SIGNIFICANT ACTIVITIES

VIOLENT CRIMINAL THREAT (VCT) Branch

OVERALL SOPHISTICATED TECHNIQUES/STATS

METHODS	ARRESTS	CONVICTIONS	DISRUPTIONS	DISMANTLEMENTS
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

YTD=Year to Date

I. **Major Operational Matters (**Arrests/Indictments/Convictions/Sentences /Searches/Drug Buys**)**

[redacted]

[redacted]

[redacted]

[redacted]

C-19; 9A-NY-3217706; SUBJECT -"RINGER", VICTIM- [redacted], EXTORTION, THREATENING COMMUNICATIONS; C/A SA [redacted]: On 01/08/2020, a cooperating defendant in the JEFFREY EPSTEIIN case reported to the FBI that he/she was receiving Overt Extortion threats via email. The subject was communicating via an application called CRIPTEXT and sending daily emails since 01/01/2020 to the victim, requesting money via paypal and Bitcoin in exchange to keep the subject from exposing information about the victim's relationship with JEFFREY EPSTEIN and others. If the subject did not receive payment, the subject would fabricate false emails appearing to be sent by the victim, to the subject, and then post these emails on a Twitter account. The subject followed through with posting when the money was not received. The emails contained information that was false in nature, but slandered the reputation of the victim. No information on CRIPTEXT was not found in any bureau system regarding cases using this application etc.

CRIPTEXT was established in 2014 and is a fairly small company. The company provides end to end encryption for users to use they GMAIL and mask their IPs via VPNs. SA [redacted] contacted the company via email, and eventually spoke to the CEO. The CEO had never had legal services requested and was unfamiliar with the protocol, however was willing to assist in anyways possible. SA [redacted] explained the subpoena process to the CEO as well as how other companies handle legal request such as law enforcement portals and Emergency Disclosure Requests. SA [redacted] also answered questions the CEO had on how to assist LEO's in investigations. Ultimately the CEO provided the requested information within a 24 hour period which identified the subject sending the threats, who is based in Sweden. SA [redacted] was able to build the relationship with the CEO and bridge it with the FBI. The CEO stated until the portal is in place, that FBI could contact the company at abuse@criptext.com and ask for him directly if necessary. An Intel product with all of the above information is in draft.

SA [redacted] then contacted ALAT [redacted], who is assisting in obtaining a DOB for the identified suspect, [redacted] to assist SA [redacted] in placing a travel alert on DEKKER. [redacted] has also stated he will see if Sweden can admonish DEKKER.

Numerous other subpoenas have been served where after unmasking IP addresses, the addresses resolve to Sweden, and additional open source research corroborates the subject is [redacted].

SA [redacted] was contacted by [redacted] of San Francisco who was handling a bomb threat in Kiev, where the subject was using Criptext as well. SA [redacted] was able to pass along the above information to assist him on his case.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]