Pre-released portions of the FBI file on Google

 Obtained (via FOIA) and posted by AltGov2

 www.altgov2.org
Dear Mr. Kick:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act (FOIA). Below you will find informational paragraphs relevant to your request. Please read each item carefully.

☐ A search of the Central Records System maintained at FBI Headquarters indicated that records responsive to your request have been sent to the National Archives and Records Administration (NARA). Since these records were previously processed under the provisions of the Freedom of Information Act, we are providing you a copy of the previously processed documents.

Please be advised if this release of previously processed material does not satisfy your information needs for this request, you may make a request to NARA at the following address, using file number insert FILE NUMBER as a reference:

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

☐ A search of the Central Records System maintained at FBI Headquarters indicated that records responsive to your request were destroyed on DATE IF KNOWN. 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. Since these records were previously processed under the provisions of the Freedom of Information Act, we are providing you a copy of the previously processed documents.

Enclosed are 150 pages of previously processed documents and a copy of the Explanation of Exemptions. This release is being provided to you at no charge.

Documents or information referred to other Government agencies were not included in this release.

Please be advised that additional records potentially responsive to your subject may exist. If this release of previously processed material does not satisfy your information needs for this 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.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.
For questions regarding our determinations, visit the [www.fbi.gov/foia](http://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://foiaonline.regulations.gov/foia/action/public/home](https://foiaonline.regulations.gov/foia/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)
EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) 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.

FBI/DOJ
SOURCE, who is not in a position to testify, was in contact with SA via telephone and e-mail. SOURCE provided the following information:

The telephone number is in control of several distributed denial of service (DDoS) networks. He lives with his mother, has taken the computer away for getting in trouble with them previously, and has threatened to take them away permanently if he causes more trouble.

He may be the owner of the Internet web site and the file is suppose to be a picture of claims to run the Internet service business also claims to be attacking every server on the IRC network simultaneously, Google (for one hour), and last one for 12 hours. He also claims to have control of 85 compromised "gov" computers, including one "fbi" computer.

are installed on a compromised Internet computer, the attempt to connect to The address resolved to different Internet protocol (IP) addresses at different times. On 01/06/03, the domain name resolved to all of the following IP addresses at the same time:

Investigation on 01/06/03 at Chicago

File # 288A-SF-133411,  

Date dictated 01/06/03

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.
I conducted attacks on computers with the following Internet addresses:

<table>
<thead>
<tr>
<th>IP address</th>
<th>date &amp; time</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>01/06/03 02:49:11 GMT</td>
<td>udp</td>
</tr>
<tr>
<td></td>
<td>01/06/03 02:49:16 GMT</td>
<td>udp</td>
</tr>
<tr>
<td></td>
<td>01/06/03 02:49:19 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/06/03 02:11:02 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/06/03 02:20:25 GMT</td>
<td>packet</td>
</tr>
</tbody>
</table>

I conducted the following attacks against the Google web site, www.google.com (IP address):

<table>
<thead>
<tr>
<th>IP address</th>
<th>date &amp; time</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>01/02/03 10:58:16 GMT</td>
<td>udp</td>
</tr>
<tr>
<td></td>
<td>01/02/03 10:58:23 GMT</td>
<td>packet</td>
</tr>
</tbody>
</table>

I also conducted the following attacks against the Google web site using the command [ ], which caused:

<table>
<thead>
<tr>
<th>Webpage</th>
<th>date &amp; time</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.google.com">http://www.google.com</a></td>
<td>01/02/03 10:58:54 GMT</td>
</tr>
<tr>
<td><a href="http://www.google.com">http://www.google.com</a></td>
<td>01/02/03 10:58:54 GMT</td>
</tr>
<tr>
<td><a href="http://www.google.com">http://www.google.com</a></td>
<td>01/02/03 10:58:54 GMT</td>
</tr>
<tr>
<td><a href="http://www.google.com">http://www.google.com</a></td>
<td>01/02/03 10:58:55 GMT</td>
</tr>
<tr>
<td><a href="http://www.google.com">http://www.google.com</a></td>
<td>01/02/03 10:58:55 GMT</td>
</tr>
</tbody>
</table>

I conducted attacks on computers with the following Internet addresses:

<table>
<thead>
<tr>
<th>IP address</th>
<th>date &amp; time</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>01/06/03 19:21:45 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/06/03 19:29:54 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/06/03 20:11:13 GMT</td>
<td>packet</td>
</tr>
</tbody>
</table>

I conducted attacks on computers with the following Internet addresses:

<table>
<thead>
<tr>
<th>IP address</th>
<th>date &amp; time</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>01/06/03 21:33:55 GMT</td>
<td>packet</td>
</tr>
<tr>
<td>Date</td>
<td>Time</td>
<td>GMT</td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td>01/03/03</td>
<td>17:51</td>
<td>45</td>
</tr>
<tr>
<td>01/03/03</td>
<td>18:45</td>
<td>57</td>
</tr>
<tr>
<td>01/03/03</td>
<td>18:53</td>
<td>28</td>
</tr>
<tr>
<td>01/03/03</td>
<td>19:03</td>
<td>50</td>
</tr>
<tr>
<td>01/03/03</td>
<td>19:09</td>
<td>23</td>
</tr>
<tr>
<td>01/03/03</td>
<td>19:20</td>
<td>15</td>
</tr>
<tr>
<td>01/03/03</td>
<td>19:41</td>
<td>25</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:36</td>
<td>20</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:40</td>
<td>17</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:41</td>
<td>57</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:44</td>
<td>04</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:45</td>
<td>37</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:46</td>
<td>09</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:46</td>
<td>12</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:46</td>
<td>13</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:46</td>
<td>24</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:46</td>
<td>44</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:47</td>
<td>00</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:47</td>
<td>12</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:47</td>
<td>31</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:47</td>
<td>39</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:47</td>
<td>48</td>
</tr>
<tr>
<td>01/06/03</td>
<td>01:48</td>
<td>19</td>
</tr>
<tr>
<td>01/05/03</td>
<td>23:31</td>
<td>03</td>
</tr>
<tr>
<td>01/05/03</td>
<td>23:35</td>
<td>11</td>
</tr>
<tr>
<td>01/06/03</td>
<td>00:05</td>
<td>04</td>
</tr>
<tr>
<td>01/03/03</td>
<td>18:43</td>
<td>58</td>
</tr>
<tr>
<td>01/03/03</td>
<td>15:22</td>
<td>31</td>
</tr>
<tr>
<td>01/03/03</td>
<td>18:31</td>
<td>59</td>
</tr>
<tr>
<td>01/03/03</td>
<td>17:56</td>
<td>31</td>
</tr>
<tr>
<td>01/03/03</td>
<td>17:56</td>
<td>39</td>
</tr>
<tr>
<td>01/03/03</td>
<td>18:21</td>
<td>30</td>
</tr>
<tr>
<td>01/03/03</td>
<td>18:24</td>
<td>16</td>
</tr>
<tr>
<td>01/03/03</td>
<td>18:24</td>
<td>25</td>
</tr>
<tr>
<td>01/03/03</td>
<td>17:53</td>
<td>42</td>
</tr>
<tr>
<td>01/03/03</td>
<td>17:53</td>
<td>28</td>
</tr>
<tr>
<td>01/03/03</td>
<td>15:41</td>
<td>36</td>
</tr>
<tr>
<td>01/05/03</td>
<td>23:31</td>
<td>30</td>
</tr>
<tr>
<td>01/03/03</td>
<td>18:26</td>
<td>19</td>
</tr>
<tr>
<td>01/03/03</td>
<td>18:30</td>
<td>10</td>
</tr>
<tr>
<td>01/03/03</td>
<td>18:30</td>
<td>10</td>
</tr>
<tr>
<td>01/03/03</td>
<td>18:30</td>
<td>53</td>
</tr>
<tr>
<td>01/03/03</td>
<td>18:31</td>
<td>06</td>
</tr>
<tr>
<td>01/03/03</td>
<td>16:06</td>
<td>44</td>
</tr>
<tr>
<td>01/03/03</td>
<td>16:07</td>
<td>23</td>
</tr>
</tbody>
</table>
On 01/08/03 at 9:00 the domain name resolved to the IP address and contained have conducted attacks on computers with the following Internet addresses:

<table>
<thead>
<tr>
<th>IP address</th>
<th>date &amp; time</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>01/05/03 23:32:52 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/05/03 23:34:45 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/05/03 23:30:32 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/05/03 23:46:42 GMT</td>
<td>udp</td>
</tr>
<tr>
<td></td>
<td>01/05/03 23:53:48 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/05/03 23:56:54 GMT</td>
<td>udp</td>
</tr>
<tr>
<td></td>
<td>01/05/03 23:57:12 GMT</td>
<td>udp</td>
</tr>
<tr>
<td></td>
<td>01/05/03 23:45:38 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/05/03 23:56:04 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/05/03 23:57:58 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/05/03 23:57:59 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/05/03 23:59:17 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/06/03 00:01:37 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/03/03 15:50:25 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/03/03 16:02:30 GMT</td>
<td>packet</td>
</tr>
<tr>
<td></td>
<td>01/03/03 16:57:41 GMT</td>
<td>packet</td>
</tr>
</tbody>
</table>
ATTENTION

The following documents appearing in FBI files have been reviewed under the provisions of The Freedom of Information Act (FOIA) (Title 5, United States Code, Section 552), Privacy Act of 1974 (PA) (Title 5, United States Code, Section 552a), and/or Litigation.

<table>
<thead>
<tr>
<th>Requester</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Computer or Case Identification Number</th>
<th>Title of Case</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* File

<table>
<thead>
<tr>
<th>Serial(s) Reviewed</th>
<th>Release Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>*File</td>
</tr>
</tbody>
</table>

This file section has been scanned into the FOIPA Document Processing System (FDPS) prior to National Security Classification review. Please see the documents located in the FDPS for current classification action, if warranted. Direct inquiries about the FDPS to RIDS Service Request Unit, 202-32.  

<table>
<thead>
<tr>
<th>File Number</th>
<th>Serial(s) Reviewed</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>200A-9F-13411-1A</td>
<td>ALL</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FOIPA Requester</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FOIPA Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FOIPA Computer Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>99/994</td>
</tr>
</tbody>
</table>

THIS FORM IS TO BE MAINTAINED AS THE TOP SERIAL OF THE FILE, BUT NOT SERIALIZED

ATTENTION

DO NOT REMOVE FROM FILE
<table>
<thead>
<tr>
<th>SF</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF 1</td>
<td>ORIGINAL NOTES RE INTERVIEW OF [ ]</td>
</tr>
<tr>
<td>SF 2</td>
<td>WEBSITE [ ]</td>
</tr>
<tr>
<td>SF 3</td>
<td>WHO IS ON [ ]</td>
</tr>
<tr>
<td>SF 4</td>
<td>ORIGINAL NOTES RE INTERVIEW OF [ ] ON 1/16/2003</td>
</tr>
<tr>
<td>SF 5</td>
<td>WHO IS [ ]</td>
</tr>
<tr>
<td>SF 6</td>
<td>EMAIL ON 1/8/03</td>
</tr>
<tr>
<td>SF 7</td>
<td>EMAIL 1/16/2003</td>
</tr>
<tr>
<td>SF 8</td>
<td>WEB PAGES ON DISK AND PAPER</td>
</tr>
<tr>
<td>SF 9</td>
<td>WHO IS ON [ ]</td>
</tr>
<tr>
<td>SF 10</td>
<td>FLOPPY DISK CONTAINING EMAIL AND ATTACHMENTS (1-6-2003) (13:30:00)</td>
</tr>
<tr>
<td>SF 11</td>
<td>ORIGINAL NOTES RE INTERVIEW OF [ ]</td>
</tr>
<tr>
<td>SF 12</td>
<td>CD'S OF [ ] MACHINE FROM [ ]</td>
</tr>
<tr>
<td>SF 13</td>
<td>IP SCAN [ ]</td>
</tr>
<tr>
<td>SF 14</td>
<td>IP SCAN [ ]</td>
</tr>
<tr>
<td>SF 15</td>
<td>IP SCAN [ ]</td>
</tr>
<tr>
<td>SF 16</td>
<td>SOURCE EMAILS</td>
</tr>
<tr>
<td>SF 17</td>
<td>EMAIL FROM [ ] WITH BOT ATTACHMENTS</td>
</tr>
<tr>
<td>SF 18</td>
<td>ONE CD ROM CONTAINING IRC LOG [ ]</td>
</tr>
<tr>
<td>SF 19</td>
<td>EMAIL</td>
</tr>
<tr>
<td>SF 20</td>
<td>ONW (1) CDR WITH IRC LOG OF [ ] CHANNEL [ ]</td>
</tr>
<tr>
<td>SF 21</td>
<td>SUBPOENA RETURN</td>
</tr>
<tr>
<td>SF 22</td>
<td>PHOTO ON 3.5&quot; FLOPPY OF [ ] NOTES FROM [ ] PHONE CALL</td>
</tr>
<tr>
<td>SF 23</td>
<td>ORIGINAL NOTES RE INTERVIEW OF [ ]</td>
</tr>
<tr>
<td>SF 24</td>
<td>ORIGINAL NOTES RE INTERVIEW OF [ ]</td>
</tr>
</tbody>
</table>
Universal Case File Number  288A-SF-133411

Field Office Acquiring Evidence  HAYWARD

Serial # of Originating Document

Date Received  1-3-2003

From

(Name of Contributor)

(Address of Contributor)

(City and State)

By

To Be Returned  No

Receipt Given  No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure  No

Federal Taxpayer Information (FTI)  No

Title: UNSUB(s); GOOGLE - VICTIM
SUNNYVALE, CA
NIPE - IMPERTINENCE

Reference: FD-302 DATED 1-3-2003

(Communication Enclosing Material)

Description: Original notes re interview of

288A-SF-133411"
1-3-03

1) 9:23 a.m.
   (google)
   microbial threat

2) 10:00 a.m.
   google security
   b7c
   detected attacks on google
   for 11:00 PST on 1-2-03 attack
   google checked logs noticed
   2-7 mm (UDP flood) ping flood
   included > 4,000 hosts distributed
   network handled traffic close to fail

later afternoon, before 3p PST
   hit again, syn flood
   largescale, global effect on network
   lost of 3 incoming searches affected
   5-2 mm
   said IRC server host failed
   'locked reconnection'
   (the time attack hit
   assume it's the same person (google)
   - global threat - name from 10 or early
   commands issued to
   - global threat - at one point affiliated
   with
Servers attacked - Santa Clara, Virginia
1. - Santa Clara only
2. - Both

Google checking logs for IP spoofing
Most of bots live on /class 'A'

Uses changes of a target

Damages - working numbers (def $5,000)
Universal Case File Number: 2881A-SF-133411

Field Office Acquiring Evidence: HAYWARD

Serial # of Originating Document: ____________________________

Date Received: 1/16/2003

From: ____________________________

(Name of Contributor)

(Address of Contributor)

(City and State)

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

Federal Taxpayer Information (FTI): ☐ Yes ☑ No

Title: 1 UNSUB(S);

GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment

01/02/2003

Reference: 1 FD-302 116703

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

WEB SITE

2881A-SF-133411-1A(2)
You are an unregistered user. Please register, it's FREE! thanks. registering offers many enhancements, including customizable themes, headlines, webmail etc. So check it out!

IRCd Up!

Thanks!

Update!

Own a shell/webhosting provider now! Cheap, High Quality shell's, Hosting: bots, websites, IRCd's, and more! We will also custom build shells for you for any type of hosting you can think of! It is the solution for your hosting needs!
Membership:
- Latest: 
- New Today: 0
- New Yesterday: 0
- Overall: **16**

People Online:
- Visitors: 3
- Members: 0
- Total: 3

Hits

We received **3255** page views since November 18, 02
The IRC Bot related forum

![phpBB Logo]

- FAQ
- Search
- Memberlist
- Usergroups
- Register
- Profile
- Login to check your private messages

Login to check your private messages

The time now is Wed Jan 15, 2003 5:22 pm

### Forum Index

<table>
<thead>
<tr>
<th>Forum</th>
<th>Topics</th>
<th>Posts</th>
<th>Last Post</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bots</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Bot Talk</td>
<td>1</td>
<td>1</td>
<td>Wed Nov 20, 2002 2:53 pm</td>
</tr>
<tr>
<td>Talk generally about IRC bot's, zombies, drones. this is NOT a trading channel, to trade visit the bot trading section. Thanks.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dedicated forum</td>
<td>2</td>
<td>3</td>
<td>Wed Dec 04, 2002 5:27 am</td>
</tr>
<tr>
<td>Forum dedicated to get your own forum on for your own bot, drop a privmsg to and it will be promptly added.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Mark all forums read

All times are GMT

### Who is Online

- Our users have posted a total of 4 articles
- We have 4 registered users
- The newest registered user is
- In total there is 1 user online :: 0 Registered, 0 Hidden and 1 Guest
- Most users ever online was 2 on Tue Nov 19, 2002 1:37 am
- Registered Users: None

This data is based on users active over the past five minutes

### Login

Login to check your private messages

Username: Password: Log me on automatically each visit

- New posts
- No new posts
- Forum is locked

Powered by phpBB 2.0.3 © 2001, 2002 phpBB Group

http: 1/15/2003
<table>
<thead>
<tr>
<th>#</th>
<th>Username</th>
<th>Email</th>
<th>Location</th>
<th>Joined</th>
<th>Posts</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>19 Nov 2002</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td>20 Nov 2002</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td>26 Nov 2002</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>01 Dec 2002</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
when i come here like 10 days ago...

when i come here 10 days ago... i see the info of new version of pos.tt, wp ... and i see something like psybnc... feature.... is this real? and... is possible to implement in next versions? thanks..

anybody here have the manual

Display posts from previous: [All Posts] [Oldest First] [Go]

Page 1 of 1

You can post new topics in this forum
You can reply to topics in this forum
You cannot edit your posts in this forum
You cannot delete your posts in this forum
You cannot vote in polls in this forum

Powered by phpBB 2. 0.36 2001, 2002 phpBB Group

http://viewtopic.php?t=3&highlight=i%2A&sid=e1cd606ae112905e861da346bf... 1/15/2003
where is it???

Guest

when r u gonna have it up for download? if u cant find a place to host it just host it and ask for pass until u can find a better place
You are an unregistered user. Please register, it's FREE! Registering offers many enhancements, including customizable themes, headlines, webmail, etc. So check it out!

IRCd Up!

If it doesn't resolve, use ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ________ ----
Universal Case File Number: 288A-SF-133411

Field Office Acquiring Evidence: HAYWARD

Serial # of Originating Document:

Date Received: 1-16-2003

From ________________________________

(Name of Contributor)

(Address of Contributor)

(City and State)

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

Federal Taxpayer Information (FTI) ☐ Yes ☐ No

Title: UNSUBJ

GOOGLE.COM - VICTIM

Reference: FD-302 DATEQ 1/1/03

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

WHO IS ON

288A-SF-133411-14(3)
This is a PAIDDOMAIN.TK domain name. On this domain name the PAIDDOMAIN.TK terms and conditions apply.

The registrant of this domain name is:

- Company
- Name
- Address
- Postal code/zip code
- City
- State
- Country
- Phone number
- Fax number
- Email address
- Name servers

WHOIS search on another domain name

www.________.tk

CONTINUE >>
Universal Case File Number: 288A-SF-133411

Field Office Acquiring Evidence: AWARD

Serial # of Originating Document:

Date Received: 1/16/2003

From: (Name of Contributor)

(Address of Contributor)

(City and State)

By: SA

To Be Returned: ☐ Yes ☑ No

Receipt Given: ☐ Yes ☑ No

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

☐ Yes ☑ No

Federal Taxpayer Information (FTI):

☐ Yes ☑ No

Title: UNSUB(S);
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003

Reference: FD-302 1/16/03

(Communication Enclosing Material)

Original notes re interview of

Description:

288A-SF-133411-1A(4)
been with Google for (month)

Logs unclear

Work with [ ] on loss estimate

for many years

b7c
Universal Case File Number: Z881A-SF-133411

Field Office Acquiring Evidence: HAYWARD

Serial # of Originating Document

Date Received: 1-16-2003

From

(Name of Contributor)

(Address of Contributor)

(City and State)

By

To Be Returned

Receipt Given

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

Federal Taxpayer Information (FTI)

Title: UNSUBS:

GOOGLE.COM - VICTIM

Reference: FD-302 DATED 1/8/03

(Communication Enclosing Material)

Description:

Original notes re interview of

WHOIS ON

288-SF-133411 - 14 (S)
WHOIS

Selected domain name

This is a PAIDDOMAIN.TK domain name. On this domain name the
PAIDDOMAIN.TK terms and conditions apply.

The registrant of this domain name is:

Company
Name
Address
Postal code/zipcode
City
State
Country
Phone number
Fax number
Email address
Name servers

WHOIS search on another domain name

WWW.

CONTINUE >>
Universal Case File Number: 288A-SF-133411
Field Office Acquiring Evidence: HAYWARD
Serial # of Originating Document:
Date Received: 1-11-2003
From: S [Name of Contributor]
(Address of Contributor)
(City and State)
By: S [Name of Contributor]

To Be Returned: [ ] Yes [ ] No
Receipt Given: [ ] Yes [ ] No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure: [ ] Yes [ ] No
Federal Taxpayer Information (FTI): [ ] Yes [ ] No
Title: UNSUB(S);
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003
Reference: FD-302 1/16/03
(Communication Enclosing Material)

Description: [ ] Original notes re interview of
MAIL ON 1/8/03

288A-SF-133411-126
From: 
To: 
cc: 
Date: Wed, January 08, 2003, 16:20:00
Subject: Interesting URLs

As I promised in our earlier phone conversation, here are a few web pages that seem to refer to [redacted] or his associates. I'm afraid that they don't look particularly promising.

However, one of our engineers, through a friend-of-a-friend sort of chain, came up with a name, address, and phone number for [redacted]

I have a meeting tomorrow evening to discuss what information in our logs we can provide. I'll contact you on Friday about this.

Sincerely,

[redacted]

Information Security Officer

Google, Inc. 2400 Bayshore Parkway, Mountain View, CA 94043
Phone: [redacted] Fax: [redacted]
Universal Case File Number: 288A-SF-133411

Field Office Acquiring Evidence: HAYWARD

Serial # of Originating Document:

Date Received: 1-16-2003

From:

(Name of Contributor)

(Address of Contributor)

(City and State)

By: SA

To Be Returned: □ Yes □ No

Receipt Given: □ Yes □ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6(e)

Federal Rules of Criminal Procedure:

□ Yes □ No

Federal Taxpayer Information (FTI):

□ Yes □ No

Title: UNSUB(S);

GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003

Reference:

FDB02 1/16/03

(Communication Enclosing Material)

Description:

□ Original notes re interview of

EMAIL 1/16/03

288A-SF 133411-14(7)
Below are the incident notes I took:

National Wildlife Refuge.

I'm making a copy of the Ghosted image to send you right now. Let me know if you need anything else.

NCC Security Response Team

NOTES:
1/6/03 9am

- Called FBI agent (Chicago) back regarding voice mail (8am) he left.

Notes from FBI conversation:
- FBI Case#288a-sf-13341 out of San Fran
- Victim IP
- Exploit: Open shares bot affecting WIN2k machines without admin passwords
- IP first joined IRC channel on Jan3rd 2003, 8:14:29pm GMT (1:14:29 MST), look in logs for IP acquired around that time
- Check for listening on ports and talking of
- Possibly being used as an attack platform in network.
- I sent note to and regarding event as FYI.
- Called and left voice mail regarding event.
- Went through logs and found IP assigned to userid during that time.
- Copies of relevant log events:
  - Jan-03-2003 13:13:29 Accounting start record for use
  - start_time=1041624777, timezone=MST, service=ppp
  - Jan-03-2003 13:47:40 Accounting stop record for use
  - start_time=1041624777, timezone=MST, service=nnc, protocol=udp
  
- Filled out Incident Response Form and sent to and CCed for her to make initial contact with to brief him on the incident.
- Called FBI, to inform him we found the victim and received directions from him on what to look for, ie,
  - Called and informed him that his machine has been hacked and gave him directions to back up his sensitive data and send machine (just the box) to me at the NCC in Denver. I requested he do nothing to any other files except back up his important ones and that we need the machine for further forensic analysis and will have it for an estimated 4 weeks.

1/8/03
7am- Sent note to [ ], informing him we should be getting the box this week.

10am Received the box: Gateway E Series, WIN2k-SP3, Intel P4, 2.0 GHz, 524 Megs RAM
Computer name [ ]
no modem (must be external, I called and confirmed attached to an external modem)
no admin password
NO mirc.ini file (been removed by [ ])

Malware files - C:\WINNT\system32\dhcp

Malware services running:
FireDaemon Service: [ ] Automatic
Serv-U FTP Server [ ] Automatic

Website explaining the attack in detail - [ ]

1/9 - Called [ ] back at FBI and he said someone from San Fran office will be calling me about the box.

1/10 - Ghosted image to network. 1.9 gigs.

1/13- Burned image to 3 CDs and removed image from network server. I had an e-image machine with WIN2000 Pro and give it an admin password. Will send machine back to [ ] when re-image is complete.

1/16- Sent box back to [ ] in South Dakota.
Subject: Attention- Agent (FWS incident 01/06/03)
Universal Case File Number 288A-SF-133411

Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document

Date Received 1-16-2003

From

(Name of Contributor)

(Address of Contributor)

(City and State)

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

Federal Taxpayer Information (FTI)

□ Yes  □ No

Title:

Reference: FD-302 DA760 1-16-2003

(Communication Enclosing Material)

Description: □ Original notes re interview of b7C

WEB PAGES ON DISK+PAPER

288A-SF-133411-10(8)
You can contact me or ___________and/or___________via_________channel

You can also contact me at Contact Me

I am also contactable via telephone, but it is NOT recommended unless it's very urgent, but I can be contacted at ___________. Some phone restrictions may apply, you are responsible for the long-distance telephone bill, not me.

For sales inquiries contact Sales Department
For support please either visit ___________or ___________ for email Support Department

http://Contact.htm 1/15/2003
Contact us

You can contact me on [contact channel] or email [contact me via email]. I am also contactable via telephone, but it is NOT recommended unless it is very urgent, and I can be contacted at [contact telephone]. Some phone restrictions may apply, you are responsible for the long-distance telephone bill, not me.

For sales inquiries, contact the Sales Department at [sales email]. For support please either visit [support website] or email [support email].
About

is owned and maintained by and his friends. He can be reached on

I can be reached by phone at

Their’s more of a chance you will get helped in either the chatroom(s) or email me at the contact link on the menubar of this site. Thanks.

is here to give you the best prices for the best products we can give! NOTE: We dont get much profit out of this, we charge what it COSTS to keep it running. no more. and theirs many sales, reductions available, lets say you referr some people, you will get a discount, or have money refunded back through our merchant system.

is here to give you quality services, we do not supply you with "public" Vhost's, or anything like that. You can get "private" vhosts for your self like: yourname but not stuff like i.am.a.leet.mof we ONLY accept 1 subdomain on the reverse DNS, sorry!

As far as webhosting goes, we only limit you on space, we do not limit your email accounts, parked domains, subdomains or anything! and cPanel is a professional package, which allows easy usage of your webhosting package! you will enjoy it immensely! one click and you can have ecommerce, one click and you can have phpnuke, and much, much more!

http://yoursite.com/about.htm

1/15/2003
Universal Case File Number: 288A-SF-133411

Field Office Acquiring Evidence: HAYWARD

Serial # of Originating Document: ______________________________

Date Received: 1-16-2003

From: ______________________________

(Name of Contributor)

(Address of Contributor)

(City and State)

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

Federal Taxpayer Information (FTI): □ Yes □ No

Title: UNSUB.

GOOGLE.COM - VICTIM

Reference: INSERT DATED 1-16-03

(Communication Enclosing Material)

Description: □ Original notes re interview of

WHOIS ON

288A-SF-133411 - IA(9)
The data in The .tv Corp. whois database is provided by The .tv Corp. to assist persons in obtaining information about or related to a domain name registration record. .tv does not guarantee its accuracy. By submitting a whois query, you agree that you will use this data only for lawful purposes and that, under no circumstances, will you use this data to allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail (spam). The .tv Corp. reserves the right to modify this policy at any time.
WHOIS Search Results

WHOIS Record for

Back-order this name Make an unsolicited offer

Registrar:

Domain Name

Administrative Contact:

Technical Contact:
VeriSign, Inc. (HOST-ORG)
VeriSign, Inc.
21355 Ridgetop Circle
Dulles, VA 20166
US
1-888-642-9675
namehost@WORLDNIC.NET

Record expires on 04-Feb-2011.
Record created on 06-Feb-2001.
Database last updated on 14-Jan-2003 16:17:01 EST.

Search the Web with Dogpile

NOTICE AND TERMS OF USE: You are not authorized to access or query our WHOIS database through the use of high-volume, automated, electronic processes. The Data in Network Solutions' WHOIS database is provided by Network Solutions for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. Network Solutions does not guarantee its accuracy. By submitting a WHOIS query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to Network Solutions (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of Network Solutions. You agree not to use high-volume, automated, electronic processes to access or query the WHOIS database. Network Solutions reserves the right to terminate your access to the WHOIS database in its sole discretion, including without limitation, for excessive querying of the WHOIS database or for failure to otherwise abide by this policy. Network Solutions reserves the right to modify these terms at any time.

http://www.networksolutions.com/cgi-bin/whois/whois?STRING=&SearchType=do 1/14/2003
Universal Case File Number 288A - SF - 133411

Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document

Date Received 1-6-2003

From

(Name of Contributor)

(Address of Contributor) CHICAGO, IL

(City and State)

By SA

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure ☐ Yes ☑ No

Federal Taxpayer Information (FTI) ☐ Yes ☑ No

Title: UNSUB(S):
 GOOGLE - VICTIM
 SUNNYVALE, CA
 NPC - IMPAIRMENT
 11/2/2003

Reference: FD-302 DA760 1-6-2003 (Communication Enclosing Material)

Social 24

Description: ☐ Original notes re interview of

FLOPPY DISK CONTAINING EMAIL AND ATTACHMENTS (1-6-2003, 13:30:00)
Universal Case File Number 288A-SF-133411

Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document

Date Received 1-8-2003

From

(Name of Contributor)

(Address of Contributor)

(City and State)

By SA

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure ☐ Yes ☒ No

Federal Taxpayer Information (FTI) ☐ Yes ☒ No

Title: UNSUB(s);
GOOGLE - VICTIM
SUNNYVALE, CA
MPM - IMPAIRMENT
01/02/2003

Reference: FD-302 DATED 1-8-2003 (Communication Enclosing Material)

Social 25

Description: ☐ Original notes re interview of

288A-SF-133411-14(11)
1-7-03

b7c

(0)

(4)

b7c

DATE ADDRESS

2:17p

Range

b7d

Bob found research of one IP connected 3
times during day, links back to

AM

Spike of incoming traffic corresponds to due
of commands on IRC channel

PM - same

Attack in AM indicates

Starting to

Should have

2:29p
Universal Case File Number: 288A-SF-133411
Field Office Acquiring Evidence: HAYWARD
Serial # of Originating Document:
Date Received: 1/21/03
From:

(City and State)

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
Federal Taxpayer Information (FTI): ☐ Yes ☑ No
Title:

GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment

Reference: (Communication Enclosing Material)

Description: ☉ Original notes re interview of

288A-SF-133411-14(A)
**Domain Info**

Here you can get information about the selected domain. The query result includes owner name, contacts and other useful information. The query works with com/net/org (ICANN and CORE) as well as gov, mil, edu and most of the two letter country DNS zones (like co.uk or ru).

Tips:

- Type an IP address instead of the domain name for the reverse query or go to the "Reverse IP Lookup" for more information about a host with known IP address.
- If you are not certain about the name of the site, use DNS search screen to find it. It includes search by separate parts, fuzzy search, similar to a spellchecker and other powerful features. After you find the name, follow the (i) link to see information from this page.

<table>
<thead>
<tr>
<th>Domain Info</th>
<th>Domain Search</th>
<th>Register.com</th>
<th>Reverse IP Lookup</th>
<th>Trace Route</th>
<th>Hot Topics</th>
<th>Home Contacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>eAmnesia.com</td>
<td>The Domain Name Search Engine™</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IP Information**

Reverse IP Lookup

This is the powerful tool to find information about an Internet host by its IP address. The result includes information about owner of the IP address, its DNS name(s) and so on. The lookup works against any IP address on the Internet. This utility is much more powerful, then reverse IP lookup.

Just in case, IP address looks like four numbers, separated by dots (For example 192.168.12.34) If you have one long number (like 132468197), type or copy/paste it in the field for the whole address and press "Convert" button to translate it to canonical form.

Tips:

- Use the "whole address" field if you want to copy/paste the IP address from the clipboard.
- While entering IP address into separate fields, type dot on the keyboard to jump to the next fields. Unfortunately it does not work on every version of the browser.

Result of the Reverse Lookup

WHOIS Query Result for

OrgName: 
OrgID: 
NetRange: 
CIDR: 
NetName: 
NetHandle: 
Parent: 
NetType: 
NameServer: 
NameServer: 
Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate: 2002-05-31
Updated: 2002-05-31
TechHandle: ZMA1-ARIN
TechName: 

AMNESI the Domain Name Search Engine. Reverse IP lookup finds info for any IP addr...

# ARIN Whois database, last updated 2003-01-22 20:00
# Enter ? for additional hints on searching ARIN's Whois database.

Universal Case File Number: 288A-SF-133411
Field Office Acquiring Evidence: HAYWARD
Serial # of Originating Document:
Date Received: 1/23/03
From:
(Name of Contributor)
(Address of Contributor)
(City and State)
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
Federal Taxpayer Information (FTI): Yes/No
Title:
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003
Reference: FY302 1/23/03
(Communication Enclosing Material)
Description:
Original notes re interview of

288A <SF-133> 411 - 10(4)
Domain Info

Here you can get information about the selected domain. The query result includes owner name, contacts and other useful information. The query works with com/net/org (ICANN and CORE) as well as gov, mil, edu and most of the two letter country DNS zones (like co.uk or ru).

Tips:

- Type an IP address instead of the domain name for the reverse query or go to the "Reverse IP Lookup" for more information about a host with known IP address.
- If you are not certain about the name of the site, use DNS search screen to find it. It includes search by separate parts, fuzzy search, similar to a spellchecker and other powerful features. After you find the name, follow the (i) link to see information from this page.

IP Information

Would you rather have
WWW.THISWASTHEONLYNAMELEFT.COM...
Reverse IP Lookup

This is the powerful tool to find information about an Internet host by its IP address. The result includes information about owner of the IP address, its DNS name(s) and so on. The lookup works against any IP address on the Internet. This utility is much more powerful, then reverse IP lookup.

Just in case, IP address looks like four numbers, separated by dots (For example 192.168.12.34) If you have one long number (like 132468197), type or copy/paste it in the field for the whole address and press "Convert" button to translate it to canonical form.

Tips:

- Use the "whole address" field if you want to copy/paste the IP address from the clipboard.
- While entering IP address into separate fields, type dot on the keyboard to jump to the next fields.
  Unfortunately it does not work on every version of the browser.

Result of the Reverse Lookup

<table>
<thead>
<tr>
<th>IP address</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

WHOIS Query Result for

*OrgName:* 

*OrgID:* 

*NetRange:* 

*CIDR:* 

*NetName:* 

*NetHandle:* 

*Parent:* 

*NetType:* Direct Allocation

*NameServer:* 

*Comment:* ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

*RegDate:* 1999-09-14

*Updated:* 2001-01-04

*TechHandle:* 

*TechName:* Network Administrator, CyberGate
TechPhone:  
TechEmail:  

# ARIN Whois database, last updated 2003-01-22 20:00
# Enter ? for additional hints on searching ARIN's Whois database.
Contact Us
Your questions and comments are important to us.

Shared Hosting

Call Me Back
Never wait on hold again! Have a representative call you. (Available in over 190 countries.)
• Sales 24 hours a day, 7 days a week
• Technical Support 7 days a week, 24 hours a day.
• Customer Service Mon - Fri, 9am - 10pm ET

Search our Solution Database
A database of customers' most Frequently Asked Questions (FAQs), arranged by popularity and searchable by keyword.

Let’s Chat
Chat online with a representative.
• Sales Mon - Fri, 8am - 9pm ET
• Technical Support 7 days a week, 9am - 10pm ET
• Customer Service Mon - Fri, 9am - 5:30pm ET

Email Your Question
If you don't find your answer in the Solution Database, email your question and we'll provide a detailed response within 24 hours.

Contact Us By Phone:

Sales
Sales Numbers:
1-800-WE-HOST-U
800.934.6788
954.334.3871

International Toll Free Sales Numbers:
UK 00-800-7888-7888
Germany 0 0-800-7888-7888
Ireland 0 0-800-7888-7888
New Zealand 0 0-800-7888-7888
Australia 0 011-800-7888-7888
Japan 0 061-800-7888-7888 IDC
001-800-7888-7888 KDD
0041-800-7888-7888 ITJ

Tech Support
Technical Support Hours:
24 hours / day - 7 days / week

Technical Support Numbers:
800.522.1093
954.334.3449

Customer Service
Customer Service Hours:
Monday - Friday: 9am - 10pm ET
Saturday - Sunday: Closed

Customer Service Numbers:
800.522.1093
954.334.3449

Dedicated Hosting

Let’s Chat
Chat online with a representative.
• Sales 24 hours a day, 7 days a week

Access Support
Email us support-related inquiries, search solution database, manage your account.

Contact Us By Phone:

Sales
Sales Hours:

Customer Service
Customer Service Hours:
Contact Us

24 hours / day - 7 days / week

Sales Numbers:
888.846.5522
954.334.8333 (US & International)
Fax 954.334.8005

Tech Support
Technical Support Hours:
24 hours / day - 7 days / week

Technical Support Numbers:
888.846.5522
954.334.8333 (US & International)

Corporate Headquarters

Corporate Headquarters
Address:
3250 W. Commercial Blvd.
Ft. Lauderdale, FL 33309

Phone Number
954.334.8000

FAX Number:
954.334.8001

Monday - Friday: 9am - 5pm ET
Saturday - Sunday: Closed

Customer Service Numbers:
888.846.5522
954.334.8333 (US & International)

TERMS AND POLICIES | COPYRIGHT @2002 AFFINITY INTERNET INC.
Universal Case File Number: 2884-SF-133411

Field Office Acquiring Evidence: HAYWARD

Serial # of Originating Document: 

Date Received: 1/23/03

From: 

(Name of Contributor)

(Address of Contributor)

(City and State)

By: 

(Signed) b7c

To Be Returned: □ Yes □ No

Receipt Given: □ Yes □ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure: □ Yes □ No

Federal Taxpayer Information (FTI): □ Yes □ No

Title: GOOGLE - VICTIM SUNNYVALE, CA NIPC - Impairment 01/02/2003

Reference: FD-302 1/23/03

(Communication Enclosing Material)

Description: □ Original notes re interview of

 b7c

Reference: 2884-SF-133411 1/23/03
Domain Info

Here you can get information about the selected domain. The query result includes owner name, contacts and other useful information. The query works with com/net/org (ICANN and CORE) as well as gov, mil, edu and most of the two letter country DNS zones (like co.uk or ru).

Tips:

- Type an IP address instead of the domain name for the reverse query or go to the "Reverse IP Lookup" for more information about a host with known IP address.
- If you are not certain about the name of the site, use DNS search screen to find it. It includes search by separate parts, fuzzy search, similar to a spellchecker and other powerful features. After you find the name, follow the (i) link to see information from this page.

Domain Name: [adomain.com]
Reverse IP Lookup

This is the powerful tool to find information about an Internet host by its IP address. The result includes information about owner of the IP address, its DNS name(s) and so on. The lookup works against any IP address on the Internet. This utility is much more powerful, then reverse IP lookup.

Just in case, IP address looks like four numbers, separated by dots (For example 192.168.12.34) If you have one long number (like 132468197), type or copy/paste it in the field for the whole address and press "Convert" button to translate it to canonical form.

Tips:

- Use the "whole address" field if you want to copy/paste the IP address from the clipboard.
- While entering IP address into separate fields, type dot on the keyboard to jump to the next fields. Unfortunately it does not work on every version of the browser.

Result of the Reverse Lookup

<table>
<thead>
<tr>
<th>IP address</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>b7C</td>
</tr>
</tbody>
</table>

WHOIS Query Result for

OrgName: One Call Communications
OrgID: OCCI
NetRange: Direct Allocation
CIDR: 
NetName: 
NetHandle: 
Parent: 
NetType: Direct Allocation
NameServer: 
NameServer: 
Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate: 2002-01-30
Updated: 2002-10-16
NOCHandle: TECHN2-ARIN
NOCName: Technical Contact
NOCPhone: +1-888-223-8633
NOCEmail: noc@onecall.net
NOCHandle: DNSTE-ARIN
NOCName: DNS Technical
NOCEmail: dnstech@onecall.net
TechHandle: TW66-ARIN
TechName:
TechPhone
TechEmail

# ARIN Whois database, last updated 2003-01-22 20:00.
# Enter ? for additional hints on searching ARIN's Whois database.
OCI Contacts

General Comments    webmaster@onecall.net
Technical Sales       888-223-8633 9-5 EST Mon-Fri
techsale@onecall.net
Security/UCE Complaints/Questions
Acceptable Use Policy (AUP)
Complaint Guidelines (please read) abuse@onecall.net
NAP/MAE Peering Ops peering@onecall.net
NOC Technical Support 888-223-8633 24x7x365
noc@onecall.net

Billing Inquiries 866-223-8633 9-5 EST Mon-Fri

http://www.onecall.net/contact.html
Universal Case File Number 288A-SF-133411
Field Office Acquiring Evidence Chicago
Serial # of Originating Document
Date Received 1/8/03
From SOURCE
(Name of Contributor)
(Address of Contributor)
(City and State)
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
Federal Taxpayer Information (FTI)
□ Yes □ No
Title: UNSUB(j)
GOOGLE-VICTIM
SUNNYVALE, CA
NPPC IMPAIRMENT
Reference: EC 1/8/03
(Communication Enclosing Material)
Serial 20
Description: □ Original notes re interview of
SOURCE EMAIL

288A-SF-133411-1A (16)
Universal Case File Number  288A-SF-133411

Field Office Acquiring Evidence  HA-YUMO

Serial # of Originating Document

Date Received  1-31-03

From  
(Name of Contributor)

(Address of Contributor)

(City and State)

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

Federal Taxpayer Information (FTI)

Title: GOOGLE – VICTIM SUNNYVALE, CA NIPC – Impairment

Reference:  FD-302 DA-750  1-31-03, (Communication Enclosing Material)

Description:  □ Original notes re interview of

EMAIL FROM WITH

BOT ATTACHMENTS

288A-SF-133411-14 (17)
Field File No. 288A - SF - 133411
Serial # of Originating Document
OO and File No.
Date Received 1/10/03
From SOURCE (Name of Contributor)
(Address of Contributor)

By (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: UNSUBC
GOOGLE VICTIM
SUNNYVALE, CA
NIPC - IMPAIRMENT

Reference: (Communication Enclosing Material)

Description: ☑ Original notes re interview of

1 CD-12 containing NIC log

288A - SF - 133411 - IA(8)
Universal Case File Number 288A-SF-133411
Field Office Acquiring Evidence HAYWARD
Serial # of Originating Document
Date Received 2/13/03
From
(Name of Contributor) GOOGLE
(Address of Contributor)

(City and State)

By SA

To Be Returned ☐ Yes ☐ No
Receipt Given ☐ Yes ☐ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6(e) Federal Rules of Criminal Procedure ☐ Yes ☐ No
Federal Taxpayer Information (FTI) ☐ Yes ☒ No

Title: GOOGLE - VICTIM SUNNYVALE, CA NIPC - Impairment
Reference: F03022 2/13/03 (Communication Enclosing Material)

Description: ☐ Original notes re interview of 

288A-SF 12/24/11 12/20/09
Attached is the estimate of our damages from the January 2 denial of service attack. As I mentioned we have experienced additional attacks since then and would like to report the details to you as soon as possible. Can you let me know when you might be able to visit?

Regards

ddos_damages.doc
To: FBI
From: [Insert Name] VP and General Counsel, Google

Per our conversation the other day, the following is our preliminary estimate of the economic loss Google suffered from the distributed denial of service attacks that took place on January 2, 2003:

1. Lost Revenue. The attacks caused us to lose search queries that would otherwise have been performed on our and our partners’ sites. We generate revenue from these queries through our various advertising programs. We estimate these losses at approximately $5,000.

2. Potential Liability to Search Partners: The loss of queries on certain of our partners’ sites may subject us to penalties under the service level agreements with those partners. We estimate these losses at approximately $40,000.

3. Employee and Management Time. Our operations employees, certain engineers and our management team spent a significant amount of time responding to the attacks and managing relations with our customers and others. We estimate these losses at approximately $4,500.

Please note that these are preliminary estimates that may increase as we continue our investigation. Please do not hesitate to contact me if you have any questions. I can be reached at [Insert Contact Information].
Universal Case File Number 288A-SE-133411

Field Office Acquiring Evidence Chicago

Serial # of Originating Document

Date Received 02/20/03

From SOURCE

(Name of Contributor)

(Address of Contributor)

(City and State)

By SA

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure ☐ Yes ☑ No

Federal Taxpayer Information (FTI) ☑ Yes ☐ No

Title: Google - Victim

Sunnydale, CA

NIPC - Impassant

Reference: EC 92103, Serial 46

Communication Enclosing Material

Description: ☑ Original notes re interview of

Original code withDecoration

channel

288A-SE-133411-1400)
Universal Case File Number: 288A-SF-133411
Field Office Acquiring Evidence: Hayward
Serial # of Originating Document: 33

Date Received: [b3 Rule 6(e)]
From: [Name of Contributor]

To Be Returned: [No]
Receipt Given: [Yes]
Grand Jury Material - Disseminate Only Pursuant to Rule 6(e)
Federal Rules of Criminal Procedure: [Yes]
Federal Taxpayer Information (FTI): [No]

Title: GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment

Reference: SBEA 33

Description: Original notes re interview of
SUB PO SSA 2005051022 288A-SF-133411 - 14(21)
Universal Case File Number 288A-SF-13341

Field Office Acquiring Evidence HAYWARD

Serial # of Originating Document

Date Received 4/16/2003

From (Name of Contributor)

DELAVARE S.P.

(Address of Contributor)

(City and State)

By (Name of Contributor)

To Be Returned □ Yes □ No

Receipt Given □ Yes □ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure □ Yes □ No

Federal Taxpayer Information (FTI) □ Yes □ No

Title: GOOGLE - VICTIM

SUNNYVALE, CA

NIPC - Impairment

Reference: FD-302 4/16/03

(Communication Enclosing Material)

Description: □ Original notes re interview of PHOTO ON 3.5" FLOPPY OF

NOTES FROM PHONE CALL

FAX OF ITEM SEIZED

NOTES FROM AN

APP + ARC
Here are the documents you requested. I gave a copy of the search/arrest warrants as well as my report. I will forward the tape and a CD with Digital images as soon as I can get them packed up.
<table>
<thead>
<tr>
<th>Item</th>
<th>Location Searched</th>
<th>Date</th>
<th>Time</th>
<th>Description of Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>12:31</td>
<td>Wirespeed Box w/powercord &amp; cable, Model</td>
</tr>
<tr>
<td>2</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>12:35</td>
<td>Linksys DSL Router w/ 2 CAT5 cables attached for</td>
</tr>
<tr>
<td>3</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>12:41</td>
<td>IBM Black Mouse Model</td>
</tr>
<tr>
<td>4</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>12:44</td>
<td>(11) Compact Disk-Recordable (CD-R) from top of Dell Computer</td>
</tr>
<tr>
<td>5</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>12:54</td>
<td>Misc Cable &amp; Mic, gray USB cable, Sharp PDA cradle w/power cord, Powered USB Hub</td>
</tr>
<tr>
<td>6</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>12:56</td>
<td>Dell Tower Power Cord</td>
</tr>
<tr>
<td>7</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>12:56</td>
<td>(2) Dell Speakers w/ power supply and connection cables</td>
</tr>
<tr>
<td>8</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>12:56</td>
<td>Dell Tower Computer Dimension 4500 Model D9M SN running Windows XP</td>
</tr>
<tr>
<td>9</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>13:04</td>
<td>I-Box (for mini tower S/N) Running Linux</td>
</tr>
<tr>
<td>10</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>13:05</td>
<td>NEC Monitor S/N Running Linux</td>
</tr>
<tr>
<td>11</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>13:04</td>
<td>Monthly Billing Statement from w/ Defendant's Address, (1) PNC MAC receipt</td>
</tr>
<tr>
<td>12</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>13:14</td>
<td>Silver Optical Mouse Model</td>
</tr>
<tr>
<td>14</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>13:15</td>
<td>Aiptek VGA Digital Camera w/ gray case (SJ</td>
</tr>
<tr>
<td>15</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>13:30</td>
<td>(14) Compact Disk-Recordable (CD-R), (2) Mini Compact Disk-Recordable (CD-R), (1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Plastic Jewel Case</td>
</tr>
<tr>
<td>16</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>13:30</td>
<td>Bundle of Numerous Compact Disk-Recordable (CD-R)</td>
</tr>
<tr>
<td>17</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>13:32</td>
<td>Financial Papers, Tax Papers, Business License all for</td>
</tr>
<tr>
<td>18</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>13:39</td>
<td>Fax cover sheet w/email address</td>
</tr>
<tr>
<td>19</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>13:40</td>
<td>(2) Money Mover debit cards w/defendant's name on it and the Card Holder Agreement</td>
</tr>
<tr>
<td>20</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>13:46</td>
<td>Dell Monitor w/power cord and cable, Model</td>
</tr>
<tr>
<td>21</td>
<td>Computer Desk</td>
<td>04/15/2003</td>
<td>13:46</td>
<td>Lexmark Printer/Fax/Copier model X83 w/ PNC check #</td>
</tr>
<tr>
<td>22</td>
<td>Kitchen Counter</td>
<td>04/15/2003</td>
<td>13:49</td>
<td>Gray CD case with numerous Compact Disks</td>
</tr>
<tr>
<td>24</td>
<td>Kitchen Counter</td>
<td>04/15/2003</td>
<td>13:49</td>
<td>(5) Compact Disk-Recordable, (3) Mini Compact Disk-Recordable</td>
</tr>
<tr>
<td>25</td>
<td>Kitchen Counter</td>
<td>04/15/2003</td>
<td>13:49</td>
<td>Vivitar Digital Camera w/ gray case S/N</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(1) Smart Card reader &amp; USB T-100 Pack</td>
</tr>
</tbody>
</table>

Investigating Officer: DSP Troop 4

Delaware State Police
Search Warrant Seized Property Inventory

Date: 04/15/2003
<table>
<thead>
<tr>
<th>Item</th>
<th>Location Seized</th>
<th>Date</th>
<th>Description of Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>Kitchen Counter</td>
<td>04/15/2003</td>
<td>Linksys DSL Router Manual, Dell Computer Account Information, Money Order Receipt,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Unauthorized Credit Card Transaction Paperwork, Fedex Envelope &amp; receipt, Various</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>County Bank Papers, PNC Bank papers, Sharp &quot;Personal Digital Assistant (PDA)&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ethernet adapter.</td>
</tr>
<tr>
<td>27</td>
<td>Kitchen Counter</td>
<td>04/15/2003</td>
<td>Battlefield 1942 Box, Sharp PDA program CD, Quake III Arena Team Case and CD, XS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Case and Game, Back Digital Camera Case, USB Power Centry Hub w/power cord.</td>
</tr>
<tr>
<td>28</td>
<td>Kitchen Table Area</td>
<td>04/15/2003</td>
<td>Quantum Fireball hard drive 3.5&quot;</td>
</tr>
<tr>
<td>29</td>
<td>Suspect Bedroom</td>
<td>04/15/2003</td>
<td>Receipts from Staples Office Supply and Register.Com (Top of Dresser)</td>
</tr>
<tr>
<td>30</td>
<td>Suspect Bedroom</td>
<td>04/15/2003</td>
<td>Shipping Box from UPS (Top Shelves)</td>
</tr>
<tr>
<td>31</td>
<td>Suspect Bedroom</td>
<td>04/15/2003</td>
<td>Sharp Personal Digital Assistant (Left side 2nd drawer of Dresser)</td>
</tr>
<tr>
<td>32</td>
<td>Suspect Bedroom</td>
<td>04/15/2003</td>
<td>(1) Compact Disk-Recordable under bed</td>
</tr>
</tbody>
</table>

End of List
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal Case File Number</td>
<td>288A-SF-133411</td>
</tr>
<tr>
<td>Field Office Acquiring Evidence</td>
<td>Hayward</td>
</tr>
<tr>
<td>Serial # of Originating Document</td>
<td></td>
</tr>
<tr>
<td>Date Received</td>
<td>4/22/03</td>
</tr>
<tr>
<td>From</td>
<td>(Name of Contributor) D SPD</td>
</tr>
<tr>
<td>(Address of Contributor)</td>
<td></td>
</tr>
<tr>
<td>(City and State)</td>
<td></td>
</tr>
<tr>
<td>By</td>
<td>5A</td>
</tr>
<tr>
<td>To Be Returned</td>
<td>☐ Yes ☑ No</td>
</tr>
<tr>
<td>Receipt Given</td>
<td>☐ Yes ☑ No</td>
</tr>
<tr>
<td>Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure</td>
<td>☐ Yes ☑ No</td>
</tr>
<tr>
<td>Federal Taxpayer Information (FTI)</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>GOOGLE - VICTIM</td>
</tr>
<tr>
<td>SUNNYVALE, CA</td>
<td></td>
</tr>
<tr>
<td>NIPC - Impairment</td>
<td></td>
</tr>
</tbody>
</table>
| Reference | FD 302 4/22 |}

(Communication Enclosing Material) 8

Description: ☑ Original notes re interview of 288A-SF-133411 - A(23)
Interview

Mom refused to pay $ to get him out

UPS delivered a bunch of PKEs

To be possibly interviewed

In state family custody
Universal Case File Number: 2884 - SF - 133411

Field Office Acquiring Evidence: 84

Serial # of Originating Document:

Date Received: 4-15-03

From:

(Name of Contributor)

(Address of Contributor)

(City and State)

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

Federal Taxpayer Information (FTI):

□ Yes □ No

Title:

Reference: FD 302 4/15/03

(Communication Enclosing Material)

Description: Original notes re interview of

2884 - SF 133411 - 14(24)
Precedence: ROUTINE

Date: 04/07/2005

To: Jacksonville
Attn: Cyber
San Francisco
Attn: Cyber
Washington Field
Attn: Cyber

From: Dallas
Cyber
Contact: SA

Approved By:

Drafted By: tc

Case ID #: DL 288A-0 (Pending)

Title:
GOOGLE;
COMPUTER INTRUSION

Synopsis: Set Leads for Receiving Offices

Enclosure(s): Enclosed for Receiving Offices

(1) Copies of email correspondences between and

Details: On 4/6/05, GLC Ventures contacted the Dallas FBI alleging that his business is being extorted to be placed back on the results of Google searches. GLC Ventures is a business specializing in the marketing of internet based companies and products. The co-owners of the business are

According to over 100 GLC Venture websites advertising GLC Venture products, and other products of companies having a working relationship with GLC Ventures, were removed from the results of Google searches. The websites were removed from Google searches around 12/27/04. Shortly afterwards, received emails and telephone calls from individuals named and offering to have the GLC Ventures websites "readded" to the results of Google searches for a monetary fee stated that he had contact with individuals at Google that could correct the problem. The GLC Ventures websites are being hosted by Above Net, 1807 Michael Faraday Court, Reston, VA 20190, telephone number 877/479-7378.
To: Jacksonville  From: Dallas  
Re: DL 288A-0, 04/07/2005

LEAD(s):

Set Lead 1: (Discretionary)

JACKSONVILLE

AT NAVARRE, FL

At discretion of Jacksonville Office, determine lead value of the information contained herein including possible investigation.

Set Lead 2: (Discretionary)

SAN FRANCISCO

AT MOUNTAIN VIEW, CA

At discretion of Newark Office, determine lead value of the information contained herein including possible investigation.

Set Lead 3: (Discretionary)

WASHINGTON FIELD

AT RESTON, VA

At discretion of Washington Field Office, determine lead value of the information contained herein including possible investigation.

♦♦
stated that the business loss to GLC Ventures is $500,000.
Precedence: ROUTINE

To: San Francisco

From: San Francisco
Squad 14G-Cybersquad, San Jose Resident Agency
Contact:

Approved By:

Drafted By:

Case ID #: 288A-SF-NEW (Pending)

Title: UNSUB(S),
AKA MYDOOM VIRUS;
GOOGLE - VICTIM;
YAHOO - VICTIM;
LYCOS - VICTIM;
COMPUTER INTRUSIONS-CRIMINAL MATTERS

Synopsis: Request to open a new 288A case at San Francisco based on reports that users of popular internet search engines were unable to access major search engine websites or experienced slowness due to the MyDoom virus, which flooded major search engines with automated searches.


Details: On 07/26/2004, CNN.com (http://www.cnn.com) reported that internet search engines, such as Google (http://www.google.com), Yahoo (http://www.yahoo.com), and Lycos (http://www.lycos.com) were unable to provide search results to a number of web surfers probably due to a new variant of the MyDoom virus. The problem began at approximately 11:30AM Eastern Time.

The virus uses search engines on infected computers to look for more e-mail addresses in order to keep replicating itself.

It is recommended that this matter be opened and assigned to SA

O&A as 288A-SF-NEW

Opened & Assigned

to SA

MA 7/26/04

07/26/04
o http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.m@mm.html
o http://www.f-secure.com/v-descs/mydoom.m.shtml

5. Attachments:

None.
Google: MyDoom virus caused problems

- Video coach prepares athletes for Athens
- Bloggers get convention credentials
- 'Bin Laden suicide' virus hits Web

Dems stress unity in Boston

- CNN/Money: Big money behind conventions
- GOP: Kerry undergoing 'extreme makeover'
- Google blames MyDoom virus
<table>
<thead>
<tr>
<th>Case ID: 288A-SF-136551-1A</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF 1 ORIGINAL NOTES RE INTERVIEW OF Lycos</td>
</tr>
<tr>
<td>SF 2 ORIGINAL NOTES RE INTERVIEW OF Google Legal Council</td>
</tr>
<tr>
<td>SF 3 ORIGINAL NOTES RE INTERVIEW OF McAfee</td>
</tr>
<tr>
<td>SF 4 STAS TECHNICAL LEAD ANALYSIS</td>
</tr>
</tbody>
</table>

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED.

DATE 07-06-2009 NY 60322/UC/LLP/PL/isd
<table>
<thead>
<tr>
<th>Item</th>
<th>Date Filed</th>
<th>To be returned</th>
<th>Disposition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Field Office Acquiring Evidence: SF

Serial # of Originating Document: 

Date Received: 3/4/05

From: FBI HQ

(Name of Contributor/Interviewee)

(Address)

(City and State)

By: SA

To Be Returned: No

Receipt Given: No

Grand Jury Material - Disseminate Only Pursuant to Rule 6(e)

Federal Rules of Criminal Procedure: No

Federal Taxpayer Information (FTI): No

Title: MyDoom

Reference: (Communication Enclosing Material)

Description: Original notes re interview of STAS Technical Lead Analysis of MyDoom Virus

File Number: 288A-SF 136551
FEDERAL BUREAU OF INVESTIGATION

Precedence: Routine
To: Director, FBI

Attn: Computer Investigations Unit, Room 11887
Computer Investigations and Infrastructure
Threat Assessment Center
(CID/NSD)

From: SAC, San Francisco
Approved By: [Signature]
Drafted By: [Signature]

Case ID #: 288A-SF-136551-02

Date: 07/29/2004

Case OPENED: 07/26/2004
CASE CLOSED: 07/26/2004

SUBMISSION: ☑ Initial ☐ Supplemental ☐ Closed

CASE CLOSED: ☑ 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
San Francisco

VICTIM

Company name/Government agency: Google, Mt. View, CA; Yahoo, Santa Clara, CA;
Altavista, Palo Alto, CA; Lycos, Waltham, MA

Address/location: Internet Search Engines

Purpose of System: Unknown

Highest classification of information stored in system: Unknown
To: Director, FBI

Re: 28A-SF-136551, Date 07/29/2004

System Data:

Hardware/Configuration (CPU): Unknown
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: DDOS (list provided)

Path of intrusion:
addresses: 1. __________ 2. __________ 3. __________ 4. __________ 5. __________
country: 1. __________ 2. __________ 3. __________ 4. __________ 5. __________
facility: 1. __________ 2. __________ 3. __________ 4. __________ 5. __________

Subject: Unknown
Age: __________________ Race: __________________
Sex: __________________ Education: __________________
Alias(es): __________________ 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: Unknown
Estimated dollar loss to date: Unknown
Category of Crime:

Impairment:
- [ ] Malicious code inserted
- [x] Denial of service
- [ ] Destruction of information/software
- [ ] Modification of information/software

Theft of Information:
- [ ] Classified information compromised
- [ ] Unclassified information compromised
- [ ] Passwords obtained
- [ ] Computer obtained
- [ ] Telephone services obtained
- [ ] Application software obtained
- [ ] Operating software obtained

Intrusion:
- [ ] Unauthorized access
- [ ] Exceeding authorized access

**REMARKS**

On 07/26/2004, popular internet search engines were unable to provide search results to a number of web surfers due to a new variant of the MyDoom virus.

The virus uses search engines to look for more e-mail addresses in order to keep replicating itself.
### Technology(s) Used:

#### Top Screen

**Protocol Attacks:**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Attacks</th>
</tr>
</thead>
</table>
| IP       | ![ ]( ) spoofing attack  
|          | ![ ]( ) source routing  
| TCP      | ![ ]( ) sequence number attack  
| UDP      | ![ ]( ) spoofing attack  
|          | ![ ]( ) flooding  
| FTP      | ![ ]( ) vulnerable version  
|          | ![ ]( ) SITE EXEC  
|          | ![ ]( ) overload FTP buffer  
|          | ![ ]( ) anonymous FTP  
| Telnet   | ![ ]( ) highjacking  
|          | ![ ]( ) packet sniffing  
| TFTP     | ![ ]( ) r commands  
|          | ![ ]( ) rsh  
|          | ![ ]( ) rlogin  
| SMTP     | ![ ]( ) vulnerable version  
|          | ![ ]( ) spoofing  
|          | ![ ]( ) embedded postscript attack  
|          | ![ ]( ) trojan horse attack  
|          | ![ ]( ) syslog attack  
|          | ![ ]( ) flooding  
|          | ![ ]( ) MIME  
| HTTP     | ![ ]( ) flooding  
|          | ![ ]( ) Telnet to HTTP port  
| gopher   | ![ ]( )  
| X11 window | ![ ]( )  

#### Secondary Screen

<table>
<thead>
<tr>
<th>Attacks</th>
</tr>
</thead>
</table>
| ![ ]( ) spoofing attack  
| ![ ]( ) source routing  
| ![ ]( ) sequence number attack  
| ![ ]( ) spoofing attack  
| ![ ]( ) flooding  
| ![ ]( ) vulnerable version  
| ![ ]( ) SITE EXEC  
| ![ ]( ) overload FTP buffer  
| ![ ]( ) anonymous FTP  
| ![ ]( ) highjacking  
| ![ ]( ) packet sniffing  
| ![ ]( ) r commands  
| ![ ]( ) rsh  
| ![ ]( ) rlogin  
| ![ ]( ) vulnerable version  
| ![ ]( ) spoofing  
| ![ ]( ) embedded postscript attack  
| ![ ]( ) trojan horse attack  
| ![ ]( ) syslog attack  
| ![ ]( ) flooding  
| ![ ]( ) MIME  
| ![ ]( ) flooding  
| ![ ]( ) Telnet to HTTP port  

Page 4
Top Screen

☐ DNS
☐ SNMP
☐ FSP
☐ NFS

Other Attacks:
☒ Worm
☐ Social engineering
☐ Scavenging and reusing
☐ Masquerading
☐ Scanning
☐ Trojan Horse
☐ Other

Secondary Screen

☐ vulnerable version
☐ flooding
In Reply, Please Refer to File No. 288A-SF-106551-4

450 Golden Gate Ave.
PO Box 36015
San Francisco, CA 94102
(415) 553-7400
July 28, 2004

Attention: Lycos Legal Department

Dear [Name]

This letter is to document the conversation yesterday, 07/27/2004, regarding our investigation into the impact of the MYDOOM COMPUTER VIRUS on your organization. Parties to the conversation included yourself, Special Agents [Names] and [Names].

If you have any further questions, or additional information, please contact Special Agent [Name].

Sincerely,

Mark J. Mershon
Special Agent in Charge

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED
DATE 07-06-2009 BY 60322/UC/LPP/PLJ/sdb

By: [Name]

Supervisory Special Agent
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Type</th>
<th>Identification</th>
<th>Duration</th>
<th>Pages</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 28</td>
<td>3:42pm</td>
<td>Fax Sent</td>
<td></td>
<td>0:22</td>
<td>1</td>
<td>OK</td>
</tr>
</tbody>
</table>
On August 11, 2004, [blank] Legal Counsel at Google, in Mountain View, California, telephone number 650/623-6048, was interviewed telephonically and advised of the identity of the interviewing agent and the nature of the interview. [blank] provided the following information:

GOOGLE is not currently experiencing any affects from the MYDOOM virus that initially struck on July 26, 2004. [blank] advised that representatives from GOOGLE are working on preparing an analysis of the financial loss suffered by GOOGLE due to the MYDOOM virus. [blank] believes it will be approximately $100,000.

[blank] advised that she has the IP addresses of the first ten hosts that queried the GOOGLE search engine related to the MYDOOM attack and said that she would send the information to me via email. The resulting email is attached to and made a part of this FD-302.
On July 27, 2004, ________________, a representative of Lycos in San Francisco, California, telephone number (650)428-5000, was interviewed telephonically and advised of the identity of the interviewing agents and the nature of the interview. ___________ provided the following information:

Between 8:30AM and 9:00AM Eastern Daylight Time (EDT) on 07/26/2004, the servers at Lycos were impacted by the MYDOOM virus. Between 9:00AM and 10:00AM eastern, legitimate web users' availability to search results conducted by LYCOS was at 37%. By 11:00AM eastern, availability was less than 4%.

By 7:30PM eastern, Lycos had implemented filters on searches coming into the servers on certain text strings like "mail", "reply", "rcpt", and "contact" that they noted were being queried by the virus. By applying these filters, they were able to block the searches committed by the virus and allow regular users to access the search functions of LYCOS. Lycos could not simply block an Internet Protocol (IP) address or range of IP addresses because of the distributed nature of the virus.

_______ noted that traffic to the LYCOS website was at approximately 50 times normal levels on 07/26/2004 and continues to fluctuate between 30 and 50 times normal levels on 07/27/2004, but that, due to the filters implemented by LYCOS, their search functions are running normally for most users.
On July 27, 2004, [redacted] MCAFEE, telephone number (503)466-4484, were interviewed telephonically and advised of the identity of the interviewing agents and the nature of the interview. [redacted] and [redacted] provided the following information:

The 15th variant of the MYDOOM virus was first noticed by MCAFEE on July 26, 2004 at approximately 6:30AM pacific time. The virus affected major search engines while trying to search for additional email addresses to send itself to, as well as several corporate customers whose mail servers were temporarily overwhelmed.

The virus harvests email addresses from a local, infected computer, then searches the domain name of the email addresses through the major internet search engines, in an attempt to locate additional email addresses. While the search engines were flooded with searches, [redacted] and [redacted] believe they were not the primary target.

The virus also installs a backdoor on TCP Port 1034 that future users and/or viruses can exploit. MCAFEE has already seen viruses discovered on July 27, 2004 that exploit this open port, but does not think they were necessarily written by the same author as the MYDOOM virus.

[redacted] and [redacted] noted that there was nothing unique or identifying about the virus executable. They do not have the source code of the virus.
FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/17/2004

To: San Francisco

From: San Francisco

Squad 14G-Cybersquad, San Jose Resident Agency

Contact: SA

Approved By: 

Drafted By: 

Case ID #: 288A-SF-136551-6 (Pending)

Title: UNSUB(S)
aka MYDOOM VIRUS;
GOOGLE - VICTIM;
YAHOO - VICTIM;
LYCOS - VICTIM;
COMPUTER INTRUSIONS-CRIMINAL MATTERS

Synopsis: Request to close captioned matter.

Details: At 11:30AM Eastern time on 07/26/2004, internet search engines Google (http://google.com), Yahoo (http://yahoo.com), and Lycos (http://lycos.com) were unable to provide search results to a number of users for several hours due to a variant of the MyDoom virus (Mydoom.m) and Zindos worm.

On 07/28/2004, Special Technologies and Applications Section (STAS) assistance was requested in analyzing the source code of Mydoom.m and Zindos.

On 12/14/2004, STAS advised that the analysis of Mydoom.m and Zindos was complete. Strings and source code of the virus/worm were examined for clues as to the identity of the author, but none were found.

Determination of the original author is therefore deemed impossible and the case is being closed.

SF Field Intelligence Group
Potential Intel Value: Yes ☑ No ☐

Reviewed By: 
Date: 12/17/04

S-Drive Location: 2884-SF-136551-8

Case closed on 03/21/05
The following investigation was conducted by Special Agent [redacted].

On December 14, 2004, Special Agent [redacted] received from STAS the Technical Lead Report on the Analysis of Mydoom-M/Zindos Worms. The report found no clues as to the identity of the author of either computer worm. The report is attached to and made a part of this document.
### Analysis of Mydoom-m/Zindos Worms

**Electronic Location:** `\smb00\cases\ProductReports\2004_Reports\STAS-`

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prepared By</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Phone Number</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Approved</strong></td>
<td>XXX</td>
</tr>
<tr>
<td><strong>Phone Number</strong></td>
<td>XXX</td>
</tr>
<tr>
<td><strong>STAS Control File</strong></td>
<td>288A-SF-136551</td>
</tr>
<tr>
<td><strong>Primary Report ID</strong></td>
<td>STAS04-XXX</td>
</tr>
<tr>
<td><strong>MATS ID</strong></td>
<td>2004-XXX</td>
</tr>
</tbody>
</table>

---

**TO:**

**DISTRIBUTION TO:** XXX

**Date:** 11/22/04

**Submitter's Case Number:** 288A-SF-136551

**RE:** Analysis of Mydoom-m/Zindos Worms

**Title:** Analysis of Mydoom-m/zindos worms

---

THIS REPORT IS FURNISHED FOR OFFICIAL USE ONLY. NO PART OF THIS REPORT MAY BE DISCLOSED TO ANY THIRD PARTY WITHOUT THE EXPRESS WRITTEN CONSENT OF THE FBI/CYD

---

**UNCLASSIFIED**
1. Media Type and Quantity: 1 CD w/zip file containing Mydoom-m worm

2. Analysis Requested:
   - Assist in analysis of Mydoom-M Virus
   - Obtain a copy of zindos worm and analyze

3. Executive Summary:
   A copy of the Zindos worm was obtained. Both Zindos and Mydoom-m (provided) were analyzed using IDA Pro (static disassembly of binary). Strings and code were examined for clues as to the identity of the author, but none were found.

4. Details of Analysis:

   Zindos worm
   - A copy of the zindos worm was obtained from a 3rd party source.
   - It was loaded into IDA Pro for disassembly and analysis
   - Disassembly revealed that zindos goes into a tight loop (every 50ms) trying to connect to www.microsoft.com
   - The code was examined looking for identifying information such as names, email addresses, comments or IP addresses that might help identify the author. None were found.

   Mydoom-m worm
   - The worm was run in isolation and network traffic was recorded. Without being able to reach the Internet, the worm performs lookups for the mail server (MX) for the following domains:
     13 cvs.tartarus.org: type MX, class inet
     13 gto.net.om: type MX, class inet
     13 kohls.com: type MX, class inet
     14 lebanon-online.com.lb: type MX, class inet
     14 msdirectservices.com: type MX, class inet
     17 petri.co.il: type MX, class inet
     14 target.com: type MX, class inet
     14 tucows.com: type MX, class inet
     13 ultraschallpiloten.com: type MX, class inet
     (the number in front is a count of the occurrences during the test run).

   [Analyst Comment on above list: It is likely that this is a list of known “open relays” at the time the worm was released. The intent is likely to use them to send the initial round of messages.]

   - Mydoom-m was loaded into IDA Pro for disassembly and static analysis. A cursory analysis of the code was consistent with analysis provided by commercial anti-virus vendors and security organizations at

     o http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM MYDOOM.M
Google says MyDoom virus caused problems

Monday, July 26, 2004 Posted: 4:21 PM EDT (2021 GMT)

(CNN) - The No. 1 Internet search engine on Monday was unable to provide search results to a number of Web surfers, probably because of a variant of the MyDoom virus.

Users of other popular search engines such as Yahoo and Lycos may also have experienced some sluggish behavior.

Google released a statement to CNN at 3 p.m. ET saying the site "experienced slowness for a short period of time early today because of the MyDoom virus, which flooded major search engines with automated searches.

"A small percentage of our users and networks that have the MyDoom virus have been affected for a longer period of time. At no point was the Google Web site significantly impaired, and service for all users and networks is expected to be restored shortly."

According to several media accounts, the problem began about 11:30 a.m. ET, and by 3 p.m. the site seemed to be running smoothly again.

The SANS Institute and other security firms issued a release shortly after the problem was detected saying a new variant of the MyDoom virus could be to blame. The latest incarnation of the troublesome virus uses search engines on infected computers to look for more e-mail addresses in order to keep replicating itself.

Experts contacted by CNN were unable to determine the exact magnitude of the problem.

Some users across the United States reported no trouble with Google or other search engines.

For other people, although the main Google page was able to load, they reported seeing a "server error" message when trying to conduct a search.

Google also announced details of its initial public offering Monday, with share prices of between $108 and $135. Experts consider those figures to be very high, leading some observers to initially speculate that Google was the victim of a vindictive hacker attack.
FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 04/07/2005

To: Jacksonville
San Francisco
Washington Field

Attn: Cyber
Attn: Cyber
Attn: Cyber

From: Dallas
Cyber

Contact: SA

Approved By:

Drafted By: ___________ 1:tc

Case ID #: DL 288A-0 (Pending)

Title: GOOGLE;
COMPUTER INTRUSION

Synopsis: Set Leads for Receiving Offices

Enclosure(s): Enclosed for Receiving Offices

(1) Copies of email correspondences between ________ _______.

Details: On 4/6/05, GLC Ventures, mobile telephone number contacted the Dallas FBI alleging that his business is being extorted to be placed back on the results of Google searches. GLC Ventures is a business specializing in the marketing of internet based companies and products. The co-owners of the business are

According to over 100 GLC Venture websites advertising GLC Venture products, and other products of companies having a working relationship with GLC Ventures, were removed from the results of Google searches. The websites were removed from Goggle searches around 12/27/04. Shortly afterwards, received emails and telephone calls from individuals named _______ and _______ offering to have the GLC Ventures websites "readded" to the results of Google searches for a monetary fee. _______ stated that he had contact with individuals at Goggle that could correct the problem. The GLC Ventures websites are being hosted by Above Net, 1807 Michael Faraday Court, Reston, VA 20190, telephone number 877/479-7378.
To: Jacksonville  From: Dallas  
Re: DL 288A-0, 04/07/2005

LEAD(s):

Set Lead 1: (Discretionary)

   JACKSONVILLE
   AT NAVARRE, FL
   At discretion of Jacksonville Office, determine lead value of the information contained herein including possible investigation.

Set Lead 2: (Discretionary)

   SAN FRANCISCO
   AT MOUNTAIN VIEW, CA
   At discretion of Newark Office, determine lead value of the information contained herein including possible investigation.

Set Lead 3: (Discretionary)

   WASHINGTON FIELD
   AT RESTON, VA
   At discretion of Washington Field Office, determine lead value of the information contained herein including possible investigation.

++
stated that the business loss to GLC Ventures is $500,000.
08/16/2005

San Jose, California

288A-HN-18606

Not Dictated
Precedence: ROUTINE

To: Atlanta

From: San Francisco
Squad 14G/San Jose RA
Contact: SSA

Date: 11/29/2005

Case ID #: SF 62F-0

Title: UNSUB, aka
SUSPICIOUS ACTIVITY
AT GOOGLE FACILITY IN
LITHIA SPRINGS, GEORGIA

Synopsis: To forward alleged suspicious activity by one (female) at an unmarked Google data center located at 101 Aguila Way, Lithia Springs, Georgia.

Enclosure(s): Enclosed for Atlanta is one Internet e-mail from San Francisco Division, San Jose RA.

Details: On 11/27/2005, Google, 1600 Amphitheater Parkway, Mountain View, California, telephone number (650)623-6011, sent SSA an Internet e-mail documenting suspicious activity by one allegedly a re-contacted and learned that had no further information to provide. noted that the data center where the alleged activity occurred is considered by Google as one of their corporate "critical infrastructure assets."

advised that at approximately 3:55 p.m., on 11/25/2005, entered the "North" parking lot of an unmarked Google data center in Lithia Springs, Georgia. Google personnel noted took digital photographs of the building, which was ultimately confirmed from a surveillance video which Google possesses. was confronted by Google physical security personnel and she provided conflicting statements, and she did not have a legitimate reason for being on the property. Instead, ultimately told the personnel that she was lost. declined a request from the security personnel to view the photographs she had taken.
LEAD(s):

Set Lead 1: (Info)

ATLANTA

AT ATLANTA, GEORGIA

Read and Clear.

♦♦
Local police were not contacted, and [REDACTED] was asked to leave the property. [REDACTED] was driving a rental vehicle from Airport Rent-A-Car of Atlanta. The car did not have license plates, but was described as a tan/gold Mitsubishi. Google security personnel asked [REDACTED] for identification, and she produced a United Kingdom - Great Britain passport (no further information). Google personnel also determined [REDACTED] was staying at the Renaissance-Atlanta Hotel, 590 West Peach Street, NW, Atlanta, Georgia. Google determined [REDACTED] checked out of the hotel on 11/26/2005.

Enclosed with this communication is an Internet e-mail from Google to SSA [REDACTED] with additional self-explanatory facts regarding George's contact with Google personnel in Georgia.

This information is being forwarded to Atlanta for intelligence purposes and for whatever action deemed appropriate. San Francisco is taking no further action.
Precedence: ROUTINE

To: San Francisco
From: San Francisco

Date: 01/03/2006

Squad 14G/SJRA

Contact: SA

Case ID #: 288A-SF-NEW (Pending)

Title: UNSUB(s);

SYANTY WORM;
GOOGLE INC. - VICTIM

Synopsis: To open and assign a new case on the Santy worm.

Details: On December 22, 2005, Google Inc., reported Google search engine queries originating from computers compromised by the Santy worm was affecting performance of their website. Further described the direct effects and damages to Google caused by the different variants of the Santy worm. The Santy worm, written in Perl script language, exploits a vulnerability in the phpBB bulletin board/web forum software to spread and it uses the Google search engine to find additional vulnerable servers running phpBB software. This worm has been plaguing Google for the last 12-18 months as Google has attempted to filter out the search requests caused by the worm. As Google filters out certain string search phrases, within minutes, the subjects modify the search phrase to once again, bypass Google's filters. Unfortunately, because the worm is attempting to propagate using the Google search engine, Google is beginning to block many legitimate requests to the Google search engine.

Currently, Google has an engineering team devoted to blocking the variants of the worm. Google preliminarily estimated that it has sustained approximately $250,000 - $500,000 in damages just trying to control the spread of the worm. This loss calculation is based on man hours dedicated to the problem in addition to lost revenues.

Google engineers have analyzed the script from one flavor of the Santy worm and discovered gmail addresses for a technical contact posted in the comment section of the script. This may be the email address of the creator of that particular variant of
To: San Francisco  From: San Francisco
Re: 288A-SF-NEW, 01/03/2006

the worm. The following gmail addresses were found in the script: ___________________________ and ___________________________.

It is recommended that a new case be opened and assigned to SA's ___________________________ and ___________________________ as co-case agents.

♦♦
YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

PLACE
United States District Court
United States Courthouse
280 South First Street
San Jose, CA 95113

COURTROOM
As directed by the court

DATE AND TIME
January 18, 2006 at 9:30am

YOU ARE ALSO COMMANDED to bring with you the following document(s) or object(s):

-SEE ATTACHMENT-

COMPLIANCE WITH THE SUBPOENA WILL BE DEEMED SATISFACTORY WHEN YOU PROVIDE ALL THE REQUIRED MATERIALS TO THE AGENT SERVING THIS SUBPOENA AND NO APPEARANCE WILL BE NECESSARY.

☐ Please see additional information on reverse

This subpoena shall remain in effect until you are directed to depart by the court or by an officer acting on behalf of the court.

RICHARD W. WIEKING
(By) Deputy Clerk

This subpoena is issued on application of the United States of America
KEVIN V. RYAN
United States Attorney

ATTORNEY'S NAME, ADDRESS AND PHONE NUMBER:
AUSA, MATTHEW A. FARRELL
U.S. Attorney's Office, 150 Almaden Blvd., Suite 900
San Jose, CA 95113 (408) 535-5081
Special Agent Dana Marino, FBI (408) 535-4685

Date:
January 4, 2006
Re: Grand Jury Investigation
Request for Non-Disclosure

Dear Custodian of Records:

Pursuant to an investigation being conducted by the Federal Grand Jury for the Northern District of California with regard to possible felony violations of the United States Code, it is requested that you furnish the information requested in the grand jury subpoena.

In addition, we request that you not disclose the existence of this request and the production of records. Any such disclosure could impede the investigation being conducted and thereby interfere with the enforcement of the law. Thank you very much for your assistance in this matter.

Very truly yours,

KEVIN V. RYAN
United States Attorney

MATTHEW A. PARRELLA
Assistant United States Attorney

MAP: lg
RETURN OF SERVICE

RECEIVED BY SERVER | DATE | PLACE
---|---|---
| 14/2006 | San Jose, CA

SERVED | DATE | PLACE
---|---|---
| 14/2006 | Mountain View, CA

SERVED ON (PRINT NAME)

SERVED BY (PRINT NAME) | TITLE
---|---
Special Agent

STATEMENT OF SERVICE FEES

<table>
<thead>
<tr>
<th>TRAVEL</th>
<th>SERVICES</th>
<th>TOTAL</th>
</tr>
</thead>
</table>

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Return of Service and Statement of Service Fees is true and correct.

Executed on 14/2006

Signature of Server

FBI, 950 S Buscain Ave, SJ, CA

Address of Server

Additional Information

Note: Served via facsimile

ALL FBI INFORMATION CONTAINED HEREIN IS UNCLASSIFIED
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

1 As to who may serve a subpoena and the manner of its service see Rule 17(d), Federal Rules of Criminal Procedure, or Rule 45(c), Federal Rules of Civil Procedure.

2 Fees and mileage need not be tendered to the witness upon service of a subpoena issued on behalf of the United States or an officer or agency thereof (Rule 45(c), Federal Rules of Civil Procedure; Rule 17(d), Federal Rules of Criminal Procedure) or on behalf of certain indigent parties and criminal defendants who are unable to pay such costs (28 USC 1625, Rules 17(b) Federal Rules of Criminal Procedure).
Precedence: ROUTINE  

Date: 01/31/2006

To: San Francisco

From: San Francisco  
Squad 14G/ SJRA
Contact: SA

Approved By: Jr.

Drafted By: dm

Case ID #: 288A-SF-139138 (Closed)

Title: UNSUB(s);  
SANTY WORM;  
GOOGLE INC. - VICTIM

Synopsis: Google is not interested in pursuing this matter. It is recommended this case be closed.

Details: On January 30, 2006, Google Inc., advised that the legal department of Google is not interested in conducting any further investigation into this matter.

Inasmuch as Google is the victim and their assistance in the form of providing logs and other supporting documentation is necessary to pursue prosecution, it is recommended this case be administratively closed.

SF Field Intelligence Group

Potential Intel Value: Yes □ No □

Reviewed By: □ Date: 2/7/06
S-Drive Location: ___________

Close

Case closed 2/7/06
San Francisco FBI Cyber Squad 14G

Facsimile Coversheet

Fax Date: 1/4/06
Fax Time: 

Number of Pages: 4
(including cover page)

To: 

Recipient's Fax Number: 

Subject: This subpoena is related to the one sent yesterday.

From: Special Agent
Federal Bureau of Investigation
950 South Bascom Avenue, Suite 3011
San Jose, California 95128
TO: [Blank]

ALL FBI INFORMATION CONTAINED HEREIN IS UNCLASSIFIED
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

SUBPOENA TO TESTIFY BEFORE GRAND JURY

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

PLACE
United States District Court
United States Courthouse
280 South First Street
San Jose, CA 95113

COURTROOM
As directed by the court

DATE AND TIME
January 11, 2006 at 9:30am

YOU ARE ALSO COMMANDED to bring with you the following document(s) or object(s):*

-SEE ATTACHMENT-

COMPLAINCE WITH THE SUBPOENA WILL BE DEEMED SATISFACTORY WHEN YOU PROVIDE ALL THE REQUIRED MATERIALS TO THE AGENT SERVING THIS SUBPOENA AND NO APPEARANCE WILL BE NECESSARY.

☐ Please see additional information on reverse

This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer acting on behalf of the court

U.S. MAGISTRATE JUDGE OR CLERK OF COURT

RICHARD W. WIEKING
(By) Deputy Clerk

This subpoena is issued on application of the United States of America
KEVIN V. RYAN
United States Attorney

ATTORNEY PHONE NUMBER: USA, MATTHEW A. PARRELLA
U.S. Attorney's Office, 150 Almaden Blvd., Suite 900
San Jose, CA 95113 (408)535-5061
Special Agent Dana Marino, FBI (408) 535-4685

*If not applicable, enter "none"

DATE
December 28, 2005

288A-SF-139138-3
December 28, 2005

Re: Grand Jury Investigation
Request for Non-Disclosure

Dear Custodian of Records:

Pursuant to an investigation being conducted by the Federal Grand Jury for the Northern District of California with regard to possible felony violations of the United States Code, it is requested that you furnish the information requested in the grand jury subpoena.

In addition, we request that you not disclose the existence of this request and the production of records. Any such disclosure could impede the investigation being conducted and thereby interfere with the enforcement of the law. Thank you very much for your assistance in this matter.

Very truly yours,

KEVIN V. RYAN
United States Attorney

MATTHEW A. PARRELLA
Assistant United States Attorney

MAP: lg
**RETURN OF SERVICE**

<table>
<thead>
<tr>
<th>RECEIVED BY SERVER</th>
<th>DATE</th>
<th>PLACE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3/06</td>
<td>San Jose, CA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SERVED</th>
<th>DATE</th>
<th>PLACE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3/06</td>
<td>Mountain View, CA</td>
</tr>
</tbody>
</table>

SERVED ON (PRINT NAME)

SERVED BY (PRINT NAME)

STATEMENT OF SERVICE FEES

<table>
<thead>
<tr>
<th>TRAVEL SERVICES TOTAL</th>
</tr>
</thead>
</table>

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Return of Service and Statement of Service Fees is true and correct.

Executed on 3/06/2006

Signature of Server

FBI 950 S. Buscom, S.F., CA

Address of Server

---

1 As to who may serve a subpoena and the manner of its service see Rule 17(d), Federal Rules of Criminal Procedure, or Rule 45(c), Federal Rules of Civil Procedure.

2 "Fees and mileage need not be tendered to the witness upon service of a subpoena issued on behalf of the United States or an officer or agency thereof (Rule 45(c), Federal Rules of Civil Procedure; Rule 17(d), Federal Rules of Criminal Procedure) or on behalf of certain indigent parties and criminal defendants who are unable to pay such costs (28 USC 1825, Rules 17(b) Federal Rules of Criminal Procedure)."

Additional Information

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED

DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb
### Last Transaction

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Type</th>
<th>Identification</th>
<th>Duration</th>
<th>Pages</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 4</td>
<td>4:24pm</td>
<td>Fax Sent</td>
<td></td>
<td>2:08</td>
<td>4</td>
<td>OK</td>
</tr>
</tbody>
</table>

*ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED*

DATE 07-06-2009 BY 60322/UC/PLJ/sdb
Total Deleted Page(s) = 7
Page 21 ~ b1; b7E;
Page 23 ~ b6; b7C;
Page 24 ~ b5; b7E;
Page 25 ~ b5; b7E;
Page 26 ~ b5; b7E;
Page 27 ~ b5; b7E;
Page 28 ~ b5; b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X  Deleted Page(s)  X
X  No Duplication Fee  X
X  For this Page  X
XXXXXXXXXXXXXXXXXXXXXXXX
Corporate Addresses

Facebook
1601 S. California Avenue
Palo Alto, CA 94304

Google, Inc.
1600 Amphitheatre Parkway
Mountain View, California 94042

Microsoft
1 Microsoft Way
Redmond, WA, 98052
“Going Dark”
Meeting Attendees
11/16 -11/17/2010

**Google, 11:00 a.m. on 11/16/2010**
Eric Schmidt, *CEO*
Kent Walker, *General Counsel*
Richard Salgado, *Corporate Attorney*
Bill Coughran, *Technologist*

**Facebook, 2:00 p.m. on 11/16/2010**
Sheryl Sandberg, *Chief Operating Officer*
Joe Sullivan, *Chief Security Officer*

**Microsoft, 8:30 a.m. on 11/17/2010**
Steve Ballmer, *CEO*
Brad Smith, *Senior Vice President & General Counsel*
Scott Charney, *Corporate Vice President*
Background Information
Director Robert S. Mueller, III

Meeting with Google Inc.
November 16, 2010

Time/Location: 11:00 a.m., Tuesday, November 16, 2010, at Google Headquarters, 1600 Amphitheater Parkway, Building 43, Mountain View, California.

Event: Meeting with Google Executives

Attendees: Eric Schmidt, Chief Executive Officer
Kent Walker, General Counsel
Richard Salgado, Corporate Attorney
Bill Coughran, Technologist

Note: See enclosed biographies.

FBI Attendees
Valerie Caproni, General Counsel
Senior Technical Advisor
Special Assistant

Miscellaneous: When you arrive at Google Headquarters, you will be greeted by __________. You will then be escorted to Google’s conference room to meet with their executives. You will have approximately one hour to discuss Going Dark issues and initiatives as related to Google.

Note: See enclosed biographies.

The event is CLOSED to the media.

POC:
Administrative Assistant
(cell)
Director’s Special Assistant
SSA
Director’s Research Group
Google Incorporated Company Overview

Google is a multinational public corporation invested in Internet search, cloud computing, and advertising technologies. Google hosts and develops a number of Internet-based services and products, and generates profit primarily from advertising. The company's stated mission is "to organize the world's information and make it universally accessible and useful."

As of 2009, Google has a global annual revenue of $26.65 billion and as of 2010, 23,300 employees in dozens of countries worldwide. Google operates over one million servers in data centers around the world, and processes over one billion search requests every day. Google's rapid growth has triggered a chain of products, acquisitions, and partnerships beyond the company's core search engine. The company offers online productivity software, such as e-mail software and social networking tools. Google's products extend to the desktop as well, with applications such as a web browser, photo organization and editing software, and an instant messaging application. Notably, Google leads the development of a mobile phone operating system, used on a number of smartphones.

Google is known for having an informal corporate culture. On Fortune magazine's list of best companies to work for, Google ranked first in 2007 and 2008, and fourth in 2009 and 2010. Also in 2010, Google was ranked first in both the business and engineering categories by Universum Communication as the "World's Most Attractive Employer" to graduating students.

Founded by Larry Page and Sergey Brin on September 4, 1998, in Menlo Park, California, Google originally began in January, 1996, as a research project while both Mr. Page and Mr. Brin were Doctor of Philosophy students at Stanford University. Google is the dominant search engine provider in the United States, and has captured more than 65 percent market share.
San Francisco Input
Google

[X] San Francisco is assigned the Cyber/CI intrusion case announced publicly by Google and widely publicized in the media in January 2010. This case involved the exfiltration of Google source code and other highly sensitive files.

[)][)(]

(U) At one time in the recent past, Google was concerned with the lack of sufficient numbers of Cyber Agents in the San Francisco Division to handle cases in a timely manner. However, during the past two years the Cyber Division has provided additional FSL to San Francisco and cooperated with the Transfer Unit to ensure qualified Cyber tracked Agents were transferred to San Francisco. Since January 2010, San Francisco Cyber staffing has increased significantly and Google appears to be pleased with the increased staffing. The increased staffing allowed San Francisco to add a fourth Cyber squad.

(U) Despite the challenges encountered immediately after the January attack, San Francisco has several primary contacts in Google’s risk management/investigation, legal compliance, and legal department. All of these contacts have assisted San Francisco and other divisions on numerous occasions prior to, and since, the attack. In fact, since the attack announcement

(U) On the criminal side, San Francisco has a criminal intrusion case where a subject had compromised close to 1 million YouTube users’ accounts. The subject has been identified and will be indicted in December of this year.
Since joining Google in 2001, Eric Schmidt has helped grow the company from a Silicon Valley startup to a global enterprise. Under his leadership, Google has dramatically scaled its infrastructure and broadened its offerings while maintaining a culture of strong innovation. His background uniquely prepares him to lead Google’s efforts toward technological solutions that focus on users. With founders Sergey Brin and Larry Page, and the rest of the executive team, he oversees the company’s technical and business strategy.

Prior to joining Google, Mr. Schmidt was the Chairman and CEO of Novell, and Chief Technology Officer at Sun Microsystems, Inc., where he led the development of Java, Sun’s platform-independent programming technology. He was a member of the research staff at Xerox Palo Alto Research Center and held positions at Bell Laboratories and Zilog.

Mr. Schmidt received a Bachelor’s degree in Electrical Engineering from Princeton University, as well as a Master’s degree and Ph.D. in Computer Science from the University of California, Berkeley.

Mr. Schmidt is a member of President Obama’s Council of Advisors on Science and Technology. In 2006, he was elected to the National Academy of Engineering. In 2007, he was inducted into the American Academy of Arts and Sciences as a fellow. Mr. Schmidt also chairs the Board of the New America Foundation.
W. M. Coughran, Jr.
Senior Vice President, Engineering
Google Inc.

W.M. Coughran joined Google engineering in early 2003. He leads the broad systems infrastructure group underlying Google's products and services, including cluster management, storage, search systems, and a number of product engineering efforts.

Throughout his extensive career in computing, Mr. Coughran has been involved with networking, secure and distributed systems, as well as computational science and engineering. Prior to joining Google, he co-founded and served as CEO and in other executive roles at Entrisphere in Silicon Valley. He was head of Bell Labs' Computing Sciences Research Centre, where C, C++, Unix, Plan 9, and Inferno were created.

Mr. Coughran serves on the Board of Directors for nSolutions Inc. and Clearwell Systems Inc. Additionally, he is the author of more than 50 publications and has served on several scientific boards, committees, and technical advisory bodies. He has held adjunct and visiting positions at Stanford, the ETH, and Duke.
Kent Walker
Vice President and General Counsel
Google Inc.

Kent Walker is responsible for managing Google's global legal team and advising the company's board and management on legal issues and corporate governance matters.

Prior to joining Google, Mr. Walker held senior legal positions at a number of leading technology companies. Most recently, he was Deputy General Counsel of eBay Incorporated where he managed corporate legal affairs, litigation, and legal operations. He served as the Executive Vice President of Liberate Technologies, a leading provider of interactive services software founded by Oracle and Netscape Communications. He also served as Associate General Counsel for Netscape and America Online, and Senior Counsel for AirTouch Communications, which was later acquired by Vodafone.

Mr. Walker was previously an Assistant United States Attorney with the U. S. Department of Justice, where he specialized in the prosecution of technology crimes and advised the Attorney General on management and technology issues.

Mr. Walker has served on numerous boards of technology industry trade associations and is on the steering committee of the annual Computers, Freedom and Privacy conference. He graduated magna cum laude and Phi Beta Kappa from Harvard College, and graduated with distinction from Stanford Law School.
Richard P. Salgado
Senior Counsel
Google Inc.

Richard Salgado began his career with Google in 2009. He also is currently employed as a Lecturer in Law at Stanford Law School.

From 2004 to 2009, he served as a Senior Corporate Counsel for Yahoo, Incorporated. From 2001 to 2004, he was an Adjunct Professor of Law, Computer Crimes, at Georgetown University Law Center. In 2000, he served as an Adjunct Professor of Law, Computer Crimes, at George Mason University School of Law.

From 1996 to 1999, Mr. Salgado was employed by Cooley Godward LLP as a Senior Associate. From 1995 to 1996, he was employed by the Republic of Palau Supreme Court as a Senior Court Counsel. From 1991 to 1995, he was an Associate with Williams Youle & Koenigs. From 1981 to 1991, he served as a Judicial Clerk for Chief Judge Lewis T. Babcock, U.S. District Court for the District of Colorado.

Mr. Salgado received a Bachelor of Art from the University of New Mexico and a Juris Doctor from Yale Law School.
Googling the Censors  

In most repressive countries, government censors like to toil in the shadows, maintaining a cover of deniability as they block citizens’ access to information. It is gratifying to see that the Internet and Google are making their job tougher.

Four months ago, Google unveiled a tool that allows users to monitor the requests received from governments to take down material or report data on the users of their search engine and other services. This month, it released another tool that will expose less overt attempts by governments to curtail its various services, including YouTube and Gmail.

The new tracker shows how traffic on YouTube in Iran fell to zero after the disputed presidential election last year. And how YouTube traffic collapsed in Libya in January after it aired videos of demonstrations by families of murdered prisoners and videos of partying relatives of Col. Muammar el-Qaddafi, the Libyan leader.

The tracker shows the ebbs and flows of traffic but not the cause of disruptions – whether a government directive or a cut cable. Still, it adds an important new source of information.

For starters, it suggests that repressive governments are most fearful of YouTube – an effective vehicle to disseminate dissenting views and evidence of government repression.
SAN FRANCISCO – Google has spent the last few months arguing to anyone who will listen that its new advertising businesses – including ads with images and video and on cellphones – will fuel its next phase of growth. On Thursday, the company finally gave some numbers to support the claim.

Search advertising revenue still drove Google’s better-than-expected performance in the third quarter, when revenue climbed 23 percent and net income rose 32 percent. But for the first time Google said on a call with analysts, display ads – non-text ads with images and video on YouTube and other Web sites – are on track to generate more than $2.5 billion in revenue in the coming year, while mobile ads are on track to contribute another $1 billion.

“Where’s the next multibillion-dollar business after search?” said Jonathan Rosenberg, senior vice president of product management at Google, on the call. “There’s your answer. It’s display and it’s already here.” About mobile, he said, “Clearly this is the future of search and the Internet.”

Still, $3.5 billion in revenue from the new types of advertising is a small piece of the $30 billion in annual revenue expected from Google, and not yet big enough to significantly affect its financial results, said Jordan Rohan, a managing director for Internet and digital media research at Stifel Nicolaus. That will probably not change until about 2012, he said.

“What matters is how much longer can Google grow at 20 percent or more, which is considered rapid growth, double the rate of Internet advertising at this point,” Mr. Rohan said. If the company can continue to grow at that rate, he said, “it would suggest that they’ve extended gracefully into display and mobile.”

Google said net income in the quarter ending Sept. 30 rose to $2.17 billion, or $6.72 cents a share, from $1.64 billion, or $5.13 a share, in the year-ago quarter. Excluding the cost of stock options and the related tax benefits, Google’s third-quarter profit was $7.64 a share. The company said revenue climbed to $7.29 billion, from $5.94 billion. Net revenue, which excludes commissions paid to advertising partners, was $5.48 billion, up from $4.38 billion a year ago.

The results beat the expectations of Wall Street analysts, and Google’s stock price rose about 9 percent in after-hours trading.
Because Google’s search revenue is so large, it needs to go after even bigger ad businesses to move the needle, said Colin W. Gillis, a technology analyst at BGC Partners.

“The next big pool of dollars are the brand dollars, the television dollars, and Google is starting to chase after that, but very slowly,” Mr. Gillis said. “Television’s ripe for disrupting as people are fast-forwarding through TV ads.”

This month, Google introduced Google TV, which lets people access the Web on their television screens. Though it does not yet include advertising, it could eventually help Google get some of the $50 billion television advertising market, Mr. Gillis said.

The percentage of revenue that the new ad businesses account for is less important than what Google can now offer advertisers, Susan Wojcicki, a vice president of product management at Google who is responsible for ad products, said in an interview.

“If you’re an advertiser, you can do display, mobile and search with Google,” she said.

Google said paid clicks on ads on Google sites and other sites that run Google ads grew 16 percent compared with the same period a year ago and 4 percent compared with the second quarter.

Mr. Rosenberg said Google Instant, the search tool that the company introduced in September to predict search queries and adjust the results as people type, had had minimal effect on Google’s revenue. Some analysts predicted that it would increase clicks on the more expensive ads that appear alongside the most common search queries, since people no longer necessarily finish typing their full query.

Google has recently been rapidly investing in other areas, which weighs on its profit margins and “causes some investors to wince,” Mr. Gillis said.

But on Thursday, the company’s executives made it clear that they intended to maintain the same level of investment in both employees and new products.

“Simply put, we’re on this growth agenda at full throttle,” said Patrick Pichette, Google’s chief financial officer.

Google hired 1,526 people in the quarter, which included the postgraduation hiring months, bringing the total number of employees to 23,331.

Google has also been investing in its new businesses that are not yet generating revenue. These include its Android mobile phones, Chrome browser and operating system and its social networking efforts, meant to head off competition from Facebook. They also include some more surprising businesses, like robotic cars that do not need drivers and wind energy farms in the Atlantic Ocean.
FCC opens inquiry into Google data collection
Federal Communications Commission to probe Google collection of data over Wi-Fi networks
By Joelle Tessler
Posted: November 10, 2010 [Source: Yahoo! News]

WASHINGTON (AP) -- The Federal Communications Commission is investigating whether Google Inc. broke the law by inadvertently sucking up fragments of e-mails, Internet passwords, Web surfing behavior and other online activities over public Wi-Fi networks while photographing neighborhoods for its "Street View" mapping feature.

The probe by the FCC comes two weeks after the Federal Trade Commission concluded its own inquiry into the problem, which Google said it discovered following an investigation by German regulators.

While the FTC criticized the search giant for collecting potentially sensitive information over unsecured wireless networks for several years before realizing it, the agency said it is satisfied that Google has taken adequate measures to improve its internal privacy controls. Those include privacy training for all 23,000 of the company's employees.

The FCC inquiry, first reported by The Wall Street Journal, will focus on whether Google violated a federal law that prohibits the unauthorized publication or use of messages intercepted over radio networks.

"As the agency charged with overseeing the public airwaves, we are committed to ensuring that the consumers affected by this breach of privacy receive a full and fair accounting," Michele Ellison, head of the FCC's Enforcement Bureau, said in a statement.

Google has said it gathered about 600 gigabytes of data -- enough to fill about six floors of an academic library -- in more than 30 nations and wants to delete all of the information as soon it's cleared to do so in all affected countries. But the company is facing a number of investigations both in the U.S. and overseas.

In addition to the FCC, a coalition of state attorneys general is examining the data collection and several prominent House members have criticized the company. Authorities in several other countries, including Italy, are also looking into the problem.

Last month, an investigation by Canada's Privacy Commissioner concluded that Google violated Canadian privacy law by collecting highly sensitive personal information -- including complete e-mail messages, e-mail addresses, telephone numbers and even personal medical details -- affecting thousands of citizens. The report blamed the episode on "an engineer's careless error as well as a lack of controls to ensure that necessary procedures to protect privacy were followed."
Reacting to the FCC inquiry on Wednesday, Google stressed that the incident was simply a mistake, that it did not want the data and that it has never used the information in any of its products and services. "As we have said before, we are profoundly sorry for having mistakenly collected payload data from unencrypted networks," the company said in a statement.
Entire Google work force to get 10% raises
Associated Press
Posted: 11/10/2010 [Source: The Detroit News]

New York—Google is reminding its 23,300 employees how much they are appreciated by giving them all 10 percent raises next year.

The Internet search leader also is shifting a portion of the annual bonuses into workers' regular paychecks. Google Inc. CEO Eric Schmidt celebrated the good news in an internal memo Tuesday to employees.

The planned raises, earlier reported by the technology blog Silicon Alley Insider, were confirmed today by the Associated Press.

Schmidt says Google wants to reward its employees for their hard work, but it also could be meant to prevent rivals such as Facebook from luring its workers away.

The raises are also the latest sign that Google expects to continue growing at a robust rate. The company has added 3,500 workers so far this year.
Google Cars Drive Themselves, in Traffic Networks Are Absent
By John Markoff

MOUNTAIN VIEW, Calif. – Anyone driving the twists of Highway 1 between San Francisco and Los Angeles recently may have glimpsed a Toyota Prius with a curious funnel-like cylinder on the roof. Harder to notice was that the person at the wheel was not actually driving.

The car is a project of Google, which has been working in secret but in plain view on vehicles that can drive themselves, using artificial-intelligence software that can sense anything near the car and mimic the decisions made by a human driver.

With someone behind the wheel to take control if something goes awry and a technician in the passenger seat to monitor the navigation system, seven test cars have driven 1,000 miles without human intervention and more than 140,000 miles with only occasional human control. One even drove itself down Lombard Street in San Francisco, one of the steepest and curviest streets in the nation. The only accident, engineers said, was when one Google car was rear-ended while stopped at a traffic light.

Autonomous cars are years from mass production, but technologists who have long dreamed of them believe that they can transform society as profoundly as the Internet has.

Robot drivers react faster than humans, have 360-degree perception and do not get distracted, sleepy or intoxicated, the engineers argue. They speak in terms of lives saved and injuries avoided – more than 37,000 people died in car accidents in the United States in 2008. The engineers say the technology could double the capacity of roads by allowing cars to drive more safely while closer together. Because the robot cars would eventually be less likely to crash, they could be built lighter, reducing fuel consumption. But of course, to be truly safer, the cars must be far more reliable than, say, today’s personal computers, which crash on occasion and are frequently infected.

The Google research program using artificial intelligence to revolutionize the automobile is proof that the company’s ambitions reach beyond the search engine business. The program is also a departure from the mainstream of innovation in Silicon Valley, which has veered toward social networks and Hollywood-style digital media.

During a half-hour drive beginning on Google’s campus 35 miles south of San Francisco last Wednesday, a Prius equipped with a variety of sensors and following a route programmed into the GPS navigation system nimbly accelerated in the entrance lane and merged into fast-moving traffic on Highway 101, the freeway through Silicon Valley.
It drove at the speed limit, which it knew because the limit for every road is included in its database, and left the freeway several exits later. The device atop the car produced a detailed map of the environment.

The car then drove in city traffic through Mountain View, stopping for lights and stop signs, as well as making announcements like “approaching a crosswalk” (to warn the human at the wheel) or “turn ahead” in a pleasant female voice. This same pleasant voice would, engineers said, alert the driver if a master control system detected anything amiss with the various sensors.

The car can be programmed for different driving personalities – from cautious, in which it is more likely to yield to another car, to aggressive, where it is more likely to go first.

Christopher Urmson, a Carnegie Mellon University robotics scientist, was behind the wheel but not using it. To gain control of the car he has to do one of three things: hit a red button near his right hand, touch the brake or turn the steering wheel. He did so twice, once when a bicyclist ran a red light and again when a car in front stopped and began to back into a parking space. But the car seemed likely to have prevented an accident itself.

When he returned to automated “cruise” mode, the car gave a little “whir” meant to evoke going into warp drive on “Star Trek,” and Dr. Urmson was able to rest his hands by his sides or gesticulate when talking to a passenger in the back seat. He said the cars did attract attention, but people seem to think they are just the next generation of the Street View cars that Google uses to take photographs and collect data for its maps.

The project is the brainchild of Sebastian Thrun, the 43-year-old director of the Stanford Artificial Intelligence Laboratory, a Google engineer and the co-inventor of the Street View mapping service.

In 2005, he led a team of Stanford students and faculty members in designing the Stanley robot car, winning the second Grand Challenge of the Defense Advanced Research Projects Agency, a $2 million Pentagon prize for driving autonomously over 132 miles in the desert.

Besides the team of 15 engineers working on the current project, Google hired more than a dozen people, each with a spotless driving record, to sit in the driver’s seat, paying $15 an hour or more. Google is using six Priuses and an Audi TT in the project.

The Google researchers said the company did not yet have a clear plan to create a business from the experiments. Dr. Thrun is known as a passionate promoter of the potential to use robotic vehicles to make highways safer and lower the nation’s energy costs. It is a commitment shared by Larry Page, Google’s co-founder, according to several people familiar with the project.
The self-driving car initiative is an example of Google’s willingness to gamble on technology that may not pay off for years, Dr. Thrun said. Even the most optimistic predictions put the deployment of the technology more than eight years away.

One way Google might be able to profit is to provide information and navigation services for makers of autonomous vehicles. Or, it might sell or give away the navigation technology itself, much as it offers its Android smart phone system to cellphone companies.

But the advent of autonomous vehicles poses thorny legal issues, the Google researchers acknowledged. Under current law, a human must be in control of a car at all times, but what does that mean if the human is not really paying attention as the car crosses through, say, a school zone, figuring that the robot is driving more safely than he would?

And in the event of an accident, who would be liable – the person behind the wheel or the maker of the software?

“The technology is ahead of the law in many areas,” said Bernard Lu, senior staff counsel for the California Department of Motor Vehicles. “If you look at the vehicle code, there are dozens of laws pertaining to the driver of a vehicle, and they all presume to have a human being operating the vehicle.”

The Google researchers said they had carefully examined California’s motor vehicle regulations and determined that because a human driver can override any error, the experimental cars are legal. Mr. Lu agreed.

Scientists and engineers have been designing autonomous vehicles since the mid-1960s, but crucial innovation happened in 2004 when the Pentagon’s research arm began its Grand Challenge.

The first contest ended in failure, but in 2005, Dr. Thrun’s Stanford team built the car that won a race with a rival vehicle built by a team from Carnegie Mellon University. Less than two years later, another event proved that autonomous vehicles could drive safely in urban settings.

Advances have been so encouraging that Dr. Thrun sounds like an evangelist when he speaks of robot cars. There is their potential to reduce fuel consumption by eliminating heavy-footed stop-and-go drivers and, given the reduced possibility of accidents, to ultimately build more lightweight vehicles.

There is even the farther-off prospect of cars that do not need anyone behind the wheel. That would allow the cars to be summoned electronically, so that people could share them. Fewer cars would then be needed, reducing the need for parking spaces, which consume valuable land. And, of course, the cars could save humans from themselves.

“Can we text twice as much while driving, without the guilt?” Dr. Thrun said in a recent talk. “Yes, we can, if only cars will drive themselves.”
Google TV Announces Its Programming Partners, but the Top Networks Are Absent
By Claire Cain Miller and Brian Stetler

Google announced on Monday its first content partners for Google TV, its effort to marry two mediums – the Internet and television. But the announcement underscored the difficulties companies face as they try to work their way into the living room.

The major television networks – ABC, CBS, Fox and NBC – will not participate, at least for the moment. However, several Internet companies and media outlets, including HBO, CNBC, Twitter, Netflix and Amazon, will work with Google to offer Web content and programming via television sets, the company said. They will allow on-demand viewing or build apps for TV screens.

James L. McQuivey, a principal analyst at Forrester, the technology research firm, called the partnerships “underwhelming.” Still, he said, other Google TV features, like the ability to search the Web for information about an actor or chat with friends on Twitter while watching TV, are more important to its success.

“They don’t actually need content partners to start their little revolution,” he said. “They don’t need the major broadcasters to play along because they can do a lot of cool things with you as a viewer without having to share any of the money.”

Google TV is the latest and most prominent service to connect TVs to the Web, promising to make all the living room’s audio and video as searchable and instantly accessible as the Internet’s content. That promise requires significant cooperation from media companies, and many have been reluctant to help.

With Google TV, the company wants to be a leader in the budding industry of Internet-connected television sets, which Forrester expects to be in 43 million United States homes by 2015, up from two million this year.

The average American watches five hours of TV a day, making it the biggest medium for advertisers. “One of our goals with Google TV is to finally open up the living room and enable new innovation from content creators, programmers, developers and advertisers,” Ambarish Kenghe, developer product manager for Google TV, wrote in the company blog post on Monday. Google faces competition from makers of set-top boxes including Apple, TiVo, Boxee and Roku, and from television distributors.

In addition to media companies’ caution, they all face another overarching challenge: TV viewers unimpressed with Internet-connected televisions. Just 3 percent of people own or intend to buy one, and almost two-thirds have not heard of them, according to Forrester. Of those who own them, a quarter do not use the Web capabilities. Still, major
players in the technology and media sectors are largely in agreement that Internet-connected sets are poised to take off.

The Google TV technology, which was announced in May and will be available to consumers in the coming weeks, will be built into new Sony high-definition televisions and Blu-ray players, and into a Logitech set-top box that viewers can use with their existing sets. Google will make its software available to other makers of TVs and set-top boxes. The companies have not yet said how much the equipment would cost.

Logitech is building a remote control for searching the TV and the Web, and viewers can also use their Android phones or iPhones as a remote control and “fling” a video they are watching on their phones to the television.

Google TV has been in talks with the major networks and Hollywood studios about optimizing their Web sites for TV screens and about obtaining data about their programs for search purposes. But one executive described the relationship between Google and the networks as being at the “first date” stage.

According to executives involved, some networks want Google to share revenue from the ads that it overlays on videos. Some want Google to weed out illegal Internet sources of their shows and make sure that their marquee programs still stand out on a service that potentially levels the playing field for all makers of video.

The executives insisted on anonymity because the networks uniformly declined on Monday to comment on Google TV, and because they did not want to perturb a company as big as Google.

One of Google TV’s deals is with Turner Broadcasting, which owns TBS, TNT and other cable channels. Turner said it would optimize the Web sites of its channels for big-screen viewing.

HBO, which like Turner is a unit of Time Warner, will make its online on-demand Web site HBO Go available through Google TV, though only for HBO subscribers. Apps are another priority for Google TV, and another area where the company needs help from content providers. NBC Universal said it would deploy CNBC Real-Time, which allows for stock tracking on the screen alongside the live broadcast of the CNBC business channel, and the National Basketball Association said it would modify its existing N.B.A. Game Time app for TV screens.

Several media and Internet companies have also built new versions of their Web sites for viewing on televisions. These include the music services Vevo, Pandora and Napster, along with YouTube, Twitter, USA Today and The New York Times.
Due Diligence Checks

Google:

The investigation is ongoing.

288A-SF-133411-Case was opened January 3, 2003. Google.com was a victim of two Denial of Service (DOS) attacks on January 2, 2003. Investigation led to the identification and eventual arrest.
Attached is a copy of the Director's thank you letters to Google CEO Eric Schmidt, Facebook COO Sheryl Sandberg, and Microsoft CEO Steve Ballmer for meeting with the FBI about the Going Dark Initiative. No hard copies will follow. Please further disseminate as needed.

Thanks,

[Signature]

Supervisory Writer-Editor
Office of the Executive Secretariat
FBIHQ - Room 6147

SENSITIVE BUT UNCLASSIFIED
Mr. Eric Schmidt  
Chairman of the Board and  
Chief Executive Officer  
Google Inc.  
1600 Amphitheatre Parkway  
Mountain View, CA 94043

Dear Mr. Schmidt:

It was a pleasure meeting with you earlier this week and hearing your thoughts. My colleagues and I found the discussion with your delegation to be very productive, and we look forward to continued dialogue in the future.

Sincerely yours,

Robert S. Mueller, III  
Director
"Going Dark"
Meeting Attendees
11/16-11/17/2010

Google, 11:00 a.m. on 11/16/2010
Eric Schmidt, CEO
Kent Walker, General Counsel
Richard Salgado, Corporate Attorney
Bill Coughran, Technologist

Facebook, 2:00 p.m. on 11/16/2010
Sheryl Sandberg, Chief Operating Officer
Joe Sullivan, Chief Security Officer

Microsoft, 8:30 a.m. on 11/17/2010
Steve Ballmer, CEO
Brad Smith, Senior Vice President & General Counsel
Scott Charney, Corporate Vice President
Google Meeting, 11:00 a.m., 11/16/2010