FD-1057 (Rev. 5-8-10)

UNCLASSIFIED

Official Record

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) To open investigation on "Cyberguy" **Date:** 03/26/2015

CC: BLACKSTONE MICHELLE
Patrice M. Heelan

From: CHICAGO
CG-VC-2
Contact: SA Ingri Carr Hartwig, 312-829-5622

Approved By: SSA DUGAN BRIAN C

Drafted By: SA Ingri Carr Hartwig

Case ID #: 305D-CG-6232109 (U) "Cyberguy;"
Victim Unknown;
Possessors of Child Pornography

Synopsis: (U) To open investigation on "Cyberguy"

Full Investigation Initiated: 03/26/2015

Reference: 305A-HQ-4366094-LEADS Serial 72
803I-CG-133153-INTELPRODS Serial 12

Details:

Operation Downfall II - Other Hidden Services / TorChat

Shortly after Freedom Hosting was seized, several hidden services were set up on new, unknown servers. Due to this, in early 2014, the MCCU initiated Operation Downfall II to target these websites and users of these websites. Examples of these hidden services are "The Love Zone," "7axxn," and "Boy Vids 4."

In mid-2014, the FBI, MCCU, obtained the ability to identify IP addresses associated with certain users of TorChat and certain hidden services. To-date, the true IP addresses of hundreds of TorChat users, as well as several hidden services, have been identified. These hidden

services include "The Love Zone (TLZ)" and "7axxn," which were two of the largest child pornography websites within Tor.

Review of the IP addresses associated with "TLZ" and "7axxn" revealed that "TLZ" was hosted in The Netherlands, with the head administrator residing in Australia, and that "7axxn" was hosted in New Zealand. The head administrator of "7axxn" also resided in New Zealand.

Pursuant to the above information, in late 2014, the Queensland Police Service (QPS) in Australia and the New Zealand Police and Department of Internal Affairs (DIA) in New Zealand seized control of both sites. After seizing control, the QPS and DIA then operated the websites for a period of time in an undercover capacity.

During a portion of this time, the QPS and DIA uploaded a hyperlink to each of the sites. The hyperlink, which was available to any registered member of the sites, was advertised as a preview of a child pornography website with streaming video capabilities. When users clicked on the hyperlink, they were advised they were attempting to access a video file from an external website. If users chose to open the file, a video file began to play; resulting in the QPS/DIA being able to capture true IP addresses of the users as the file utilized an Internet connection outside of the Tor network.

(*It should be noted the streaming video contained various images of child pornography depicting prepubescent females. The use of actual child pornography images is a lawful investigative technique in Queensland, Australia.)

Approximately 33 members of "TLZ" accessed the video from an IP address within the United States. Reports for each of these users were then generated by the QPS/DIA and provided to the MCCU for further identification.

As part of the investigation, the QPS also provided periodic backup copies of the "TLZ" website to the MCCU for review. These copies contained all user activity on the site, including private messages

Title: (U) To open investigation on "Cyberguy"
Re: 305D-CG-6232109, 03/26/2015

sent/received by users. Upon receiving these copies, the MCCU entered the data into a previously established database that allows for easy searching and generating of reports.

Pursuant to the above information, one of the 33 users identified as having accessed the video hyperlink was a user known as "cyberguy."

Investigation into TLZ user "cyberguy"

After the user "cyberguy" was identified as having accessed the video hyperlink described above, the MCCU signed into "TLZ" utilizing an undercover account and captured selected posts made by this user.

According to the site, the user "cyberguy" initially registered to "TLZ" (referred to as Website 19 in the search warrant affidavit) on 8/3/2014. This user made a total of 68 posts from 8/3/2014 through the date of the undercover session on 12/9/2014. Examples of these posts are as follows:

On September 10, 2014, the user "cyberguy" made a post containing 16 images, the majority of which contained child pornography depicting prepubescent females, including the oral penetration of the female by an adult male's penis.

On October 10, 2014, the user "cyberguy" made a post containing 16 images, the majority of which contained child pornography depicting prepubescent females, including the vaginal penetration of the female by an adult finger.

A review of the MCCU user report for "cyberguy" also revealed that this user sent 19 private messages and received 7 private messages from 8/8/2014 through 11/8/2014. A copy of this report will be included in the package copy.

Identification of TLZ user "cyberguy"

According to the QPS, the user "cyberguy" utilized 73.8.83.152 on 11/11/2014 to access the streaming video. This IP address resolved to

Title: (U) To open investigation on "Cyberguy"
Re: 305D-CG-6232109, 03/26/2015

Comcast Communications.

An administrative subpoena issued to Comcast Communications in December 2014 then identified the following account holder:

DENY MITROVICH
4926 N KEDZIE AVE APT 3N
CHICAGO, IL 60625-5019

A check of CLEAR also identified Deny Mitrovich, DOB: 5/27/1978 as residing at the above address.

A check of Sentinel and the Illinois Sex Offenders Registry was met with negative results.

Due to the above, it is believed the true identity of "cyberguy" is Deny Mitrovich, 4926 N Kedzie Ave, Apt. 3N, Chicago, IL.

It is requested that an investigation be opened and assigned to SA Ingri Hartwig.

♦♦