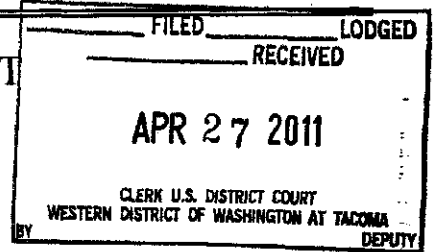


# UNITED STATES DISTRICT COURT

for the  
Western District of Washington



In the Matter of the Search of  
*(Briefly describe the property to be searched  
or identify the person by name and address)*

The residence located at  
3921 55th Street Ct NW  
Gig Harbor, WA 98335

Case No. MJ11-5078

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, which is incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

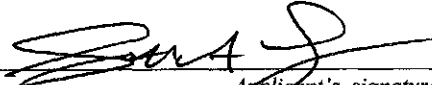
The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. 1030	Fraud and Related Activity in Connection with Computers

The application is based on these facts:

See attached affidavit of Special Agent Scott Love, attached hereto and incorporated herein.


- Continued on the attached sheet.
- Delayed notice of        days (give exact ending date if more than 30 days:       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
\_\_\_\_\_  
*Applicant's signature*

Scott Love, Affiant  
\_\_\_\_\_  
*Printed name and title*

Sworn to before me and signed in my presence.

Date: 4/26/11

  
\_\_\_\_\_  
*Judge's signature*

City and state: Tacoma, Washington

J. Richard Creatura, United States Magistrate Judge  
\_\_\_\_\_  
*Printed name and title*

**AFFIDAVIT**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

STATE OF WASHINGTON )  
 )  
COUNTY OF PIERCE ) SS

I, Scott A. Love, being first duly sworn on oath, do hereby depose and state:

**I. INTRODUCTION**

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since March 2010. I am currently assigned to the Los Angeles Field Division, Cyber Crimes Squad. In that assignment, I am responsible for investigating computer and high-technology crimes, and I am trained and authorized to investigate the offenses alleged herein. While working as a Special Agent of the FBI, I have participated in the service of search warrants involving searches and seizures of computers, computer equipment, software, electronically stored information, and instrumentalities of fraud. In addition to attending the 21-week FBI Academy in Quantico, Virginia, I have attended FBI training on basic techniques for computer crime investigations, computer technology, computer fraud, intellectual property crimes, and white collar crime. Prior to becoming an FBI agent, I was employed in the private sector for eight years. Additionally, I have a Bachelor of Science degree in Information Technology.

**II. PURPOSE OF AFFIDAVIT**

2. This affidavit is submitted in the United States District Court for the Western District of Washington in support of an application for a warrant to search the premises of DARRIN M. LANTZ, 3921 55th Street CT NW, Gig Harbor, Washington 98335 ("SUBJECT RESIDENCE"), which is described more specifically in Attachment A, for evidence and/or instrumentalities of violations of Title 18, United States Code, Section 1030 (Fraud and Related Activity In Connection With Computers).

1 3. The statements contained in this affidavit are based upon my training and  
2 experience, information provided to me by other investigators, other law enforcement  
3 officers, and witnesses as part of this investigation. Because this affidavit is submitted  
4 for the limited purpose of securing a search warrant, I have not included each and every  
5 fact known to me concerning this investigation. I have only set forth facts that I believe  
6 are necessary to the determination of probable cause to believe that evidence of violations  
7 of Title 18, United States Code, Section 1030 is presently located at the SUBJECT  
8 RESIDENCE. Furthermore, unless specifically indicated otherwise, all conversations and  
9 statements described in this affidavit are not related verbatim, but are related in substance  
10 and in part only.

11 **III. RELEVANT LEGAL STATUES**

12 4. Title 18, United States Code, Section 1030(a)(5) states, in pertinent part,  
13 that

14 Whoever -

15 (A) knowingly causes the transmission of a program,  
16 information, code, or command, and as a result of such  
17 conduct, intentionally causes damage without  
authorization, to a protected computer;

18 (B) intentionally accesses a protected computer without  
19 authorization, and as a result of such conduct,  
recklessly causes damage; or

20 (C) intentionally accesses a protected computer without  
21 authorization, and as a result of such conduct, causes  
22 damage and loss

23 shall be punished as provided in this statute.

24 **IV. SUMMARY OF INVESTIGATION**

25 5. On October 21, 2010, Berry Mallen, attorney for Gene Simmons  
26 ("VICTIM"), reported a Distributed Denial of Service attack ("DDoS") which affected his  
27 client's websites www.genesimmons.com, www.simmonsrecords.com, and  
28 www.kissonline.com . The attacks were launched on October 14, 2010, ten days after the

1 VICTIM made comments relating to anti-piracy during an appearance at MIPCOM, a  
2 media content-related event held annually in Cannes, France.

3 6. At the time of the attacks, the VICTIM's servers were hosted by  
4 BCSWebCo in Florida. BCSWebCo took the websites offline due to the DDoS attacks  
5 and prepared to transition the sites to another host server operated by Sheppard  
6 Communications Inc., located in California and run by Mark Sheppard. Sheppard was  
7 able to get the VICTIM's websites back online within thirty-six (36) hours of the attacks.

8 7. Once the websites were back online, the VICTIM posted a message on his  
9 site indicating, to an extent, he and law enforcement would track down the attackers. On  
10 or about October 18, 2010, the servers at Sheppard Communications Inc., experienced a  
11 DDoS attack, which lasted through October 22, 2010. To date, the attacks on the  
12 VICTIM's websites have cost the VICTIM approximately \$20,000 to \$25,000 in  
13 downtime and costs associated with changing computer servers and website hosts.

14 8. Both attacks on the VICTIM's websites were claimed by an internet activist  
15 group named "Anonymous" (Anonymous), which titled their attacks "Operation  
16 Payback." Review of several online news reports and tech sites such as myce.com  
17 (<http://www.myce.com/news/this-week-operation-payback-targets-gene-simmons-mpaa-3>  
18 [5461](http://www.myce.com/news/this-week-operation-payback-targets-gene-simmons-mpaa-3)), dated October 16, 2010; softpedia.com (<http://news.softpedia.com/news/gene>  
19 [-simmons-angers-anonymous-161476.shtml](http://news.softpedia.com/news/gene)), dated October 18, 2010; myce.com  
20 (<http://www.myce.com/news/gene-simmons-threatens-anonymous-gets-ddosed-again-355>  
21 [03](http://www.myce.com/news/gene-simmons-threatens-anonymous-gets-ddosed-again-355)), dated October 19, 2010; and techworld.com (<http://news.techworld.com/security/>  
22 [3244964/gene-simmons-battles-anonymous-group-after-new-ddos-attacks](http://news.techworld.com/security/)), dated October  
23 20, 2010, reveal how Anonymous took responsibility for the attacks. Anonymous has  
24 also claimed to have launched DDoS attacks on the Motion Picture Association of  
25 America, the Recording Industry Association of America, the United States Copyright  
26 Office, Visa, MasterCard, and PayPal.

1 **V. BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND**  
2 **INTERNET COMMUNICATION**

3 9. Internet. The Internet is a collection of computers and computer networks  
4 which are connected to one another via high-speed data links and telephone lines for the  
5 purpose of communicating and sharing data and information. Connections between  
6 Internet computers exist across state and international borders; therefore, information sent  
7 between two computers connected to the Internet frequently crosses state and  
8 international borders even when the two computers are located in the same state.

9 10. Internet Service Providers. Individuals and businesses obtain access to the  
10 Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide  
11 their customers with access to the Internet using telephone or other telecommunications  
12 lines; provide Internet e-mail accounts that allow users to communicate with other  
13 Internet users by sending and receiving electronic messages through the ISPs' servers;  
14 remotely store electronic files on their customers' behalf; and may provide other services  
15 unique to each particular ISP. ISPs maintain records pertaining to the individuals or  
16 businesses that have subscriber accounts with them. Those records often include  
17 identifying and billing information, account access information in the form of log files,  
18 e-mail transaction information, posting information, account application information, and  
19 other information both in computer data and written record format.

20 11. IP Addresses. An Internet Protocol address ("IP address") is a unique  
21 numeric address used by each computer on the Internet. An IP address is a series of four  
22 numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every  
23 computer attached to the Internet must be assigned an IP address so that Internet traffic  
24 sent from and directed to that computer may be properly directed from its source to its  
25 destination. Most ISPs control a range of IP addresses.

26 12. When a customer logs into the Internet using the service of an ISP, the  
27 computer used by the customer is assigned an IP address by the ISP. The customer's  
28

1 computer retains that IP address for the duration of that session (i.e., until the user  
2 disconnects), and the IP address cannot be assigned to another user during that period.

3 13. Internet Addresses. Every device on the Internet has an address that allows  
4 other devices to locate and communicate with it. An IP address is a unique number that  
5 identifies a device on the Internet. Other addresses include Uniform Resource Locator  
6 addresses ("URL address"), such as <http://www.fbi.gov>, which are typically used to  
7 access web sites or other services on remote devices. Domain names of Web sites, host  
8 names, and machine addresses are other types of addresses associated with Internet use.  
9 Domain name registrars contain registration information concerning the identity of the  
10 owner of a domain name.

11 14. Internet Relay Chat ("IRC"). A system for Internet-based "chatting" that  
12 uses client/server software. Using IRC, one can start a chat group (called a "channel") or  
13 join an existing chat group. Generally, a channel is dedicated to a particular topic, which  
14 may be reflected by the channel's name. Participants in chat channels commonly use  
15 nicknames instead of their real names to identify themselves. In addition, users with  
16 privileged access to IRC are called IRC operators, network administrators, or server  
17 administrators. These users have the power to forcibly disconnect users from IRC by  
18 issuing a "kill" command, the power to ban users, and the power to change network  
19 routing by disconnecting or connecting servers.

20 15. Based on my knowledge, training, and experience, I know IRC is a common  
21 mode of communication used by hackers for discussion of who committed recent  
22 computer intrusions and new techniques for computer intrusions.

23 16. Web hosting. This essentially means providing space for a website, or  
24 content, on the Internet. This content can include IRC server space. Typically when  
25 someone registers a domain, he or she points that domain to the location of the  
26 corresponding website or service, whether it is located on a computer or server owned by  
27 the end user or one owned by a web hosting service. The owner of a domain is free to  
28

1 change hosting providers at any time. All he or she would have to do is provide the new  
2 IP address of the host location to the registry service.

3 17. Domain Name Service ("DNS"). An Internet resource for converting  
4 alphanumeric names into IP addresses. DNS provides several features, including the  
5 ability to refer to Internet addresses by easy-to-remember names rather than  
6 difficult-to-remember numbers. DNS provides other benefits, including the ability to  
7 change the underlying IP address while preserving the availability of the resource. Users  
8 would still request the resource by name, and DNS would resolve the name to the new IP  
9 address. DNS also provides the ability to have a name resolve to multiple IP addresses,  
10 for performance and load-balancing reasons or to provide some protection against the  
11 failure of a single IP address or computer.

12 18. Domain Name. Naming system designed to organize internet traffic.  
13 Organized hierarchically and read right-to-left, the right-most component is the "top level  
14 domain." This includes the ".com," ".gov," ".mil," and ".edu" domains as well as many  
15 others. Top level domains are owned and managed by the Internet sanctioning  
16 organizations. The second part of the domain name is owned by the registrant who first  
17 registered the name with the sanctioning organizations. It is common to refer to a  
18 registered domain and top-level domain combination as a "domain name". Examples  
19 include "google.com" and "cybercrime.gov." Domain name owners can then create  
20 sub-domains to provide addresses to resources they own and/or control. For example, the  
21 DNS sub-domain "www" ("World Wide Web") is generally used to denote an  
22 organization's web server, so "www.google.com" would, and does, point to Google's main  
23 website. Domain names are commonly inserted into the URL on a web browser  
24 application in order to "point" the computer user to that particular resource or service on  
25 the internet. World Wide Web URLs begin with http://.

26 19. Distributed Denial of Service Attack (or "DDoS attack").  
27 A DDoS attack is a type of malicious computer activity by which an attacker causes a  
28 network of computers to "flood" a victim computer with large amounts of data or specific

1 commands. As a result, the victim computer is unable to handle legitimate network  
2 traffic and legitimate users are denied the services of the computer. Depending on the  
3 type and strength of the DDoS attack, the victim computer and its network may become  
4 completely disabled and unable to perform their intended functions without significant  
5 repair.

6 20. Access/Error Logs. List of all requests for individual files that people have  
7 requested from a Web site. These files could include the HTML files and their imbedded  
8 graphic images and any other associated files that get transmitted. In general, an access  
9 log can be analyzed to tell you the number of visitors (unique first-time requests) to a  
10 home page, the origin of the visitors in terms of their associated server's domain name,  
11 how many requests were received for each page at the site (which can be presented with  
12 the pages with most requests listed first), and usage patterns in terms of time of day and  
13 day of week.

14 21. Packet. The unit of data that is routed between an origin and destination on  
15 the Internet or any other packet-switched network. When any file (e.g., e-mail message,  
16 Graphics Interchange Format file (\*.gif, one of the ways in which pictures or photographs  
17 are transmitted via the Internet), Uniform Resource Locator request) is sent from one  
18 place to another on the Internet, the Transmission Control Protocol (TCP) layer divides  
19 the file into "chunks" of an efficient size for routing. Each of these packets is separately  
20 numbered and includes the Internet address of the destination (i.e., the IP address). The  
21 individual packets for a given file may travel different routes through the Internet; when  
22 all the packets arrive at the destination, they are reassembled into the original file by the  
23 TCP layer at the receiving end.

24 22. Low Orbit Ion Cannon/High Orbit Ion Cannon (LOIC/HOIC). LOIC/HOIC  
25 are packet flooding tools using User Datagram Protocol ("UDP"), TCP, and Hypertext  
26 Transfer Protocol ("HTTP") methods. LOIC/HOIC are open source computer programs  
27 that were designed as network stress testing applications. Attackers can use this tool to  
28 send extremely large numbers of packets over the network to attempt to overwhelm a



1 target. When used collectively from multiple sources, a DDoS can occur against a target  
2 site by flooding the site with TCP packets, UDP packets, or HTTP requests with the  
3 intention of disrupting the service of the target site. LOIC can be used in two ways,  
4 manual or HIVE Mode (Hive Mind). If using manual mode, the user must enter a target,  
5 such as an IP address or the http address of the target.

6 a. HIVE and/or HIVE Mind. This mode of LOIC/HOIC enables the  
7 user to connect LOIC/HOIC to an IRC server, allowing someone else to control which  
8 specific target all connected LOIC/HOIC clients are aimed at. The user is basically  
9 agreeing to participate in a "voluntary" BotNet.

10 23. BotNet. A term for a collection of computers, sometimes referred to as  
11 bots, which run autonomously. While the term "BotNet" can be used to refer to any  
12 group of bots, such as Internet Relay Chat (IRC) bots, the word is generally used to refer  
13 to a collection of compromised machines running programs, usually referred to as worms,  
14 Trojan horses, or backdoors, under a common "command and control" (C&C)  
15 infrastructure. A BotNet's originator, referred to as a "botherder" can control the group  
16 remotely through communications using a specific protocol, usually IRC, and usually for  
17 nefarious purposes. Individual programs manifest as IRC bots. Often the command and  
18 control takes place via an IRC server or a specific channel on a public IRC network. A  
19 bot typically runs hidden, that is, the user of the infected computer is not aware that it is  
20 running the bot program. Generally, the perpetrator of the BotNet has compromised a  
21 series of systems using various tools (exploits, buffer overflows, as well as others).  
22 BotNets have become a significant part of the Internet, albeit increasingly hidden. Due to  
23 the fact that most conventional IRC networks have taken measures to block access to  
24 previously hosted BotNets, botherders must now find their own servers. Often, a BotNet  
25 will include a variety of connections, ranging from dial-up, DSL, and cable modems, and  
26 a variety of network types, including educational, corporate, government and even  
27 military networks. Sometimes, a botherder will hide an IRC server installation on an  
28

1 educational or corporate site, where high speed connections can support a large number of  
2 bots.

3 24. Command and Control ("C&C") node or server. A C&C node/server is a  
4 computer managing a particular network of bots. There can be one or many, including a  
5 hierarchy, of C&C computers managing a BotNet.

6 25. Twitter. A website owned and operated by Twitter, Inc., which offers  
7 social networking and microblogging service that enables its users to send and read  
8 messages called "tweets." Tweets are publicly visible by default; however, senders can  
9 restrict message delivery to their followers. Users may subscribe to other users' tweets.

#### 10 VI. PROBABLE CAUSE

11 26. On November 5, 2010, the FBI received a call from Mark Sheppard of  
12 Sheppard Communications, Inc. Sheppard explained he had captured the DDoS attacks  
13 on the VICTIM's websites and was willing to make copies for the FBI to review.

14 27. On November 8, 2010, Mark Sheppard delivered three DVD-R discs  
15 containing access and error logs from the VICTIM's websites to the Los Angeles Field  
16 Office. The time frame for data contained on the three DVD-R discs was October 18,  
17 2010 to October 22, 2010.

18 28. The data provided by Sheppard was considered to be raw data, meaning a  
19 program would have to be used in order to organize and pull out trends. Log parser tools  
20 were used to review the access and error logs. These programs and methods were used to  
21 determine how many times a specific IP address attacked the websites in the time frame  
22 of October 18, 2010 to October 22, 2010, and to record those unique specific IP addresses  
23 and their counts.

24 29. Results from these methods and programs provided several unique IP  
25 addresses. Each IP address was shown to have attacked the websites at an extremely high  
26 rate. One such IP address, 207.118.30.112, attacked the website 48,471 times during the  
27 time frame of October 19, 2010, at 21:11:04 MST to October 19, 2010, at 21:58:28 MST,  
28 a period of 47 minutes and 24 seconds.

1           30.    On November 30, 2010, an IP address locator was used to determine the  
2 ISP for IP address 207.118.30.112. The results returned CenturyLink as the ISP for IP  
3 Address 207.118.30.112.

4           31.    On December 7, 2010, a Federal Grand Jury subpoena was served on  
5 CenturyLink, requesting subscriber information for IP address 207.118.30.112 on  
6 October 19, 2010 at 21:11:04 MST.

7           32.    On December 9, 2010, a response was received from CenturyLink. A  
8 review of the results revealed the subscriber to the IP address as Darrin M. Lantz, with a  
9 service location of 3921 55th Street CT NW, Gig Harbor, Washington, 98335, the  
10 SUBJECT RESIDENCE. Information provided by Century Link did not state whether  
11 the subscriber was utilizing the service through a wired connection, a secured wireless  
12 connection, or an unsecured wireless connection. Additional research into the DSL  
13 services provided by Century Link reveals that they supply Westell brand modems to their  
14 customers.

15           33.    On March 2, 2011, FBI Agents verified a wireless connection in the area of  
16 the SUBJECT RESIDENCE. One wireless network, named "Westell3428," appeared  
17 secured, meaning the wireless network needed a password in order to access it. Another  
18 wireless network, "La Casa Sandoval," was also verified in the area of the SUBJECT  
19 RESIDENCE. This network was unsecured; after researching the name "Sandoval," no  
20 connection between that wireless network name and any residence in the area was found.  
21 It cannot be determined with absolute certainty that the secured wireless network  
22 "Westell3428" came from the SUBJECT RESIDENCE, however, due to the strength of  
23 the signal the Agents picked up directly in front of the residence, and the fact that Westell  
24 brand modems were found to be used with the SUBJECT RESIDENCE's ISP for DSL  
25 service, there is reason to believe the SUBJECT RESIDENCE is using the secured  
26 "Westell3428" wireless network. On March 4, 2011, FBI Agents verified a vehicle  
27 parked in the driveway of the SUBJECT RESIDENCE to be registered to Rhoda D.  
28 Lantz, the wife of Darrin Lantz.

1           34.    The wireless network appearing in or around the SUBJECT RESIDENCE  
2 was secured requiring the use of a password to access and utilize the wireless network.  
3 Based on the use of a secured wireless network, in conjunction with the IP address  
4 recovered from the logs of the VICTIM'S websites linking back to the SUBJECT  
5 RESIDENCE, I believe that someone with access to the computer at the SUBJECT  
6 RESIDENCE, took part in the DDoS attacks. Alternatively, if the computer at the  
7 SUBJECT RESIDENCE was compromised prior to the DDos attacks, a forensic  
8 examination of the computer would reveal evidence relating to the activities of  
9 compromised computer use.

#### 10                   **VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES**

11           35.    As used below, the term "digital device" includes any electronic system or  
12 device capable of storing and/or processing data in digital form, including: central  
13 processing units, laptop and notebook computers, personal digital assistants, wireless  
14 communication devices such as mobile telephones (i.e., cell phones); related  
15 communications devices such as modems; storage media such as hard disk drives, floppy  
16 disks, compact disks, magnetic tapes used to store digital data (excluding analog tapes  
17 such as VHS), and memory chips; and security devices. Based on my knowledge,  
18 training, and experience, as well as information related to me by agents and others  
19 involved in the forensic examination of digital devices, I know that data in digital form  
20 can be stored on a variety of digital devices and that during the search of the premises it is  
21 not always possible to search digital devices for digital data for a number of reasons,  
22 including the following:

23                   a.    Searching digital devices can be a highly technical process that  
24 requires specific expertise and specialized equipment. There are so many types of digital  
25 devices and software in use today that it is impossible to bring to the search site all of the  
26 necessary technical manuals and specialized equipment necessary to conduct a thorough  
27 search. In addition, it may also be necessary to consult with specially trained personnel  
28

1 who have specific expertise in the type of digital device, software application or operating  
2 system that is being searched.

3           b.       Digital data is particularly vulnerable to inadvertent or intentional  
4 modification or destruction. Searching digital devices can require the use of precise,  
5 scientific procedures that are designed to maintain the integrity of digital data and to  
6 recover "hidden," erased, compressed, encrypted or password-protected data. As a result,  
7 a controlled environment, such as a law enforcement laboratory or similar facility, is  
8 essential to conducting a complete and accurate analysis of data stored on digital devices.

9           c.       The volume of data stored on many digital devices will typically be  
10 so large that it will be highly impractical to search for data during the execution of the  
11 physical search of the premises. A single megabyte of storage space is the equivalent of  
12 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes,  
13 is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of  
14 storing 500 gigabytes (GB) of data are now commonplace in desktop computers.  
15 Consequently, each non-networked, desktop computer found during a search can easily  
16 contain the equivalent of 240 million pages of data, that, if printed out, would completely  
17 fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 GB drive could contain as  
18 many as approximately 450 full-run movies or 450,000 songs.

19           d.       Electronic files or remnants of such files can be recovered months or  
20 even years after they have been downloaded onto a hard drive, deleted, or viewed via the  
21 Internet. Electronic files saved to a hard drive can be stored for years with little or no  
22 cost. Even when such files have been deleted, they can be recovered months or years  
23 later using readily-available forensics tools. Normally, when a person deletes a file on a  
24 computer, the data contained in the file does not actually disappear, rather, that data  
25 remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or  
26 remnants of deleted files, may reside in free space or unallocated/slack space, i.e., space  
27 on the hard drive that is not allocated to an active file or that is unused after a file has  
28 been allocated to a set block of storage space for long periods of time before they are

1 overwritten. In addition, a computer's operating system may also keep a record of deleted  
2 data in a swap or recovery file. Similarly, files that have been viewed via the Internet are  
3 automatically downloaded into a temporary Internet directory or cache. The browser  
4 typically maintains a fixed amount of hard drive space devoted to these files, and the files  
5 are only overwritten as they are replaced with more recently viewed Internet pages. Thus,  
6 the ability to retrieve residue of an electronic file from a hard drive depends less on when  
7 the file was downloaded or viewed than on a particular user's operating system, storage  
8 capacity, and computer habits. Recovery of residue of electronic files from a hard drive  
9 requires specialized tools and a controlled laboratory environment.

10 e. Although some of the records called for by this warrant might be  
11 found in the form of user-generated documents (such as word processor, picture, and  
12 movie files), digital devices can contain other forms of electronic evidence as well. In  
13 particular, records of how a digital device has been used, what it has been used for, who  
14 has used it, and who has been responsible for creating or maintaining records, documents,  
15 programs, applications and materials contained on the digital devices, are called for by  
16 this warrant. Those records will not always be found in digital data that is neatly  
17 segregable from the hard drive image as a whole. Digital data on the hard drive not  
18 currently associated with any file can provide evidence of a file that was once on the hard  
19 drive but has since been deleted or edited, or of a deleted portion of a file (such as a  
20 paragraph that has been deleted from a word processing file). Virtual memory paging  
21 systems can leave digital data on the hard drive that show what tasks and processes on the  
22 computer were recently used. Web browsers, e-mail programs, and chat programs store  
23 configuration data on the hard drive that can reveal information such as online nicknames  
24 and passwords. Operating systems can record additional data, such as the attachment of  
25 peripherals, the attachment of USB flash storage devices, and the times the computer was  
26 in use. Computer file systems can record data about the dates files were created and the  
27 sequence in which they were created. This data can be evidence of a crime, indicate the  
28 identity of the user of the digital device, or point toward the existence of evidence in other

1 | locations. Recovery of this data requires specialized tools and a controlled laboratory  
2 | environment.

3 |           f.       Further, evidence of how a digital device has been used, what it has  
4 | been used for, and who has used it, may be found in the absence of particular data on a  
5 | digital device. For example, to rebut a claim that the owner of a digital device was not  
6 | responsible for a particular use because the device was being controlled remotely by  
7 | malicious software, it may be necessary to show that malicious software that allows  
8 | someone else to control the digital device remotely is not present on the digital device.  
9 | Evidence of the absence of particular data on a digital device is not segregable from the  
10 | digital device. Analysis of the digital device as a whole to demonstrate the absence of  
11 | particular data requires specialized tools and a controlled laboratory environment.

#### 12 |                           **VIII. PRIOR EFFORTS TO OBTAIN EVIDENCE**

13 |       36.     Any other means of obtaining the necessary evidence to prove the elements  
14 | of computer/Internet-related crimes, for example, a consent search, would result in an  
15 | unacceptable risk of the loss and/or destruction of the evidence sought. At this point in  
16 | the investigation, given the sophistication of the DDoS attack on the VICTIM's websites,  
17 | I believe that whoever participated in the DDoS attack, most likely someone within the  
18 | SUBJECT RESIDENCE, has a high level of computer skill and that there is an actual risk  
19 | of data loss or destruction. Thus, the only effective means of collecting and preserving  
20 | the required evidence is through a search warrant.

#### 21 |                           **IX. ITEMS TO BE SEIZED**

22 |       37.     Based on the foregoing, I respectfully submit that there is probable cause to  
23 | believe that the following items, which constitute evidence of violation of Title 18,  
24 | United States Code, Section 1030 (Fraud and Related Activity In Connection With  
25 | Computers), will be found at the SUBJECT RESIDENCE:

##### 26 |                   Physical Items

27 |       a.     Any physical digital device and/or computer used to commit or store  
28 | evidence of the offenses listed above;

1           b. Any physical equipment used to facilitate the offenses listed above  
2 by the transmission, creation, display, encoding or storage of digital data, including word  
3 processing equipment, modems, routers, and encryption devices;

4           c. Any physical magnetic, electronic, or optical storage devices used to  
5 store data related to the offenses above, such as floppy disks, hard disks, tapes,  
6 CD-ROMS, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart  
7 cards, memory sticks, thumb drives, smartphones, electronic tablets;

8           d. Any physical keys, encryption devices, dongles and similar physical  
9 items that are necessary to gain access to the digital device or data stored on the digital  
10 device;

11                   **Digital / Electronic Items**

12           e. Any and all digital records, documents, and materials that relate to  
13 malicious software, code, or other programs associated with Trojans, BotNets, denial of  
14 service attacks, to include but not limited to, LOIC and/or HOIC;

15           f. Any and all digital records, documents, and materials that relate to  
16 communications between the seized computer hard drive and other computers involved in  
17 the denial of service attack, as well as to any individuals that may be controlling the  
18 denial of service attack or participating in the attack, to include IRC chat logs, other  
19 online chat logs, personal messages, Twitter tweets, and/or email related to the denial of  
20 service attacks;

21           g. Any and all digital records, documents, and materials that relate to  
22 the administration, maintenance, operation, use or propagation of the denial of service  
23 tools, to include but not limited to, LOIC/HOIC;

24           h. Any and all digital records, documents, and materials that relate to  
25 the identification and locations of person(s) using or controlling or disseminating denial  
26 of service software;



1 i. Any and all digital records, documents, and materials that relate to  
2 the identification and location of other computers comprising part of the denial of service  
3 attack and/or BotNet;

4 j. Any and all digital data gathered or collected by means of the  
5 operation of the denial of service attack and/or BotNet;

6 k. Any digital logs and other transactional information, to include but  
7 not limited to, internet history, maintained in relation to computer(s) at the SUBJECT  
8 RESIDENCE;

9 **Physical or Digital Items**

10 l. Any physical or digital records, documents, communications, names,  
11 handles/monikers, email accounts, IP addresses and materials (i.e., Word documents,  
12 Excel spreadsheets, chat logs, e-mails) that relate to the denial of service attack;

13 m. Any physical or digital documentation, operating logs, and reference  
14 manuals regarding the operation of the digital device or software used in the digital  
15 device;

16 n. Any physical or digital application, utility programs, compilers,  
17 interpreters, and other software used to facilitate direct or indirect communication with  
18 the digital device; and

19 o. Any physical or digital passwords, password files, test key,  
20 encryption codes, or other information necessary to access the digital device or data  
21 stored on the digital device.

22 38. As used above, the terms records, documents, programs, applications, or  
23 materials include records, documents, programs, applications, or materials created,  
24 modified, or stored in any form, including in digital form on any digital device, and any  
25 forensic copies thereof. The term "digital device" is used as defined above in paragraph  
26 35.

1 39. In accordance with the information in this affidavit, law enforcement  
2 personnel will execute the search of digital devices seized pursuant to this warrant as  
3 follows:

4 a. Upon securing the search site, the search team, comprised of Agents  
5 who have undergone computer training at the FBI Academy in Quantico, Virginia and a  
6 trained Computer Analysis Response Team examiner, will conduct an initial review of  
7 any digital devices/systems to determine whether the ESI contained therein can be  
8 searched and/or duplicated on site in a reasonable amount of time and without  
9 jeopardizing the ability to accurately preserve the data.

10 b. If, based on their training and experience, and the resources available  
11 to them at the search site, the search team determines it is not practicable to make an  
12 on-site search, or to make an on-site copy of the ESI within a reasonable amount of time  
13 and without jeopardizing the ability to accurately preserve the data, then the digital  
14 devices will be seized and transported to an appropriate law enforcement laboratory for  
15 review and to be forensically copied ("imaged") as appropriate.

16 c. In order to examine the ESI in a forensically sound manner, law  
17 enforcement personnel with appropriate expertise will produce a complete forensic image  
18 of any digital device that is found to contain data or items that fall within the scope of  
19 Attachment B of this Affidavit. In addition, appropriately trained personnel may search  
20 for and attempt to recover deleted, hidden, or encrypted data to determine whether the  
21 data fall within the list of items to be seized pursuant to the warrant. In order to search  
22 fully for the items identified in the warrant, law enforcement personnel may then examine  
23 all of the data contained in the forensic image/s and/or on the digital devices, that fall  
24 within the time frame of October 4, 2010 to November 5, 2010. I believe this time frame  
25 to be the most relevant time frame for purposes of this investigation, because the VICTIM  
26 made his public anti-piracy comments on October 4, 2010, as described in paragraph 5  
27 above. These comments were the basis of the first DDoS attack, launched on or about  
28 October 14, 2010. The second DDoS attack was launched on or about October 18, 2010,

1 and I believe it is reasonable to search for data up until November 5, 2010, approximately  
2 two weeks after the second attack, because this leaves a window in which there can still  
3 be evidence of talk/chatter about the crime.

4           d.       The search techniques will involve the use of a “hash value” library  
5 to exclude normal operating system files, standard software files, and other “known  
6 good” files that do not need to be searched. The “hash value” library also contains known  
7 software that can be used for malicious purposes, such as computer hacking. The search  
8 techniques will also include the use of text searches for known file names, and for files  
9 that contain the responsive text identified in this affidavit. The search techniques that will  
10 be used will be only those methodologies, techniques and protocols as may reasonably be  
11 expected to find, identify, segregate and/or duplicate the items authorized to be seized  
12 pursuant to Attachment B to this Affidavit.

13           e.       If, after conducting its examination, law enforcement personnel determine  
14 that any digital device is an instrumentality of the criminal offenses referenced above, the  
15 government may retain that device during the pendency of the case as necessary to,  
16 among other things, preserve the instrumentality evidence for trial, ensure the chain of  
17 custody, and litigate the issue of forfeiture. If law enforcement personnel determine that a  
18 device was not an instrumentality of the criminal offenses referenced above, it shall be  
19 returned to the person/entity from whom it was seized within 90 days of the issuance of  
20 the warrant, unless the government seeks and obtains authorization from the court for its  
21 retention.

22           f.       Unless the government seeks an additional order of authorization  
23 from any Magistrate Judge in the District, the government will return any digital device  
24 that has been forensically copied, that is not an instrumentality of the crime, and that may  
25 be lawfully possessed by the person/entity from whom it was seized, to the person/entity  
26 from whom it was seized within 90 days of seizure.

27           g.       If, in the course of their efforts to search the subject digital devices,  
28

1 using the techniques described in paragraph 39(d) above, law enforcement agents or  
2 analysts discover items outside of the scope of the warrant that are evidence of other  
3 crimes, that data/evidence will not be used in any way unless it is first presented to a  
4 Magistrate Judge of this District and a new warrant is obtained to seize that data, and/or  
5 to search for other evidence related to it.

6 40. In order to search for data that is capable of being read or interpreted by a  
7 digital device, law enforcement personnel are authorized to seize the following items,  
8 subject to the procedures set forth above:

9 a. Any digital device, as defined above, capable of being used to  
10 commit, further, or store evidence of the offense listed above;

11 b. Any equipment used to facilitate the transmission, creation, display,  
12 encoding, or storage of digital data, including word processing equipment, modems,  
13 routers, and encryption devices;

14 c. Any magnetic, electronic, or optical storage device capable of storing  
15 data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical  
16 disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic  
17 dialers, electronic notebooks, cellular telephones, and personal digital assistants;

18 d. Any documentation, operating logs, and reference manuals regarding  
19 the operation of the digital device or software used in the digital device;

20 e. Any applications, utility programs, compilers, interpreters, and other  
21 software used to facilitate direct or indirect communication with the digital device;

22 f. Any physical keys, encryption devices, dongles, and similar physical  
23 items that are necessary to gain access to the digital device or data stored on the digital  
24 device; and

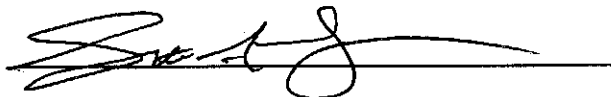
25 g. Any passwords, password files, test keys, encryption codes, or other  
26 information necessary to access the digital device or data stored on the digital device.

27 41. Based on the information in this Affidavit, I also believe that the digital  
28

1 device(s) with Internet capability at the SUBJECT RESIDENCE are instrumentalities of  
2 crime and constitute the means by which violations of Title 18, United States Code,  
3 Section 1030 (Fraud and Related Activity in Connection With Computers) have been  
4 committed. Therefore, I believe that in addition to seizing the digital devices to conduct a  
5 search of their contents as set forth herein, there is probable cause to seize those digital  
6 devices as instrumentalities of the criminal activity.

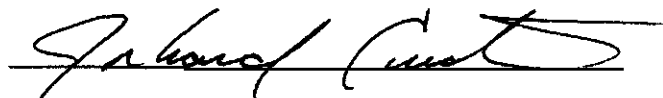
7  
8 **X. CONCLUSION**

9 42. Based on the foregoing facts, I further respectfully submit that there is  
10 probable cause to search the SUBJECT RESIDENCE and to seize evidence, contraband,  
11 fruits, and/or instrumentalities of crimes, namely, Title 18, United States  
12 Code, Section 1030 (Fraud and Related Activity In Connection With Computers).

13  
14 

15 SCOTT A. LOVE, Special Agent  
16 Federal Bureau of Investigation  
17

18  
19 Sworn to before me this 26<sup>th</sup> day of April, 2011.  
20

21  
22 

23 J. RICHARD CREATURA  
24 United States Magistrate Judge  
25  
26  
27  
28

**ATTACHMENT A**

**SUBJECT RESIDENCE**

The physical address of the SUBJECT RESIDENCE is 3921 55th Street Ct. NW, Gig Harbor, Washington 98335. The SUBJECT RESIDENCE is on a residential block located one block off 56th Street NW. The residence is a single story home, light green with dark green trim. The front door faces 55th Street Ct. NW and has a white storm door attached. The majority of the storm door is made up of a large screen/glass area. There is a two car garage attached to the right side of the residence. Dark numerals "3921" are affixed to the garage directly above the garage doors. The property does not appear to have any type of fence surrounding it.

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other storage medium) that constitute evidence, instrumentalities, or fruits of violations of Title 18, United States Code, Section 1030 (Fraud and Related Activity in Connection With Computers), which may be found at the SUBJECT RESIDENCE, including but not limited to:

**Physical Items**

- a. Any physical digital device and/or computer used to commit or store evidence of the offenses listed above;
- b. Any physical equipment used to facilitate the offenses listed above by the transmission, creation, display, encoding or storage of digital data, including word processing equipment, modems, routers, and encryption devices;
- c. Any physical magnetic, electronic, or optical storage devices used to store data related to the offenses above, such as floppy disks, hard disks, tapes, CD-ROMS, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, memory sticks, thumb drives, smartphones, electronic tablets;
- d. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device or data stored on the digital device;

**Digital / Electronic Items**

- e. Any and all digital records, documents, and materials that relate to malicious software, code, or other programs associated with Trojans, BotNets, denial of

1 service attacks, to include but not limited to, LOIC and/or HOIC;

2 f. Any and all digital records, documents, and materials that relate to  
3 communications between the seized computer hard drive and other computers involved in  
4 the denial of service attack, as well as to any individuals that may be controlling the  
5 denial of service attack or participating in the attack, to include IRC chat logs, other  
6 online chat logs, personal messages, Twitter tweets, and/or email related to the denial of  
7 service attacks;

8 g. Any and all digital records, documents, and materials that relate to  
9 the administration, maintenance, operation, use or propagation of the denial of service  
10 tools, to include but not limited to, LOIC/HOIC;

11 h. Any and all digital records, documents, and materials that relate to  
12 the identification and locations of person(s) using or controlling or disseminating denial  
13 of service software;

14 i. Any and all digital records, documents, and materials that relate to  
15 the identification and location of other computers comprising part of the denial of service  
16 attack and/or BotNet;

17 j. Any and all digital data gathered or collected by means of the  
18 operation of the denial of service attack and/or BotNet;

19 k. Any digital logs and other transactional information, to include but  
20 not limited to, internet history, maintained in relation to computer(s) at the SUBJECT  
21 RESIDENCE;

22 **Physical or Digital**

23 l. Any physical or digital records, documents, and materials (i.e., Word  
24 documents, Excel spreadsheets, chat logs, e-mails) that relate to communications, names,  
25 handles/monikers, email accounts, or IP addresses of those either at the SUBJECT  
26 RESIDENCE or those participants in the denial of service attack;

27 m. Any physical or digital documentation, operating logs, and reference  
28



1 manuals regarding the operation of the digital device or software used in the digital  
2 device;

3 n. Any physical or digital application, utility programs, compilers,  
4 interpreters, and other software used to facilitate direct or indirect communication with  
5 the digital device; and

6 o. Any physical or digital passwords, password files, test key,  
7 encryption codes, or other information necessary to access the digital device or data  
8 stored on the digital device.

9 2. With respect to any digital devices falling within the scope of the foregoing  
10 search categories, or any digital devices containing evidence falling within the scope of  
11 the foregoing search categories, records, documents, programs, applications or materials,  
12 or evidence of the absence of same, sufficient to show the actual user(s) of the digital  
13 device during the time period between October 4, 2010 to November 5, 2010.

14 3. Any other evidence from the digital device(s) necessary to understand how  
15 the digital device was used during the time period between October 4, 2010 to November  
16 5, 2010, the purpose of its use, and who used it during the time period between October 4,  
17 2010 to November 5, 2010.

18  
19 **THE SEIZURE OF DIGITAL DEVICES AND/OR THEIR COMPONENTS AS**  
20 **SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH**  
21 **WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES**  
22 **CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY**  
23 **DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING**  
24 **OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE,**  
25 **INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.**  
26  
27  
28