FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1439355-000

Total Deleted Page(s) = 36
Page 3 ~ Duplicate;
Page 4 ~ Duplicate;
Page 7 ~ Duplicate;
Page 8 ~ Duplicate;
Page 9 ~ Duplicate;
Page 10 ~ Duplicate;
Page 11 ~ Duplicate;
Page 12 ~ Duplicate;
Page 13 ~ b3; b6; b7C; b7E; OTHER - Pursuant with United States Court Order;
Page 14 ~ Duplicate;
Page 15 ~ b3; b6; b7C; OTHER - Purusant with United States Court Order;
Page 16 ~ b3; OTHER - Pursuant with United States Court Order;
Page 17 ~ b3; OTHER - Pursuant with United States Court Order;
Page 18 ~ b3; OTHER - Pursuant with United States Court Order;
Page 19 ~ b3; b6; b7C; b7E; OTHER - Pursuant with United States Court Order;
Page 20 ~ Duplicate;
Page 21 ~ b3; b6; b7C; OTHER - Pursuant with United States Court Order;
Page 22 ~ b3; b6; b7C; OTHER - Purusant with United States Court Order;
Page 23 ~ b3; b6; b7C; OTHER - Pursuant with United States Court Order;
Page 24 ~ b3; b6; b7C; OTHER - Purusuant with United States Court Order;
Page 25 ~ b3; b6; b7C; OTHER - Pursuant with United States Court Order;
Page 26 ~ b3; OTHER - Pursuant with United States Court Order;
Page 27 ~ b3; OTHER - Purusant with United States Court Order;
Page 28 ~ Duplicate;
Page 29 ~ Duplicate;
Page 30 ~ Duplicate;
Page 31 ~ Duplicate;
Page 32 ~ Duplicate;
Page 33 ~ Duplicate;
Page 34 ~ Duplicate;
Page 35 ~ b3; b6; b7C; b7E; OTHER - Pursuant with United States Court Order;
Page 36 ~ b3; b6; b7C; OTHER - Purusant with United States Court Order;
Page 37 ~ b3; b6; b7C; OTHER - Pursuant with United States Court Order;
Page 38 ~ b3; b6; b7C; OTHER - Pursuant with United States Court Order;
Page 39 ~ b3; b6; b7C; OTHER - Pursuant with United States Court Order;
Page 41 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

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

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Contact with [redacted] **Date:** 03/26/2013

To: [redacted]

From: DENVER
DN-CR-7
Contact: [redacted]

b3
b6
b7C
b7E

Approved By: SSRA [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) [redacted]
BLACKSHADES;
COMPUTER INTRUSION
OO:NY

Synopsis: (U) Document contact with [redacted] regarding [redacted]

Full Investigation Initiated: 02/28/2013

Reference: [redacted]

b3
b6
b7C
b7E

Administrative Notes: (U) Retelcall between SA [redacted] New York, and SA [redacted] Cheyenne RA, on March 26, 2013.

Details:

On March 26, 2013, SA [redacted] contacted [redacted] The purpose of the contact was to obtain contact information for [redacted] It should be noted that [redacted] is a business which offers virtual office services, mail forwarding services and registered agent services in which they accept legal process for individuals/business.

UNCLASSIFIED

FD-302 (Rev. 5-8-10)

b3
b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION

Date of entry 04/03/2013

owner of was interviewed telephonically. After being advised of the identity of the interviewing agent and Computer Scientist provided the following information.

b6
b7C

leases computer servers from another provider. The servers are operating with either Xen server or OpenVZ, depending on the server. The physical servers have twelve 1TB hard drives in a raid 1+0 configuration, with approximately 6TB of actual data. The servers are then divided into virtual machines configured with 100GB hard drives and leased out to customers. has remote access to the server which hosts the virtual machines, but does not have access to the physical servers or to the customers leased virtual machines. There is no console access at the data center in Chicago, Illinois, where his servers are located. has never been to the data center in Chicago, Illinois.

Investigation on 04/03/2013 at New York, New York, United States (Phone)

File Date drafted 04/03/2013

by

b3
b6
b7C
b7E

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

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) To document approval for the use of a PRTT **Date:** 03/27/2013

From: NEW YORK
NY-CY02
Contact:

b3
b6
b7C
b7E

Approved By: SSA

Drafted By:

Case ID #: (U) BLACKSHADES; COMPUTER INTRUSION OO:NY

Synopsis: (U) To document approval for the use of a PRTT

Full Investigation Initiated: 02/28/2013

Details:

Blackshades malware allows an individual to infect and gain control of other computers without the owner's permission. The victim computer communicates directly with the Blackshades customer's computer, commonly through the use of a dynamic DNS service. A PRTT on the Blackshades operator's Internet connection will allow the FBI to determine current malware activity and identify victims.

The investigation into Blackshades malware has revealed that an individual located at was involved in the marketing and sale of Blackshades malware. The individual created and maintained several accounts with a managed DNS provider containing the domains bv1.zapto.org and bv1.no-ip.org.

b3
b6
b7C
b7E

UNCLASSIFIED

[redacted]

Title: (U) To document approval for the use of a PRTT
Re: [redacted] 03/27/2013

b3
b7E

♦♦

Title: (U)
Re: 03/26/2013

advised that provides mail forwarding services for All mail received on behalf of LP is forwarded to has been providing mail forwarding services for since September 2011. The package originally sent by New York Division via Federal Express to LP on March 23, 2013, was in the outgoing mail at for shipment to

b3
b6
b7C
b7E

It should be noted that in addition to providing mail forwarding services for on November 2, 2011. Neither or have a physical presence in the State of Wyoming.

b6
b7C
b7E

Denver considers the lead to obtain the contact information for covered.

♦♦