FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1450436-000

Total Deleted Page(s) = 38
Page 8 ~ b5; b6; b7C; b7D;
Page 16 ~ Duplicate;
Page 26 ~ b6; b7C; b7D;
Page 27 ~ b6; b7C; b7D;
Page 28 ~ b6; b7C; b7D;
Page 29 ~ b6; b7C; b7D;
Page 30 ~ b6; b7C; b7D;
Page 31 ~ b6; b7C; b7D;
Page 32 ~ b6; b7C; b7D;
Page 33 ~ b6; b7C; b7D;
Page 34 ~ b6; b7C; b7D;
Page 35 ~ b6; b7C; b7D;
Page 36 ~ b6; b7C; b7D;
Page 37 ~ b6; b7C; b7D;
Page 38 ~ b6; b7C; b7D;
Page 39 ~ b6; b7C; b7D;
Page 40 ~ b6; b7C; b7D;
Page 41 ~ b6; b7C; b7D;
Page 45 ~ b6; b7C; b7D;
Page 46 ~ b6; b7C; b7D;
Page 47 ~ b6; b7C; b7D;
Page 48 ~ b6; b7C; b7D;
Page 49 ~ b6; b7C; b7D;
Page 50 ~ b6; b7C; b7D;
Page 51 ~ b6; b7C; b7D;
Page 52 ~ b6; b7C; b7D;
Page 53 ~ b6; b7C; b7D;
Page 55 ~ b3; b6; b7C; b7D; b7E;
Page 56 ~ b3; b6; b7C; b7D; b7E;
Page 57 ~ b3; b6; b7C; b7D; b7E;
Page 58 ~ b3; b7E;
Page 59 ~ b3; b7E;
Page 64 ~ Duplicate;
Page 65 ~ Duplicate;
Page 66 ~ Duplicate;
Page 68 ~ b3; b6; b7C; b7D; b7E;
Page 69 ~ b3; b7D; b7E;
Page 73 ~ b3; b7D; b7E;

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

To: Phoenix From: Phenix
Re: [redacted] 08/05/2011 b3 b7E

computer industry along with removal and blocking techniques. Writer has also seen a decrease in the number of infections of [redacted] infected with Confiker Worm. b7D

Writer requests that the above captioned investigation be closed.

♦♦

(Rev. 06-04-2007)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/11/2009

To: Phoenix

From: Phoenix
C-2
Contact: SA

Approved By:

Drafted By:

Case ID #: (Pending)
(Pending)

b3
b6
b7C
b7E

Title:

Synopsis: To open investigation and assign to SA

b6
b7C

Details: CHS reported on about devices infected within Arizona by the Confiker Worm to included the following:

b7D
b7E

CHS

b6
b7C
b7D

Writer requests an investigation to be opened and assigned to effectively identify and disrupt known Confiker Worm infections within the Phoenix Division and provide additional support to

b3
b7E

♦♦

b3
b6
b7C
b7E

I: 1280.EC

From Case ID : [redacted]
To Case ID . : [redacted]

Documents . : 1
Last Serial : 4

b3
b7E

Old Serial	New Serial	FIF
1	5	

Total Documents Consolidated : 1

****** Statistical Information from Universal Index *****

Old Case ID	:	[redacted]
New Case ID	:	
Mains	:	1
References	:	1
Total records processed	:	2

b3
b7E

FD-340 (Rev. 4-11-03)

File Number [redacted] b3 b7E

Field Office Acquiring Evidence Phoenix

Serial # of Originating Document 3

Date Received 06/11/2007

From _____
(Name of Contributor/Interviewee)

_____
(Address)

_____
(City and State)

By SA [redacted] b6 b7C

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title: [redacted] b3 b7E

Reference: _____
(Communication Enclosing Material)

Description: ☒ Original notes re interview of [redacted] b6 b7C b7D

[redacted] and [redacted]

Precedence: ROUTINE Date: 06/18/2009

To: Phoenix

From: Phoenix
C-2
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)
[redacted] (Pending)

Title: [redacted]

b3
b6
b7C
b7E

Synopsis: To document statistical accomplishment of contacting a victim of Conficker.

Details: On [redacted] [redacted] was informed of IP Address [redacted] reporting to [redacted]

b6
b7C
b7D
b7E

Accomplishment Information:

Number: 1
Type: CIP VICTIM CONTACTED/INTERVIEWED
ITU: COMPUTER ASSISTANCE
Claimed By:
SSN:
Name: [redacted]
Squad: C2

b6
b7C

LEAD(s):

Set Lead 1: (Action)

PHOENIX

Case ID : [redacted]

b3
b7E

AT PHOENIX, ARIZONA

Read and clear.

**

FD-542 (Rev. 04-29-2008)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/18/2009

To: Phoenix

From: Phoenix
C-2
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)
(Pending) [redacted]

Title: [redacted]

Synopsis: To document statistical accomplishment of contacting a victim of Conficker.

Details: On [redacted] was informed of IP Address [redacted] reporting to [redacted]

b3
b6
b7C
b7E

b6
b7C
b7D
b7E

b3
b6
b7C
b7E

I: [redacted] 162 82 542 [redacted]

To: Phoenix From: Phoenix
Re: [redacted] 06/18/2009 b3 b7E

Accomplishment Information:

Number: 1
Type: CIP VICTIM CONTACTED/INTERVIEWED
ITU: COMPUTER ASSISTANCE
Claimed By:
SSN: [redacted]
Name: b6 b7C
Squad: C2

To: Phoenix From: Phoenix
Re: [redacted] 06/18/2009

b3
b7E

LEAD(s):

Set Lead 1: (Action)

PHOENIX

AT PHOENIX, ARIZONA

Read and clear.

♦♦

06/16/2009

On 06/11/2009, [redacted] telephone number [redacted] cellular telephone number [redacted] email address [redacted] was interviewed at [redacted] located at [redacted] Also attending the meeting was [redacted] After being advised of the identity of the interviewing agents and the purpose of the interview, [redacted] furnished the following information:

b6
b7C
b7D

The interview was set up after information was provided to [redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

Case ID : [redacted]

b3
b7E

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/16/2009

On 06/11/2009, [redacted] number [redacted] cellular telephone number [redacted] email address [redacted] was interviewed at [redacted] located at [redacted] Also attending the meeting was [redacted] After being advised of the identity of the interviewing agents and the purpose of the interview, [redacted] furnished the following information:

b6
b7C
b7D

The interview was set up after information was provided to [redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C

I [redacted] 169B1-302

Investigation on 06/11/2009 at Phoenix, Arizona

File # [redacted] Date dictated Not dictated

by SA [redacted]
SA

b3
b6
b7C
b7E

Precedence: ROUTINE Date: 06/24/2009

To: Phoenix

From: Phoenix
C-2
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: [redacted]

Synopsis: To combine [redacted] with [redacted]

Details: All files and serials in [redacted] Title: [redacted] should be placed in [redacted] The two cases are the same and two opening EC were submitted in error. [redacted] should be closed once files are moved.

**

b3
b6
b7C
b7E

b3
b7E

Case ID : [redacted]

b3
b7E

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/24/2009

To: Phoenix

From: Phoenix
C-2
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) [redacted]

Title: [redacted]

Synopsis: To combine [redacted] with [redacted]

Details: All files and serials in [redacted] Title: [redacted] should be placed in [redacted] The two cases are the same and two opening EC were submitted in error. [redacted] should be closed once files are moved.

♦♦

b3
b6
b7C
b7E

b3
b7E

UNCLASSIFIED

I:\ [redacted] 17581.EC [redacted]

b3
b6
b7C
b7E

Precedence: ROUTINE Date: 05/19/2009

To: Phoenix

From: Phoenix
C-2
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: [redacted]

Synopsis: To open an investigation and assign it to SA [redacted]

Details: Conficker has had several versions with Conficker D receiving the most world press with a activation date of 04/01/2009. Conficker E is the latest version of the Conficker worm and it is pulling binary information from Waledec nodes. UWaledec is self-propagating malware often associated with the Storm Worm. Waledec like Storm infects PCs to convert them into spam-sending bots that can be remotely controlled by a malicious user. Waledec has been associated with being sent via fake ecards to loading fake spyware protection programs.

Writer has a CHS that can and has provided information regarding computers in the Arizona area that are infected with the Conficker worm. Writer has talked to the case agent on [redacted] and concurs that data collected should be used to identify and notify users of infected systems as well as provide additional data to [redacted]

Writer requests and investigation be opened and assigned.

**

Case ID : [redacted]

b3
b6
b7C
b7E

(Rev. 06-04-2007)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/14/2009

To: Phoenix

Cyber

Cyber Criminal Section
CCU-3/Pat-3
SSA [redacted] b6 b7C

From: Phoenix
C-2
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted] b3 b6 b7C b7E

Case ID #: [redacted] (Pending) [redacted]
(Closed)

Title: [redacted]

Synopsis: To document opening new [redacted] investigation to Cyber Criminal Section.

Administrative: Lead set to correct administrative error in not including Cyber Criminal Section/CCU-3 in opening of investigation.

Details: CHS's reported on [redacted] about [redacted] devices infected within Arizona by the Confiker Worm to included the following: [redacted] b7D b7E

[redacted]

CHS [redacted]

[redacted] b6 b7C b7D b7E

I:\ [redacted] 1.1581.CC [redacted] b3 b6 b7C b7E

To: Phoenix From: Phoenix
Re: [redacted] 07/14/2009

b3
b7E

On 06/24/2009 All files and serials in [redacted] b3
b7E
[redacted] were placed in [redacted]
The two cases are the same and two opening EC were submitted in error.

To: Phoenix From: Phoenix
Re: [redacted] 07/14/2009

b3
b7E

LEAD(s):

Set Lead 1: (Action)

CYBER

AT WASHINGTON, DC
Read and clear.

♦♦

FD-542 (Rev. 03-23-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 09/30/2009

To: Phoenix

From: Phoenix
C-2
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)
[redacted] (Pending)

Title: [redacted]

b3
b6
b7C
b7E

Synopsis: To document statistical accomplishment regarding the above caption investigations.

Details: On 09/29/2009, [redacted] was contacted by [redacted] acknowledged receipt of the information and will forward it to [redacted]

b6
b7C
b7D
b7E

UNCLASSIFIED

I: [redacted] 77381.542 [redacted]

b3
b6
b7C
b7E

To: Phoenix From: Phoenix
Re: [redacted] 09/30/2009 b3 b7E

Accomplishment Information:

Number: 1
Type: CIP VICTIM CONTACTED/INTERVIEWED
ITU: AGENT INTERVIEW
Claimed By:
SSN: [redacted] b6
Name: [redacted] b7C
Squad: C2

To: Phoenix From: Phoenix
Re: [redacted] 09/30/2009

b3
b7E

LEAD(s):

Set Lead 1: (Action)

PHOENIX

AT PHOENIX, ARIZONA

Read and clear.

♦♦

FD-542 (Rev. 03-23-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 09/30/2009

To: Phoenix

From: Phoenix
C-2
Contact: SA

Approved By:

Drafted By:

Case ID #: (Pending)
(Pending)

Title:

b3
b6
b7C
b7E

Synopsis: To document statistical accomplishment regarding the above caption investigations.

Details: On 09/29/2009, telephone number email address was contacted by telephone and email. was provided with

b6
b7C
b7D

UNCLASSIFIED

b3
b6
b7C
b7E

27380.542

To: Phoenix From: Phoenix
Re: [redacted] 09/30/2009 b3 b7E

Accomplishment Information:

Number: 1
Type: CIP VICTIM CONTACTED/INTERVIEWED
ITU: AGENT INTERVIEW
Claimed By:
SSN: [redacted] b6 b7C
Name:
Squad: C2

To: Phoenix From: Phoenix
Re: [redacted] 09/30/2009

b3
b7E

LEAD(s):

Set Lead 1: (Action)

PHOENIX

AT PHOENIX, ARIZONA

Read and clear.

♦♦

b6
b7C

(Rev. 05-01-2008)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 10/23/2009

To: Phoenix

From: Phoenix
C-2
Contact: SA

Approved By:

Drafted By:

Case ID #: (U) (Pending
(U) (Pending)

b3
b6
b7C
b7E

Title: (U)

Synopsis: (U) To qualify portions of CHS report provided that should be classified.

b7D

~~Derived From : FBI NSISCG-20080301~~
~~Declassify On: 20341005~~

(U)

Details: ~~(S)~~ On CHS

b7D

(U) ~~(S/NF)~~ Based on the sensitivity of the follow information it should not be released

b6
b7C
b7D
b7E

(U) ~~(S)~~

b6
b7C
b7D
b7E

~~SECRET//NOFORN~~

b3
b6
b7C
b7E

29780.ec

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 10/27/2009

To: Cyber **Attn:** TFU-1
SSA [redacted] b6 b7C

From: Phoenix
C-2
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted] b3 b6 b7C b7D b7E

Case ID #: [redacted] (Pending) [redacted]
(Pending)

Title: [redacted]

Synopsis: Request [redacted] b7E

Details: Writer, who is assigned to the Cyber Squad in Phoenix, is working with a CHS who is [redacted] b7D

[redacted] [Note: Conficker Worm was first tracked in November 2008 and has infected thousands of business networks and millions of PCs. Conficker has the capability to launch attacks that can download code that has the possibility to be devastating to the Internet.] [Note: Botnet refers to a type of bot running on a computer installed with a trojan and connecting to IRC networks for command and control. Botnets have the capability to steal computer users credentials and well as wage Distributed Denial of Service (DDoS) attacks on other systems.]

CHS prefers to communicate via email. CHS is [redacted] b7D b7E

I: [redacted] 30080.ec [redacted] b3 b6 b7C b7E

To: Cyber From: Phoenix
Re: [redacted] 10/27/2009

b3
b7E

[redacted]

b7E

[redacted]

b7D
b7E

[redacted]

b7E

In summary, Phoenix requests [redacted]

[redacted]

b6
b7C
b7E

To: Cyber From: Phoenix
Re: [redacted] 10/27/2009 b3 b7E

LEAD(s):

Set Lead 1: (Action)

CYBER

AT WASHINGTON, D.C.

Provide concurrence for [redacted] b7E

[redacted]

♦♦

Hi [redacted]
I got this document and this was already in my file but was not linked to [redacted]

I inadvertently scanned it, now I see it's already in there. Sorry, can't change out. Not sure what to do with it. [redacted]

b3
b6
b7C
b7E

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/17/2010

To: Finance **Attn:** [redacted] b6 b7C
Asset Management Unit

Phoenix **Attn:** [redacted]

From: Phoenix
Contact: SA [redacted]

Approved By: [redacted] b3 b6 b7C b7E

Drafted By: [redacted]

Case ID #: [redacted] (Pending)
[redacted] (Pending)
(Pending)

Title: Property Matters
Phoenix Division

Synopsis: To request [redacted] b7E

[redacted] b3 b6 b7C b7E

♦♦

[redacted] b3 b7E

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 03/16/2010

To: Cyber Attn: TFU-II
SSA [redacted] b6 b7C

From: Phoenix
C-2
Contact: SA [redacted]

Approved By: [redacted] b3 b6 b7C b7D b7E

Drafted By: [redacted]

Case ID #: [redacted] (Pending) [redacted] (Pending)

Title: [redacted]

Synopsis: Request [redacted] b7E

Details: Writer, who is assigned to the Cyber Squad in Phoenix, is working with a CHS who is [redacted] b7D

[Note: Conficker Worm was first tracked in November 2008 and has infected thousands of business networks and millions of PCs. Conficker has the capability to launch attacks that can download code that has the possibility to be devastating to the Internet.] [Note: Botnet refers to a type of bot running on a computer installed with a trojan and connecting to IRC networks for command and control. Botnets have the capability to steal computer users credentials and well as wage Distributed Denial of Service (DDoS) attacks on other systems.]

CHS prefers to communicate via email. CHS is [redacted] b7D b7E

[redacted] b3 b7E

To: Cyber From: Phoenix
Re: [redacted] 03/16/2010

b3
b7E

[redacted]

b7E

[redacted]

b7D
b7E

[redacted]

b7E

In summary, Phoenix requests [redacted]

[redacted]

b6
b7C
b7E

To: Cyber From: Phoenix
Re: [redacted] 03/16/2010

b3
b7E

LEAD(s):

Set Lead 1: (Action)

CYBER

AT WASHINGTON, D.C.

Provide concurrence for [redacted] b7E

[redacted]

♦♦

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/05/2011

To: Phoenix

From: Phenix
C-2
Contact: SA

Approved By:

Drafted By:

Case ID #: (Pending)

Title:

b3
b6
b7C
b7E

Synopsis: To request captioned case be closed.

Details: Writer opened investigation to identify and disrupt known Confiker Worm infections within the Phoenix Division and

b3
b7E

Writer utilized the resources of a CHS that reported on possible infections within Phoenix Divisions AOR.

CHS

b7D

Writer has made several notifications to

b7D

that have showing devices infected with the Confiker Worm. The Confiker Worm is well documented in the

UNCLASSIFIED

I: 21780.EC

b6
b7C

Precedence: ROUTINE Date: 06/11/2009

To: Phoenix

From: Phoenix
C-2
Contact: SA [redacted] b6 b7C b7E

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)
(Pending) b3 b7E

Title: [redacted]

Synopsis: To open investigation and assign to SA [redacted] b6 b7C

Details: CHS reported on [redacted] about [redacted] devices infected within Arizona by the Confiker Worm to included the following: [redacted] b7D b7E

[redacted]

CHS [redacted]

[redacted] b6 b7C b7D

Writer requests an investigation to be opened and assigned to effectively identify and disrupt known Confiker Worm infections within the Phoenix Division and provide additional support to [redacted] b3 b7E

**

Case ID : [redacted] b3 b7E