United States Department of Justice

United States Attorney
District of Connecticut

157 Church St., 25th floor
New Haven, Connecticut 06510

(203) 821-3700
Fax (203) 821-5373

May 24, 2021

VIA ELECTRONIC MAIL

Hon. Michael P. Shea
United States Courthouse
450 Main St.
Hartford, CT 06103

Re: *United States v. Oleg Koshkin*, 3:19 Cr. 251 (MPS)

Dear Judge Shea:

I am writing to provide information that may assist the Court in reviewing the Jabber and Skype chat communications that the government addressed in its trial memorandum [Dkt No. 113]. As the government indicated, it believes that the chat communications not involving admin@crypt4u.com are either covered by the co-conspirator exception, are not being offered for the truth of the matter asserted, or are necessary to render the transcripts intelligible.

With respect to the co-conspirator exception specifically:

- Exhibit 7: This is a chat with support@crypt4u.com. The government submits that the name of the account, and the discussion that takes place concerning payment for services, support a finding that the individual using the account was a member of the conspiracy. Additional support for such a finding can be found in defense exhibit 1010, which is the full transcript of the chat. On the first page of that transcript, there is discussion of "feed redirection" and the "bot for redirect."

- Exhibits 13-18 & 25-26: These are chats with info@crypt.am. In exhibits 15 and 16, there are discussions concerning the size of the loader after being crypted. Specifically, it is stated that the loader cannot be too large, otherwise the user will leave the web page with the exploit; a loader that is too large is bad for exploit kits.

- Exhibits 21-23, 27, 32, 34-35 & 37: These are chats with vxxxxv@0n1ine.at, 01@xmpp.re, and 00001@exploit.im. The government believes that these accounts were all used by the same individual, and as shown in defense exhibit 1015, the defense apparently agrees. Exhibits 22 and 34 both contain references to the crypting of a "Socksbot."

- Exhibits 28-31 & 33: These are chats with crp4u@default.rs. In Exhibit 31, there is a list of antivirus programs that are identifying a crypted file as containing malware. Moreover, defense exhibit 1007 provides the full transcript of the chat, and on the first page of that transcript, reference is made to the crypting of a "socksbot."

- Exhibit 36: This is a chat with russian8@xta.im. Again, there is discussion about the need for the loader to be small, but that the size of the actual "bot" is not critical. There is also discussion about using a new crypter to avoid detection by a specific antivirus program "which nobody bypasses."

- Exhibit 62: This is a Jabber chat found on Koshkin's laptop, in which Koshkin is communicating with 00001@exploit.im as referenced above. The chat is replete with references to crypting and crypters.

- Exhibits 65-72: These are Skype chats found on Koshkin's Galaxy S7 cell phone. The communications by Koshkin are statements by a party opponent and therefore not hearsay. The communications by the other parties are not being offered for the truth of the matters asserted, but to establish Koshkin's continuing participation in the crypt4u service and to provide necessary context for Koshkin's statements.

Thank you for your consideration of this matter.

Very truly yours,

LEONARD C BOYLE
ACTING UNITED STATES ATTORNEY

Edward Chang

EDWARD CHANG
ASSISTANT UNITED STATES ATTORNEY

RYAN K.J. DICKEY
SENIOR COUNSEL
COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE

Cc: (via email)
Cheryl E. Heffernan, Esq.