BRYAN SCHRODER
United States Attorney

ADAM ALEXANDER
Assistant United States Attorney
Federal Building & U.S. Courthouse
222 West 7th Avenue, Room 253
Anchorage, Alaska 99513-7567
Phone: (907) 271-5071
Fax: (907) 271-1500
Email: Adam.Alexander@usdoj.gov

CATHERINE ALDEN PELKER
Trial Attorney
Computer Crime & Intellectual Property Section
1301 New York Avenue NW, Suite 600
Washington, DC 20005
Telephone: (202) 514-1026
Facsimile: (202) 514-6113
Email: Catherine.Pelker@usdoj.gov

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. KENNETH SCHUCHMAN, Defendant.	)	Case No. 3:18-cr-00095-TMB-DMS

GOVERNMENT'S SENTENCING MEMORANDUM

SUMMARY OF THE JOINT SENTENCING RECOMMENDATION

TERM OF IMPRISONMENT ……..12 Months

SUPERVISED RELEASE …….. Three Years

COMMUNITY CONFINEMENT ……18 Months (Special Condition)

COMES NOW the United States of America, by and through undersigned counsel, and hereby files this Sentencing Memorandum. For the reasons stated herein, the United States respectfully asks the Court to impose a sentence of 12 months and one day of imprisonment, followed by a three-year term of supervised release, with a special condition of 18 months of community confinement following his term of imprisonment. The defendant joins this recommendation.

I. INTRODUCTION

a) Summary

The defendant has pleaded guilty to aiding and abetting computer intrusions, a violation of 18 U.S.C. §§ 1030(a)(5)(A) and 2. The charge pertains to a long-running scheme in which the defendant and his co-conspirators developed distributed denial of service (DDoS)[1] botnets.[2] Initially, the botnets were based largely on the source code previously developed by other individuals to create the Mirai botnet familiar to the Court here. However, Mr. Schuchman and his associates added additional features over time, so that the botnets grew more complex and effective. At various times, these successor botnets were known as "Masuta," "Satori," "Okiru," and "Tsunami"/"Fbot." This court has already sentenced the three creators of the Mirai botnet: Josiah White, Paras Jha, and Dalton Norman.

[1] DDoS attacks occur when multiple computers acting in unison flood the Internet connection of a targeted computer or computers. The amount of traffic generated by such an attack quickly overwhelms the capacity of the target computer, resulting in the target computer being unable to send, receive, or respond to commands. DDoS attacks are often directed at servers that host websites, with the intent of rendering those websites unavailable to the public. They may also be directed at personal computers or corporate networks.

[2] A botnet is a collection of computers infected with malicious software and controlled as a group without the knowledge or permission of the computers' owners.

While the defendant and his co-conspirators utilized these successor Mirai variant botnets to conduct DDoS attacks themselves, their primary focus was selling access to paying customers in order to generate illicit proceeds. The defendant and his associates used an array of complex means to compromise the devices in order to force them to participate in botnets that then conducted DDoS attacks against separate victims.

b) Botnet Evolution

In August 2017, the defendant's botnet operated under the name "Satori." This version extended the Mirai DDoS botnet's capabilities and compromised approximately 100,000 devices, including devices located in the District of Alaska. The defendant's associates at this time were individuals known to the Government who utilize the nicknames "Vamp" and "Drake." Vamp served as the primary developer and coder for the botnet at this time. Drake took the lead in managing the sales and customer support. Schuchman developed and acquired exploits used to infect new devices for the botnet and provided development support.

By in or about September or October 2017, the defendant and others made improvements to the Satori botnet, which they rebranded under the name "Okiru."

In or about November 2017, the defendant, Vamp, Drake, and others further evolved Satori and Okiru, naming the updated version "Masuta." Masuta targeted vulnerable Huawei devices and vulnerable Gigabit Passive Optical Network (GPON) devices, infecting up to 700,000 devices. Logs during the time-period that Masuta was deployed show that a large number of attacks were launched at the end of November 2017 by the defendant, Drake, and others, including customers. At this time, the defendant also operated his own distinct DDoS botnet which he himself utilized to conduct attacks.

In or about January 2018, the defendant, Drake, and others focused on combining elements of both Mirai and Satori to exploit devices largely based in Vietnam in order to expand the size and power of the resulting botnet.

By in or about March 2018, the defendant, Drake, Vamp, and others further improved the botnet, which at this time came to be known as "Tsunami" and "Fbot". Tsunami/Fbot consisted predominantly of new and exploited vulnerable Goahead camera devices. During the time-period that Tsunami/Fbot was deployed, the botnet infected up to 30,000 devices and was utilized primarily to target gaming servers. During this development period, Mr. Schuchman and his co-conspirators discovered approximately 650,000 vulnerable High Silicon DVR systems. Test attacks using a small number of these DVR systems resulted in extremely powerful attacks, with estimated bandwidths exceeding 100 Gigabits per second. Mr. Schuchman infected approximately 35,000 of these devices by conducting brute force credential attacks for common login credentials.

In April 2018, Mr. Schuchman and others developed a new Qbot-derived DDoS botnet which briefly put Mr. Schuchman in competition with Vamp. By July 2018, when Mr. Schuchman was first interviewed by the FBI, he was again working with Vamp and Drake to improve their active series of DDoS botnets.

c) Additional Post-Indictment Conduct

As described in greater detail in the Presentence Report, the defendant's performance on pretrial supervision has been spectacularly poor. See PSR at 3-9. After his arraignment in the instant criminal case in August 2018, the defendant was released to pretrial supervision under conditions set by the court at Docket 12; over the next month, he flouted those conditions of

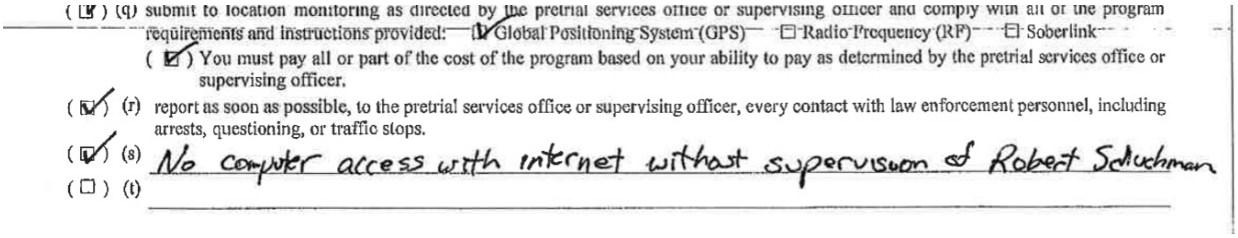
release in spectacular fashion, by **continuing to create and operate a DDoS botnet** – the very conduct for which he had been charged, as will be described in greater detail below**.**

A brief description of the nature of those initial October violations referenced briefly in the PSR at 3 bears further description and is relevant to the court's consideration at sentencing. Shortly after the defendant was released on the conditions set out in the order at Docket 12, the FBI gained access to chats dated October 3, 2018, between the defendant and a co-conspirator using the nickname using the alias "ViktorLast Monday." The true identity of "Viktor" (also known as "Vamp") is known to the Government.

The chats begin with "Viktor" greeting the defendant by saying "hello Alaskan police," a reference to contemporary media coverage of the MIRAI conspirators who at that point had been recently sentenced by this court. The defendant responded "idk [I don't know] what's gonna happen im just playing dumb for now." "Viktor" asks the defendant "how much money is the fbi paying you to inform?" to which SCHUCHMAN responds "im on house arrest . . . i said that i did so many drugs i cant remember most events of late."

Later in the chat the defendant stated "i got a new phone too deleted all my gmail, twitter, etc only kept disc imam make new alias." "Viktor" advises the defendant that he had seen his "court docs" (conditions of release at Docket 12) and that he knows "your dad has to supervise your comp use too well internet use." The defendant responded: "yes, but he doesn't care." "Viktor" then sends SCHUCHMAN a link that is still live as of writing to a screen capture from his own conditions of release in this case at Docket 12, copied below.[3]

[3] https://cdn.discordapp.com/attachments/484359134041341952/491170205775560704/Screenshot_20180917-095443.jpg


(☑) (q) submit to location monitoring as directed by the pretrial services office or supervising officer and comply with all of the program requirements and instructions provided: ☑ Global Positioning System (GPS) ☐ Radio Frequency (RF) ☐ Soberlink
(☑) You must pay all or part of the cost of the program based on your ability to pay as determined by the pretrial services office or supervising officer.
(☑) (r) report as soon as possible, to the pretrial services office or supervising officer, every contact with law enforcement personnel, including arrests, questioning, or traffic stops.
(☑) (s) No computer access with internet without supervision of Robert Schuchman
(☐) (t)

The defendant responded by writing "ya lol [laughing out loud] i didn't know those were public lol." Following that exchange, the defendant asks "Viktor" "do you trust discord" [the chat service being used] before writing "we need to talk Like as one person to another There's things you need to know I noticed a pattern in some things Ur [You're] gonna want to know And I am not cooperating with them." The defendant then wrote "Serously [sic] if I made a deal to cooperate I would not be allowed to talk to you let alone be open with everyone about what's going on When I spoke to my attorney he said it might backfire on me that if I had signed anything I'd he [be] in major shit for talking to anyone about an ongoing investigation."

The defendant then wrote shortly after "I'm not using a home connection and I'm with on mobile or live USB of Debian," referring to his unsuccessful attempts to obfuscate his continuing criminal conduct while on supervised release. The defendant then tells his co-conspirator "Viktor," who suspected that the defendant was cooperating with law enforcement, "If anything lm [I'm] hanging my neck out talking to you . . . Because it's the right thing to do." "Viktor" responds to the defendant's entreaties by stating "dude you're a compulsive liar and known manipulator."

As a result of the defendant's extensive pretrial release violations, the Court issued a warrant and the defendant was re-arrested on October 19, 2018. PSR at 3. The defendant was ultimately ordered released to an inpatient substance abuse treatment program on November 29, 2018; however, within a week of discharge from the program in February 2019, he tested positive for Suboxone and was removed from his sober living residence. PSR at 4. He

accumulated numerous drug-related violations in the ensuing months and was ultimately ordered detained again on August 21, 2019. PSR at 5. The defendant was subsequently released to another residential treatment program on September 4, 2019, but was discharged from the program a month later due to possession of drug contraband. PSR at 6. The defendant then absconded from pretrial supervision and was rearrested on November 21, 2019. PSR at 7.

The circumstances surrounding the defendant's most recent re-arrest are troubling. The management staff at the defendant's father's apartment complex, where the defendant was residing while on abscond status, reported numerous complaints against the defendant, including invitations to underage children to swim naked in the pool. When the U.S. Marshals Service (USMS) entered the apartment unit to apprehend the defendant, they found him using a computer, in violation of his conditions of release. Just prior to his arrest, Mr. Schuchman "began hitting buttons on the keyboard," PSR at 8, and subsequently told his father to destroy the computer. Though the device was seized by USMS, the defendant had succeeded in encrypting the device, and the defendant and his father have declined to provide the passwords needed to access the files contained therein, although efforts by law enforcement to access the laptop are ongoing. The defendant admitted to USMS that he had received and viewed videos of "juvenile[s[engaging in sexual acts with other juvenile[s]" on the laptop, PSR at 9.

II. PROCEDURAL HISTORY AND SENTENCING

a) Procedural History

The defendant was charged by Indictment in the District of Alaska on August 21, 2018, with two counts of violating the Computer Fraud and Abuse Act, 18 U.SC. § 1030(a)(5)(A). ECF 2. The court issued a summons, and the defendant was arraigned on the Indictment on

August 31, 2018. On September 3, 2019, the defendant pleaded guilty to Count 1 of the Indictment, pursuant to the terms of the plea agreement filed at Docket 89.

The defendant was released to Pretrial Supervision on August 31, 2018 and absconded from a residential treatment program on or about October 14, 2019. He was arrested on November 21, 2019, and has been detained since that date.

b) Presentence Report

The presentence report filed at Docket 115 (PSR) accurately calculates the defendant's adjusted offense level as follows: base offense level of six for a violation of 18 U.S.C. § 1030(a)(5)(A) pursuant to U.S.S.G. § 2B1.1; with a two-level enhancement for an offense involving 10 or more victims pursuant to § 2B1.1(b)(2)(A); an increase to a level 12 for the use of sophisticated means pursuant to § 2B1.1(b)(10); and a four-level enhancement resulting from the offense of conviction pursuant to 2B1.1(b)(19)(ii), resulting in an adjusted offense level of 16. PSR at 8-9. Given the defendant's criminal history, he is in Criminal History Category III, and his guidelines sentencing range as noted in the PSR is 27 to 33 months of incarceration. PSR at 17, 47.

c) Probations' Sentencing Recommendation

United States Probations recommends a substantially below-guidelines sentence of time-served and five-years' probation. This recommendation was based in part on the sentences imposed by this Court in the matters related to the Mirai botnet. For reasons the Court is aware of, those cases are not analogous to this matter. The Probation Office also pointed to the sentence imposed in U.S. v. Bukoski, 3:18-CR-00154-01-TMB. While Mr. Bukoski similarly engaged in a lengthy and significant computer crime enterprise, his guidelines range, 12 to 18 months, was significantly lower than the defendant's. Furthermore, Mr. Bukoski's acceptance of

responsibility, performance on pretrial release (including, unlike the defendant, refraining from committing additional computer crimes), and lack of criminal history and life-threatening medical conditions did not give rise to the same concern for recidivism raised in this case regarding the defendant.

d) Sentencing Recommendation of the United States

Consistent with the terms of the plea agreement filed at Docket 89 and the factors for the court's consideration pursuant to 18 U.S.C. §3553(a), the United States and the defense jointly recommend that the court impose a sentence of one year and one day, to be followed by three years of supervised release with a special condition of supervision requiring18 months of community confinement as defined by U.S.S.G. § 5F1.1, which can be satisfied with placement in a residential treatment facility. There are not many similarly situated youthful defendants convicted of violating the Computer Fraud and Abuse Act who will come before the court for sentencing with as serious a history of substance abuse as is presented here. As described in the PSR, the defendant's involvement with the criminal justice system began when he was 15, and has been characterized since by repeated failures to comply with court orders and a disregard for treatment. PSR at 41-46.

The United States submits that a guidelines sentence is appropriate here, given the serious nature of the offense, the extent and length of the defendant's criminal conduct, and the high likelihood of recidivism. However, the Government also recognizes the defendant's sincere need for lengthy in-patient treatment and is aware that Residential Drug Abuse Program (RDAP) placement is not likely to be an option for the defendant if sentenced to a guidelines term of imprisonment. The defendant has been approved for admission at Akeela House's 12 to 18-month residential recovery program. The jointly recommended sentence will allow for the

defendant to receive treatment through the 18 month term of community confinement recommended by the parties as a special condition of supervised release, which would allow him – if he chooses - to complete the Akeela House program rather than serving the full guidelines sentence in a federal detention facility. The eighteen month term of community detention proposed by the parties following the approximately 12 months he has already served in prison does approximate a high-end guidelines sentence as calculated by Probations if considered as a composite sentence.

In the context of the nature and circumstances of the offense of conviction as well as the history and characteristics of the defendant himself, this recommended sentence is consistent with the imperatives of 18 U.S.C. § 3553(a), prioritizing the need for the sentence imposed to afford adequate deterrence; protect the public from further crimes of the defendant; and provide the defendant with needed educational or vocational training as well as medical care or other treatment in the most effective manner.

Application Note 2 to § 5F1.1 provides that "[c]ommunity confinement generally should not be imposed for a period in excess of six months," but further states that "[a]longer period may be imposed to accomplish the objectives of a specific rehabilitative program, such as drug rehabilitation." Here, the parties are in agreement that the defendant is in need of both inpatient substance abuse and mental health treatment to address the diagnoses described in the Defense expert report attached as a sealed addendum to the Pre-Sentence Report, and the D has agreed, to his credit, to recommend a sentence to a term of supervised release including a special condition requiring 18 months of community confinement that may be satisfied by his admission to and successful completion of the 18 month Akeela house program, or the 12 month program

followed by 6 months of structured residential follow-on transitional treatment as determined by Probations.

The defendant aided and abetted extensive computer intrusions through his development and operation of the DDoS botnets. The sentencing calculation does not reflect the true loss figures caused by the defendant, which could have substantially increased the sentencing guidelines range. The defendant effectively masked the extent of his activity, including by periodically wiping the logs from his servers. As a result, the Government is unable to quantify the actual financial impact of the defendant's criminal activity and identify or confirm all of his victims. Nonetheless, the Government has contacted dozens of victims as part of its victim notification efforts. As is often the case in cyber investigations, these victims are generally and understandably reluctant to be publicly confirmed as victims of cyber attacks or to provide information regarding the losses that they incurred. In at least one other instance, the Government has been unable to confirm whether a potential victim – who alone reportedly incurred tens of thousands of dollars of damage – was in fact victimized by DDoS attacks launched Mr. Schuchman's botnets, in part due to Mr. Schuchman's efforts to conceal his activity. Unfortunately, this results in an undercalculation of the loss figure to be applied at sentencing pursuant to USSG § 2B1.1(b)(1), and thus an undercalculation of the defendant's guidelines range.

It is appropriate for the court to take into consideration the defendant's comparative youth and personal characteristics, but those mitigating conditions should be weighed against the significant universe of victims harmed by the defendant's actions and the concurrent need to not only specifically deter him from engaging in such conduct in the future, but also to serve as a deterrent to similarly situated individuals and protect the public from this type of criminal

activity. The Government respectfully believes that its recommended sentence achieves that objective and the other goals of Section 3553, particularly given the current circumstances and the fact that Bureau of Prisons RDAP may not be immediately available upon placement in a BOP facility.

III. CONCLUSION

For the above-stated reasons, the United States respectfully recommends a sentence of no less than 12 months and a day, to be followed by three years of supervised release with a special condition of 18 months of community confinement.

RESPECTFULLY SUBMITTED this 18th Day of June, 2020, in Anchorage, Alaska.

BRYAN SCHRODER
United States Attorney

s/ Adam Alexander
ADAM ALEXANDER
Assistant United States Attorney
United States of America

CERTIFICATE OF SERVICE

I hereby certify that on June 18. 2020,
a true and correct copy of the foregoing
was served electronically via
the CM/ECF system on the following:

Barry Flegenheimer

s/ Adam Alexander
Office of the U.S. Attorney