UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
CENTRAL DIVISION
LEXINGTON

CRIMINAL ACTION NO. 5:18-CR-73-JMH

UNITED STATES OF AMERICA

V. **UNITED STATES' SENTENCING MEMORANDUM**

COLTON GRUBBS

* * * * *

Colton Grubbs pleaded guilty to conspiring to illegally access computers, concealing evidence, and conspiring to launder his income from his computer intrusion conspiracy (R. 25). As a condition of his plea agreement, Grubbs agreed that he made over $150,000 from his crimes, that he obstructed justice, and that his computer crime conspiracy included both sophisticated means and a special skill (R. 25 at ¶ 7). The United States requests that the Court impose a sentence of at least three years, within the range calculated under the Sentencing Guidelines.

A three-year sentence is appropriate "to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense." 18 U.S.C. § 3553(a)(2)(A). Grubbs is not merely a computer hacker. The object of Grubbs' conspiracy was to profit by helping thousands of people around the world break their countries' laws by hacking the computers of friends and strangers (R. 25 at ¶ 5). Under the alias "KFC Watermelon," Grubbs developed and sold his hacking software, LuminosityLink, in the "Hacking Tools and Programs" section of the "Hackforums.net"

website He boosted his sales by offering extensive customer support, by advising (and organizing others to advise) his customers how to control other people's computers, steal sensitive information, and spy on their victims.

Although Grubbs' business involved daily violations of computer intrusion and privacy laws, Grubbs vigorously defended his copyright by maintaining an online licensing system to ensure that each LuminosityLink user would have to buy a separate copy of his software, and by threatening people who attempted to copy his software. After turning eighteen, Grubbs sold malware to over 6,000 customers who each paid him $39.99, which he spent on his personal expenses until it was seized by the Government.

Grubbs admitted that he sold his software knowing that his customers used it for illegal purposes. At Grubbs' website luminosity.link, he hypocritically advertised his product as surveillance software but promised to preserve the privacy and anonymity of purchasers paying him money. *See* Exhibit 1. Grubbs marketed his product by emphasizing its anti-detection and persistence features: that LuminosityLink prevented notifications to victims that it was installed or running on their computers, restarted when victim computers were turned on, and copied itself into new directories under different names to combat antivirus ("AV") software. He also advertised its malicious features: allowing customers to download passwords and usernames information from their victims' computers; log all keystrokes; use victim computers to "mine" cryptocurrency or launch denial-of-service computer attacks; and secretly activate the camera/microphone on their victims' computers to record victims in their homes.

Grubbs was not only the creator of hacking software, he was a user. He not only helped thousands of co-conspirators commit computer crimes at arms-length; he also conducted his own hacks and exploits and boasted about them on Skype:

a. On December 31, 2013, "kfcwatermelonhf" sent the messages "Want to hear some funny stories" "I had some buddies over last night, we were bored as fuck. Fired up my VPS and seen I had 11 bots on Plasma RAT" "so I setup the darkcomet and used my Inject via RunPE to inject DC into memory on the bots" "You know the audio capure and audio recording?" "You can record yourself and send it to the other user?" "This guy had this audio system setup on his PC" "And we screamed 'SUCK MY DICK' and heard it echo throughout his house" "5 seconds later this dude runs to his PC" "and he was on facebook, he was like 'wtf facebook'" "also this girl was watching porn" "and getting into it" "so we recorded ourself moaning" "and sent it to her" "and she was like WTF," "she was odd" "she was watching like" "strap on porn" "or some shit" "and her facial expressions on the webcam" "she didn't make any noise though"
b. On January 2, 2014, "kfcwatermelonhf" sent the messages "wanna know the best feature ever" "Audio capture and send audio" "I always record myself moaning and send it to people" "while they watch porn" "and watch their reaction" "swear its the funniest shit ever" "dude will be walking porn and ill moan and send it to his PC" "he'll freak the fuck out" "im not gay" "I had 2

friends over" "and we fucked with PCs so hard" "we screamed 'SUCK MY DICK' and it echoed throughout this persons house" "they had a nice audio setup" "and a nice house" "Was the funniest shit ever" "also this chick was watching porn" "and we'd moan and send it to her pc" "so fucking funny" "using audio capure we heard her mic so we knew she heard us"

c. On January 2, 2014, "kfcwatermelonhf" sent the messages "I had this really attractive Russian chick about 16 id say on my RAT" "her lil bro was on" "I said 'Hey, can you get your sister to come here?'" "and he like" "turned around" "said some russian shit" "she left the room" "and then her father came in" "this guy was so stereotypical russian" "anyways" "he like looked in temp directory" "and opened task manager" "then he got on facebook and played a game" "never seen her since" "my rat victims are on this time" "one of my RAT victims are watching a 6 hour mozart piano classical music playlist"

d. On January 2, 2014, "kfcwatermelonhf" sent the messages "SHES LIKE SIX YEAR OLD" "just sent her a audio clip of myself moaning" "LMFAO" "heard it" "6" "DAMN" "SHE TURNED THE PC OFF" "DUE TO ME MOANING"

As part of his customer service, Grubbs personally and routinely responded through Hackforums.net direct messages to customers' questions about hacking and reselling LuminosityLink abroad as authorized affiliates:

a. On July 16, 2016, "cabane2" and "KFC Watermelon" exchanged the messages "is your luminosity legacy still on and very stable? it used to fetch me more

slaves than the new one. just wanna know if its advisable to be using the old luminosity." "New version is more stable."

b. On July 20, 2016, "KJTR1" and "KFC Watermelon" exchanged the messages "Which DNS provider do you recommend for this rat?" "Any of them listed within the eBook will work without issue. My personal recommendation is using a $1 domain at NameCheap." "Is the miner built into the client or do they have to be binded together?" "It's built in"

c. On August 8, 2016, "Valentino Rossi" and "KFC Watermelon" exchanged the messages "I am unable to get saved passwords from clients, im using 1.4.2 and i tried to configure station by clicking reset url on password recovery, when i clicked test file, it says link not valid, please help." "It's online in 1.5.1. Will have to look into 1.4.2, which is really outdated"

d. On August 17, 2016, "KFC Watermelon" sent "Pharmacist" the messages "I created PlasmaRAT source. I am the original copyright holder." "I will directly send a DMCA complaint about another user using copyrighted content in their product."

e. On December 6, 2016, "Mirakuru" and "KFC Watermelon" exchanged the messages "bro do you have reseller price? i want to sell LuminosityLink my turkish customers." "Yes. $30 per copy, you can resell for $40."

To more efficiently help his customers break the law, Grubbs also recruited and organized at least nineteen other computer users into a Skype support network to answer various customers questions about hacking using LuminosityLink:

a. On January 5, 2016, "Saturn" and "Luis" exchanged the messages "xZ can u explain me the utility of power management, it keep connection with client if clients are in sleep/hibernate mode?" "no it simulate that the pc is in sleep mode but it isnt in sleep mode it is just black Screen and Monitor off" "the Utility is that Client stay connected"

b. On January 7, 2016, "- Chris (FuxXER@Da-seul.) -" and "Saturn" exchanged the messages "my bought another LL license, how come no victims inside? im using same existing dns setting.. humm" "just user id and different laptop.." "have connection there but 0 victims" "now I logoff this new id" "I sign-in my existing id" "in same laptop" "victims all poping up" "gonna get kfc to solve this" "Btw. Once again do not use the term 'victims' to speak about your clients pleas. (ty - Chris (XzZ.) (y)"

c. On January 9, 2016, "Zor" and "Phi" exchanged the messages "anyone can give me some advices about cloudcrypter?" "it gets detected really fast" "why?" "i suppose it gets detected so fast because it's so cheap and a lot of people who don't know not to scan on virustotal do that" "it's a good starter crypter"

d. On January 13, 2016, kfcwatermelonhf sent the messages “no it’s not up to us to create crypting guides, that’s crypter coders job” and “I have a good crypting thread”

e. On January 15, 2016, “Saturn,” “Yacine,” and “LilDurk” exchanged the messages “Are you guys losing your clients after a few days? Can’t seem to keep them for more than 2 days…” “have they an AV active?” “yes; but I am FUD (cloud crypter) on scantime.. things is I lost all of them (around 12, not a lot to be statiscally probant but still)” “so, the clients us lost = probably bcs of detections” “how can I update my slaves” “for another virus” “like all of them in one time” “please LilDurk, don’t talk about Slaves, it’s clients :)”

f. On January 16, 2016, “emanuel emenike,” “Saturn,” “Sheena York,” and “aaaa” exchanged the messages “I try open Server.exe another Windows 8.1 , Windows 10 computers too.. But Not working.. I cant connect victims and I cant see in machine list them.”

g. On January 27, 2016, “Zor,” “Владислав,” and “Cat” exchanged the messages “Hi guys” “A victim executed my crypted ll stub. And I did a file guard with encrypt. So, this is an extra stub? And my victims would be online for a long time? Right?” “Depends on the client tbh” “I can use File guard for my ll stub” “I suppose”

h. On January 30, 2016, “Saturn,” “Zor,” and “Tun Cef” exchanged the messages “persistence on rat builder OR crypter = detection most of time” “i advice u to

use LL startup but without rootkit (persistence)" "persistence is good, but it's better to get a stable connection, install rdp/remove AV etc, fake ico etc, and then put back persistence" "risky bro" "to use rootkit" "Why is that?" "Just detections?" "Why is it risky to use LL rootkit?" "read me bro, bcs rootkit is a persistence feature, and AV easily flag it"

i. On February 19, 2016, "Toxyiic" and "Jackson" exchanged the messages "i've tried both" "and i've tried 3 different crypters" "And have you tried it on your friends pc / your vm or on infected randoms?" "lol" "it was randoms first"

j. On March 14, 2016, "General K" and "Zor" exchanged the messages "You know what I can do to LL server so browser will not see it as a virus" "buy a server" "host the file on that" "almost all browsers report RAT server as malicious" "Can anything be don about that?" "get an offshore server"

k. On March 15, 2016, "Saturn" and "Heaven vi Britannia" exchanged the messages "for the price this stuff is just amazing" "instant run, no alert prompt" "Yeah, lumen is nice"

Grubbs made a business of flouting the law (except where it benefitted him) and profited from helping less sophisticated people commit computer intrusions. His messages show that he has no respect for the law, and show contempt for moral rules and social norms. His crimes and conspiracies require a lengthy sentence. Grubbs' personal history also indicates that a sentence of imprisonment will "provide the defendant with

needed educational or vocational training, medical care, or other correctional treatment in the most effective manner." § 3553(a)(2)(D).

A three-year sentence is appropriate "to afford adequate deterrence to criminal conduct." § 3553(a)(2)(B). Here, the need for deterrence is not theoretical. Grubbs created thousands of computer hackers worldwide, first by developing and selling LuminosityLink, and then by providing help, for example, to customers who "need support regarding a third party product (VPN, Crypter, etc.)" to make LuminosityLink fully undetectable ("FUD") by victims' antivirus computer software. *See* Exhibit 2. Grubbs admitted selling LuminosityLink to more than 6,000 people who conducted countless computer attacks. One cybersecurity firm, Palo Alto Networks, reported that Grubbs' software was used 72,000 times in actual or attempted attacks on just 2,500 of their customers.[1] Grubbs' sentence of imprisonment must be lengthy enough to ensure that these and other hackers understand that computer crimes are taken seriously, so that they will be deterred from further computer intrusions.

Grubbs admitted making over $150,000 selling LuminosityLink after he turned eighteen (R. 25 at ¶ 7(c)), and that he lived for years exclusively off of his income from his hacking software (PSR ¶ 68). During its investigation, the United States obtained court orders seizing some of the unspent money: $45,007 cash from Grubbs' bedroom, $52,482 in Grubbs' bank account, and 114.8 bitcoin (currently worth over $725,000,

[1] *See* https://researchcenter.paloaltonetworks.com/2018/02/unit42-rat-trapped-luminositylink-falls-foul-vermin-eradication-efforts/

previously worth over $2 million). But Grubbs may not claim that the forfeiture of his remaining profits is sufficient punishment or deterrence, because § 3553(a)(2)(B) requires "*the sentence* imposed . . . to afford adequate deterrence to criminal conduct" (emphasis added).

Imprisonment for three years is appropriate "to protect the public from further crimes of the defendant." § 3553(a)(2)(C). Grubbs is a criminal who broke the law every day for years, and he has ignored every chance and warning to stop his immoral and criminal conduct. In September 2016 and March 2017, days after Grubbs learned of the arrests of similar sellers of computer intrusion software,[2] he adjusted his software's default settings (but did not remove its malicious features) and drafted elaborate disclaimers that he thought would immunize him from responsibility (R. 1 at ¶ 19). When Grubbs was banned from PayPal for selling malware, he began a money laundering conspiracy to continue to collect money from the sales of LuminosityLink software (R. 25 at ¶ 5(e)). When Grubbs learned that the FBI wanted to search his apartment, he told his money laundering co-conspirator and his roommate to "clean their rooms," *see* Exhibit 3; removed evidence from his home that he has never provided to law enforcement (R. 25 at ¶ 5(f)); and then scattered his bitcoin proceeds into multiple new accounts to conceal it from law enforcement (R. 1 at ¶ 24).

[2] Alex Bessell, who received 24 months imprisonment for running the business Aiobuy and selling computer intrusion software; Taylor Huddleston, who received 33 months imprisonment for developing and selling the NanoCore computer intrusion software.

Grubbs' plea agreement describes only his conduct after his eighteenth birthday, but the Court may consider any information for the purpose of imposing an appropriate sentence. 18 U.S.C. § 3661. Grubbs has been an active member of Hackforums.net since 2013, where he sold Plasma Rat, a similar hacking software that he claims to have invented. *See* Exhibit 4. Testimony at trial would have proven that Grubbs has been a longtime repeat denial-of-service attacker on the computers of people with whom he played video games. Grubbs continued and expanded his criminality into his adulthood and cannot now claim that his crimes were justified by his middle-class background (PSR ¶ 57) or excused by his previous youth. Grubbs is a lifelong criminal, and the only way to protect the public from Grubbs is by incapacitating him in prison.

Respectfully submitted,

ROBERT M. DUNCAN, JR.
UNITED STATES ATTORNEY

By: s/ Neeraj K. Gupta
Assistant United States Attorney
260 W. Vine Street, Suite 300
Lexington, Kentucky 40507-1612
(859) 685-4843
Neeraj.Gupta@usdoj.gov

CERTIFICATE OF SERVICE

On September 14, 2018, I electronically filed this document through the ECF system.

s/ Neeraj Gupta
Assistant United States Attorney