**U.S. Department of Justice**

**Federal Bureau of Investigation**
*Washington, D.C. 20535*

March 21, 2024

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

FOIPA Request No.: 1363960-000
Subject: MDR/FBI Intelligence Assessment, FBI Cyber National Threat Assessment – 2008 (June 22, 2009)

Dear Mr. Greenewald:

You were previously advised we were consulting with another agency concerning information related to your Freedom of Information/Privacy Acts (FOIPA) request.

A portion of that information has been returned to the FBI and is enclosed. The documents were reviewed under the FOIA/FOIPA, Title 5, United States Code, Sections (s) 552/552a. Below you will find check boxes under the appropriate statute headings which indicate the types of exemptions asserted to protect information which is exempt from disclosure. The appropriate exemptions are noted on the enclosed pages next to redacted information. The checked exemptions used to withhold information are further explained in the enclosed Explanation of Exemptions.

| Section 552 | | Section 552a |
|---|---|---|
| ☑ (b)(1) | ☐ (b)(7)(A) | ☐ (d)(5) |
| ☐ (b)(2) | ☐ (b)(7)(B) | ☐ (j)(2) |
| ☑ (b)(3) | ☑ (b)(7)(C) | ☐ (k)(1) |
| 50 U.S.C. § 3024(i)(1) | ☐ (b)(7)(D) | ☐ (k)(2) |
| 50 U.S.C. § 3605 | ☑ (b)(7)(E) | ☐ (k)(3) |
| | ☐ (b)(7)(F) | ☐ (k)(4) |
| ☐ (b)(4) | ☐ (b)(8) | ☐ (k)(5) |
| ☐ (b)(5) | ☐ (b)(9) | ☐ (k)(6) |
| ☑ (b)(6) | | ☐ (k)(7) |

26 pages were reviewed and 26 pages are being released.

☑ The appropriate redactions were made by the United States Air Force – Office of Special Investigations (AFOSI), National Security Agency (NSA), Office of the Director of National Intelligence (ODNI), and United States Cyber Command (USCYBERCOM).

Based on the information you provided, we conducted a search of the places reasonably expected to have records. For more information about records searches and the standard search policy, see the enclosed FBI FOIPA Addendum General Information Section.

This is the **final release** of information responsive to your FOIPA request. This material is being provided to you at no charge.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. **"Part 1"** of the Addendum includes standard responses that apply to all requests. **"Part 2"** includes additional standard responses that apply to all requests for records about yourself or any third party individuals. **"Part 3"** includes general information about FBI records that you may find useful. Also enclosed is our Explanation of Exemptions.

Additional information about the FOIPA can be found at www.fbi.gov/foia. Should you have questions regarding your request, please feel free to contact foipaquestions@fbi.gov. Please reference the FOIPA Request number listed above in all correspondence concerning your request.

If you are not satisfied with the Federal Bureau of Investigation's determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account following the instructions on OIP's website: https://www.justice.gov/oip/submit-and-track-request-or-appeal. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of my response to your request. 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 emailing the FBI's FOIA Public Liaison at foipaquestions@fbi.gov. 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. You may also contact the Office of Government Information Services (OGIS). The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

Michael G. Seidel
Section Chief
Record/Information Dissemination Section
Information Management Division

Enclosures

**FBI FOIPA Addendum**

**As referenced in our letter responding to your Freedom of Information/Privacy Acts (FOIPA) request, the FBI FOIPA Addendum provides information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. Part 2 includes standard responses that apply to requests for records about individuals to the extent your request seeks the listed information. Part 3 includes general information about FBI records, searches, and programs.**

**Part 1: The standard responses below apply to 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 FOIPA [5 U.S.C. § 552(c)]. FBI responses are limited to those records subject to the requirements of the FOIPA. Additional information about the FBI and the FOIPA can be found on the www.fbi.gov/foia website.

(ii) **Intelligence Records**. To the extent your request seeks records of intelligence sources, methods, or activities, the FBI can neither confirm nor deny the existence of records pursuant to FOIA exemptions (b)(1), (b)(3), and as applicable to requests for records about individuals, PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2)]. 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 any such records do or do not exist.

**Part 2: The standard responses below apply to all requests for records on 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 about any Individual—Witness Security Program Records.** The FBI can neither confirm nor deny the existence of records which could identify any participant in the Witness Security Program pursuant to FOIA exemption (b)(3) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(3), 18 U.S.C. 3521, and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.

(iii) **Requests for Confidential Informant Records.** The FBI can neither confirm nor deny the existence of confidential informant records pursuant to FOIA exemptions (b)(7)(D), (b)(7)(E), and (b)(7)(F) [5 U.S.C.§ § 552 (b)(7)(D), (b)(7)(E), and (b)(7)(F)] and Privacy Act exemption (j)(2) [5 U.S.C.§ 552a (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records would reveal confidential informant identities and information, expose law enforcement techniques, and endanger the life or physical safety of individuals. 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 and Standard Search Policy.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching systems, such as the Central Records System (CRS), or locations where responsive records would reasonably be found. The CRS is an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled by the FBI per its law enforcement, intelligence, and administrative functions. The CRS spans the entire FBI organization, comprising records of FBI Headquarters, FBI Field Offices, and FBI Legal Attaché Offices (Legats) worldwide; Electronic Surveillance (ELSUR) records are included in the CRS. The standard search policy is a search for main entity records in the CRS. Unless specifically requested, a standard search does not include a search for reference entity records, administrative records of previous FOIPA requests, or civil litigation files.

a. *Main Entity Records* – created for individuals or non-individuals who are the subjects or the focus of an investigation
b. *Reference Entity Records*- created for individuals or non-individuals who are associated with a case but are not known subjects or the focus of an investigation

(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) **Foreseeable Harm Standard.** As amended in 2016, the Freedom of Information Act provides that a federal agency may withhold responsive records only if: (1) the agency reasonably foresees that disclosure would harm an interest protected by one of the nine exemptions that FOIA enumerates, or (2) disclosure is prohibited by law (5 United States Code, Section 552(a)(8)(A)(i)). The FBI considers this foreseeable harm standard in the processing of its requests.

(iv) **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 sheet. 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.

## 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.

b6
b7C



Federal Bureau of Investigation
Intelligence
ASSESSMENT

# (U) FBI Cyber National Threat Assessment - 2008

22 June 2009

~~UNCLASSIFIED~~


Prepared by

**FBI**

**Directorate of Intelligence / Cyber Intelligence Section**

~~Derived from: Multiple Sources~~
~~Declassify on: 20340519~~

## (U) FBI 2008 Cyber National Threat Assessment

### (U) Scope Note

(U//~~FOUO~~) This intelligence assessment addresses the Cyber Threats to US Critical Infrastructure (CYBR) topic of the National Intelligence Priorities Framework (NIPF) Q-FBI-2700-001-05 and satisfies FBI requirements CYBR CyD 1-I.A.2, and CYBR CyD 1-II.B.1.

(U//~~FOUO~~) This assessment examines the cyber threats to the United States based on information derived from FBI investigations, US Intelligence Community (USIC) reporting, and open-source reporting from 30 June 2007 to 1 July 2008, with earlier material for context. It focuses on cyber threats conducted by remote system intrusions or unauthorized access against the United States and its critical infrastructure. Tactics, techniques, and procedures used against process control systems (PCS), financial institutions, government networks and the supply chain are also addressed, as is malicious actors' potential use of tools and technologies, such as IPv6 and virtual worlds.

~~(S)~~ This is the FBI's first national cyber threat assessment [redacted] ~~(S)~~ (U)

[redacted] the FBI has completed intelligence assessments on each one and identified them as cyber threat actors. [redacted] ~~(S)~~ (U)

b1
b3
b7E

UNCLASSIFIED

**(U) Source Summary Statement:** This assessment is based upon reporting from diverse sources providing a broad picture of foreign intelligence collection, cyber crime, and cyberterrorism as well as malicious use of current tools and technologies. FBI sources vary in reliability and include established sources with direct access to the information, which has been corroborated. Other FBI source reporting included first time reporting, sources with indirect access, reporting from sources of unknown reliability, of which reporting had not been corroborated, as well as open source reporting.

[redacted] ~~(S)~~ (U)

b1
b3
b7E

**(U) Key Terms**

**(U) Botnet** – Robot network. A network of compromised computers remotely controlled by an attacker.

**(U) Computer Network Operations** (CNO) - is the use of information systems to attack or exploit an adversary' s computer based networks.

- (U//~~FOUO~~) Computer Network Attack (CNA) - Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

- (U//~~FOUO~~) Computer Network Exploitation (CNE) - Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

- (U//~~FOUO~~) Computer Network Defense (CND) - Involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense (DoD) information systems and computer networks. Because this assessment only addresses direct threats to the United States, CND is not covered.

**(U) Cleared Defense Contractors (CDC)**- Organizations involved in sensitive defense/government research/weapons development, access control, encryption, Public Key Infrastructure (PKI), biometrics, strategic or tactical command components, and Weapons of Mass Destruction sites.

**(U) Critical Infrastructure/Key Resources** – Eighteen sectors defined in the National Infrastructure Protection Plan. These sectors include Agriculture and Food, Banking and Finance, Chemical, Commercial Facilities, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Government Facilities, Information Technology, National Monuments and Icons, Commercial Nuclear Reactors – Materials and Waste, Postal and Shipping, Public Health and Healthcare, Telecommunications, Transportation Systems, Drinking Water and Wastewater Treatment.

**(U) Cyberterrorism** – is defined as terrorism that is perpetrated by computer network attack (that is, via data streams) or electromagnetic means to disrupt, deny, degrade, or destroy information resident in US computers and computer networks, the computers and networks themselves, or critical infrastructures they support.

**(U) Cyber Jihad**, or **e-Jihad** – is broadly defined as the application of information technology or online campaigns to further the global jihadist movement. This includes, but is not limited to, hacking/cracking, disruptive technological application, propaganda, or the use of information technology to organize and provide material support and derive strategic intelligence.

**(U) Denial of Service** – An attack that floods a computer network with so many requests, or information, that regular service is slowed or interrupted.

**(U) Distributed Denial of Service (DDoS)** – An attack in which multiple compromised systems are used to target a single system in a Denial of Service attack.

**(U) High Technology Organizations** include backbone Internet Service Providers (ISPs), regional ISPs, organizations involved in rising technology trends (social networking, hybrid virtual realty, digital currency), hardware and software developers; Internet standards regulators (Internet Corporation for Assigned Names and Numbers, registrars, protocol developers).

**(U) Internet Protocol (IP) Address** – A unique address for a computer or device on a network.

**(U) Supply Chain** - The system of organizations, people, technology, activities, information and resources involved in moving a product or service from supplier to customer. The supply chain encompasses both equipment level (routers, thumb drives, etc.) and application level (antivirus software, operating systems, etc.).

**(U) Key Questions**

- (U//~~FOUO~~)
- (U//~~FOUO~~)
- (U//~~FOUO~~)
- (U//~~FOUO~~)
- (U//~~FOUO~~)

b7E

## (U) Executive Summary

b1
b3

[redacted] (U)

[redacted] (U)

b1
b3
b7E

(~~S//NF~~) Cyber jihadists vary in technical skill and expertise [redacted] (U) Cyber jihadists use the Internet for typical cyber crime, such as phishing and credit card fraud, as well as for communicating, financing, recruiting, and propaganda.

b1
b3

(~~U//FOUO~~) Both state and non-state actors conduct malicious cyber activity through various tactics, techniques, and procedures; chief among them is the use of botnets by cyber actors. Botnets—a network of compromised computers—can be used in criminal, intelligence collection, and cyber terrorist activity for spamming, DDoS, and information stealing. [redacted] (U)

b1
b3

(~~U//FOUO~~) According to USG and open source information, the US critical infrastructure is vulnerable to cyber attack.[iii, 1, 2] Various tools and technologies, such as botnets, are currently available and evolving that can be used by malicious actors from all over the world to conduct their activities against US critical infrastructure. [redacted] (U)

b1
b3
b7E

[ii] (U) Threat and confidence levels are defined in Appendix A.
[iii] (U//~~FOUO~~) A cyber attack is any remote attack against a computer system or network to disrupt activity or otherwise cause harm.

**(U) Foreign Intelligence Collection**

[redacted] (S) (U)

b1
b3
b7E

[redacted] Intelligence collection efforts [redacted] include computer intrusions/unauthorized access, social engineering, phishing, and supply chain attacks/infiltration.

[redacted] (S) (U)

(S//NF) In recent years the FBI has observed an increase in computer intrusions [redacted] targeting sensitive USG and private sector networks. [redacted] (S) (U)

[redacted] (S) (U)

b1 Per ODNI and FBI
b3 Per ODNI and FBI
b7E

[redacted] (S) (U)

b1
b3
b7E

[redacted] (S) (U)

b1
b3

[redacted]

b1 Per ODNI and FBI
b3 Per ODNI and FBI
b7E

(~~S~~) (U)

(~~S~~//OC) In 2005, the FBI identified a sophisticated network infrastructure that most likely was compromised [redacted] for the purpose of conducting CNO.[14] [redacted] It is difficult to determine the exact information collected [redacted] because some of the traffic was encrypted.

b1
b3
b7E

(~~S~~) (U)

(~~S~~) (U)

[redacted]

(~~S~~) (U)

b1
b3
b7E

[14] (U) A DNS query is a request to a Domain Name Server for information on a domain name.

b1
b3
b7E

(S) (U)

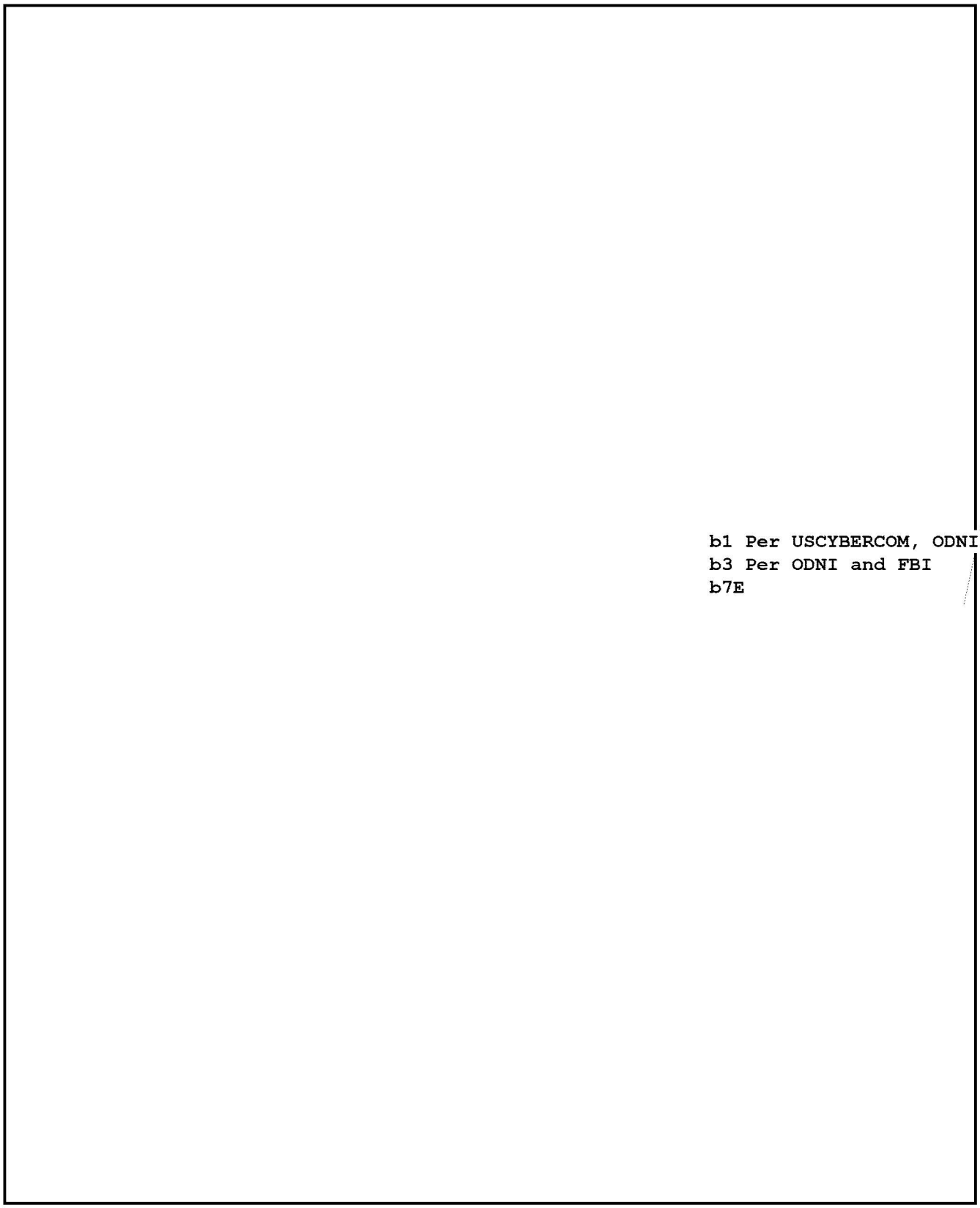
- (S//NF)

b7E

(S) (U)

b1
b3
b6
b7C
b7E

[viii] (U) Network mapping is visually representing a computer network's architecture.
[ix] (U) Encrypted data exfiltration involves the unauthorized removal or transmission of data from another computer network in an encrypted format.



(S)

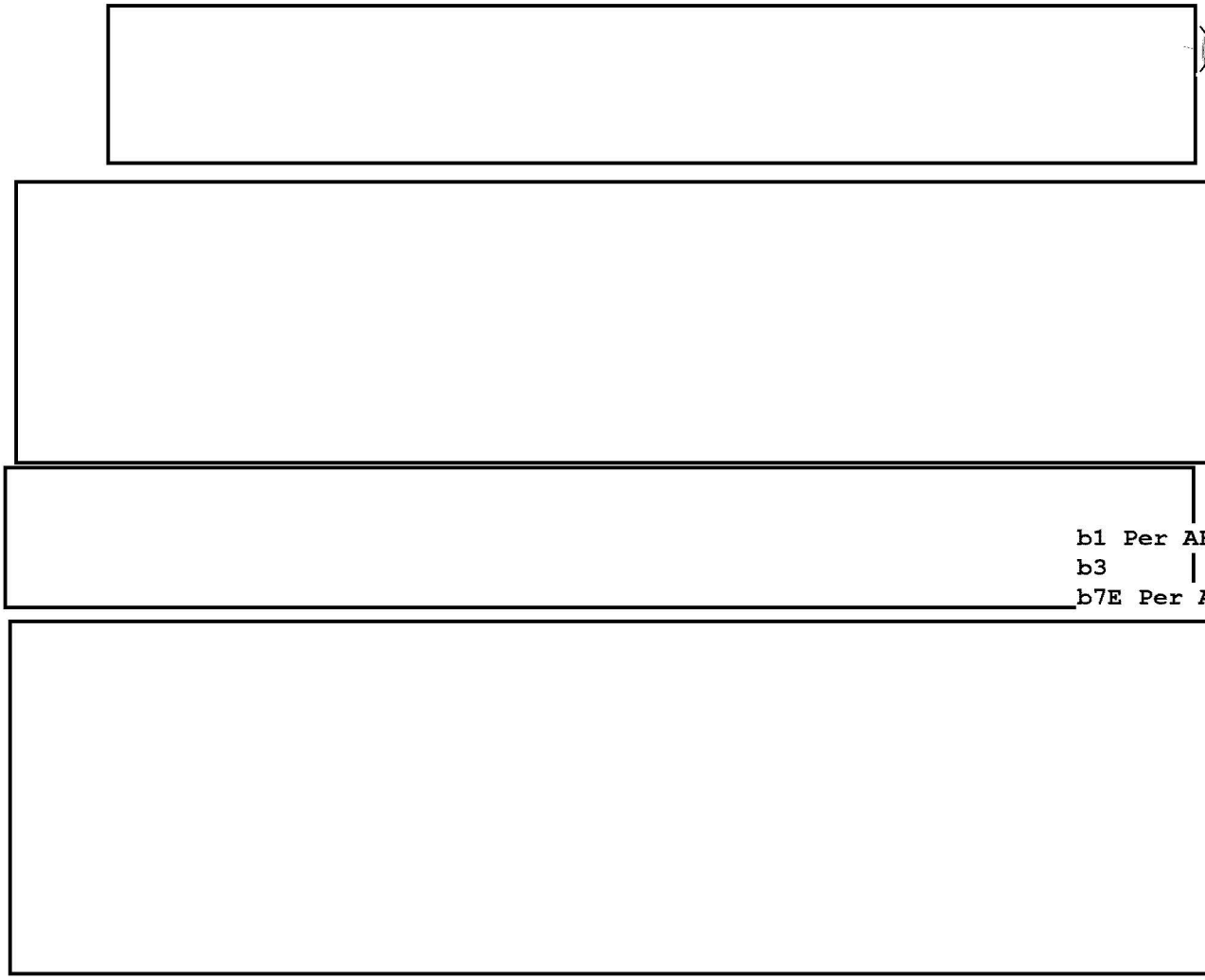
b1 Per USCYBERCOM, ODNI, and FBI
b3 Per ODNI and FBI
b7E

- (S)

(S) (U)

(S) (U)

b1
b3
b7E




**(U) Cyber Crimes**

(U//~~FOUO~~) The United States is vulnerable to several forms of cyber crime, such as phishing,[xi] credit card fraud, and unauthorized access, originating from all over the world with varying threat levels.

b7E

*(U)*

(U//~~FOUO~~) According to FBI investigations, use phishing schemes, various malware, and botnets as their primary methods to gain access to financial institutions or to obtain personal identifying information from US victims.

b7E

[x] (U) FTP, or File Transfer Protocol, is the protocol for exchanging files over the Internet. FTP is used to download a file from a server using the Internet, or to upload a file to a server.

[xi] (U) Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

(U//~~FOUO~~)

b7E

- (U//~~FOUO~~) FBI investigations determined

  FBI investigation identified b7E

- (U//~~FOUO~~)

  b7E

- (U//~~FOUO~~) According to FBI reporting and industry experts,

  b7E

- (U//~~FOUO~~)

  b7E

(U//~~FOUO~~) According to FBI investigations, businesses are the primary target of most criminal schemes, but they also target unwitting individuals for the purpose of using them as money mules[xii] to transfer illicit funds b7E

[xii] (U) A money mule is someone who is tricked into using a personal bank account to launder money.

(U//~~FOUO~~) The FBI assesses that cyber crime [redacted] will continue to grow in volume and sophistication. [redacted] cyber criminals have targeted US financial institutions since the 1990s and the FBI expects this activity to continue unabated. b7E

[redacted] (U)

b1
b3
b7E

(U//~~FOUO~~) As the political climate changes, or if relationships between [redacted] deteriorate, the FBI expects to see [redacted] b7E

*(U)* [redacted]

(U//~~FOUO~~) [redacted]

[redacted] According to FBI investigations, [redacted] b7E

- (U//~~FOUO~~) [redacted] b7E

[xiii] (U) In a SYN flood attack, the sender transmits a volume of connections to a Web site that cannot be completed. This causes the connection queues to fill up, thereby denying service to legitimate users.

[xiv] (U) [redacted] b7E

were involved in the fraud. Several fraudulent credit cards were made from each compromised account. FBI investigation identified [redacted] who sold the stolen credit card account numbers on the Internet.[45] b7E

- (U//~~FOUO~~) [redacted] b7E

(U//~~FOUO~~) [redacted] cyber crime will remain prevalent as long as it is profitable. Consequently, it is expected that [redacted] cyber criminals' tactics will also continue to evolve for bigger profit and to evade detection. b7E

(U//~~FOUO~~) [redacted] cyber crime will continue to pose a high threat to the United States. [redacted] the FBI expects to see increased activity and collaboration [redacted] b7E

*(U) Intellectual Property Rights Violations*

(U//~~FOUO~~) Malicious foreign actors are committing IPR violations and pose a moderate cyber threat to the United States. Losses to rights holders as a result of online crime are difficult to determine; however, the latest statistics available from the Motion Picture Association of America (MPAA) estimates online piracy of movies resulted in a $2.3 billion loss in 2005.[47] The International Federation of the Phonographic Industry estimates that almost 20 billion songs were illegally downloaded worldwide in 2005.[48] An estimated 35 percent of the software installed on personal computers in 2006 was obtained illegally, resulting in nearly $40 billion in global losses with almost $6.5 billion in the United States. These figures include both online download delivery and CD-R (compact disc-read) hard goods piracy, although online losses are not reported separately.[49, 50]

**(U) The Global Software Piracy Study 2007**

**(U) Damage from Software Piracy Top Offenders:**

1. (U) United States – $8 billion
2. (U) China – $6.7 billion
3. (U) Russia – $4.1 billion
4. (U) France – $2.6 billion
5. (U) India – $2 billion
6. (U) Brazil – $1.6 billion

(U) Produced by the Business Software Alliance – May 2008

(~~S~~//~~NF~~) IPR violations and trademark infringement through counterfeiting in the information technology industry [redacted] poses a threat to US national security. [redacted] b1 b3 b7E

(S) (U) [redacted] (S) (U)

(~~S~~//~~NF~~) The FBI suspect [redacted] to gain access to US sensitive but unclassified information [redacted] b1 b3 b7E

(S) (U) (S) (U)

[redacted] (U) b1 b3 b7E

(U//~~FOUO~~) Warez is digital media that has had its copyright protection defeated, or "cracked," permitting use without purchasing a license. Organized warez groups usually specialize in the distribution of products based on genre (for example, music, movies, software), trading titles among group members and with other groups, while maintaining large private storage servers of the cracked media. It is a point of pride and competition among warez groups to be the first to crack and distribute any given title. While warez groups do not seek profit, their activity can cause significant economic harm to the rights holder. FBI case data dramatically illustrate the financial loss to the rights holder of even one music album.

- (U//~~FOUO~~) In an investigation targeting a music warez group, a particular music album was released on a members-only warez server on 23 October 2006. As of 12 January 2007, the identical music file had been downloaded over 41,000 times from just one of dozens of available public music sharing sites. The retail price of this CD was $13.98, resulting in lost sales of over $500,000 in less than three months from one site for one album.[52]

(~~S~~//~~NF~~) IPR violations will likely continue in the short term [redacted]

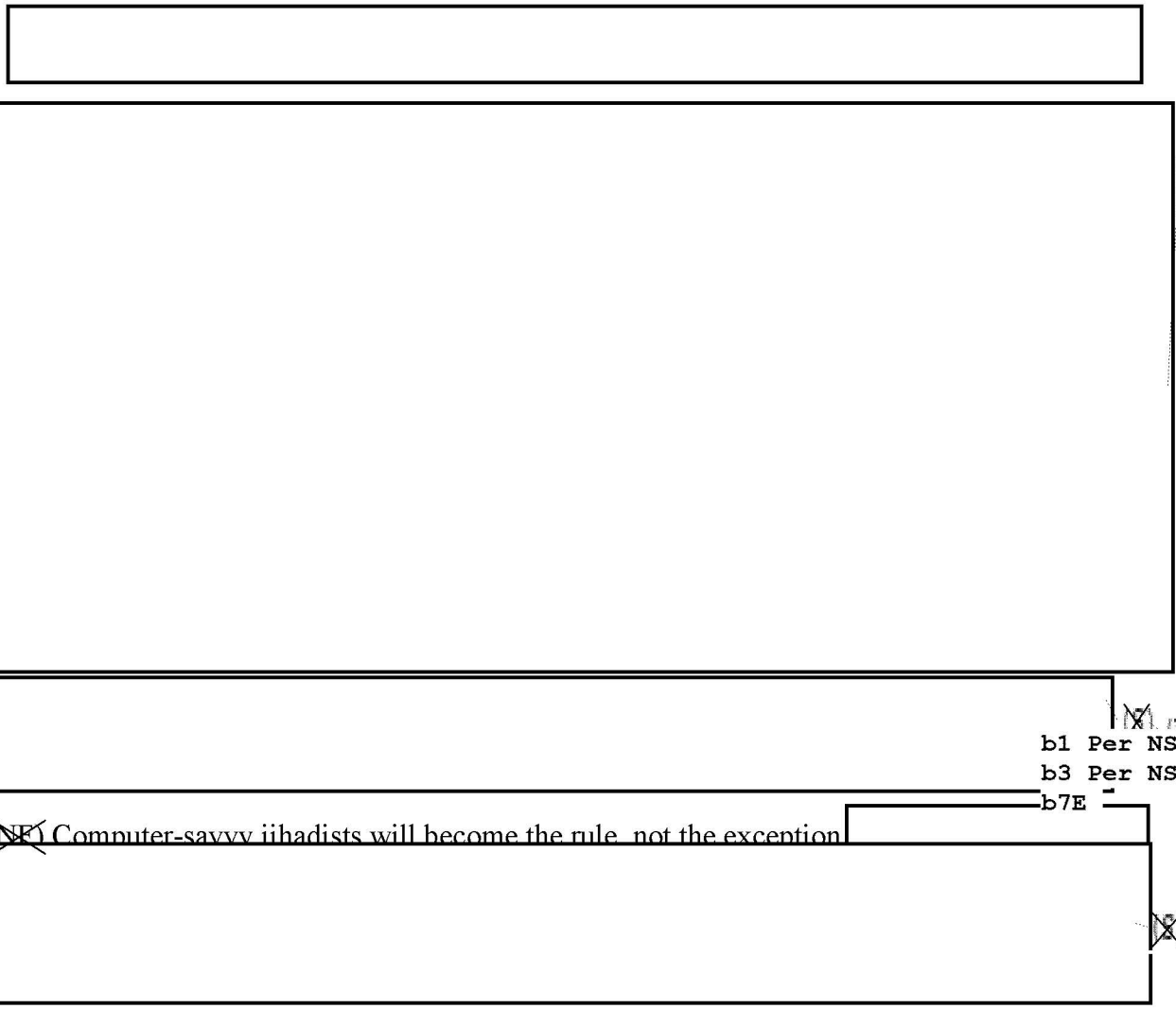
[redacted] (~~S~~) (U) b1 b3 b7E

**(U) Cyberterrorism**

[redacted] (~~S~~) b1 b3 b7E

- [redacted] b3 b7E

[redacted] b7E




**(U) Tactics, Techniques, and Procedures**


(U//~~FOUO~~) These tactics, techniques, and procedures are readily available and are continuously evolving allowing malicious actors from all over the world to conduct their activities in a dynamic manner. Chief among these tactics is the persistent use of botnets.

*(U) Botnets*

(U//~~FOUO~~) Botnets continue to pose a threat to US critical infrastructures. These networks of compromised computers can be used to wage denial of service attacks against targeted online

[xvii] (U) CVV, or Card Verification Value, is a 3- or 4-digit security code printed on the credit card itself.
[xviii] (U) See Appendix B.

entities, conduct phishing and spamming campaigns, and steal passwords and other login credentials which often lead to unauthorized transactions at victim's financial institutions.

(U//~~FOUO~~)

b7E

(U)

b1
b3
b7E

(U) FBI source reporting indicates a growing number of botnet command and control systems

(U)

b1
b3
b7E

(U//~~FOUO~~) Botnets have historically tended to exploit targets of opportunity. Attackers will often exploit vulnerabilities in operating systems and applications. However, many attackers still use social-engineering techniques to trick users into opening e-mail attachments or visiting malicious Web sites.

b7E

(U//~~FOUO~~) Attackers typically collect passwords, login credentials, keystrokes, credit card numbers, and personally identifying information from botnet victims.

(U//~~FOUO~~) Botnet attacks continue to evolve and stay ahead of security researchers and products, industry mitigation, and law enforcement investigation.

(U)

b1
b3

(U//~~FOUO~~)

b7E

(U) The FBI is also concerned with new tools and technologies that are continuously being developed. These could be used by malicious actors from all over the world to conduct their illicit activity.

(U)

b1
b3
b7E

(U)

b1
b3
b7E

(U)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

*(U) IPv6*

(U//~~FOUO~~) IPv6 is the Internet addressing scheme intended to replace the current version, IPv4. IPv6 is designed to allow more available IP addresses since these are running out due to the rapid growth of the Internet.

b7E

*(U) Virtual Worlds*

(U//~~FOUO~~) virtual worlds provide opportunities for extremists and criminals to conduct malicious activitie

~~(S)~~ (U) ~~(S)~~ (U)

b1
b3
b7E

(U//~~FOUO~~)

b7E

**(U) Outlook**

~~(S)~~ (U)

b1
b3
b7E

[xix] (U) A software update intended to repair an error in the application.

(~~S//NF~~) The Internet has become and will continue to be a theater of operation for cyber jihadists [redacted]

(U) [redacted]

(~~S~~) [redacted]

b1
b3

## (U) Intelligence Gaps

- (U) [redacted]

b1
b3
b7E

- (~~S//NF~~) [redacted]

(~~S~~) (U) [redacted]

- (~~S//NF~~) [redacted]

(~~S~~) (U) [redacted]

b1
b3
b7E

- (~~S//NF~~) [redacted]

(~~S~~) (U) [redacted]

(~~S~~) (U) [redacted]

- (U) [redacted]

b1
b3
b7E

- (U) [redacted]
- (U//~~FOUO~~) [redacted]

b7E

- (U) [redacted]

b7E

- (U) [redacted]
- (U) [redacted]

(U) This assessment was prepared by the Europe/Eurasia/Americas Cyber Intelligence Unit of the FBI. Comments and queries may be addressed to the unit chief at [redacted]

b7E

## (U) Appendix A: Confidence and Threat Level Definitions

| (U) Confidence Level Definitions |
| --- |
| |

b7E

| (U) Threat Level Definitions |
| --- |
| |

b7E

## Appendix B: Common Tactics, Techniques and Procedures of Cyber Attacks

| (U) Table 1: Common Tactics, Techniques and Procedures of Cyber Attacks | |
|---|---|
| **Port Scanner** | A piece of software designed to search a network host for open ports. This is often done by administrators to check the security of their networks and by malicious actors to compromise it. (Wikipedia) |
| **Zero-day Exploit** | An exploit that takes advantage of a vulnerability on the same day that the vulnerability becomes publicly or generally known. (Webopedia)<br><br>Used by malicious actors for exploitation of end systems for remote control. |
| **Social Engineering** | The act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information. (Webopedia)<br><br>Supports theft of credit or financial card data and personal information for identity theft. |
| **E-mail Spoofing** | Fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. (Wikipedia)<br><br>Supports theft of credit or financial card data and personal information for identity theft. |
| **Trojan Horse** | A useful or seemingly useful program that contains hidden code of a malicious nature. (NIST SP 800-46)<br><br>Used by malicious actors to compromise end systems. |
| **Rootkit** | A computer virus which consists of a program designed to take fundamental control of a computer system, without authorization by the system's owners and legitimate managers. (Reference.com)<br><br>Used by malicious actors to compromise end systems and gain administrator/root-level access. |
| **SQL Injection** | A form of attack on a database-driven Web site in which the attacker executes unauthorized SQL commands b taking advantage of insecure code on a system connected to the Internet, bypassing the firewall. (Webopedia) |
| **Botnet** | A large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack. Also called a zombie army. (TechEncyclopedia) |
| **Phishing** | The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information. (Webopedia) |

## (U) Endnotes

[1] (U) Online Article; Ben Bain; Federal Computer Week; "Critical Infrastructure Central to Cyber Threat"; 24 April 2008; http://fcw.com/Articles/2008/04/24/Critical-infrastructure-central-to-cyber-threat.aspx?p=1; UNCLASSIFIED; UNCLASSIFIED.

[2] (U) Online News Article; Financial Times; 05 September 2007; "US Concedes Danger of Cyber-Attack"; http://ft.com/cms/s/0/3b5e7d8e-5bd0-11dc-bc97-0000779fd2ac,dwp_uuid=f6e7043e-6d68-11da-a4df-0000779e2340.html; UNCLASSIFIED; UNCLASSIFIED.

[redacted] (U) b1 Per ODNI b3 b7E

[redacted] (S) (U)

[11] (U) FBI Electronic Communication; 23 July 2007; ~~SECRET~~//ORCON/~~NOFORN~~; ~~SECRET//NOFORN~~.

[12] (U) FBI Electronic Communication; 15 March 2007; ~~SECRET~~//ORCON//~~NOFORN~~; ~~SECRET//NOFORN~~.

[13] (U) FBI Electronic Communication; 09 August 2005; ~~SECRET~~; ~~SECRET~~.

[14] (U) *Ibid.*

[redacted] (S) (U) b1 b3 b7E

[17] (U) FBI Electronic Communication; 10 December 2007; ~~SECRET~~; ~~SECRET~~.

[redacted] (S) (U) b1 b3 b7E

[20] (U) FBI Electronic Communication; 25 January 2008; ~~SECRET//NOFORN~~; ~~SECRET//NOFORN~~.

[21] (U) *Ibid.*

[22] (U) *Ibid.*

[23] (U) *Ibid.*

[24] (U) [redacted] b7E

b1 Per USCYBERCOM
b3 (S) (U)
b7E

b1
b3 (S) (U)
b7E Per USAF and FBI

[redacted]

[33] (U) Online article [redacted] UNCLASSIFIED; UNCLASSIFIED. b7E
[34] (U) iDefense; "Banking Trojans: an Overview"; 31 January 2008; UNCLASSIFIED; UNCLASSIFIED.
[35] (U) FBI Electronic Communication; 06 March 2007; UNCLASSIFIED; UNCLASSIFIED.
[36] (U) FBI Electronic Communication; 15 February 2008; UNCLASSIFIED; UNCLASSIFIED.
[37] (U) FBI Electronic Communication; 16 August 2007; UNCLASSIFIED; UNCLASSIFIED.
[38] (U) FBI Electronic Communication; 11 September 2007; UNCLASSIFIED; UNCLASSIFIED
[39] (U) Online News Article; ComputerWorld; [redacted] UNCLASSIFIED; b7E
UNCLASSIFIED.
[40] (U) FBI Electronic Communication; 19 December 2007; UNCLASSIFIED; UNCLASSIFIED.
[41] (U) Berkeley Researchers; "Spamlytics: An Empirical Analysis of Spam Marketing Conversion"; October 2008; UNCLASSIFIED; UNCLASSIFIED.

[redacted] (S) (U)

b1
b3
b7E

[45] (U) FBI Electronic Communication; 4 January 2008; UNCLASSIFIED//~~FOR OFFICAL USE ONLY~~; UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~.
[46] *Ibid.*
[47] (U) Motion Picture Association of America, "2005 US Piracy Fact Sheet"; http://www.mpaa.org/USPiracyFactSheet.pdf, 2005; UNCLASSIFIED; UNCLASSIFIED.
[48] (U) International Federation of the Phonographic Industry (IFPI), Commercial Piracy Report 2006, available at http://www.ifpi.org/content/library/piracy-report2006.pdf; UNCLASSIFIED; UNCLASSIFIED.
[49] (U) Business Software Alliance, "Fourth Annual BSA and IDC Global Software Piracy Study"; http://w3.bsa.org/globalstudy; UNCLASSIFIED; UNCLASSIFIED.

[50] (U) US Customs and Border Protection: "Intellectual Property Rights Seizures Statistics: FY2007"; December

[redacted]

[52] (U) FBI Internal Report: UNCLASSIFIED: UNCLASSIFIED

b1
b3
b7E

(S) (U)

(S) (U)

b1
b3
b7E

b1 Per NSA and FBI
b3 Per NSA and FBI
b7E

(S) (U)

# FBI Customer Satisfaction Survey

Please take a moment to complete this survey and help evaluate the quality, value, and relevance of our intelligence product. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance.

**Return to:**
**Federal Bureau of Investigation**
**Production Services Unit**
**935 Pennsylvania Ave, NW, Room 11079C**
**Washington, DC 20535**

## Customer and Product Information

Intelligence Product:
Title: _(U) FBI Cyber National Threat Assessment - 2008_____
Dated: _19 May 2009_____

Customer Agency: _____

## Relevance to Your Intelligence Needs

1. The product increased my knowledge of an issue or topic. (Check one)

___5. Strongly Agree
___4. Somewhat Agree
___3. Neither Agree or Disagree
___2. Somewhat Disagree
___1. Strongly Disagree

**PSU INTERNAL USE ONLY**

Product Tracking #: _____

Return To: _____

**Actionable Value**

2. The product helped me decide on a course of action. (Check one)

___5. Strongly Agree
___4. Somewhat Agree
___3. Neither Agree or Disagree
___2. Somewhat Disagree
___1. Strongly Disagree

**Timeliness Value**

3. The product was timely to my intelligence needs. (Check one)

___5. Strongly Agree
___4. Somewhat Agree
___3. Neither Agree or Disagree
___2. Somewhat Disagree
___1. Strongly Disagree

Comments (if any):