. law enforcement, apparently after reading an article that mentioned the charges against him in the United States. After a CJA attorney was appointed to represent him, Paunescu participated in a voluntary telephonic interview pursuant to a proffer agreement with the Government, and expressed an interest in cooperating with U.S. authorities. However, because Romania repeatedly deferred its decision on the United States' request for the defendant's extradition, the Government was unable to determine whether he would have been able to provide substantial assistance, and the parties did not enter into a cooperation agreement. There was no further contact between the parties.

C. The Defendant's Arrest In Colombia In June 2021 And Extradition

In 2019, after learning that the defendant may no longer be in Romania, the United States filed a Red Notice with Interpol for Paunescu's arrest in the event he was found outside of Romania. On June 26, 2021, the United States received notice that Paunescu had been arrested on arrival in Colombia, based on the Red Notice. After his arrest in Colombia, Paunescu's wife informed U.S. law enforcement that the defendant was willing to cooperate and would consent to extradition. However, Colombia does not allow defendants wanted for extradition to waive the extradition process. To the Government's knowledge, Paunescu was continuously detained in Colombia from June 26, 2021, to July 14, 2022, when he was extradited to the United States. Since his extradition, the defendant has been detained at the Westchester County Jail. In sum, by the date of sentencing on June 12, 2023, Paunescu will have been in custody a total of approximately 2 years, 1 month, and 18 days, of which 2 months and 2 day were in Romania, 1 year and 18 days were in Colombia, and 10 months and 28 days will have been in the United States.

D. The Guilty Plea

On February 24, 2023, the defendant pleaded guilty to Count One of the Indictment, conspiracy to commit computer intrusion with intent to defraud, in violation of 18 U.S.C. §§ 1030(b) and 1030(a)(4). That offense carries a statutory maximum term of imprisonment of five years. *See* 18 U.S.C. § 18 U.S.C. 1030(c)(3)(A).

III. Guidelines Calculation

The Probation Office's calculation of the applicable sentencing range under the United States Sentencing Guidelines ("Guidelines" or "U.S.S.G.") for the offense of conviction is consistent with the Plea Agreement. According to the Presentence Report and the Plea Agreement, Paunescu's total offense level under the Guidelines is 31, which is calculated as follows:

⁵ Paunescu maintains that he was in prison in Romania for over four months. Def. Exh. A, at 1. Assuming that was the case, only two months of that period was attributable to this case.

- The offense has a base offense level of 6, pursuant to § 2B1.1(a)(2);
- 22 levels are added, pursuant to § 2B1.1(b)(1)(L) and Application Note 3(F)(i), because the loss amount was more than \$25,000,000, but not more than \$65,000,000;
- 2 levels are added, pursuant to §2B1.1(b)(2)(A)(i), because the offense involved more than 10 victims;
- 2 levels are added, pursuant to § 2B1.1(b)(10)(B) and (C), because a substantial part of the fraudulent scheme was committed from outside the United States, and the offense otherwise involved sophisticated means and the defendant intentionally engaged in and caused the conduct constituting sophisticated means;
- 2 levels are added, pursuant to U.S.S.G. § 2B1.1(b)(11)(B)(i), because the offense involved the trafficking of unauthorized access devices; and
- 3 levels are deducted, pursuant to § 3E1.1(a) and (b), because the defendant demonstrated acceptance of responsibility for the offense by timely entering a guilty plea.

Paunescu's criminal history category is I. At criminal history category I and total offense level 31, Paunescu's applicable Guidelines range is 108 to 135 months' imprisonment. (PSR ¶¶ 8, 42-54). However, the offense of conviction—conspiracy to commit computer intrusion with intent to defraud, in violation of 18 U.S.C. §§ 1030(b) and 1030(a)(4)—carries a maximum term of imprisonment of 60 months. *See* 18 U.S.C. 1030(c)(3)(A).

IV. Sentencing Legal Principles

The Guidelines are no longer mandatory, but they still provide important guidance to the Court following *United States v. Booker*, 543 U.S. 220 (2005), and *United States v. Crosby*, 397 F.3d 103 (2d Cir. 2005). “[A] district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range,” which “should be the starting point and the initial benchmark.” *Gall v. United States*, 552 U.S. 38, 49 (2007). The Guidelines range is thus “the lodestar” that “anchor[s]” the district court’s discretion. *Molina-Martinez v. United States*, 578 U.S. 189, 198-99 (2016) (quoting *Peugh v. United States*, 569 U.S. 530, 541 (2013)) (internal quotation marks omitted).

After making the initial Guidelines calculation, a sentencing judge must consider the factors outlined in Title 18, United States Code, Section 3553(a), and “impose a sentence sufficient, but not greater than necessary, to comply with the purposes” of sentencing, 18 U.S.C. § 3553(a), which are: “a) the need to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for that offense; b) the need to afford adequate deterrence to criminal conduct; c) the need to protect the public from further crimes by the defendant; and d) the need for rehabilitation.” *United States v. Cavera*, 550 F.3d 180, 188 (2d Cir. 2008) (citing 18 U.S.C. § 3553(a)(2)).

Under Section 3553(a), “in determining the particular sentence to impose,” the Court must consider: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the statutory purposes noted above; (3) the kinds of sentences available; (4) the kinds of sentence and the sentencing range as set forth in the Sentencing Guidelines; (5) the Sentencing Guidelines policy statements; (6) the need to avoid unwarranted sentencing disparities; and (7) the need to provide restitution to any victims of the offense. *See* 18 U.S.C. § 3553(a).

In light of *Booker*, the Second Circuit has instructed that district courts should engage in a three-step sentencing procedure. *See Crosby*, 397 F.3d at 103. First, the Court must determine the applicable Sentencing Guidelines range, and in so doing, “the sentencing judge will be entitled to find all of the facts that the Guidelines make relevant to the determination of a Guidelines sentence and all of the facts relevant to the determination of a non-Guidelines sentence.” *Id.* at 112; *see also United States v. Corsey*, 723 F.3d 366, 375 (2d Cir. 2013) (“Even in cases where courts depart or impose a non-Guidelines sentence, the Guidelines range sets an important benchmark against which to measure an appropriate sentence.”). Second, the Court must consider whether a departure from that Guidelines range is appropriate. *Crosby*, 397 F.3d at 112. Third, the Court must consider the Guidelines range, “along with all of the factors listed in section 3553(a),” and determine the sentence to impose. *Id.* In so doing, it is entirely proper for a judge to take into consideration his or her own sense of what is a fair and just sentence under all the circumstances. *United States v. Jones*, 460 F.3d 191, 195 (2d Cir. 2006).

V. Section 3553(a) Analysis

The Government respectfully submits that a sentence of 60 months’ imprisonment (the Stipulated Guidelines Sentence) is necessary to reflect the seriousness of Paunescu’s crime, provide just punishment, afford general deterrence, and promote respect for the law, in light of the number of cybercrime schemes that Paunescu supported with his bulletproof hosting service, the loss amount attributable to the conspiracy in which Paunescu participated, and Paunescu’s personal gain from the conspiracy. In advocating this sentence, the Government notes that the Plea Agreement has already factored in the unusual circumstances of this case, by accepting a guilty plea to an offense with a statutory maximum sentence that is significantly below the applicable Guidelines range of 108 to 135 months. Further leniency is not warranted.

A. The Nature and Circumstances of the Offense

From at least in or about 2011, through in or about November 2012, the defendant owned and operated a bulletproof hosting service, through which he knowingly rented and sold servers and IP addresses to other cybercriminals who were engaged in multiple cybercrime schemes, from stealing banking credentials to DDoS attacks to distributing spam, which is a common method for delivering malware to victims’ computers. (PSR ¶ 11). The defendant committed this crime using at least three companies that he created and controlled—Powerhost.ro, SC KLM Internet & Gaming Ltd, and Titannet.ro—to market his bulletproof hosting service to his criminal associates as well as to rent and purchase servers and other online infrastructure from legitimate internet service providers (“ISPs”), including ones in the United States, in furtherance of his illegal operation. (*See, e.g.*, PSR ¶¶ 17, 31-32, 34). Paunescu thus facilitated online criminal activity by providing the infrastructure needed to carry out such activity.

The defendant also shielded his criminal customers from law enforcement and private sector investigations by offering them anonymity. For example, proxy servers that he leased helped to frustrate investigative efforts to identify the perpetrators of Internet-based crimes. As another example, he accepted payments from customers which were hard or impossible to trace, including cash and Webmoney, a Russia-based online payment system from which it was not possible to obtain customer records. By impeding law enforcement and cybersecurity investigations, bulletproof hosters such as Paunescu make it possible for other cybercriminals to flourish. At the same time, the harm caused by bulletproof hosters is enormously difficult to quantify because they conspire with multiple other criminals involved with different variants of malware, fraud schemes, and destructive cyber attacks. To accurately measure the full extent of the loss and damage for which bulletproof hosters, like Paunescu, should be held accountable requires investigating each of the schemes they facilitate.

In addition to profiting as a bulletproof hoster for criminals who distributed malware that stole data and launched DDoS attacks, Paunescu also personally benefitted from stolen financial data. For example, on December 2, 2011, Paunescu exchanged a message with an individual identified only as “Localuser,” asking, “Where do I download those from?” “Localuser” replied by providing Paunescu with two links to two databases: coin13.us and luckydumps.us. A historical image of the coin13.us website captured on January 3, 2012, revealed that it was a password-protected site with images of credit cards and the announcement: “NEWS: USA fresh base added,” a reference to a fresh database of stolen U.S. credit/debit card data.⁶ Similarly, the term “dumps” in the cybercrime context typically denotes caches of stolen login credentials for financial accounts. A subsequent search of a server that the defendant controlled and accessed revealed that it contained several spreadsheets of stolen financial account data, including account names, numbers, and personal identification numbers or PINs. Those spreadsheets contained data pertaining to at least 36,760 credit cards that were specifically described as “CREDIT” (i.e., credit cards), and over 100,000 other cards which were not designated as credit cards, but as “DEBIT” or by the name of the payment processor (e.g., Mastercard) or issuing bank.

Another server that was used by a customer of Paunescu contained chat logs in which Paunescu asked an individual using the moniker “wmbroker” to help him exchange tens of thousands of dollars per week through Liberty Reserve, an underworld cyber-banking system that laundered money for criminals around the world by allowing criminals to send and receive secure payments without revealing their account numbers or real identities. The following are examples of those chats, which show that the defendant operated a highly lucrative illicit service:

Identification of the defendant as “Powa”

[14.05.2012 12:40:58] Powa': my name is Paunescu Mihai Ionut

⁶ See <https://web.archive.org/web/20120106174920/http://www.coin13.us/login.php>.

The duration of the defendant's use of currency exchangers

[14.05.2012 12:39:28] Powa': i used your service for a long time
[14.05.2012 12:39:32] Powa': this year and the past year
[14.05.2012 12:39:41] Powa': but i stopped using because you did not answer once
[14.05.2012 12:39:45] Powa': and i needed my money fast

[16.05.2012 12:18:04] Powa': ebuygold was my preffered excanger
[16.05.2012 12:18:07] Powa': until last week
[16.05.2012 12:18:11] Powa': i transferred
[16.05.2012 12:18:14] Powa': 1.7 mil usd
[16.05.2012 12:18:19] Powa': in past 6 months
[16.05.2012 12:18:23] Powa': last week i had
[16.05.2012 12:18:25] Powa': 100k usd
[16.05.2012 12:18:31] Powa': :) then they dissapered
[16.05.2012 12:18:37] Powa': with my money...

The large volume of crime proceeds the defendant exchanged on a weekly basis

[18.05.2012 01:18:22] Powa': i have
[18.05.2012 01:18:29] Powa': 40k usd in LR
["LR" was the digital currency offered by Liberty Reserve.]
...
[18.05.2012 18:56:27] Powa': ok i set 40000
...
[18.05.2012 19:56:19] Powa': after this money arrives safeuly
[18.05.2012 19:56:23] Powa': i will transfer 40 more
[18.05.2012 19:56:28] Powa': after that :) 40 more
[18.05.2012 19:56:29] Powa': and so on
[18.05.2012 19:56:43] Powa': i god a lot of money :) and a lot of friends

[28.05.2012 18:39:43] Powa': i have a lot of money to send :| and you are holding meback...
[meaning not sending money fast enough]
...
[28.05.2012 18:40:36] Powa': i make 200k / week
...
[28.05.2012 18:42:42] Powa': but i need that money to make bombs
[28.05.2012 18:42:49] Powa': to bomb the FBI building...
[28.05.2012 18:43:14] Powa': how can i bomb an entire city if you do not send me my money fast...

The Government has no evidence which suggests that Paunescu actually planned or engaged in any crimes of violence. However, the cavalier way in which he joked with his co-conspirator about bombs is relevant to his nature and characteristics at the time.

 [28.05.2012 21:44:36] Powa': if you send money fast

[28.05.2012 21:44:39] Powa': 2 days tops

[28.05.2012 21:44:41] Powa': say 3

[28.05.2012 21:44:46] Powa': NOT 1 FUCKING WEEK)

[28.05.2012 21:44:55] Powa': i will send 80k / week

 [01.06.2012 15:29:00] Powa': sending another 40 now

 [04.06.2012 03:07:41] Powa': this one

[04.06.2012 03:08:00] Powa': and the last 50k order :) please do not forget to process them fast

[04.06.2012 14:02:52] wmbroker.co.uk: hi, yes, i see - no worries

[05.06.2012 03:25:28] wmbroker.co.uk: do u want me to add this to ur 50k payment?

[05.06.2012 03:30:24] wmbroker.co.uk: 2306usd where do u want me to send it?

[05.06.2012 11:42:01] Powa': 2306usd send to

[05.06.2012 11:42:02] Powa': Beneficiary: Paunescu Mihai Ionut

...

[05.06.2012 12:14:45] Powa': the other 50

[05.06.2012 12:14:50] Powa': send them urgently to china

[05.06.2012 12:14:51] Powa': :)

[05.06.2012 12:15:00] Powa': cand please send them fast

[05.06.2012 12:15:03] Powa': i have many more

In sum, Paunescu was not merely a young person who made a short-lived mistake. His role as the owner and operator of a sophisticated, cross-border, lucrative criminal enterprise weighs heavily in favor of the Stipulated Guidelines Sentence.

B. History and Characteristics of the Defendant

The Government is not able to verify the defendant's family history in Romania, as detailed in the Presentence Report, but does not dispute in general the account that the defendant provided to the Probation Office. According to the Presentence Report, the defendant stated that he pursued computer engineering on his own and developed computer engineering skills. Based on materials obtained from Romania, the defendant also has an engineering degree from the Technical University of Civil Engineering in Bucharest, Romania.⁷ The Presentence Report does not contain

⁷ A copy of the diploma is available on request. It is currently available only in the Romanian language.

information regarding the defendant's employment history. Thus, it is unclear if the defendant had any legitimate employment before he created his bulletproof hosting service. Based on the defendant's May 14, 2012 message, discussed above, that he had been using the money exchanger "wmbroker" "for a long time[.] this year and the past year," he started his bulletproof hosting service in at least 2011, when he was approximately 27 years old. Both the nature of his crime and the letters of support from his friends and colleagues demonstrate that he had significant software skills. (Def. Exh. D (Paunescu's "technical expertise is unrivalled."); Def. Exh. E, at 1 (Paunescu "was a talented software engineer[.]")). Given the defendant's education and technical abilities, he had more options than many defendants who appear in this courthouse and could have made a different choice, yet did not.

The Government has no evidence to suggest that the defendant has engaged in criminal activity since his arrest in November 2012. We also believe that Paunescu's proactive outreach to U.S. law enforcement in 2014 demonstrated his genuine interest in resolving the charges against him. However, once the restrictions placed on him by the Romanian authorities were lifted in around June 2015 (Def. Exh. C, at 9 (last page of Romanian Police Supervision Schedule)), he did not attempt again to contact U.S. authorities.

C. The Need to Afford Adequate Deterrence

One of the paramount factors that the Court must consider in imposing sentence under Section 3553(a) is the need for the sentence to "afford adequate deterrence to criminal conduct." 18 U.S.C. § 3553(a)(2)(B). Courts have generally recognized that "white collar crime . . . requires heavy sentences to deter because it is potentially very lucrative." *United States v. Hauptman*, 111 F.3d 48, 52 (7th Cir. 1997). "Because economic and fraud-based crimes are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence." *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (internal quotation omitted). "Defendants in white collar crimes often calculate the financial gain and risk of loss, and white collar crime therefore can be affected and reduced with serious punishment." *Id.*

The Government does not doubt the defendant's remorse. However, there is pressing need to deter individuals like the defendant who have the skill and ability to cause massive damage to computer networks worldwide. Deterrence is particularly important in the cyber context because many victims lack the ability to detect network intrusions and data theft. Unlike NASA, one of tens of thousands of victims in this case, most victims do not have the capability to monitor their computers for the latest cyber threats. For example, another victim—a small business in New York—did not know that one of their computers had been infected with the Gozi Virus until an FBI agent examined it. Thus, in the cyber context, prevention is truly at least as important as the cure. A sentence of time-served, which the defense advocates, would ill-serve the goal of general deterrence.

VI. The Defendant's Arguments

A. The Weight To Be Accorded The Guidelines

The defense argues that the Guidelines in this case should "not be accorded much, if any, deference." Def. Ltr at 9. That assertion flies in the face of the Supreme Court's admonition that

the Guidelines range is “the lodestar” that “anchor[s]” the district court’s discretion. *Molina-Martinez*, 578 U.S. at 198-99 (quoting *Peugh*, 569 U.S. at 541) (internal quotation marks omitted). The applicable Guidelines range accurately reflects the seriousness of a sophisticated and highly lucrative cross-border scheme that facilitated damage to at least tens of thousands of computers worldwide—as discussed above, a single proxy server was communicating with over 25,000 infected computers and Paunescu provided dozens of servers—and the theft of data relating to more than 136,000 credit and debit cards.

Nonetheless, given the totality of the highly unusual circumstances of this case, including Paunescu’s proactive outreach to U.S. law enforcement in 2014, the Government accepted a plea to an offense with a statutory maximum sentence that is almost half the bottom of the applicable Guidelines range. That Stipulated Guidelines Sentence does not overstate Paunescu’s degree of culpability.


B. The Defendant’s History And Characteristics

The defense argues that Paunescu’s life since his arrest in Romania warrants a sentence of time served. The Government does not dispute the sincerity of Paunescu’s remorse, but virtually every defendant expresses similar sentiments at sentencing. As discussed above, the crime the defendant committed was extremely consequential, and a sentence of time served would not adequately reflect the seriousness of the offense or achieve the goal of general deterrence.

C. Sentences Imposed On Other Gozi Co-Conspirators

The defense next argues that Paunescu should receive a sentence of time-served because other members of the Gozi conspiracy, Nikita Kuzmin and Deniss Calovskis, received time-served sentences of 37 months and 21 months, respectively. Those comparisons are inapt because Paunescu is not similarly situated to either of those defendants. As explained below, unlike Paunescu, Kuzmin provided substantial assistance and received a 5K letter from the Government, while Calovskis was much less involved in the Gozi conspiracy and earned very little money from his offense conduct.





Calovskis was not a cooperating witness. He was a relatively low-level member of the Gozi conspiracy. Calovskis joined the Gozi conspiracy years after the Gozi Virus had been created, was not involved in creating or disseminating the actual Gozi Virus, and wrote code that was designed to manipulate the webpages of a subset of banks. In addition, the available evidence showed that he was paid only approximately \$1,000 for his programming work. A copy of the Government's sentencing submissions as to Calovskis is attached hereto as Exhibit A. In contrast, Paunescu directly facilitated multiple cybercriminals' efforts to hack into and purloin information from at least tens of thousands of infected computers. And, in the defendant's own words, he earned \$1.7 million in just six months, at a conservative rate of approximately \$40,000 a week. *See* Section V.A, *supra*.

D. Conditions Of Confinement

The Government does not dispute that the conditions of confinement in Colombia and Romania are harsher than in the United States. Should the Court consider the conditions of detention in Colombia as a § 3553(a) factor, the Government respectfully asks the Court to consider two additional factors. *First*, the defendant sought to avoid the consequences of his crime for nearly a decade, even though he "had no doubt [that this day] was coming sooner or later." Def. Exh. A, at 1. He could have contacted U.S. authorities after restrictions on him were lifted by the Romanian authorities in or about June 2015 (Def. Exh. C, at 9), or simply surrendered to the U.S. Consulate, to resolve this case. He did not. Had he done so, he could have avoided arrest and detention in Colombia. *Second*, the Stipulated Guidelines Sentence of 60 months' imprisonment is nearly *half* the bottom of the applicable Guidelines range of 108 months. The Government respectfully submits that the Stipulated Guidelines Sentence adequately accounts for the unusual circumstances of this case.

The defense also claims that the conditions at Westchester County Jail ("WCJ") during the COVID-19 pandemic merit a variance from the Stipulated Guidelines Sentence. The Government strongly disagrees. According to a Booking and Transportation Operations Captain at WCJ, Paunescu has never been placed in solitary confinement at that facility. The pandemic affects all inmates, and there is no indication that Paunescu was treated more harshly than any other inmate at WCJ. To the contrary, as the defense notes, Paunescu has been able to avail himself of a number of programs offered by WCJ "to help him cope with the PTSD and trauma he experienced," including "the Know Better, Live Better program, the substance use disorder treatment program, the Resolve to Stop the Violence program." (Def. Ltr, at 7-8).

EXHIBIT A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - - x

UNITED STATES OF AMERICA

- v -

DENISS CALOVSKIS,

Defendant.

- - - - - x

:

:

:

:

12 Cr. 487 (KMW)

THE GOVERNMENT'S SENTENCING MEMORANDUM

PREET BHARARA
United States Attorney for the
Southern District of New York
Attorney for the United States
of America

DANIEL B. TEHRANI
Assistant United States Attorney
- Of Counsel -

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - - x

UNITED STATES OF AMERICA

- v -

DENISS CALOVSKIS,

Defendant.

- - - - - x

:
:
:
:
:

12 Cr. 487 (KMW)

THE GOVERNMENT'S SENTENCING MEMORANDUM

Deniss Calovskis ("Calovskis" or the "defendant") is scheduled to be sentenced in this matter on December 14, 2015, at 12:00 p.m. The Government respectfully submits this memorandum in advance of the sentencing, and in response to the defendant's sentencing memorandum dated November 25, 2015 ("Def. Mem."), in which the defendant asks the Court to impose a below-Guidelines sentence of time served. (Def. Mem. at 1). The United States Probation Office recommends a high-end of the Guidelines sentence of 16 months' imprisonment. The Government respectfully requests that the Court impose an above-Guidelines sentence at the high-end of the Stipulated Guidelines Range of 12 to 24 months' imprisonment, as such a sentence would be sufficient but not greater than necessary to serve the legitimate purposes of sentencing.

Background

I. The Offense Conduct

The defendant, a Latvian citizen, participated in a conspiracy to distribute malware, known as the "Gozi virus," to individuals and entities throughout the world, in order to steal users' personal information. (PSR ¶¶ 10, 13). The malware worked by modifying online bank log-in screens in a manner that required users to input personal identifying information and then transmitting that information to servers controlled by the co-conspirators. (PSR ¶ 12). In total, the virus has infected more than a million computers worldwide, including at least 17,000 computers in the United States. (Id.).

The defendant's role in the scheme was to develop computer code, known as web injects, which altered how particular banking websites appeared on infected computers in order to deceive victims into divulging additional personal information. (PSR ¶¶ 19, 20). Calovskis developed web injects not only for the Gozi Virus, but also for other banking malware, such as the Zeus Trojan. (PSR ¶ 19).

II. The Plea Agreement & Guidelines Calculation

On September 4, 2015 the defendant pleaded guilty pursuant to a plea agreement (the "Plea Agreement"). As set forth in the Plea Agreement, the defendant and the Government agreed that the defendant's adjusted offense level was 15,

calculated as follows: A base offense level of six pursuant to U.S.S.G. §2B1.1(a)(2); because the loss attributable to the defendant's conduct could not be reasonably estimated, the offense level was not increased pursuant to U.S.S.G. § 2B1.1(b)(1); pursuant to U.S.S.G. §2B1.1(b)(2), because the offense involved 250 or more victims, the offense level was increased by six levels; the offense level was further increased by two levels, pursuant to U.S.S.G. § 2B1.1(b)(10), because a substantial part of the fraudulent scheme was committed from outside the United States, and by four levels pursuant to U.S.S.G. § 2B1.1(b)(18)(A)(ii), because the defendant was convicted of an offense under Title 18, United States Code, Section 1030(a)(5)(A). The adjusted offense level of 18 was reduced by three levels for timely acceptance of responsibility, resulting in a total offense level of 15.

Based on an offense level of 15 and a Criminal History Category of I (the defendant has no prior criminal history), the parties agreed that the applicable Guidelines range for the defendant's conduct was 18 to 24 months' imprisonment (the "Stipulated Guidelines Range").

The Probation Office calculates an adjusted offense level of 12, because it applies a two-level number-of-victim enhancement rather than the six-level enhancement in the Plea Agreement (because the resulting adjusted offense level is 14,

only two points are deducted for acceptance of responsibility). Because the amended November 1, 2015 applies to the defendant's sentencing, the Government agrees with Probation's calculation.¹ Ultimately, Probation recommends a high-end of the Guidelines sentence of 16 months' imprisonment. (PSR at 18).

Argument

I. A Sentence at the High-End of the Stipulated Guidelines Range Is Warranted

A sentence at the high-end of the parties' agreed upon range of 18 to 24 months' imprisonment is warranted in this case considering the factors set forth in Section 3553(a). The defendant's conduct is undoubtedly serious. The defendant participated in a massive cyber conspiracy to steal millions' of individuals' personal information. In order to obtain that highly valuable information, the defendant and his co-conspirators developed and disseminated malware that altered and/or replicated the users' interface with their online banking providers. By manipulating banking webpages, the defendant and

¹ Under the November 1, 2014 Guidelines, the victim enhancements under U.S.S.G. § 2B1.1(b)(2) were based solely on the number of victims. Because the parties agreed in the Plea Agreement that the web injects authored by the defendant affected more than 250 users, the parties agreed that the six-level enhancement applied. Under the November 1, 2015 Guidelines, however, unless the offense conduct resulted in "substantial financial hardship," the maximum enhancement under Section 2B1.1(b)(2) is two-levels. As noted above, because the losses attributable to the defendant's conduct cannot be reasonably estimated, the Government agrees that the two-level enhancement applies.

his co-conspirators tricked victims into providing them not only the information the banks typically would request, but additional information specifically requested by the conspirators. The potential scope, reach and financial magnitude of this type of cybercrime are enormous. And the fact that the defendant and his co-conspirators - with different skill sets and capabilities - were able to conspire from remote corners of the globe, without necessarily ever meeting or knowing each other's true names or identities, demonstrates the danger posed by such organized cyber activity.

Moreover, the defendant played a crucial role in the scheme. He authored the computer code - web injects - that enabled the malware to surreptitiously gather and steal victims' personal identification. Rather than using his code-writing capability productively, he instead sold it to help others carry out a massive worldwide heist of personal banking information.

Accordingly, a Guidelines sentence is necessary to reflect the seriousness of the defendant's conduct, promote respect for the law, provide just punishment, and deter the defendant and others around the world from engaging in this type of criminal activity.

Conclusion

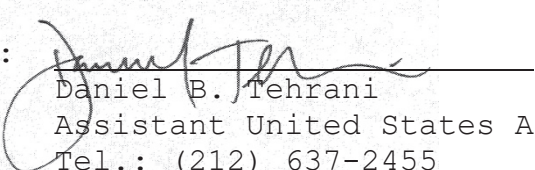
For the foregoing reasons, the Government respectfully requests that the Court impose a sentence at the high-end of the parties' Stipulated Guidelines range in this case.

Dated: New York, New York
December 7, 2015

Respectfully submitted,

PREET BHARARA
United States Attorney

By:



Daniel B. Tehrani
Assistant United States Attorneys
Tel.: (212) 637-2455

**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*

December 29, 2015

BY ECF

The Honorable Kimba M. Wood
United States District Judge
Southern District of New York
Daniel Patrick Moynihan U.S. Courthouse
500 Pearl Street
New York, New York 10007

Re: *United States v. Deniss Calovskis, 12 Cr. 487 (KMW)*

Dear Judge Wood:

The Government respectfully submits this supplemental sentencing letter in response to the Court's order, dated December 11, 2015. The Government shares the Court's concerns regarding the seriousness of the defendant's crimes and the need for general deterrence. As noted in the Government's sentencing letter, this is particularly the case given the ease with which individuals can remotely and anonymously conspire to engage in this kind of criminal activity.

The Government's recommendation of a high-end of the Stipulated Guidelines sentence – a sentence more than a year longer than the low-end of the applicable Guidelines and eight months longer than Probation's recommended sentence – weighs the need for general deterrence against the defendant's particular role in the conspiracy. In relevant respect, the defendant was not involved in creating or disseminating the actual Gozi Virus. Further, he did not begin participating in the conspiracy until years after the malware had been created. Calovskis, along with several others, was tasked with creating specific web injects that were used on a subset of infected computers to manipulate the manner in which individual banking webpages appeared. Thus, while the Court is correct that the Gozi Virus as a whole infected more than 17,000 computers in the United States, the defendant's participation in the scheme is more limited – both because of the shorter time period in which he participated and the fact that the Government believes that the web injects that he created do not exist on every computer infected by the Gozi Virus. Indeed, indicative of the defendant's more limited role in the scheme, the defendant received only approximately \$1,000 for his participation. The Government does not believe that he otherwise financially benefitted from the sale of the malware or the financial information that was stolen by the malware.

Thus, given these factors specific to the defendant's role, the Government respectfully believes that a sentence at the high-end of the Stipulated Guidelines would be appropriate in this case. That said, the Government does not disagree with the Court's view that general deterrence warrants strong consideration in this matter, and does not believe that a sentence greater than what the Government has recommended would be unreasonable.

Respectfully submitted,

PREET BHARARA
United States Attorney

By: /s/ Daniel Tehrani
Daniel B. Tehrani
Assistant United States Attorney
(212) 637-2455

cc: David Bertan, Esq. (by electronic mail)