

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA)
document clearinghouse in the world. The research efforts here are
responsible for the declassification of hundreds of thousands of pages
released by the U.S. Government & Military.

Discover the Truth at: <http://www.theblackvault.com>



April 19, 2019

MR. JOHN GREENEWALD JR.
SUITE 1203
27305 WEST LIVE OAK ROAD
CASTAIC, CA 91384

FOIPA Request No.: 1431530-000
Subject: Cult of the Dead Cow

Dear Mr. Greenewald:

The enclosed 67 pages of records were determined to be responsive to your subject and were previously processed and released pursuant to the Freedom of Information Act (FOIA). Please see the selected paragraphs below for relevant information specific to your request as well as the enclosed FBI FOIPA Addendum for standard responses applicable to all requests.

- In an effort to provide you with responsive records as expeditiously as possible, we are releasing documents from previous requests regarding your subject. We consider your request fulfilled. Since we relied on previous results, additional records potentially responsive to your subject may exist. If this release of previously processed material does not satisfy your request, you may request an additional search for records. Submit your request by mail or fax to – Work Process Unit, 170 Marcel Drive, Winchester, VA 22602, fax number (540) 868-4997. Please cite the FOIPA Request Number in your correspondence.
- Please be advised that additional records responsive to your subject exist. If this release of previously processed material does not satisfy your request, you must advise us that you want the additional records processed. Please submit your response within thirty (30) days by mail or fax to—Work Processing Unit, 170 Marcel Drive, Winchester, VA 22602, fax number (540) 868-4997. Please cite the FOIPA Request Number in your correspondence. **If we do not receive your decision within thirty (30) days of the date of this notification, your request will be closed.**
- One or more of the enclosed records were transferred to the National Archives and Records Administration (NARA). Although we retained a version of the records previously processed pursuant to the FOIA, the original records are no longer in our possession.

If this release of the previously processed material does not satisfy your request, you may make a request to NARA at the following address:

National Archives and Records Administration
8601 Adelphi Road
College Park, MD 20740-6001

- Records potentially responsive to your request were transferred to the National Archives and Records Administration (NARA), and they were not previously processed pursuant to the FOIA. You may file a request with NARA using the address above.

- One or more of the enclosed records were destroyed. Although we retained a version of the records previously processed pursuant to the FOIA, the original records are no longer in our possession. Record retention and disposal is carried out under supervision of the National Archives and Records Administration (NARA) , Title 44, United States Code, Section 3301 as implemented by Title 36, Code of Federal Regulations, Part 1228; Title 44, United States Code, Section 3310 as implemented by Title 36, Code of Federal Regulations, Part 1229.10.
- Records potentially responsive to your request were destroyed. Since this material could not be reviewed, it is not known if it was responsive to your request. Record retention and disposal is carried out under supervision of the National Archives and Records Administration (NARA) according to Title 44 United States Code Section 3301, Title 36 Code of Federal Regulations (CFR) Chapter 12 Sub-chapter B Part 1228, and 36 CFR 1229.10.
- Documents or information referred to other Government agencies were not included in this release.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. The “**Standard Responses to Requests**” section of the Addendum applies to all requests. If the subject of your request is a person, the “**Standard Responses to Requests for Individuals**” section also applies. The “**General Information**” section includes useful information about FBI records. Also enclosed is our Explanation of Exemptions.

For questions regarding our determinations, visit the www.fbi.gov/foia website under “Contact Us.” The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's FOIA online portal by creating an account on the following web site: <https://www.foiaonline.gov/foiaonline/action/public/home>. Your appeal must be postmarked or electronically transmitted within ninety (90) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked “Freedom of Information Act Appeal.” Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS) at 877-684-6448, or by emailing ogis@nara.gov. Alternatively, you may contact the FBI's FOIA Public Liaison by emailing foipaquestions@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state “Dispute Resolution Services.” Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

Sincerely,



David M. Hardy
Section Chief,
Record/Information
Dissemination Section
Information Management Division

Enclosure(s)

FBI FOIPA Addendum

As referenced in our letter, the FBI FOIPA Addendum includes information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. If you submitted a request regarding yourself or another person, Part 2 includes additional standard responses that apply to requests for individuals. If you have questions regarding the standard responses in Parts 1 or 2, visit the www.fbi.gov/foia website under “Contact Us.” Previously mentioned appeal and dispute resolution services are also available. Part 3 includes general information about FBI records that you may find useful.

Part 1: Standard Responses to All Requests: See Below for all Requests

- (i) **5 U.S.C. § 552(c).** Congress excluded three categories of law enforcement and national security records from the requirements of the Freedom of Information Act (FOIA). See 5 U.S.C. § 552(c) (2006 & Supp. IV (2010)). FBI responses are limited to those records subject to the requirements of the FOIA. Additional information about the FBI and the FOIPA can be found on the fbi.gov website.
- (ii) **National Security/Intelligence Records.** The FBI can neither confirm nor deny the existence of national security and foreign intelligence records pursuant to FOIA exemptions (b)(1) and (b)(3) and PA exemption (j)(2) as applicable to requests for records about individuals [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2); 50 U.S.C § 3024(i)(1)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3); 50 USC § 3024(i)(1). This is a standard response and should not be read to indicate that national security or foreign intelligence records do or do not exist.

Part 2: Standard Responses to Requests for Individuals: See Below for all Requests for Individuals

- (i) **Requests for Records about any Individual—Watch Lists.** The FBI can neither confirm nor deny the existence of any individual’s name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.
- (ii) **Requests for Records for Incarcerated Individuals.** The FBI can neither confirm nor deny the existence of records which could reasonably be expected to endanger the life or physical safety of any incarcerated individual pursuant to FOIA exemptions (b)(7)(E) and (b)(7)(F) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (b)(7)(F), and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.

Part 3: General Information:

- (i) **Record Searches.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching those systems or locations where responsive records would reasonably be found. Most requests are satisfied by searching the Central Record System (CRS), an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled and maintained by the FBI in the course of fulfilling its dual law enforcement and intelligence mission as well as the performance of agency administrative and personnel functions. The CRS spans the entire FBI organization and encompasses the records of FBI Headquarters (“FBIHQ”), FBI Field Offices, and FBI Legal Attaché Offices (“Legats”) worldwide. A CRS search includes Electronic Surveillance (ELSUR) records.
- (ii) **FBI Records**
Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.
- (iii) **Requests for Criminal History Records or “Rap Sheets.”** The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks –often referred to as a criminal history record or “rap sheets.” These criminal history records are not the same as material in an investigative “FBI file.” An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at www.fbi.gov/about-us/cjis/identity-history-summary-checks. Additionally, requests can be submitted electronically at www.edo.cjis.gov. For additional information, please contact CJIS directly at (304) 625-5590.
- (iv) **The National Name Check Program (NNCP).** The mission of NNCP is to analyze and report information in response to name check requests received from federal agencies, for the purpose of protecting the United States from foreign and domestic threats to national security. Please be advised that this is a service provided to other federal agencies. Private citizens cannot request a name check.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE

Date: 07/10/1997

To: Tampa

Attn: SSA [redacted]

From: Salt Lake City

Boise RA

Contact: SA [redacted], (208) 344-7843

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 9A-SU-NEW (Pending)

Title: CULT OF THE DEAD COW; - 286 LS-62852 (E)
MICRON ELECTRONICS - VICTIM
EXTORTION

Synopsis: Document complaint received from [redacted] Micron Electronics, Boise, Idaho.

b6
b7C

Details: On 07/10/1997, [redacted] Micron Electronics, contacted the FBI, Boise, Idaho, regarding an extortion message left on a recorder at Micron Electronics. [redacted] advised a female with a middle eastern accent left a message stating, "This is fiber optics in the Cult of the Dead Cow. I want \$5,000.00 cash or I will crash your systems with (ah) a tremendous virus. Later." [redacted] advised an employee at Micron, [redacted] was searching the system to determine if the origination number could be found on the 1-800 line on which the Cult of the Dead Cow contacted Micron.

b6
b7C

[redacted] was contacted directly and advised FBI, Boise, that the call came in from 813-757-5951, Plant City, Florida. [redacted] further advised that the call was received at 11:09 p.m., on 07/09/1997, at the Micron Electronics, Inc., Nampa, Idaho. She advised that the call could be identified at extension 3636 at the 813-757-5951 number.

b6
b7C

SSRA [redacted] spoke with the [redacted] Micron Electronics and found there was no additional call providing instructions to Micron Electronics for the delivery of the \$5,000.00.

b6
b7C

In the event no additional call is made to Micron Electronics with instructions for delivery of the \$5,000.00, Tampa Division will be requested to contact the individual or individuals listed at the number and specific extension.

Handwritten: OAS 7/10/97

Handwritten: QA 80-47237-1

b6
b7C

To: Tampa From: Salt Lake City
Re: 9A-SU-NEW, 07/10/1997

LEAD (s):

Set Lead 1:

TAMPA

AT PLANT CITY, FL

Determine subscriber information for Plant City, Florida, number 813-757-5951, extension 3636, and thereafter hold additional information in abeyance pending notification by Salt Lake City Division.

Results of the investigation may be forwarded directly to the Boise RA, attention: SA [redacted] For any additional information contact SA [redacted] at the Boise RA directly, (208) 344-7843.

b6
b7c


♦♦

File - Serial Charge Out
FD-5 (Rev. 10-13-89)

File 9 SU 47237 Date _____
Class. Office of Origin Case No. Last Serial

Pending Closed

Serial No.	Description of Serial	Date Charged
<u>2</u>	<u>INSERT RS 12298</u>	<u>8-27-97</u>

 _____
Employee _____

b6
b7c

RECHARGE Date _____

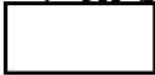
To _____ From _____



Initials of Clerk { _____

_____ } Date { _____

_____ }

9A-SU-47237



The following investigation was conducted by I.A. 
 on 7/14/97:

b6
b7C

Contact with the General Telephone Company revealed that telephone number 813-757-5951 is listed to Texaco #114 3700 Paul Buckman Road (SR39) Plant City, Florida. This is a business line.

9A-SU-47237-2

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 07/16/1997

To: Salt Lake City

Attn: Boise RA
SA [redacted]

[redacted] 208-344-7843

b6
b7c

From: Tampa

Squad 4

Contact: I.A. [redacted]

Approved By [redacted]

Drafted By: [redacted]

Case ID #: 9A-SU-47237-3 (Pending)

Title: CULT OF THE DEAD COW;
MICRON ELECTRONICS - VICTIM
EXTORTION

Synopsis: Subscriber information requested.

Reference: 9A-SU-47237 Serial 1

Enclosures: Original and one copy of investigative insert of
I.A. [redacted]

b6
b7c

Details: Subscriber information requested is attached.
Investigation being held in abeyance.

♦♦

9A-SU-47237-3

SEARCHED	INDEXED
SERIALIZED	FILED
JUL 18 1997	
FBI - SALT LAKE CITY	

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 10/03/1997

To: ✓ Salt Lake City

Attn: BOISE RA

SA

208-344-7843

From: Tampa

Squad 4

Contact: I.A.

Approved By

Drafted By:

Case ID #: 9A-SU-⁴7237 - 4

Title: CULT OF THE DEAD COW;
MICRON ELECTRONICS - VICTIM
EXTORTION

Synopsis: Information regarding telephone number 813-757-5951

Details: Contact with the Security Department of General Telephone revealed that telephone number 813-757-5951 is a pay station subscribed to by Texaco #114, 3700 Paul Buckman Road (SR39) Plant City, Florida.

♦♦

b6
b7C

9A-SU-47237-4

SEARCHED	INDEXED
SERIALIZED	FILED
OCT 23 1997	
FBI - SALT LAKE CITY	

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 10/20/1997

To: Tampa

Attn: SSA [redacted]

From: Salt Lake City
Boise RA

Contact: SA [redacted] (208) 344-7843

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 9A-SU-47237 (Pending)

Title: CULT OF THE DEAD COW;
MICRON ELECTRONICS - VICTIM;
EXTORTION

Synopsis: Document telcall to Tampa Division, SSA [redacted]
[redacted] from Salt Lake City Division, Boise Resident Agency,
SA [redacted] on 09/30/97.

b6
b7C

Details: The purpose of this communication is to document information provided to Tampa Division from Salt Lake City Division, Boise Resident Agency regarding the Cult of the Dead Cow. Micron Electronics has not received any additional extortion threats over the phone from Florida.

Salt Lake City Division received subscriber information for telephone number (813) 757-5951. The communication listed the subscriber at Texaco #114, 3700 Paul Buckman Road (SR 39), Plant City, Florida. This number was listed as a business line.

J
9A-SU-47237-5
Searched _____
Serialized _____
Indexed _____
Filed _____

Doc [redacted] 293 dec 12. ec ✓

b6
b7C

To: Tampa From: Salt Lake City
Re: 9A-SU-47237, 10/20/1997

LEAD (s):

Set Lead 1:

TAMPA

AT PLANT CITY, FL

Contact subscriber for telephone number (813) 757-5951 at address Texaco #114, 3700 Paul Buckman Road (SR 39), Plant City, Florida. Attempt to determine identity of caller who made the extortion threat to Micron Electronics in Boise, Idaho. In the event the individual caller is unable to be identified, advise the office manager or person in charge of the nature of the call and reveal that Micron Electronics has a tape recording of the extortion threat. Further emphasize that should additional calls be generated from that subscriber, the U.S. Attorney will be contacted to proceed with prosecution in this matter.

Results of the above lead may be forwarded directly to Salt Lake City Division, Boise Resident Agency, attention

[REDACTED]

b6
b7c

◆◆

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/03/1997

To: Salt Lake City

Attn: SAC

From: [redacted]

Boise RA

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 9A-SU-47237 (Closed)

Title: CULT OF THE DEAD COW;
MICRON ELECTRONICS - VICTIM
EXTORTION

b6
b7c

Synopsis: Document contact with Micron Electronics [redacted] and, close of investigation.

Details: On 11/06/1997, Micron Electronics [redacted] was contacted at telephone number (208) 898-3021, Nampa, Idaho, regarding the outcome of the lead sent to FBI, Tampa. [redacted] was advised Tampa Division conducted a subscriber search on the number provided to the FBI by Micron Electronics, (813) 757-5951, and determined the telephone number was for a pay telephone at Texaco Station Number 114, located at 3700 Paul Buckman Road, Plant City, Florida. [redacted] advised no additional extortion calls had been made to Micron Electronics. [redacted] was advised that should additional extortion calls be received by Micron Electronics he could contact the Boise FBI Office.

b6
b7c

In view of the fact the Tampa Division lead was covered, Micron Electronics has received no additional extortion calls, and there is no additional investigative activity required, this matter will be considered closed.

♦♦

*1/12/98
C-H
yca*

9A-SU-47237-6

SEARCHED	SERIALIZED
INDEXED	FILED
DEC 13 1997	
FBI - SALT LAKE CITY	

b6
b7c

DOI: [redacted] 33702015.ec

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1431530-0

Total Deleted Page(s) = 5

Page 3 ~ b7D;

Page 4 ~ b7D;

Page 5 ~ b7D;

Page 6 ~ b7D;

Page 7 ~ b7D;

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

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1259995-0

Total Deleted Page(s) = 5

- Page 3 ~ b7D;
- Page 4 ~ b7D;
- Page 5 ~ b7D;
- Page 6 ~ b7D;
- Page 7 ~ b7D;

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

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 10/25/1999

To: Criminal Investigative
National Security

Attn: IRU-1, SSA [redacted]
Attn: [redacted]

From: Moscow

Contact: ALAT [redacted]

011-7-095-956-4408/10 fax

b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 163H-MC-467 (Pending)

Title: CULT OF THE DEAD COW
FPC-WCC

*Reviewed
on 3/18/00
[signature]*

Synopsis: Request information on subject.

Details: [redacted]

[Large redacted area]

b7D

[Handwritten notes and signature]

b6
b7C

*8/15/00
Left in SSJ on
AC
Voice mail requests on [redacted]*

*Set 60 day
toller for
[redacted] TICKLER ASSIGNED
[redacted]*

163H-MC-467-2

[redacted] 961EC-298 ✓

file

b6
b7C

To: Criminal Investigative From: Moscow
Re: 163H-MC-467, 10/25/1999

LEAD (s):

Set Lead 1: (Adm)

CRIMINAL INVESTIGATIVE

AT WASHINGTON, DC

Read and clear.

Set Lead 2:

NATIONAL SECURITY

AT NIPC

Provide information suitable for dissemination to
 about the Cult of the Dead Cow hacker group.

b7D

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/14/1998

To: NSD

Attn:

[Redacted]
UC [Redacted]

b7E
b6
b7C

From: Atlanta

[Redacted]
Contact: [Redacted]

(404) 679-6456

b7E

Approved By: Daulton Jack A

[Redacted]

b6
b7C

Drafted By:

[Redacted]

Case ID #: 288A-AT- (Pending)

Title: UNSUB(S), aka;
DETH VEGETABLE;
NET NINJA;
dba CULT OF THE DEAD COW (CDC);
MINDSPRING ENTERPRISES,
1430 PEACHTREE ST.,
ATLANTA, GA., 30309 - VICTIM;
INTRUSION - INFO SYSTEMS;
IDENTITY THEFT;
CONSPIRACY

Synopsis: To open an assign captioned matter.

Details: On 11/10/1998, the Atlanta division hosted a conference on Computer Fraud and Economic Espionage Investigations. In attendance were security representatives from Mindspring Enterprises, Inc. (Mindspring). Mindspring advised at that time that they were encountering a new Trojan horse program known as 'BACK ORIFICE' (BO). Mindspring advised that innocent subscribers to Mindspring were being inadvertently infected with the BO program, and that the UNSUB(s) who were exploiting the victim's computers were using the victim's electronic user identification (userid) and password to illegally access Mindspring and thereby the Internet using fictitious identification.

Back Orifice is a take-off of the Microsoft, Inc., name of Back Office. Back Office is a suite of software used to

Handwritten: OEA to SA [Redacted] 12/14/98 [Signature]

Handwritten: APO

Handwritten: 288A-AT-87389-1

b6
b7C

To: NSD From: Atlanta
Re: 288A-AT-, 12/14/1998

operate and control server class computers. Back Orifice was published for free download and use by a group known as the "Cult of the Dead Cow" (CDC) from their Internet web site at <<http://www.cultdeadcow.com>>. CDC claims to have previously gained access or "hacked" into US Government computers including Department of Defense computer systems. CDC claims to have been in existence since the mid 1980's. On 8/3/1998, CDC released the BO program for download from it's web site. CDC advises that BO is a "remote administration tool" for Windows 95/98/NT, however the information released with BO clearly indicates that BO is a "hacker" tool. Once installed, BO allows unauthorized users to execute privileged operations on the affected computer, whether over a local area network (lan) or over the Internet.

As early as three days after the release of BO, computer security groups such as CERT and Internet Security Systems, Inc., began issuing advisories on the dangers of the BO program. In November 1998, Mindspring advised that they were seeing approximately two BO intrusions every day. Information available through CERT <<http://www.cert.org>> indicates that tens of thousands of computers may be infected. Information has been developed that many of the affected computers send Internet messages to servers used by CDC to alert the UNSUB(s) that the infected computer is currently available for illegal access.

On 12/11/98, Mindspring advised that an Internet web site with an address of <<http://www.bobastard.com>> was publishing userids and passwords of BO infected customers of Mindspring. Mindspring security provided the information via e-mail to the Atlanta office.

The investigative strategy for this matter will be to collect information on the nature and scope of CDC, with an intent to prosecute for violations of T18 sec 1030 (Computer Intrusions), T18 sec 1028 (Identity Theft), and T18 sec 371 (Conspiracy). To this end, [redacted] Agents in Atlanta will undertake a Group II UCO, [redacted]

b7E

To: NSD From: Atlanta
Re: 288A-AT-, 12/14/1998

On 12/14/98, Agents from the [redacted] group met with AUSA [redacted], Northern District of Georgia, who was advised of the proposed investigation and strategy. AUSA stated that there did not appear to be an entrapment issue, and he concurred with the investigative strategy.

b7E
b6
b7C

In order to expeditiously address this matter, Atlanta needs to [redacted] prior to it's use in an investigation. Atlanta is requesting [redacted]

b7E

[Large redacted area]

◆◆

01/07/99 #11
13:01:50

FD-192

ICMIPR01
Page 1

Title and Character of Case:

VEGETABLE, DETH
NINJA, NET

Date Property Acquired: Source from which Property Acquired:

12/18/1998

b6
b7C

Anticipated Disposition: Acquired By:

Case Agent:

Description of Property:

Date Entered

1B 1

ONE OPTICAL DISK

Barcode: E1622226

Location: ECR

CAB1

01/07/1999

Evidence DESTROYED by SA [redacted]
On 4/13/00 SEE IA 3

b6
b7C

288A-AT-87389-SFIB1

Case Number: 288A-AT-87389-1B
Owning Office: ATLANTA

**FD-192
INVESTIGATIVE
FILE COPY**

**ORIGINAL FD-192
LOCATED IN SFIB
MAINTAINED IN ECU**

SEARCHED _____	INDEXED _____
SERIALIZED _____	FILED _____
JAN 11 1999	
FBI-ATLANTA	

[Signature]

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/29/98

✓ To: Atlanta

✓ Attn: Evidence Technician

From: Atlanta

Approved By: Daulton, Jack A. *JAD/WJD*

[Redacted]

Drafted By:

[Redacted]

Case ID #: 288A-AT-87389 (Pending) -4

Title: DETH VEGETABLE;
NET NINJA;
CITA MATTERS

b6
b7C

Synopsis: To report delayed entry of evidence into the Evidence Control Room.

Details: On 12/17/98 an image was made of the hard drive on a computer belonging to [Redacted]. This was done with his consent. The Optical disk containing the image was turned over to this writer on 12/18/98. It has been in my custody since that time. During that time I have been looking for a media (hard drive) large enough to restore the image.

b6
b7C

♦♦

RE: 1B1

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/14/1998

To: NSD

Attn:

[Redacted] UC [Redacted]

b7E
b6
b7C

From: Atlanta

[Redacted]
Contact: [Redacted]

(404) 679-6456

b7E

Approved By: Daulton Jack A

[Redacted]

b6
b7C

Drafted By:

[Redacted]

Case ID #: 288A-AT-87389 (Pending)

Title: UNSUB(S), aka;
DETH VEGETABLE;
NET NINJA;
dba CULT OF THE DEAD COW (CDC);
MINDSPRING ENTERPRISES,
1430 PEACHTREE ST.,
ATLANTA, GA., 30309 - VICTIM;
INTRUSION - INFO SYSTEMS;
IDENTITY THEFT;
CONSPIRACY

Synopsis: To advise the [Redacted] of a new investigation.

b7E

Details: On 11/10/1998, the Atlanta division hosted a conference on Computer Fraud and Economic Espionage Investigations. In attendance were security representatives from Mindspring Enterprises, Inc. (Mindspring). Mindspring advised at that time that they were encountering a new Trojan horse program known as 'BACK ORIFICE' (BO). Mindspring advised that innocent subscribers to Mindspring were being inadvertently infected with the BO program, and that the UNSUB(s) who were exploiting the victim's computers were using the victim's electronic user identification (userid) and password to illegally access Mindspring and thereby the Internet using fictitious identification.

Back Orifice is a take-off of the Microsoft, Inc., name of Back Office. Back Office is a suite of software used to operate and control server class computers. Back Orifice was published for free download and use by a group known as the 'Cult of the Dead Cow' (CDC) from their Internet web site at <http://www.cultdeadcow.com>. CDC claims to have previously

SEARCHED	INDEXED
SERIALIZED	FILED
DEC 21 1998	
FBI - ATLANTA	

b6
b7C

To: NSD From: Atlanta
Re: 288A-AT-87389
12/14/1998

gained access or hacked into US Government computers including Department of Defense computer systems. CDC claims to have been in existence since the mid 1980's. On 8/3/1998, CDC released the BO program for download from it's web site. CDC advises that BO is a remote administration tool for Windows 95/98/NT, however the information released with BO clearly indicates that BO is a hacker tool. Once installed, BO allows unauthorized users to execute privileged operations on the affected computer, whether over a local area network (lan) or over the Internet.

As early as three days after the release of BO, computer security groups such as CERT and Internet Security Systems, Inc., began issuing advisories on the dangers of the BO program. In November 1998, Mindspring advised that they were seeing approximately two BO intrusions every day. Information available through CERT <<http://www.cert.org>> indicates that tens of thousands of computers may be infected. Information has been developed that many of the affected computers send Internet messages to servers used by CDC to alert the UNSUB(s) that the infected computer is currently available for illegal access.

On 12/11/98, Mindspring advised that an Internet web site with an address of <<http://www.bobastard.com>> was publishing userids and passwords of BO infected customers of Mindspring. Mindspring security provided the information via e-mail to the Atlanta office.

The investigative strategy for this matter will be to collect information on the nature and scope of CDC, with an intent to prosecute for violations of T18 sec 1030 (Computer Intrusions), T18 sec 1028 (Identity Theft), and T18 sec 371 (Conspiracy). To this end, [redacted] Agents in Atlanta will undertake a Group II UCO. [redacted]

b7E

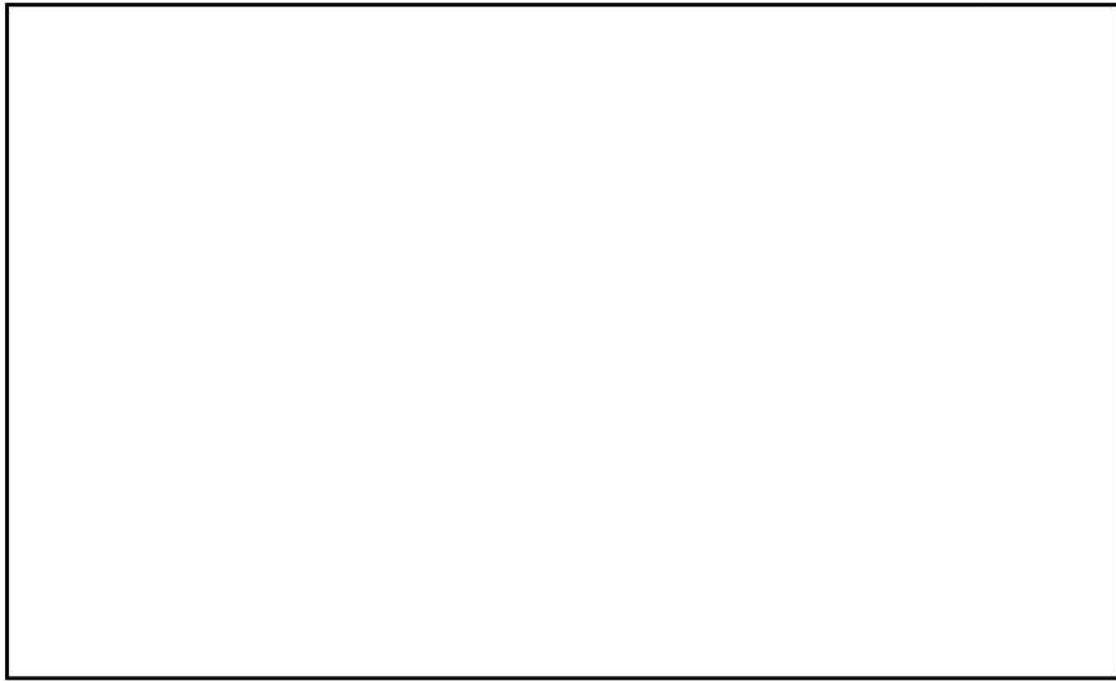
On 12/14/98, Agents from the [redacted] group met with AUSA [redacted], Northern District of Georgia, who was advised of the proposed investigation and strategy. AUSA [redacted] stated that there did not appear to be an entrapment issue, and he concurred with the investigative strategy.

b7E
b6
b7C

To: NSD From: Atlanta
Re: 288A-AT-87389
12/14/1998

In order to expeditiously address this matter, Atlanta
needs to [redacted]
[redacted] prior to it's use in an investigation. Atlanta is
requesting [redacted]
[redacted]

b7E



- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/21/98

SA [redacted] Computer Analysis Response Team (CART) field examiner, conducted an examination as outlined below. The examination was done following the procedures and using the tools provided by the FBI Laboratory.

b6
b7C

A generic minitower, no serial number, was made available for examination. This system belonged to [redacted] and was examined at his residence. The system contained a 3.5" diskette drive and a CD drive. The system also had an internal modem card installed.

b6
b7C

The following items were accomplished to this system:

Write Protect Hard Drive
Image Hard Drive

At the conclusion of the examination, the computer remained in the custody of [redacted]. CART notes and documentation were placed in Atlanta's Evidence Control Room.

b6
b7C

Investigation on 12/17/98 at Lawrenceville, Georgia

File # 288A-AT-87389

Date dictated 12/21/98

by SA [redacted]

b6
b7C

In Reply, Please Refer to

File No. 288-AT-87560 **H**

FBI CASE STATUS FORM

Date: 01/22/1999

To: Honorable Richard H. Deane, Jr., 75 Spring Street, Atlanta, GA. 30335

From: SAC Jack A. Daulton (Name and Address of USA) **b6**
Jack A. Daulton (Signature of Official in Charge) **b7C**
RE: UNSUB. - BELLSOUTH.NET-VICTIM:

RE: (Name of Subject) AUSA [] Age Sex
You are hereby advised of action authorized by (Name of USA or AUSA) **b6**
SA [] on 1/25/99 **b7C**
on information submitted by Special Agent (Name) (Date)

X
(Check One)

- Request further investigation
- Immediate declination
- Filing of complaint
- Presentation to Federal Grand Jury
- Filing of information
- Other

For violation of Title 18, USC. Section(s) 1030 (a) (5)

Synopsis of case: BellSouth.net has reported a denial of service attack affecting one of their clients, AmSouth Bank causing as yet a undetermined amount of money. The attacks came through UUNET and Cable Wireless and both ISP's are aware of the attack.

AUSA [] was advised and he stated, if proven, this would be a violation if Title 18, Section 1030, for which he would prosecute.

b6
b7C

2-US ATTORNEY'S OFFICE
② 288-AT-87560
1-SA []

288-AT-87560-4

In Reply, Please Refer to

File No. 288-AT-87560

FBI CASE STATUS FORM

Date: 01/22/1999

To: Honorable Richard H. Deane, Jr., 75 Spring Street, Atlanta, GA. 30335
(Name and Address of USA)

From: SAC Jack A. Daulton [Redacted] *for Jack A. Daulton*
(Name of Official in Charge and Field Division) (Signature of Official in Charge)

RE: UNSUB. - BELLSOUTH.NET-VICTIM:
(Name of Subject) Age Sex b6
b7C

You are hereby advised of action authorized by AUSA [Redacted]
(Name of USA or AUSA)
on information submitted by Special Agent SA [Redacted] on 1/25/99
(Name) (Date)

X
(Check One)

- Request further investigation
- Immediate declination
- Filing of complaint
- Presentation to Federal Grand Jury
- Filing of information
- Other

For violation of Title 18, USC, Section(s) 1030 (a) (5)

Synopsis of case: BellSouth.net has reported a denial of service attack affecting one of their clients, AmSouth Bank causing as yet a undetermined amount of money. The attacks came through UUNET and Cable Wireless and both ISP's are aware of the attack.

AUSA [Redacted] was advised and he stated, if proven, this would be a violation if Title 18, Section 1030, for which he would prosecute.

b6
b7C

SEARCHED _____	INDEXED _____
SERIALIZED _____	FILED _____
JAN 22 1999	
FBI - ATLANTA	

b6
b7C

2-US ATTORNEY'S OFFICE
② 288-AT-87560
1-SA [Redacted]

FEDERAL BUREAU OF INVESTIGATION

12/29/98

Date of transcription

[redacted] was contacted at his residence, [redacted] on 12/17/98. [redacted] is a white male, dob [redacted] ssan [redacted] and is employed at [redacted] phone [redacted] (W), [redacted] (H). [redacted] was advised of the identity of the interviewing Agent and the nature of the interview. Thereafter [redacted] provided the following.

b6
b7C

[redacted] is a subscriber to MindSpring Enterprises Inc. (MindSpring), Internet service provider (ISP). [redacted] who has only one computer, noticed on the last two bills from MindSpring that he was billed for simultaneous logons. This would indicate that more than one computer was using the same user id and password to access MindSpring at the same time. [redacted] also stated that his monthly usage went from about 150 hours to over 600 hours. [redacted] could not account for these changes in ISP usage. [redacted] notified MindSpring about the unusual bills. [redacted] was notified by MindSpring that his computer may have possibly been infected with a Trojan horse program known as Back Orifice. MindSpring also advised [redacted] that he should contact the interview Agent. [redacted] then contacted the interviewing Agent and a time was set for an interview.

b6
b7C

[redacted] was asked if the interviewing Agent and another Agent could make an image of [redacted] computer hard drive in order to determine if, in fact, [redacted] computer had been infected with the Back Orifice program. [redacted] executed a FD-26 Consent to Search form. A search of the files on [redacted] computer disclosed a file with the name windll.dll which is an indication of a Back Orifice program. An image copy of [redacted] computer hard drive was made and kept for evidentiary purposes. No physical items were removed from [redacted] custody. [redacted] was also advised to immediately implement MindSpring instructions to remove the Back Orifice program.

b6
b7C

At this point the interview was terminated.

Investigation on 12/17/98 at Lawrenceville, Ga.

File # 288A-AT-87389 *S*

Date dictated 12/29/98

by [redacted]

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 1/27/99

To: National Security

Attn:

[Redacted] SSA [Redacted]

b7E
b6
b7C

From: Atlanta

[Redacted] Contact: [Redacted]

(404) 679-6456

b7E

Approved By: Daulton Jack A

JAD

[Redacted]

b6
b7C

Drafted By:

[Redacted]

Case ID #: 288A-AT-87389-6 (Pending)

Title: UNSUB(S), aka;
dba Cult of the Dead Cow (CDC);
MINDSPRING ENTERPRISES,
1430 PEACTREE ST.,
ATLANTA, GA. 30309 - VICTIM
INTRUSION - INFO SYSTEMS
IDNETITY THEFT
CONSPIRACY

Synopsis: Request for equipment, as discussed in telcall between SSA [Redacted] and SA [Redacted] Atlanta on 12/22/98.

b6
b7C
b7E

Details: Captioned investigation was opened 12/14/1998, at Atlanta based on information from MINDSPRING that CDC had published for free a hacker program known as Back Orifice (BO). MINDSPRING alerted customers to the BO Trojan horse virus. MINDSPRING has documented over sixty (60) BO attacks since August 1998 when the BO program was released.

Agents from the Atlanta office succeeded in locating a MINDSPRING subscriber victim who agreed to a consent search of the victims computer and hard drive. Atlanta Agents located a file (windll.dll) on the victims computer that is indicative of a BO intrusion. Windll.dll is alledged to control keystroke logging for the hacker. Atlanta also obtained an image of the victim's 4.5GB hard disk. AUSA [Redacted] Northern District of Georgia, has advised that he will consider prosecution and that he concurs with the investigative strategy.

b6
b7C

288A-AT-87389-6

To: National Security From: Atlanta
Re: 288A-AT-87389, 1/27/99

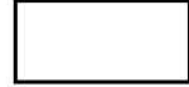
[Redacted]
[Redacted] Atlanta is requesting
[Redacted] Being sent by facsimile is [Redacted]
[Redacted]

b7E

◆◆

OLLIER IS LEAVING TO
ENTER NAVY. NO
follow-up.

288A-At-87389-7



b6
b7c

TELEPHONE CALL REPORT

b7E

DATE 1/29/99
TIME 4:00 am/pm

PERSON RECEIVING CALL: [redacted]

Based on your best judgement and experience hearing the spoken word fill out the caller profile: (circle as appropriate)

b6
b7C

<u>Sex</u>	<u>Age Band</u>	<u>Ethnic Origin</u>
<input checked="" type="radio"/> Male <input type="radio"/> Female	Child Teenage Young Adult Mature Adult Elderly	<input checked="" type="radio"/> White <input type="radio"/> Black <input type="radio"/> Hispanic <input type="radio"/> Oriental <input type="radio"/> Middle East <input type="radio"/> Indian/Pakistan <input type="radio"/> Undetermined

CALLER'S NAME (IF PROVIDED) [redacted]
TELEPHONE # [redacted]

ADDRESS: [redacted] b6
b7C

GENERAL TEXT OF CALL: Caller had someone access his Computer twice, trying to get info off his Computer.
Warthen, GA.

SPEECH WAS:

Clear Rational Slow Fast Soft Loud Nasal Lisp Stutter

Rambling Confused Intoxicated Disguised Distressed Laughing

Threatening Calm Excited Crying Angry

Univ of Md Microbiology

ACCENT: U.S. (regional) Foreign

Is this person a repeat Caller? Yes No If Yes When? _____

What has He/She called about? Computer Crime How Often? _____

Check as Appropriate:

- Caller requested to speak with Agent
- Caller wanted to report a crime
- Caller asked about FBI employment.
- Caller referred to other Federal Agency: _____
- Caller referred to local agency/Police: _____
- Caller requested an FBI call back at (time/date) _____

Copy of this report forwarded to [redacted] Supervisor or Invest.Asst. b7E

ANSWER TELEPHONE: "FBI, MAY I HELP YOU?"
BE COURTEOUS AND PROFESSIONAL AT ALL TIMES

SA [redacted]

I don't think we can do anything with this, but please call & talk to this guy. I'm concerned that U of Md Microbiology is involved and someone might be using this to bounce off into another system.

b6
b7C



b6
b7c

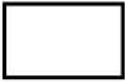
Please make contact and
see if we have an issue

288A-At-87389-8

SK



No Action



[Redacted] TELEPHONE CALL REPORT

b7E

DATE 1/31/99
TIME 4:40 am/pm

PERSON RECEIVING CALL: [Redacted]

b6
b7C

Based on your best judgement and experience hearing the spoken word fill out the caller profile: (circle as appropriate)

<u>Sex</u>	<u>Age Band</u>	<u>Ethnic Origin</u>
<u>Male</u> Female	Child Teenage Young Adult <u>Mature Adult</u> Elderly	<u>White</u> Black Hispanic Oriental Middle East Indian/Pakistan Undetermined

CALLER'S NAME (IF PROVIDED) [Redacted]
 TELEPHONE # [Redacted] ADDRESS: [Redacted]

b6
b7C

GENERAL TEXT OF CALL: *Caller stated that his personal computer has been hacked and it had his credit card and checking account info. Caller stated that a message was entered "Now you see what we can do." Caller stated that he would cancel all credit cards and checking account, but would like to press charges, if possible.*

SPEECH WAS:

Clear Rational Slow Fast Soft Loud Nasal Lisp Stutter
 Rambling Confused Intoxicated Disguised Distressed Laughing
 Threatening Calm Excited Crying Angry

ACCENT: U.S. (regional) Foreign

Is this person a repeat Caller? Yes No If Yes When? _____
How Often? _____

What was he/she called about? _____

Check as Appropriate:
 Caller requested to speak with Agent Caller wanted to report a crime
 Caller asked about FBI employment.
 Caller referred to other Federal Agency: _____
 Caller referred to local agency/Police: _____
 Caller requested an FBI call back at (time/date) _____

Copy of this report forwarded to [Redacted] Supervisor or Invest. Asst _____

b7E

Attn: [Redacted]
 ANSWER TELEPHONE: "FBI, MAY I HELP YOU?"
 BE COURTEOUS AND PROFESSIONAL AT ALL TIMES

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/28/1999

To: Atlanta

From: Atlanta

[Redacted]
Contact: [Redacted]

x6456

b7E

Approved By: [Redacted]

b6
b7C

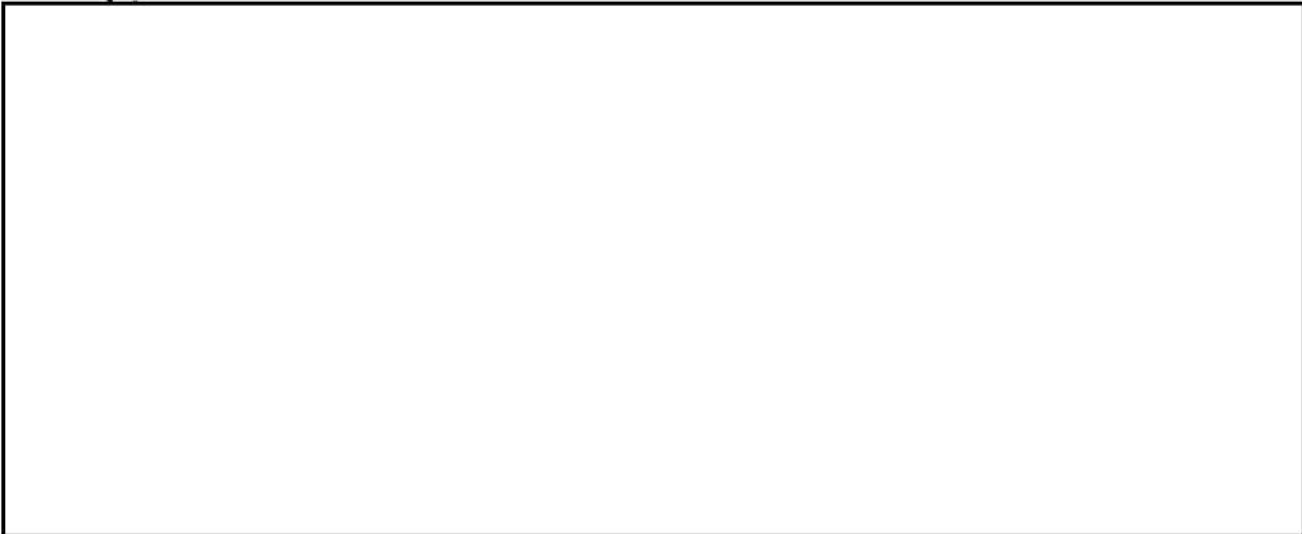
Drafted By: [Redacted]

Case ID #: 288A-AT-87389 (Pending)

Title: UNSUB(S), AKA;
DETH VEGETABLE;
NET NINJA;
DBA CULT OF THE DEAD COW (CDC);
MINDSPRING ENTERPRISES - VICTIM;
INTRUSION - INFO SYSTEMS
IDENTITY THEFT;
CONSPIRACY

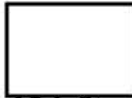
Synopsis: To close captioned matter.

Details: Due to the retirement of the case Agent it is recommended that this investigation be closed. In the event that a decision is made to continue with the investigation, the following course of action would seem logical.



b7E

Rotor
Resign
SA



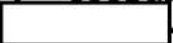
b6
b7C

288A-AT-87389-9
Rotor Rec'd 1-13-99

To: Atlanta From: Atlanta
Re: 288A-AT-87389, 05/28/1999



b7E

7. Coordinate all aspects with the US Attorney's office and .

Without available, trained Agent resources captioned matter should be closed.

♦♦

0005 MRI 01077/189

OO AFO FBIAT ALO

DE RUCNFB #0063 1892234

ZNY EEEEE

O 081834Z JUL 99

FM DIRECTOR FBI (288-HQ-1234199)

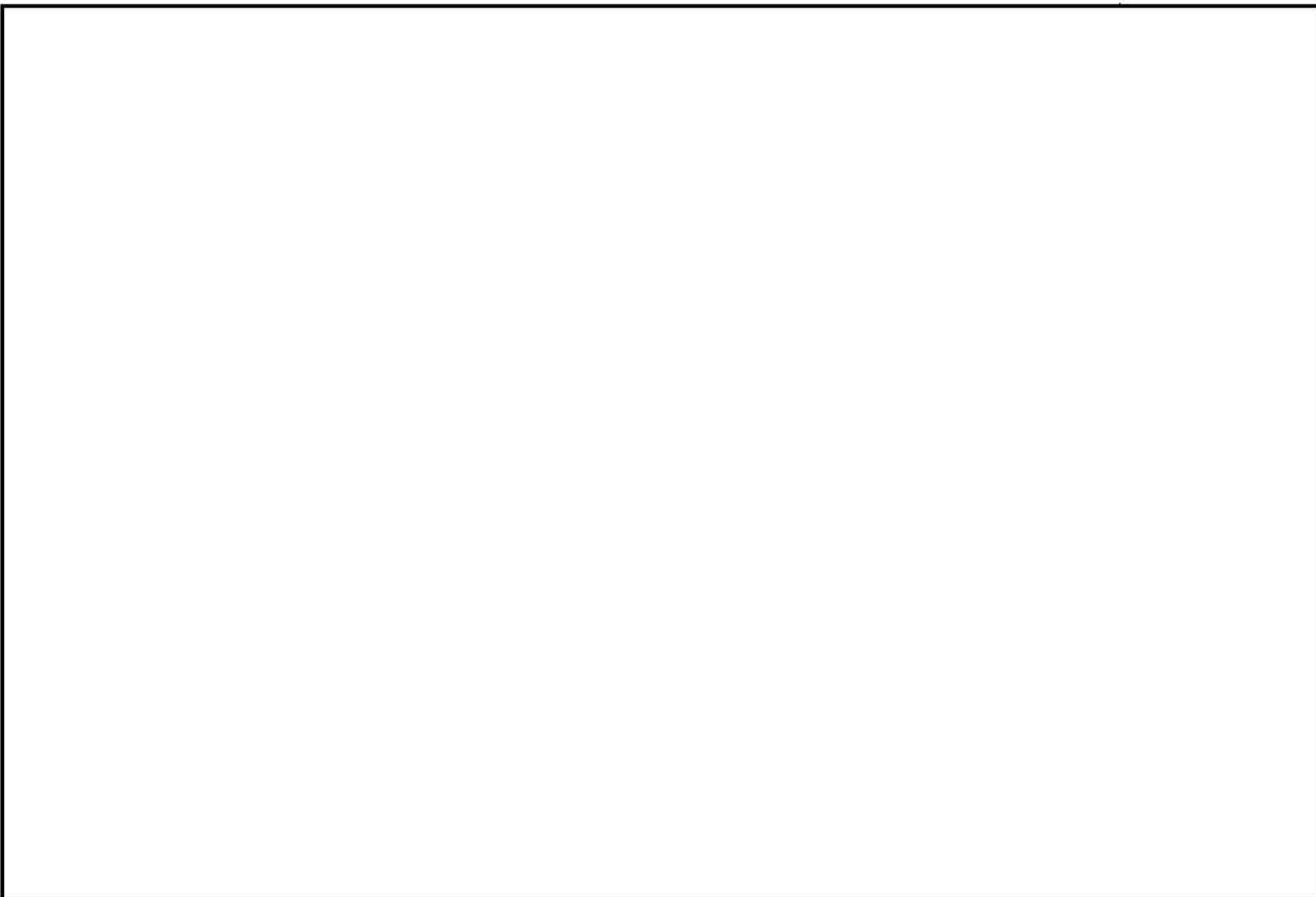
TO ALL FBI FIELD OFFICES/IMMEDIATE/

Route to

A/SSA



b6
b7C



INDEX
○

b7E



283A-AT-87389-10

SEARCHED	INDEXED
SERIALIZED	FILED
<input type="checkbox"/> AT - OMS	<input type="checkbox"/> SV FOIMS
<input type="checkbox"/> AT GENERAL	<input type="checkbox"/> SV GENERAL
<div data-bbox="1037 1825 1308 1962" data-label="Text"><p>JUL - 8 1999</p></div>	
<div data-bbox="1091 1989 1252 2021" data-label="Text"><p>FBI-ATLANTA</p></div>	

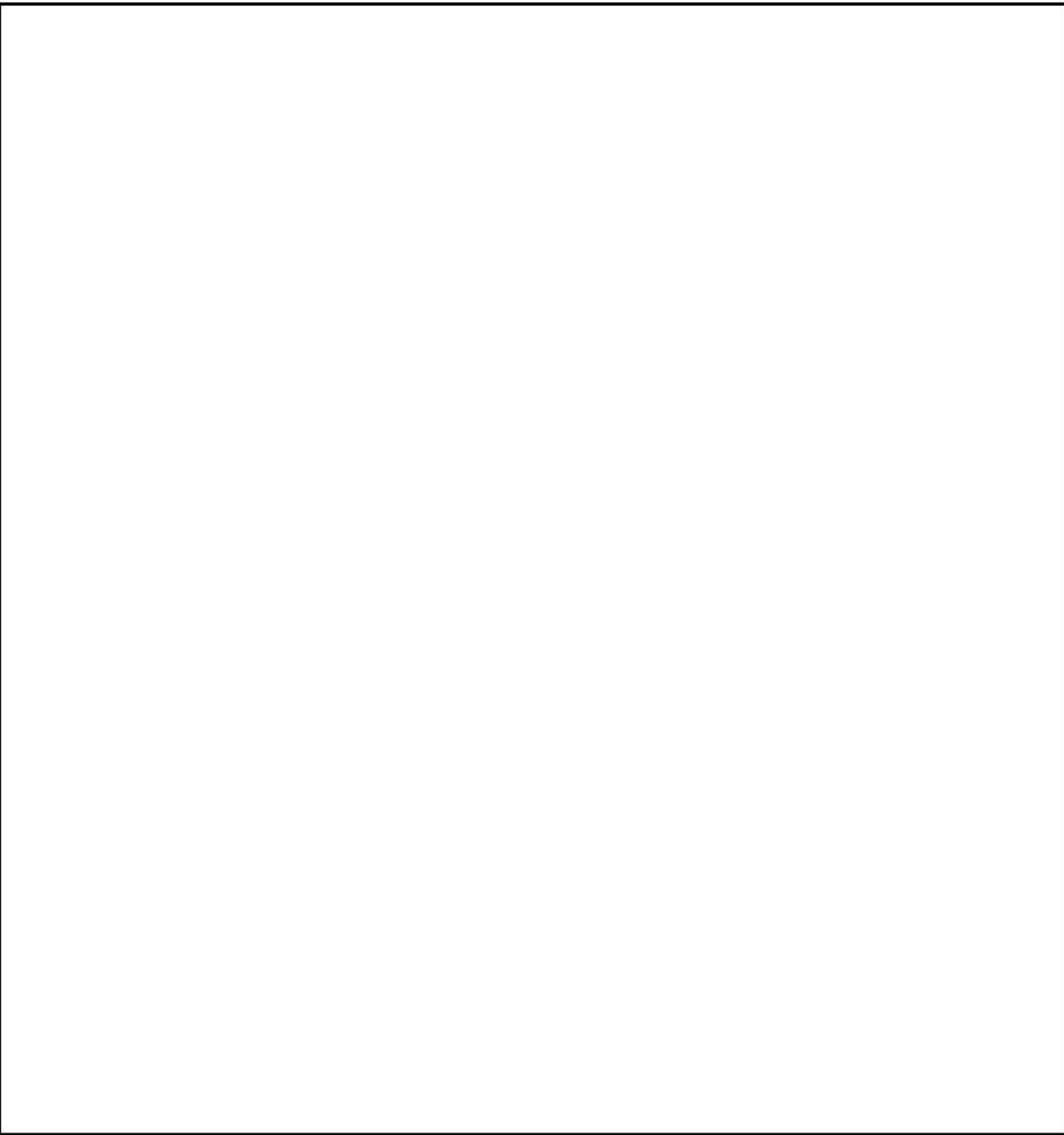
b6
b7C

No Action
7/8/99

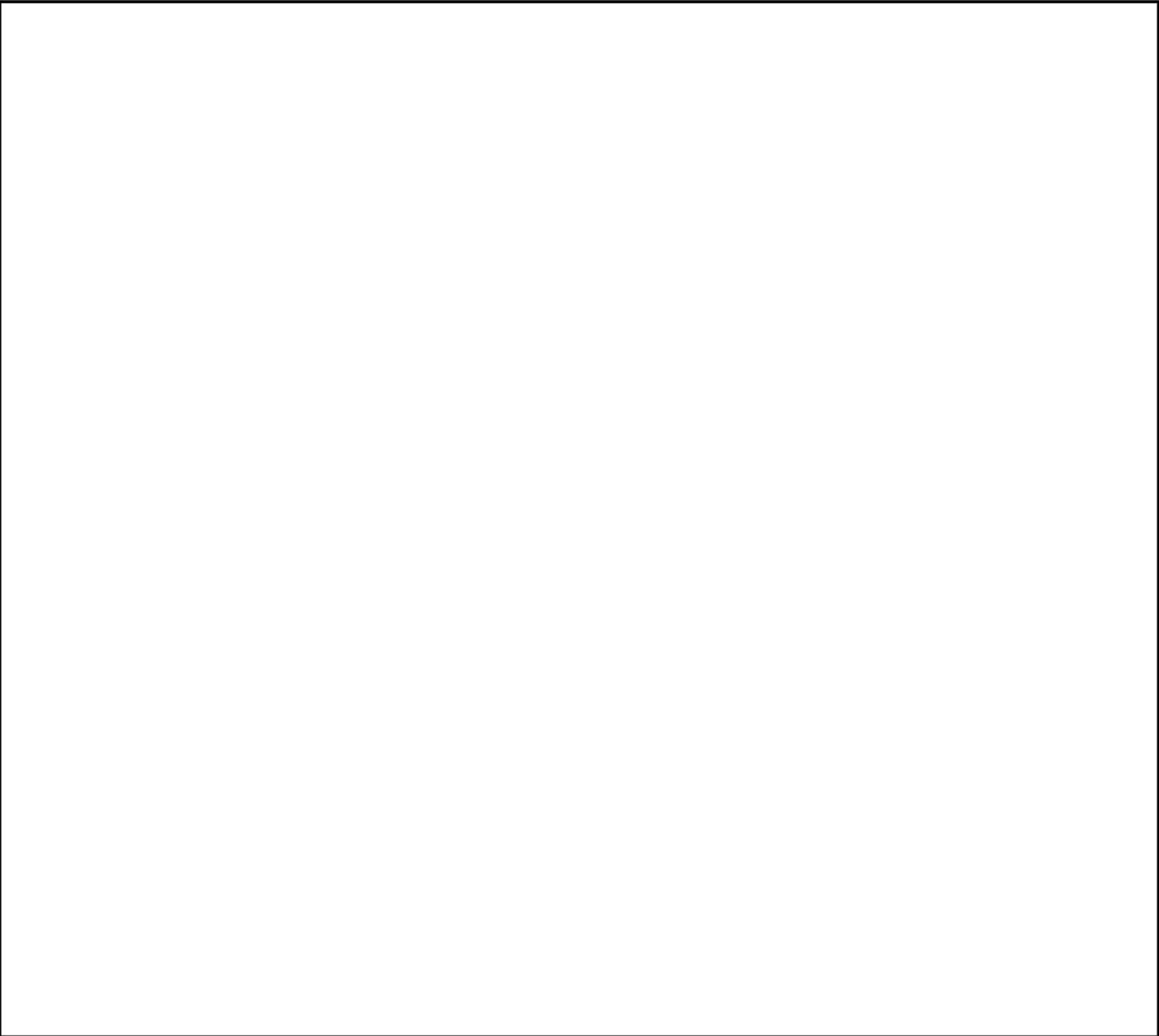


b7E





b7E



b7E



b7E

BT

UNCLAS E F T O FOR OFFICIAL USE ONLY

SECTION ONE OF THREE SECTIONS

CITE: //1301//

PASS: NIC WARNING STAFF TO NATIONAL WARNING COMMUNITY; JTF-CND
APPROPRIATE DOD FACILITIES, SERVICE COMPONENTS AND TARGET

LOCATIONS; [REDACTED]

SUBJECT: [REDACTED]

b7E

GROUP IN EXISTENCE SINCE 1984) RELEASED A PRODUCT CALLED QUOTE
BACK ORIFICE UNQUOTE AT LAST YEAR'S DEFCON VI HACKER CONVENTION.
CDC HAS ANNOUNCED PLANS TO RELEASE A NEW VERSION OF BACK ORIFICE
(BACK ORIFICE 2000) ON JULY 10TH AT THE DEFCON VII CONVENTION
LAS VEGAS. THE PRODUCT WILL BE MADE AVAILABLE AS A FREE DOWNLOAD
ON THAT DATE.

2. (U) THE ORIGINAL 1998 RELEASE OF BACK ORIFICE INCLUDED THE
FOLLOWING CAPABILITIES:

A. RETRIEVAL OF SYSTEM INFORMATION INCLUDING CURRENT USER, CPU
TYPE, WINDOWS VERSION, MEMORY USAGE, MOUNTED DISKS AND DRIVE
INFORMATION, SCREENSAVER PASSWORD, AND PASSWORDS CACHED BY USERS
(DIAL-UPS, WEB AND NETWORK ACCESS, ETC).

B. FILE SYSTEM CONTROL: COPY, RENAME, DELETE, VIEW, SEARCH,

SEARCHED	INDEXED
SERIALIZED	FILED
<input type="checkbox"/> AT OMS	<input type="checkbox"/> SV FOIMS
<input type="checkbox"/> AT GENERAL	<input type="checkbox"/> SV GENERAL
JUL - 8 1999	
FBI-ATLANTA	

PAGE SIX DE RUCNFB 0063 UNCLAS E F T O

COMPRESS, AND DECOMPRESS FILES.

C. PROCESS CONTROL: LIST, SPAWN, KILL.

D. REGISTRY CONTROL: LIST, CREATE, DELETE, SET KEYS AND VALUES.

E. NETWORK CONTROL.

F. MULTIMEDIA CONTROL (INCLUDING SCREEN CAPTURE).

G. PACKET REDIRECTION AND SNIFFING.

H. APPLICATION REDIRECTION (SPAWN MOST APPLICATIONS ON A SPECIFIC PORT, SUCH AS TELNET).

I. HTTP SERVER (UPLOAD AND DOWNLOAD FILES).

J. RUNS ON START-UP WITH NO ENTRY IN THE TASK LIST.

3. (U) BACK ORIFICE 2000 WILL REPORTEDLY INCLUDE SEVERAL FEATURES NOT FOUND IN THE ORIGINAL VERSION, INCLUDING WINDOWS NT COMPATIBILITY (THE ORIGINAL PROGRAM ONLY WORKED ON WINDOWS 95/98), OPEN PLUG-IN ARCHITECTURE FOR 3RD PARTY ADD-ONS, STRONG CRYPTOGRAPHY, AND OPEN SOURCE CODE AVAILABLE UNDER GNU PUBLIC LICENSE.

4. (U) ASSESSMENT.

A. (FOUO) BACK ORIFICE 2000 WINDOWS NT COMPATIBILITY COULD

BT

#0063

NNNN

0006 MRI 01078/189

OO AFO FBIAT ALO

DE RUCNEB #0064 1892235

ZNY EEEEE

O 081834Z JUL 99

FM DIRECTOR FBI (288-HQ-1234199)

TO ALL FBI FIELD OFFICES/IMMEDIATE/

b7E



b7E

b7E



b7E

BT

UNCLAS E F T O FOR OFFICIAL USE ONLY

SECTION TWO OF THREE SECTIONS

CITE: //1301//

PASS: NIC WARNING STAFF TO NATIONAL WARNING COMMUNITY; JTF-CND

APPROPRIATE DOD FACILITIES, SERVICE COMPONENTS AND TARGET

LOCATIONS; [REDACTED]

SUBJECT: [REDACTED]

b7E

TEXT CONTINUES:

GREATLY INCREASE THE POTENTIAL FOR DAMAGE TO NETWORK INFRASTRUCTURE. THE PREVIOUS VERSION ONLY AFFECTED WINDOWS 95/98 MACHINES, GENERALLY USED AS NETWORK CLIENTS. HOWEVER, INFECTION OF NETWORK SERVERS (COMMONLY RUNNING WINDOWS NT) COULD DRAMATICALLY INCREASE THE POTENTIAL IMPACT OF AN INFECTION IN TERMS OF BOTH DATA LOSS AND CONNECTIVITY DISRUPTION.

B. (FOUO) THE EXPECTED COMBINATION OF OPEN SOURCE CODE AND PLUG-IN ARCHITECTURE WOULD MAKE BACK ORIFICE 2000 POTENTIALLY MORE DESTRUCTIVE AND DIFFICULT TO ERADICATE THAN ITS PREDECESSOR. THE ORIGINAL BACK ORIFICE WAS FOLLOWED BY A SMALL NUMBER OF THIRD-PARTY ADD-ONS; IT APPEARS THAT CDC IS MAKING AN EFFORT TO ENCOURAGE THIRD-PARTIES TO ENHANCE BACK ORIFICE 2000, IN LINE.

PAGE SIX DE RUCNFB 0064 UNCLAS E F T O

WITH THE GENERAL PHILOSOPHY OF OPEN-SOURCE PROGRAMMING ADVOCATES. EXPECT SIGNIFICANT VARIANTS TO APPEAR AFTER THE INITIAL RELEASE WHICH COULD INCLUDE VARIOUS PROPAGATION FEATURES, REMOTE INFORMATION TRANSMISSION, OR CORRUPTION AND DESTRUCTION OF DATA. THESE VARIANTS MAY REQUIRE ANTI-VIRUS SOFTWARE AND NETWORK PROTECTION UPDATES. EXPECTED BACK ORIFICE 2000 FEATURES COULD EASILY INCORPORATE CUSTOMIZED MALICIOUS CODE WITH THE BASIC PRODUCT.

5. ~~(FOUO)~~ RECOMMENDATIONS. BACK ORIFICE 2000 WILL LIKELY BE USED IN A SELECTIVE OR TARGETED MANNER SIMILAR TO PREVIOUS NETWORK SECURITY EXPLOITS. EXPECTED NT COMPATIBILITY WILL MAKE CORPORATE, GOVERNMENT, AND MILITARY SYSTEMS INCREASINGLY ATTRACTIVE TARGETS. THESE COMMONLY TARGETED GROUPS SHOULD AGGRESSIVELY REVIEW AND MONITOR COMPREHENSIVE SECURITY MEASURES TO PROTECT AGAINST THE KIND OF EXPLOITS CAUSED OR SUPPORTED BY BACK ORIFICE 2000. ADDITIONALLY, SUBSEQUENT MODIFICATION OF BACK ORIFICE 2000 FOR EXPANDED MALICIOUS IMPACT IS POSSIBLE, AND SHOULD BE IMMEDIATELY REPORTED.

BT

#0064

NNNN

0007 MRI 01079/189

OO AFO FBIAT ALO

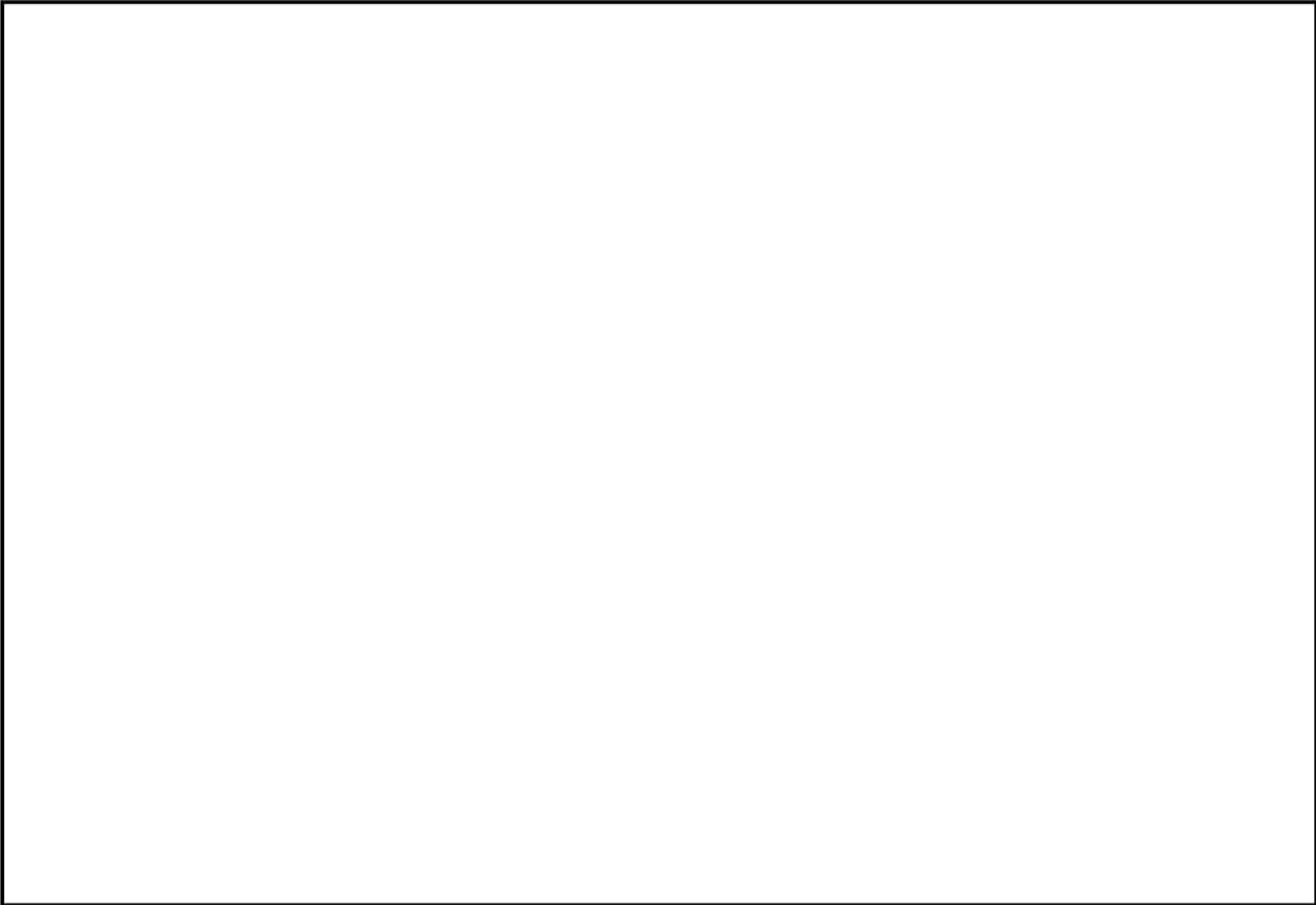
DE RUCNFB #0065 1892236

ZNY EEEEE

O 081834Z JUL 99

FM DIRECTOR FBI (288-HQ-1234199)

TO ALL FBI FIELD OFFICES/IMMEDIATE/



b7E

b7E

b7E



b7E

BT

PAGE FIVE DE RUCNFB 0065 UNCLAS E F T O

UNCLAS E F T O FOR OFFICIAL USE ONLY

SECTION THREE OF THREE SECTIONS

CITE: //1301//

PASS: NIC WARNING STAFF TO NATIONAL WARNING COMMUNITY; JTF-CND

APPROPRIATE DOD FACILITIES, SERVICE COMPONENTS AND TARGET

LOCATIONS; [REDACTED]

b7E

SUBJECT: [REDACTED]

TEXT CONTINUES:

6. (U) QUESTIONS AND REPORTS SHOULD BE DIRECTED TO THE [REDACTED]

b7E

[REDACTED] AS APPROPRIATE. [REDACTED]

CAN BE

REACHED AT [REDACTED] (COMMERCIAL) OR [REDACTED]

(CLASSIFIED) FROM 6AM TO 11PM WASHINGTON LOCAL TIME, OR E-MAIL AT

[REDACTED]
BT

#0065

NNNN

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 07/22/1999

To: Atlanta

From: Atlanta

Contact: [Redacted]

X6185

b7E

Approved By: [Redacted]

b6

b7C

Drafted By: [Redacted]

Case ID #: 288A-AT-87389 (Closed)

Title: UNSUB (S);
 AKA: DETH VEGETABLE;
 NET NINJA;
 DBA: CULT OF THE DEAD COW;
 MINDSPRING ENTERPRISES - VICTIM;
 INTRUSION - INFO SYSTEMS;
 IDENTITY THEFT;
 CONSPIRACY

Synopsis: It is recommend that the above captioned case be closed.

Details: The above captioned group has been in existence since 1984. At lasts years DEFCON VI HACKER CONVENTION, the group released a product called "BACK ORIFICE". At this years convention which was held on July 10, 1999 in Las Vegas, Nevada, the group released a newer version called "BACK ORIFICE 2000". The product will be made available as a free download.

BACK ORIFICE 2000 will allow an individual to gain access to a persons computer and retrieve system information including current user, cpu type, windows version, memory usage, mounted disks, drive information, screen saver password, and passwords cached by users. It will also allow the individual to have file system control, process control, registry control, network control, multimedia control, packet redirection, sniffing, application redirection and HTTP server.

BACK ORIFICE 2000 will reportedly include several features not found in the original version, including windows NT compatibility.

BACK ORIFICE 2000 will likely be used in a selective or targeted manner similar to previous network security exploits.

Re O/S A 3/6/00
 [Redacted]

8704 Close case
2/15/00
 [Redacted] *5.25.00*
C-4 5/25/00

b6
b7C

288A-AT-87389-11

To: Atlanta From: Atlanta
Re: 288A-AT-87389, 07/22/1999

FBIHQ is aware of the release of the virus, file number 288-HQ-1234199 and they have sent out an advisory notice.

It is recommended that each incidence be opened separately and worked on a case by case basis.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/20/2003

To: Cyber Division

Attn:

[Redacted]

b7E

From: Atlanta

Approved By:

[Redacted]

b6
b7C

Drafted By:

Case ID #: 288A-AT-87389 *12*
288-AT-C82244 SUB FD801 *112*

Title: UNSUB (S), AKA
DETH VEGETABLE;
NET NINJA,
DBA CULT OF THE DEAD COW;
MINDSPRING ENTERPRISES - VICTIM;
COMPUTER INTRUSION - CRIMINAL

SUBMISSION: Initial Supplemental Closed

CASE OPENED: 12/16/1998

CASE CLOSED: 05/25/2000

- No action due to state/local prosecution (Name/Number _____)
- USA declination
- Referred to Another Federal Agency (Name/Number: _____)
- Placed in unaddressed work
- Closed administratively
- Conviction

COORDINATION: FBI Field Office _____
 Government Agency _____
 Private Corporation _____

VICTIM

Company name/Government agency: Mindspring Enterprises
 Address/location: Atlanta, GA
 Purpose of System: ISP
 Highest classification of information stored in system: Unclassified

b6
b7C

[Redacted]

To: Cyber Division From: Atlanta
Re: 288-AT-87389, Date: 06/20/2003

System Data:

Hardware/configuration (CPU):
Operating System:
Software:

Security Features:

Security Software Installed: yes (identify _____) no
Logon Warning Banner: yes no

INTRUSION INFORMATION

Access for intrusion: Internet connection dial-up number LAN (insider)

If Internet: Internet address:
Network name:

Method:

Technique(s) used in intrusion: (list provided)

Path of intrusion:

addresses: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
country: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
facility: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Subject:

Age: _____ Race: _____
Sex: _____ Education: _____
Alias(s): _____ Motive: _____
Group Affiliation: _____
Employer: _____
Known Accomplices: _____
Equipment used:
Hardware/configuration (CPU):
Operating System:
Software:

Impact:

Compromise of classified information: yes no
Estimated number of computers affected: Undetermined
Estimated dollar loss to date: Undetermined

To: Cyber Division From: Atlanta
Re: 288-AT-87389, Date: 06/20/2003

Category of Crime:

Impairment:

- Malicious code inserted
- Denial of service
- Destruction of information/software
- Modification of information/software
- Telephone services obtained
- Application software obtained
- Operating software obtained

Intrusion:

- Unauthorized access.
- Exceeding authorized access

Theft of Information:

- Classified information compromised
- Unclassified information compromised
- Passwords obtained
- Computer processing time obtained

REMARKS

The above captioned group has been in existence since 1984. At the 1998, DEFCON VI HACKER CONVENTION, the group released a product called BACK ORIFICE. At the annual convention held on July 10, 1999 in Las Vegas, Nevada, the group released a newer version called BACK ORIFICE 2000.

BACK ORIFICE 2000 allows an individual to gain access to a person's computer and retrieve system information, including current user, cpu type, windows version, memory usage, mounted disks, drive information, screen saver password, and passwords cached by users. It will also allow the individual to have file system control, process control, registry control, network control, multimedia control, packet redirection, sniffing, application redirection and HTTP server.

BACK ORIFICE 2000 includes several features not found in the original version, including windows NT compatibility. BACK ORIFICE 2000 will likely be used in a selective or targeted manner similar to previous network security exploits. FBIHQ is aware of the release of the virus, file number 288-HQ-1234199 and they have sent out an advisory notice.

Investigation failed to develop evidence of criminal misconduct that occurred within Georgia. Case was closed administratively.

◆◆

Universal Case File Number 288A-AT-87389-1A1

Field Office Acquiring Evidence AT

Serial # of Originating Document _____

Date Received 12/17/1996

From _____

By _____

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

Title: _____

Reference: _____
(Communication Enclosing Material)

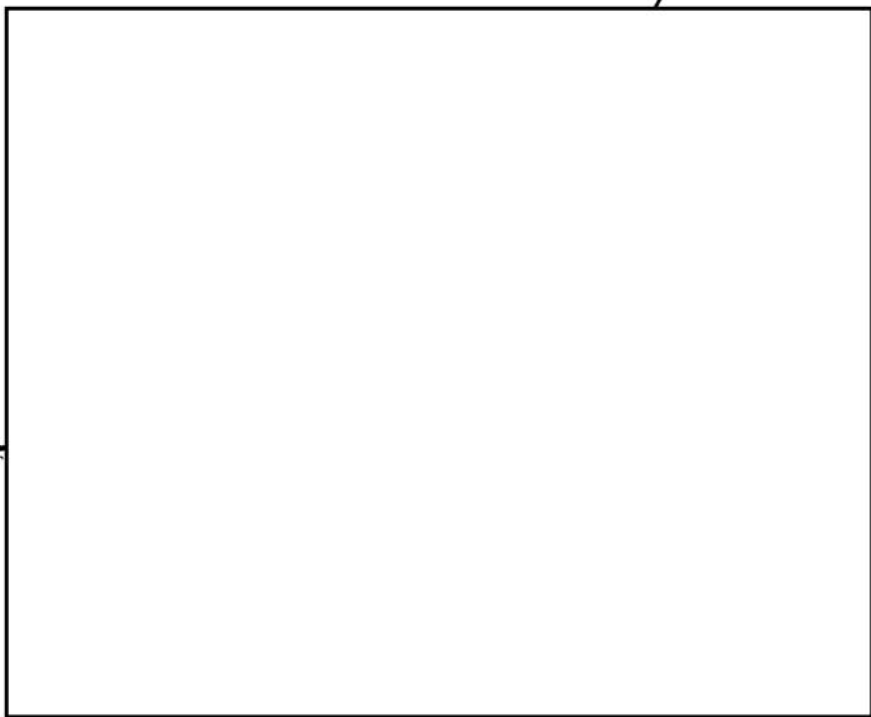
Description: Original notes re interview of

b6
b7C

b6
b7C

12/17/98
4 30
D

b6
b7c



NOTICED SIMULTANEOUS
ACCESS CHARGE \$6-
AGAIN SIM CHARGE \$38
ASKED U.S. WHY
ABUSE DEPT E-MAIL
LESS THAN 2 WEEKS

Consented to Copy
of H-D - Signed
Consent Form.

SA



Did

b6
b7c

FILE/FIND / WINDLL.DLL
LOCATED FILE,
B.O. IN FACTORY,

Universal Case File Number 288A-AT-87389-1A2

Field Office Acquiring Evidence - AT

Serial # of Originating Document _____

Date Received 12/17/98

From _____

By _____

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

Title: UNSUBS,
AKA CULT OF THE DEAD COW

Reference: _____
(Communication Enclosing Material)

Description: Original notes re interview of
CONSENT TO SEARCH

Form re _____ computer

b6
b7C

b6
b7C

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

CONSENT TO SEARCH

1. I have been asked by Special Agents of the Federal Bureau of Investigation to permit a complete search of:

(Describe the person(s), place(s), or thing(s) to be searched.)

GENERIC PC-CLONE MINI-TOWER SYSTEM
& COMPONENTS LOCATED AT

[Redacted]

[Redacted]

b6
b7C

- 2. I have been advised of my right to refuse consent.
- 3. I give this permission voluntarily.
- 4. I authorize these agents to take any items which they determine may be related to their investigation.

12/17/98
Date

430
Witness

[Redacted]

b6
b7C

[Redacted]

SA, FBI, ATLANTA

288A-11-87289-1A2

This is to certify that on _____ at _____
Special Agents of the Federal Bureau of Investigation, U.S. Department of
Justice, conducted a search of _____
I certify that nothing was removed from my custody by Special Agents of
the Federal Bureau of Investigation, U.S. Department of Justice.

(Signed) _____

Witnessed:

Special Agent
Federal Bureau of Investigation
U.S. Department of Justice

Special Agent
Federal Bureau of Investigation
U.S. Department of Justice

288A-AT-87389-1A3

Universal Case File Number _____

Field Office Acquiring Evidence _____

Serial # of Originating Document _____

Date Received *4/13/00*

From _____
(Name of Contributor)

(Address of Contributor)

By *SA* _____
(Name of Special Agent)

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

Title:

Reference: _____
(Communication Enclosing Material)

Description: Original notes re interview of
FD-142- N181 evidence
destroyed

b6
b7C

01/07/99
13:01:50

FD-192

ICMIPR01
Page 1

Title and Character of Case:

VEGETABLE, DETH
NINJA, NET

Date Property Acquired: Source from which Property Acquired:

12/18/1998

b6
b7c

Anticipated Disposition: Acquired By:

Case Agent:

Description of Property:

Date Entered:

1B 1

ONE OPTICAL DISK

Barcode: E1622226

Location: ECR

CAB1

01/07/1999

288A-AT-87389-1B1

Case Number: 288A-AT-87389-1B
Owning Office: ATLANTA

Evidence Package Copy

288A-AT-87389-1B1
E1622226

CHAIN OF CUSTODY

RECEIVED BY: [Redacted]
REASON: COLLECTED
DATE TIME: 12/18/98 10:AM

RECEIVED BY: [Redacted]
REASON: *Flowed*
DATE TIME: 12/30/98 10:00

RECEIVED BY: [Redacted]
REASON: *removed*
DATE TIME: 3/18/99 12:25 PM

RECEIVED BY: [Redacted]
REASON: *Process*
DATE TIME: 3/18/99 12:26 PM

RECEIVED BY: [Redacted]
REASON: *removed*
DATE TIME: 8/30/99 11:00 AM

RECEIVED BY: [Redacted]
REASON: *Flowed*
DATE TIME: 4/13/00 8:30 AM

RECEIVED BY: [Redacted]
REASON: *DESTROY*
DATE TIME: 4/13/00 8:38 AM

RECEIVED BY:
REASON:

RECEIVED BY:
REASON:

RECEIVED BY:
REASON:

RECEIVED BY:
REASON:

RECEIVED BY:
REASON:

RECEIVED BY:
REASON:

b6
b7c

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/29/98

✓ To: Atlanta

✓ Attn: Evidence Technician

From: Atlanta

Approved By: Daulton Jack A *JAD/WB*

[Redacted]

b6
b7C

Drafted By:

[Redacted]

Case ID #: 288A-AT-87389 (Pending) - 4

Title: DETH VEGETABLE;
NET NINJA;
CITA MATTERS

Synopsis: To report delayed entry of evidence into the Evidence Control Room.

Details: On 12/17/98 an image was made of the hard drive on a computer belonging to [Redacted] This was done with his consent. The Optical disk containing the image was turned over to this writer on 12/18/98. It has been in my custody since that time. During that time I have been looking for a media (hard drive) large enough to restore the image.

b6
b7C

♦♦

RE: 1B1

01/07799
13:01:50

FD-192

ICMIPRO1
Page 1

Title and Character of Case:

VEGETABLE, DETH
NINJA, NET

Date Property Acquired: Source from which Property Acquired:

12/18/1998

b6
b7c

Anticipated Disposition: Acquired By:

Case Agent:

Description of Property:

Date Entered

1B 1

ONE OPTICAL DISK

Barcode: E1622226

Location: ECR

CAB1

01/07/1999

288A-AT-87389-SFIB1

Case Number: 288A-AT-87389-1B
Owning Office: ATLANTA

**FD-192
INVESTIGATIVE
FILE COPY**

SEARCHED _____	INDEXED _____
SERIALIZED _____	FILED _____
JAN 11 1999	
FBI-ATLANTA	

[Signature]

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/29/98

✓ To: Atlanta

✓ Attn: Evidence Technician

From: Atlanta

Approved By: Daulton Jack A *770/W*

[Redacted]

Drafted By:

[Redacted]

Case ID #: 288A-AT-87389 (Pending) -4

Title: DETH VEGETABLE;
NET NINJA;
CITA MATTERS

Synopsis: To report delayed entry of evidence into the Evidence Control Room.

Details: On 12/17/98 an image was made of the hard drive on a computer belonging to [Redacted]. This was done with his consent. The Optical disk containing the image was turned over to this writer on 12/18/98. It has been in my custody since that time. During that time I have been looking for a media (hard drive) large enough to restore the image.

b6
b7C

b6
b7C

♦♦

RE: 1B1