UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | : | |
| | : | No. 3:17 Cr. 83 (RNC) |
| -- v. -- | : | |
| | : | |
| PETER YURYEVICH LEVASHOV, | : | |
| a/k/a "Petr Levashov," | : | |
| a/k/a "Peter Severa," | : | |
| a/k/a "Petr Severa," | : | |
| a/k/a "Sergey Astakhov," | : | |
| | : | July 13, 2021 |
| Defendant. | : | |

**GOVERNMENT'S MEMORANDUM IN AID OF SENTENCING**

For more than a decade, until his arrest in April 2017, defendant Peter Levashov was one of the most prolific spammers on the Internet. Levashov was the "bot master" for three prominent computer botnets – massive networks of compromised computers that were under his control. Levashov used those botnets to send billions of spam messages, messages which ranged in destructive potential from relatively harmless advertisements, to email messages used to conduct "pump and dump" schemes, to email messages containing malicious links that spread malware such as viruses or ransomware.

For the reasons set forth in this memorandum in aid of sentencing, the government respectfully submits that a sentence in accordance with the Sentencing Guidelines should be imposed in this case.

## Background

### A. The Offense Conduct

A "botnet" is a network of compromised computers, each of which has been infected with malicious software, *i.e.*, malware, that enables the computer to be controlled remotely

without the owner's knowledge. *See* Presentence Report, dated March 15, 2021 ("PSR"), ¶ 7. An individual with control over a botnet is known as the "bot master."

A botnet can be used to facilitate cybercrimes on a massive scale. When an individual computer is compromised, data from that computer can be stolen, or the computer can be used to send spam or launch attacks on other computers. When tens of thousands of computers are used in concert as part of a botnet to do those same things, the potential impact and damage is that much greater.

In fact, however, the potential damage from a botnet goes beyond the sum of its parts. Botnets can be used to conduct "denial of service" attacks, which disable a victim's website or network by flooding it with traffic from tens of thousands of computers. Moreover, while it is relatively easy for computer security professionals to block spam messages from a single computer, it is extremely difficult to block spam being sent from tens of thousands of computers around the Internet.

This capability is what led Levashov to become the bot master, in succession, of three of the most notorious botnets in the brief history of cybercrime: Storm Worm, Waledac, and Kelihos. *See* PSR ¶ 7. Levashov began spamming in the late 1990s, using free or commercially-available mass mailing software. At some point, working with others, Levashov helped to develop Storm Worm, a botnet that was designed to send spam from multiple compromised computers, thus making the spam more difficult to block. Levashov often used hyperbolic, weather-related topics to increase the number of people who would open the spam messages, thus giving the botnet its name. At its peak, Storm Worm reportedly sent 57 million email messages in a single day. *See* "Storm botnet," https://en.wikipedia.org/wiki/Storm_botnet (retrieved July 13, 2021).

After a rift with his partners, Levashov used the knowledge that he obtained working with Storm Worm to develop, and to pay others to develop, the Waledac botnet. Waledac was reportedly capable of sending 1.5 billion spam messages a day, or 1% of the total global spam volume. *See* "Waledac botnet," https://en.wikipedia.org/wiki/Waledac_botnet (retrieved July 13, 2021).

Microsoft orchestrated a takedown of the Waledac botnet in March 2010. Because Levashov controlled the code for Waledac, it was relatively easy for him to create a new botnet, later named Kelihos by security researchers. Kelihos was reportedly capable of sending 4 billion spam messages a day. *See* "Kelihos botnet," https://en.wikipedia.org/wiki/Kelihos_botnet (retrieved July 13, 2021).

Levashov used the botnets primarily to send spam, but he also engaged in credential harvesting and denial of service attacks. Levashov was paid by other criminals to send spam on their behalf, including spam used in pump and dump schemes and spam that contained links to malware such as computer viruses or ransomware. For example, on or about September 22, 2016, Levashov used the Kelihos botnet to distribute the "JokeFromMars" ransomware. *See* PSR ¶ 10(c).

In April 2017, following Levashov's arrest, the FBI conducted a takedown of the Kelihos botnet. *See id.* ¶ 14. At the time of the takedown, the FBI determined that the Kelihos botnet consisted at any one time of computers associated with approximately 50,000 unique IP addresses. *See id.* ¶ 13. Because computers were continuously added to, and removed from, the botnet, however, the total number of unique IP addresses detected as part of the Kelihos botnet over the entire course of the takedown operation was approximately 200,000.

## ARGUMENT

### I. The Guidelines Calculation in the Presentence Report Is Correct

The Presentence Report adopted the government's guidelines calculation as set forth in the plea agreement. *See* PSR ¶ 80. Specifically, the adjusted offense level was calculated as follows:

| | |
|---|---|
| Base offense level | 7 |
| Loss or gain greater than $3.5 million | +18 |
| Ten or more victims | +2 |
| Intentional damage to a protected computer | +4 |
| Fraud conducted overseas / Sophisticated means | +2 |
| Use of special skill | +2 |
| Acceptance of responsibility | -3 |

Based on an adjusted offense level of 32, a criminal history category of I, and the mandatory consecutive sentence required under Count 8, the recommended Sentencing Guidelines range is 145 to 175 months in prison. *See* PSR ¶ 79.

Levashov disputes the +2 adjustment for fraud that was conducted from outside the United States and/or using sophisticated means, and the +2 adjustment for use of a special skill. *See* Defendant's Objections to the Presentence Investigation Reports ("PSR") and Sentencing Memorandum, July 6, 2021 ("Def. Memo."), at 3-8.

#### A. An Adjustment Is Warranted for Sophisticated Means / Scheme Committed Outside the United States

##### 1. Applicable Law

Under the Sentencing Guidelines, a defendant's offense level is increased by 2 if "a substantial part of a fraudulent scheme was committed from outside the United States" or if "the offense otherwise involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means." U.S.S.G. § 2B1.1(b)(10) (2018).

The commentary to the guidelines defines "sophisticated means" to mean "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." *Id*. comment 9(B). Examples of sophisticated means include locating offices in different jurisdictions, and hiding assets or transactions through the use of fictitious entities, corporate shells, or offshore financial accounts. *See id.*

The sentencing enhancement applies "even if each step in the scheme was not elaborate," but "the total scheme was sophisticated in the way all the steps were linked together so that [the defendant] could perceive and exploit different vulnerabilities in different systems in a coordinated way." *United States v. Jackson*, 346 F.3d 22, 25 (2d Cir. 2003); *see also United States v. Fofanah*, 765 F.3d 141, 146-47 (2d Cir. 2014) (holding that enhancement was properly applied in light of "repetitive and coordinated nature of [the defendant's] conduct" when shipping stolen cars overseas).

**2. Levashov Committed the Scheme from Outside the United States and Used Sophisticated Means**

It is undisputed that Levashov committed the crimes of conviction while he was outside the United States. This alone is sufficient to warrant the +2 offense level adjustment under U.S.S.G. § 2B1.1(b)(10).

Levashov offers the novel argument, however, that the adjustment does not apply to cybercrimes at all, because cybercrimes occur in "cyberspace." According to Levashov, allowing the adjustment to apply to cybercrimes would mean that the "almost any cybercrime or crime committed through the internet would automatically trigger the enhancement . . . ." Def. Memo. at 4.

Levashov's argument is plainly incorrect, as there have been numerous cybercrime prosecutions that have not implicated the adjustment for crimes committed "from outside the

United States." *See, e.g.*, *United States v. Brown*, 884 F.3d 281, 283 (5th Cir. 2018); *United States v. Snowden*, 806 F.3d 1030, 1032 (10th Cir. 2015).

Moreover, Levashov's argument entirely ignores the purpose of the adjustment, which is to increase the penalty, and thus the deterrence against, crimes committed from outside the United States, as those crimes are significantly more difficult to investigate and prosecute. There is simply no authority for carving cybercrimes out from this guideline, and Levashov offers none.

As an alternative and additional basis for imposing the +2 adjustment under U.S.S.G. § 2B1.1(b)(10), the Court can and should find that Levashov utilized "sophisticated means" to carry out the crime. As observed by the Probation Office:

> [Mr. Levashov] operated the Kelihos botnet through, among other means, a virtual private network ("VPN") connection/proxy, multiple servers distributed among multiple countries, and the servers known as "bulletproof hosts." . . . The VPN and the bulletproof hosts allowed Mr. Levashov to hide transactions and the distribution of the Kelihos malware.

PSR Addendum at 2.

The government would further note that Levashov was not using off-the-shelf malware. Levashov was involved in the design and implementation of Storm Worm, and he was even more directly responsible for the development of the Waledac and Kelihos malware. Levashov also made use of crypting services, such as "crypt4u," that allowed him to distribute his malware notwithstanding the best efforts of sophisticated, commercial antivirus software providers. Levashov worked closely with the "crypt4u" group to develop a custom, automated crypting solution that supported his need for high-volume crypting. Levashov's development and use of custom, sophisticated malware, and supporting tools, constitutes the use of "sophisticated means" far beyond the typical, garden-variety computer intrusion matter.

Levashov's reliance on *United States v. Adepoju*, 756 F.3d 250 (4th Cir. 2014), is misplaced. In *Adepoju*, the defendant challenged a "sophisticated means" adjustment in connection with a bank fraud conviction, where the underlying conduct involved the deposit of two fraudulent checks into bank accounts that the defendant attempted to open using the name and Social Security number of "T.A." *Id.* at 252-53. At sentencing, the district court asked how the defendant obtained the information about "T.A." and concluded that, absent evidence that the information was publicly available on the Internet, it must have been obtained through sophisticated means. *See id.* at 254. The Fourth Circuit vacated the sentence and remanded, stating that the district court "clearly erred by essentially shifting the burden to [the defendant] to disprove sophistication." *Id.* at 257. While the court of appeals certainly made clear that "sophisticated means" would require proof of "more than the forgeries, misrepresentation, and concealment inherent in bank fraud," *id.*, the court's decision "stem[med] not from weighing the evidence but from the absence of factual findings . . . ," *id.* at 258.

In this case, as already described, it is undisputed that Levashov used custom malware, command-and-control servers in different countries, bulletproof hosting, virtual private networks, and custom crypting solutions – none of which are inherent to the crimes of which he has been convicted. These sufficiently establish Levashov's use of "sophisticated means" in committing those crimes.

**B. An Adjustment Is Warranted for Use of a Special Skill**

**1. Applicable Law**

Under the Sentencing Guidelines, a defendant's offense level is increased by 2 if "the defendant . . . used a special skill[] in a manner that significantly facilitated the commission or concealment of the offense." U.S.S.G. § 3B1.3 (2018).

The commentary to the guidelines defines "special skill" to mean "a skill not possessed by members of the general public and usually requiring substantial education, training or licensing." *Id*. comment 4. Examples of special skills include the skills possessed by pilots, lawyers, doctors, accountants, chemists, and demolition experts. *See id.*

While a "special skill" is usually acquired through education, training, or licensing, it is not necessary that a defendant have obtained the special skill though those means. Because the commentary to the guideline includes the word "usually," there is "no basis for limiting the [offense level] increase to only those with formal educations or professional skills." *United States v. Spencer*, 4 F.3d 115, 120 (2d Cir. 1993) (holding that enhancement was properly applied to "self-educated, strongly technical" chemist); *see also United States v. Sharpsteen*, 913 F.2d 59, 62 (2d Cir. 1990) (holding that enhancement was properly applied to defendant with expertise operating printing press in counterfeiting case).

**2. Levashov's Development and Operation of the Kelihos Botnet Required Special Skill**

Levashov did not become "Russia's Spam King"[*] by using stock tools and basic computer knowledge that is generally available to a lay person. To the contrary, Levashov recognized that commercially-available mass mailing programs would be substantially inferior to a custom-built botnet designed to send spam, and he used his computer science education and expertise to build and operate three such botnets over fifteen years, improving on them with each iteration. Levashov also worked closely with the "crypt4u" group to develop an automated

[*] *See* "How the FBI Took Down Russia's Spam King—And His Massive Botnet," *Wired* (Apr. 11, 2017), *available at* https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet (retrieved July 13, 2021).

crypting solution that would support the needs of the Kelihos botnet, when existing crypting tools proved to be inadequate. These facts, together with Levashov's "use of the dark web, VPNs, [and] servers known as bulletproof hosts," *see* PSR Addendum, at 3, establish that Levashov used a special skill in committing the crimes to which he pled guilty.

Levashov's reliance on *United States v. Goodman*, 223 F.3d 320 (6th Cir. 2000), is misplaced. In that case, the defendant used off-the-shelf, Adobe software to manufacture counterfeit currency. *See id.* at 322. The defendant was able to pass one counterfeit note at a Taco Bell, and another at a yard sale. *See id.* The defendant had "no formal computer education" and learned to use the software program with a friend's help "in the course of a week." *Id.* The Sixth Circuit held that the "special skill" adjustment was not warranted, where the defendant's computer skills "cannot reasonably be equated to the skills possessed" by professionals such as pilots, lawyers, or doctors, and "can be duplicated by members of the general public with a minimum of difficulty." *Id.*at 323.

*Goodman* is plainly distinguishable, because Levashov did not simply purchase and use off-the-shelf malware. To the contrary, Levashov assembled three massive botnets, using malware that he helped to design or build, and he persevered despite the best efforts of Microsoft and various antivirus software providers and antispam service providers to stop him. Levashov's use of his computer science education and expertise fully warrants the "special skill" adjustment in this case.

## II. A Guidelines Sentence Is Warranted in This Case

### A. Applicable law

Although the Supreme Court has held that the Guidelines are not mandatory, *see United States v. Booker*, 543 U.S. 220 (2005), it has also held that courts must "consult" the Guidelines and "take them into account" when fashioning a sentence. *Id.* at 264. A district court "should begin all sentencing proceedings by correctly calculating the Guidelines range," and that range is "the starting point and the initial benchmark." *Gall v. United States*, 552 U.S. 38, 49 (2007). After calculating the Guidelines, a court must consider the factors set out at 18 U.S.C. § 3553(a): "the nature and circumstances of the offense and the history and characteristics of the defendant," *id.* § 3553(a)(1); "the need for the sentence imposed" to further the four purposes of sentencing, *id.* § 3553(a)(2); "the kinds of sentences available," *id.* § 3553(a)(3); the Guidelines range itself, *id.* § 3553(a)(4); any pertinent policy statement by the Sentencing Commission, *id.* § 3553(a)(5); "the need to avoid unwarranted sentence disparities," *id.* § 3553(a)(6); and "the need to provide restitution to any victims," *id.* § 3553(a)(7). The statute directs a court, having considered these factors, to impose a sentence "sufficient, but not greater than necessary, to comply with the purposes" of federal criminal sentencing:

> (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
>
> (B) to afford adequate deterrence to criminal conduct;
>
> (C) to protect the public from further crimes of the defendant; and
>
> (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

*Id.* § 3553(a)(2).

District courts may not presume that a Guidelines sentence is appropriate. *Gall*, 552 U.S. at 50. But at the same time, "[t]he fact that § 3553(a) explicitly directs sentencing courts to consider the Guidelines supports the premise that district courts must begin their analysis with the Guidelines and remain cognizant of them throughout the sentencing process." *Id.* at 50 n.6. After all, while the Guidelines are not binding, "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), and the Guidelines are "the product of careful study based on extensive empirical evidence derived from the review of thousands of individual sentencing decisions." *Gall*, 552 U.S. at 46.

**B. A Guidelines Sentence Would Be Sufficient, But No Greater Than Necessary, In This Case**

The government respectfully submits that a Guidelines sentence should be imposed in this case, based in particular on the need to reflect the seriousness of the offense, the nature and circumstances of the offense, and the history and characteristics of the defendant.

With respect to the need to reflect the seriousness of the offense, it would be difficult to overstate the damage caused by botnets and their importance to the cyber crime ecosystem. Botnets cause damage in their own right, when they are used to steal data, to harvest account credentials, to distribute malware, and to conduct denial of service attacks. But botnets are also critical tools that are sold and shared by cyber criminals, who then use them to facilitate other cyber or cyber-enabled crimes. That is primarily how Levashov used Storm Worm, Waledac, and Kelihos – he did not conduct pump and dump schemes himself, nor did he distribute ransomware on his own behalf – but he allowed others to do so through the botnets that he controlled, and he profited handsomely from their crimes.

The nature and circumstances of the offense also support the imposition of a Guidelines sentence. Specifically, Levashov operated the botnets over a long period, nearly fifteen years in all. He continued doing so, even after the very public takedown of Waledac by Microsoft in March 2010. Levashov's insistent criminal conduct is hard to reconcile with the altruistic picture that is painted of him by the defense, except perhaps for an apparent belief that he was merely spamming – which may, in his mind, have seemed to be a victim-less crime.

Because Levashov used his botnets primarily to spam on behalf of others, it has in fact been difficult for the government to identify specific victims, *i.e.*, individuals or entities who have been "directly and proximately harmed" by his conduct. *See* 18 U.S.C. § 3771(e)(2) (2018). Given the volume of spamming conducted by Levashov over the years, nearly everybody who uses email is likely to have been a victim, at least to the extent that the receipt of spam emails causes a cognizable harm even absent a financial loss.

Finally, the history and characteristics of the defendant are, of course, an important consideration in this case. Indeed, the Probation Office suggests that the Court may consider a departure on the basis of the fact that Levashov has no prior arrests or incarceration. *See* PSR ¶ 99. The government does not believe that this factor should be considered by the Court, since it is already reflected in Levashov's criminal history category of I.

However, the government does also acknowledge that Levashov has had no disciplinary incidents since his incarceration, which started on February 2, 2018, nor violations of his release conditions, since his release on January 10, 2020. In light of Levashov's law-abiding conduct over a significant length of time, the government does not believe that the need for specific deterrence, or to protect the public from further crimes of the defendant, are significant factors that must be considered in determining an appropriate sentence.

**Conclusion**

Based on the forgoing, the government respectfully submits that the Court should adopt the Sentencing Guidelines calculation set forth in the Presentence Report and should impose a sentence under the Guidelines.

Respectfully submitted,

LEONARD C BOYLE
ACTING UNITED STATES ATTORNEY

EDWARD CHANG
ASSISTANT UNITED STATES ATTORNEY
Federal Bar No. ct26472
157 Church Street, 25th Floor
New Haven, CT 06510
T: (203)821-3826 E: Edward.Chang@usdoj.gov

**CERTIFICATE OF SERVICE**

I hereby certify that on July 13, 2021, a copy of the foregoing was filed electronically and served by mail on anyone unable to accept electronic filing. Notice of this filing will be sent by email to all parties by operation of the court's electronic filing system or by mail to anyone unable to accept electronic filing, as indicated on the Notice of Electronic Filing. Parties may access this filing through the court's CM/ECF system.

Edward Chang

EDWARD CHANG