United States District Court
Eastern District of Michigan
Southern Division

United States of America,

Plaintiff,

v.

D-1 Aleksandr Grichishkin,

Defendant.
_____ /

Hon. Denise Page Hood

Case No. 19-20478

Government's Sentencing Memorandum

I. INTRODUCTION

The United States offers this memorandum in anticipation of the August 18, 2021 (11:00 am) sentencing hearing for D-1 ALEKSANDR GRICHISHKIN ("GRICHISHKIN"). For the reasons below, the Government requests that the Court:

(1) find GRICHISHKIN's sentencing guideline range to be **87-108 months for Conspiracy to Engage in a Racketeer Influenced Corrupt Organization** (Count One), based on Offense Level 29 and Criminal History Category I, as the probation department recommends, PSR ¶¶ 49-50; and

(2) sentence GRICHISHKIN as recommended by the Government

in a separate document filed under seal.

This sentence will be sufficient, but not greater than necessary, to meet the sentencing goals of 18 U.S.C. § 3553(a).

II. BACKGROUND

Mr. GRICHISHKIN's plea agreement and presentence report ("PSR") contain extensive information about his offense that needs not be repeated here. *See* Plea Agreement, ECF No. 61, PageID.241; PSR ¶¶ 7-16. However, a general overview derived from the factual basis for GRICHISHKIN's plea is offered for context.

Defendants ALEKSANDR GRICHISHKIN, Andrei Skvortsov, Aleksandr Skorodumov, and Pavel Stassi were founders and/or members of a so-called "bulletproof" hosting organization (the "Organization"). The Organization rented Internet Protocol (IP) addresses, servers, and domains to cybercriminal clients, who used this technical infrastructure to disseminate malware used to gain access to victims' computers, form botnets, and steal banking credentials for use in frauds. Malware hosted by the Organization included Zeus, SpyEye, Citadel, and the Blackhole Exploit Kit, which rampantly attacked U.S.

companies and financial institutions between 2008 and 2015 and caused or attempted to cause millions of dollars in losses to U.S. victims. A key service provided by the defendants was to help their clients to evade detection by law enforcement and continue their crimes uninterrupted. The defendants did so by monitoring sites used to blocklist technical infrastructure used for crime, moving "flagged" content to new infrastructure, and registering all such infrastructure under false or stolen identities. The proprietors, GRICHISHKIN and Andrei Skvortsov, launched the Organization in approximately August 2008 and were its operational leaders. As the day-to-day manager, GRICHISHKIN addressed the criminal needs of the business on a routine and consistent basis for the entire period of its existence. Specific instances of his criminal conduct on behalf of the Organization are detailed in the factual basis for his plea. *See* Plea, ECF No. 61, PageID.248, ¶ 5.I(a)-(h).

III. SENTENCING GUIDELINES

U.S. Probation and the parties agree that the applicable guideline range is **87-108 months** for Conspiracy to Engage in a Racketeer

Influenced Corrupt Organization (Count One). PSR ¶¶ 49-50.

IV. SENTENCING FACTORS UNDER 18 U.S.C. § 3553(a)

1. The Nature and Circumstances of the Offense

GRICHISHKIN managed an organization that helped criminals deploy malware and steal money from others for approximately seven years. *See* Plea ¶ 5 (*passim*). As the Organization's everyday leader, GRICHISHKIN oversaw efforts to advertise their bulletproof hosting services in online cybercrime forums, set pricing for these services, negotiated and interfaced with clients seeking Internet infrastructure to be used in spamming and malware operations, managed employee hiring and compensation, and supervised the systems administrators' and other employees' work. He also regularly instructed other members of the Organization on how to "resolve" abuse notices by, among other methods, moving the affected clients' data to new, "clean" domains and IP addresses. He operated under a variety of online aliases. In doing so, he was fully aware of the Organization's criminal reach and consistently intended to (and did) help expand this reach. GRICHISHKIN embraced – on a daily basis – the Organization's

criminal purposes for approximately seven years for, in his words, "financial security." PSR ¶ 19.

During this time, the malware programs knowingly hosted by the Organization caused millions of dollars' worth of losses to U.S. financial institutions and U.S. victims (and others globally). *See* Plea ¶ 5.E. Given the significant difficulty in calculating an exact loss figure attributable to malware infections delivered by or otherwise aided by the Organization's technical infrastructure, the parties stipulated to a conservative loss amount of greater than $3.5 million in actual and attempted losses. *See* Plea ¶ 8.D. However, based on open-source research, the Government believes that these malware program caused losses (at least some of which were attributable to the Organization) that were much higher. By some estimates, Zeus caused at least $43 million in losses, and SpyEye caused between $64 million and $726 million in losses, in 2011 alone.[1] The Department of Justice's press release issued following the sentencing of Citadel's developer asserts that, "[a]ccording to industry estimates, Citadel infected approximately

[1]*See* **Ex. 1** (Financial Services Information Sharing & Analysis Center statement submitted in connection with another sentencing).

11 million computers worldwide and is responsible for over $500 million in losses."[2] Dyre, the malware involved in the 2015 intrusion described in Paragraph 5.I.h. of GRICHISHKIN's plea, was likewise estimated to have caused "many millions of dollars" in losses.[3] Finally, security company TrendMicro asserts that "[b]y 2011, …[the Blackhole Exploit Kit] was responsible for more than 90 percent of new [malware] infections documented by [anti-virus company] AVG, and it still accounted for more than half of similar incidents in 2012,"[4] strongly indicating additional and significant losses may have been caused by the Organization's distribution of Blackhole during this period.

Finally, the impact of the bulletproof hosting, and the consequent computer intrusion, identity theft, and financial fraud, was not only monetary. For example, in his/her victim impact statement, the

---

[2] *See* U.S. Dept. of Justice, *Russian Citizen Who Helped Develop the "Citadel" Malware Toolkit Is Sentenced*, July 19, 2017, https://www.justice.gov/usao-ndga/pr/russian-citizen-who-helped-develop-citadel-malware-toolkit-sentenced-0.

[3] *See* Security Intelligence, *Dyre Straits: Group Behind the Dyre Trojan Busted in Moscow?*, Feb. 9, 2015, https://securityintelligence.com/dyre-straights-group-behind-the-dyre-trojan-busted-in-moscow/.

[4] TrendMicro, *The Aftermath of the Blackhole Exploit Kit's Demise*, Jan. 29, 2014, https://blog.trendmicro.com/aftermath-blackhole-exploit-kits-demise/.

Superintendent for a school district in New York describes in detail the devastation s/he and the district suffered as a result of a malware infection aided by the Organization under GRICHISHKIN's day-to-day management. The Superintendent states:

> I was the school superintendent in [redacted] at the time the key logger was put on one of our computers which allowed the theft of millions of dollars. … [redacted] is a small district with about 800 students at that time. Parents are either middle income or work for minimum wage. Most homes, including mine, had no high-speed internet. Students without high speed at home often had to drive to the school nights or weekends and sit in the parking lot to get their schoolwork done. I just could not wrap my head around how and why the money had been stolen. How was I going to tell the taxpayers that we had lost eight (8) million dollars? How was I going to call each of my seven board members and explain it to them? How was it fair for hard working people, including people making minimum wage, to shoulder this loss? How many sports, clubs and extra-curricular events would have to be taken from the students? Needless to say, it was several terrible months for the students, taxpayers, employees and myself.
>
> It was an unthinkable attack on the school's mission as that experience nearly devastated the learning and enrichment environment for the children. The school is and has always been the hub of the rural community. Providing students the support, dedication, quality instruction and experiences they need as they strive to fulfill their dreams and aspirations for the future in a safe environment. The theft was a direct attack on that environment. The emotional impact was great for the school community. There is not a day that goes by

> that I do not think about it …The financial impact still lurks over the community and the theft has left the children without all its resources to this day.

Ex. 2 (Victim Letter (redacted)).

As the Court knows from the Plea Agreement, GRICHISHKIN's management of this Organization also affected individual victims. *See* Plea ¶¶ 5.H.b., 5.I.h. For example, under GRICHISHKIN's leadership, the Organization used a stolen U.S. passport of victim "C.D.," a real person in the United States, and a fraudulently created utility bill in C.D.'s name, to register a web-hosting account, an account that was open until approximately January 2014. *Id.* at ¶ 5.I.f. The government has been in touch with "C.D." and understands that "C.D." was aware, since at least 2010, that his personal identifying information was stolen and being used by others, all around the world, without his consent. It is hard to imagine how difficult it would be to grapple with the knowledge that one's identity is being abused, without any ability to prevent or control the effects. The sentence in this case needs to reflect the seriousness of this wrong.

The criminal organizations that purposefully aid others to disseminate malware that maliciously infiltrates computers and

ravages U.S. financial institutions and their accountholders are no less responsible for the harms these malware campaigns cause than their clients. Based on the duration of GRICHISHKIN's employment by the Organization, as well as the extensive harm the Organization caused, his offense is very serious in nature.

2. GRICHISHKIN's History and Characteristics

GRICHISHKIN appears to have been raised in a stable home and has no history of mental illness or abuse. *See* PSR ¶¶ 38, 42-43. He continues to have support from his family, including that of his wife and two children. *Id.* ¶¶ 39-40. Other than a "mild liver disorder," he appears to be a healthy man. *Id.* ¶ 41. He has no history of substance abuse (at most, "minimal alcohol and marijuana use" and nothing since at least 2013). *Id.* ¶ 44. He is highly educated, even receiving a "master's degree in civil law" from Moscow State Law Academy. *Id.* ¶ 45. He attributes his approximate seven years of criminal activity (committed from age 21 to 28 from "roughly 2008 to 2015") to his desire for "financial security," which resulted in him rationalizing his continued involvement, even after he "he learned that a large fraction of

… [the] income was derived from cyber criminal clients," because the Organization under his management did not enable "child pornography, terrorism, and fake charities." *Id.* ¶ 19.

Unlike many defendants that come before this Court, GRICHISHKIN had minimal or no barriers preventing him from succeeding in a legitimate job. By his role as a proprietor and his approximate seven years of managerial conduct in this very case, he has demonstrated he had and has the skills and savvy to be gainfully employed in a non-criminal position. He could have achieved "financial security" and avoided victimizing others simply by doing the good he was capable of. Yet, for at least seven years, he chose to manage an Organization that helped others steal money from victims. Nothing in his personal background explains why.

Nevertheless, the Government is cognizant that since approximately 2015, GRICHISHKIN appears to have made efforts to work in a "completely legitimate" manner. *Id.* ¶ 19.

3. *The Need for the Sentence Imposed to Reflect the Seriousness of the Offense, to Promote Respect for the Law, and to Provide Just Punishment for the Offense*

Malware impacts U.S. financial institutions and victimizes American citizens every day. While law enforcement labors to bring cybercriminals to justice, criminal organizations like the one GRICHISHKIN co-founded purposefully aid these cybercriminals by helping them maximize their profits and avoid law enforcement detection, thereby incentivizing their clients to continue their crimes. Because of the essential services they provide, bulletproof hosters share the criminal responsibility of their clients. A sentence that reflects this reality is necessary both to deter others who might rationalize similar criminal conduct (concluding, for example, as GRICHISHKIN did, that they are less responsible because they supported "certain ethical standards" by not disseminating malware that supported "child pornography, terrorism, and fake charities") and to increase the costs to cybercriminals (who are less able to profitably or "safely" disseminate malware without the insulation provided by bulletproof hosters). A Guideline sentence is necessary to reflect the seriousness of the offense, promote respect for the law, and provide just punishment.

4. *The Need for the Sentence Imposed to Afford Adequate Deterrence to Criminal Conduct and to Protect the Public from*

Further Crimes of GRICHISHKIN

Specific deterrence of GRICHISHKIN's criminal behavior appears unnecessary. Due to the complexity of the offense conduct, the international nature of the crime, and the length of the Government's investigation, GRICHISHKIN was not charged until 2019. He appears to have made efforts to engage in legitimate work and develop a stable family life since "around 2015." *Id.* ¶¶ 19, 39.

However, as noted above, a Guideline sentence is important to deter others who may be tempted by the allure of easy profits from these problematic crimes.

5. The Need to Avoid Unwarranted Sentencing Disparities

The sentences (of which the Government is aware) for defendants in similar cases have varied significantly based on the scope of the conduct and the losses caused, ranging from 33 months to 18 years. *See, e.g.*, *United States v. Bondarenko et al. (Leopard)*, No. 2:17-CR-306-29, ECF No. 813 (D. Nev. Mar. 24, 2021) (bulletproof hoster sentenced to 60 months' imprisonment following guilty plea and cooperation); *United States v. Sahurovs et al. (Sahurovs)*, No. 0:11-CR-177-1, ECF No. 80 (D.

Minn. Sept. 12, 2018) (bulletproof hoster sentenced to 33 months' imprisonment following guilty plea, with credit for 18 months of time-served). While not providing bulletproof hosting infrastructure, enablers of cybercrime in other cases have also received lengthy custodial sentences. *See, e.g.*, *United States v. Vega*, No. 1:07-CR-707-1, ECF No. 105 (E.D.N.Y. Dec. 18, 2013) (founder of cybercrime marketplace CarderPlanet, which was used to check validity of and sell stolen credit cards, sentenced to 18 years imprisonment following guilty plea); *United States v. Bondars et al.*, No. 1:16-CR-228, ECF No. 168, 248 (E.D. Va. Sept. 21, 2018 and Apr. 19, 2019) (defendants hosting "Scan4You," a site providing infrastructure and tools used in cybercrime, sentenced to 168 months following trial and 78 months imprisonment following plea, respectively); *United States v. Burkov*, No. 1:15-CR-245, ECF No. 53 (E.D. Va. June 26, 2020) (operator of two online forums devoted to the facilitation of payment card fraud, computer hacking sentenced to 108 months imprisonment following guilty plea); *United States v. Pleshchuk et al. (Seleznev)*, No. 1:09-CR-491-13, ECF No. 316 (N.D. Ga. Dec. 1, 2017); *United States v. Seleznev*,

1:17-CR-306-1, ECF. No. 9 (N.D. Ga. Dec. 4, 2017) (member of cybercrime forum whose members trafficked in stolen credit cards and counterfeit documents, and committed bank fraud and computer crimes, sentenced to 168 months imprisonment following guilty plea); and *United States v. Bondarenko, et al. (Okeakpu)*, No. 2:17-cr-00306-JCM-VCF, ECF No. 892 (D. Nev. July 26, 2021) (Anthony Okeakpu sentenced to 48 months of imprisonment following plea to RICO conspiracy for his low level role moderating a forum for an online criminal marketplace).

Finally, as the Guidelines calculation in his Plea Agreement reflects, GRICHISHKIN, as day-to-day manager and one of the proprietors, was a more significant participant in the Organization in comparison to codefendants Pavel Stassi (sentenced to 24 months after Government motion) and Aleksandr Skorodumov (not yet sentenced), and it would be appropriate for him to receive a higher sentence than they will. GRICHISHKIN had significant interaction with cybercriminal clients and full visibility into the full scope of the Organization's criminal activities. While serving different functions, his conduct appears to be similar to that of Andrei Skvortsov (not yet

sentenced).

For all the reasons above, the Government submits that the sentence proposed in a separate filing under seal would not create unwarranted sentencing disparities with others.

V. RESTITUTION

Restitution is mandatory. The Government has identified specific victims who suffered actual losses during GRICHISHKIN's management of the Organization. *Id.* ¶¶ 17, 60. Based on the time period that he and his coconspirators participated in the criminal activities of this Organization, the Government requests that GRICHISHKIN be held jointly and severally liable with co-defendants, Andrei Skvortsov and Aleksandr Skorodumov, for the $298,172.00 due to the victim noted in the PSR, and jointly and severally liable with co-defendant, Andrei Skvortsov, for the $497,200.00 due to another victim as noted in the PSR. *Id.*

VI. CONCLUSION

In sum, the Government respectfully requests the Court:

(1) find GRICHISHKIN's sentencing guideline range to be **87-108**

months for RICO Conspiracy (Count One); and

(2) sentence GRICHISHKIN as recommended by the Government in a separate document filed under seal.

Such a sentence will be sufficient, but not greater than necessary, to meet the sentencing goals of 18 U.S.C. § 3553(a).

Respectfully submitted,

SAIMA S. MOHSIN
Acting United States Attorney

s/Patrick E. Corbett
PATRICK E. CORBETT
Assistant U.S. Attorney
211 W. Fort Street, Suite 2001
Detroit, MI 48226
(313) 226-9703
patrick.corbett@usdoj.gov

s/Louisa K. Marion
LOUISA K. MARION
Senior Counsel
U.S. Dept. of Justice, Crim. Div.
Computer Crime and Intellectual Property Section
1301 New York Ave. NW, #600
Washington, DC 20530
(202) 514-1026
louisa.marion@usdoj.gov

Date: August 5, 2021

CERTIFICATE OF SERVICE

I hereby certify that on August 5, 2021, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF.

s/Patrick E. Corbett
PATRICK E. CORBETT
(P41182)
Assistant U.S. Attorney
211 West Fort Street, Suite 2001
Detroit, Michigan 48226
(313) 226-9703
patrick.corbett@usdoj.gov