AO 91
Rev. 11/97

# CRIMINAL COMPLAINT

| | |
|---|---|
| UNITED STATES DISTRICT COURT | CENTRAL DISTRICT OF CALIFORNIA |
| UNITED STATES OF AMERICA<br>v.<br>PAUL G. ASHLEY, JONATHAN DAVID HALL, JOSHUA JAMES SCHICHTEL, RICHARD ROBY and LEE GRAHAM WALKER | DOCKET NO.<br>MAGISTRATE'S CASE NO. |

Complaint for violations of 18 U.S.C. §§ 371, 1030(a)(5)(A)(i), and 2.

| | | |
|---|---|---|
| NAME OF MAGISTRATE JUDGE<br>STEPHEN J. HILLMAN | UNITED STATES MAGISTRATE JUDGE | LOCATION<br>Los Angeles, CA |

| | | |
|---|---|---|
| DATE OF OFFENSE<br>Unknown date to February 16, 2004 | PLACE OF OFFENSE<br>Los Angeles, California | ADDRESS OF ACCUSED (IF KNOWN) |

COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:

## COUNT ONE
## 18 U.S.C. § 371

Beginning on an unknown date and continuing to on or about February 16, 2004, within the Central District of California and elsewhere, defendants PAUL GARRETT ASHLEY, JONATHAN DAVID HALL, JOSHUA JAMES SCHICHTEL, RICHARD ROBY and LEE GRAHAM WALKER, and others, conspired and agreed with each other to knowingly and intentionally cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer, in violation of 18 U.S.C. § 1030(a)(5)(A)(i). In particular, and in furtherance of the conspiracy, on or about October 11, 2003 defendant ASHLEY caused the transfer of $900 to a co-conspirator as payment for causing the transmission.

## COUNT TWO
## 18 U.S.C. §§ 1030(a)(5)(A)(1) and 2

Beginning on October 6, 2003 and continuing through on or about October 16, 2003 within the Central District of California and elsewhere, defendants PAUL GARRETT ASHLEY, JONATHAN DAVID HALL, JOSHUA JAMES SCHICHTEL, RICHARD ROBY and LEE GRAHAM WALKER aided, abetted, counseled, commanded, induced and procured the knowing transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, namely, the computer system of Weaknees.Com, and as a result of such conduct, caused loss to 1 or more persons during a 1-year period aggregating at least $5,000 in value.

BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED: (See attached affidavit which is incorporated as part of this Complaint)

MATERIAL WITNESSES IN RELATION TO THIS CHARGE:

| | |
|---|---|
| Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge. | SIGNATURE OF COMPLAINANT<br>CAMERON MALIN<br>OFFICIAL TITLE<br>SPECIAL AGENT – FBI |

Sworn to before me and subscribed in my presence,

| | |
|---|---|
| SIGNATURE OF MAGISTRATE JUDGE(1) | DATE<br>August 25, 2004 |

1) See Federal Rules of Criminal Procedure rules 3 and 54.

AA:aa REC: Summons

# AFFIDAVIT

I, Cameron Malin, being duly sworn, hereby state as follows:

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI"), and have been so employed since May, 2002. I am currently assigned to the Los Angeles Field Division, Cyber Crimes Squad, which is responsible for the investigation of, among other things, computer intrusion offenses and attacks on computer systems. During my career as a Special Agent, I have participated in numerous investigations involving computer-related offenses, and assisted 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 FBI Academy in Quantico, Virginia, I have attended FBI training on basic techniques for computer crime investigations and numerous courses on computer networks. Prior to becoming a Special Agent, my occupation was that of an Assistant State Attorney specializing in the prosecution of computer crimes.

2. I submit this affidavit in support of an application for the issuance of a complaint and summons for PAUL GARRETT ASHLEY, JONATHAN DAVID HALL, JOSHUA JAMES SCHICHTEL, RICHARD ROBY and LEE GRAHAM WALKER for violations of 18 U.S.C. § 371, Conspiracy, and 18 U.S.C. §§ 1030(a)(5)(A)(i), 2, Knowingly Causing Damage to a Protected Computer.

3. As set forth more fully below, the FBI, with assistance from the United States Secret Service and London Metropolitan Police Service, have conducted an international investigation into the widespread use of compromised computer networks to attack the computer systems of online businesses. The investigation known as “Operation Cyberslam” has revealed that the above-named individuals conspired to use thousands of computers across the Internet infected by computer worms to launch "Distributed Denial of Service" (“DDOS”) attacks against

a number of e-commerce websites, including Weaknees.Com located in Los Angeles, California. As a result of the defendants' conduct, the victims have lost in excess of $2 million in revenue and costs associated with the attacks.

## STATUTORY VIOLATIONS

4. Title 18, United States Code Section 371 provides that if two or more persons conspire to commit an offense against the United States, and one or more persons commit any act to effect the object of the conspiracy, each person shall be subject to a fine, a maximum term of imprisonment of five years, or both.

5. Title 18, United States Code Section 1030(a)(5)(A)(i) provides that any person who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer" and as a result of such conduct, caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" is subject to a fine, a term of imprisonment of no more than ten years, or both. Under Title 18, United States Code Section 1030(e)(2)(B), a "protected computer" is defined as a computer which is used in interstate or foreign commerce or communication. Under Title 18, United States Code Section 1030(e)(8), "damage" is defined as any impairment to the integrity or availability of data, a program, a system or information and under Section 1030(e)(11), "loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

## SOURCES OF INFORMATION

6. The facts set forth below are based upon my own personal observations, my own

training and experience and reports and information provided to FBI Special Agent Michael A. Panico by the victim companies and witnesses. I have also had extensive discussions with SA Panico regarding the investigation as well as discussions with other Special Agents and FBI employees knowledgeable in computer disciplines. This affidavit is intended to show that there is probable cause for the complaint and does not purport to set forth all of my knowledge of or investigation into this matter.

7. SA Panico is also currently assigned to the Los Angeles Field Division, Cyber Crimes squad. SA Panico has been a Special Agent for eight years and has been an investigator with the Cyber Crime squad for the last two years. SA Panico has participated in numerous investigations involving computer-related offenses and the execution of search and arrest warrants for several computer intrusion violations. He has also received extensive formal and informal training in the detection and investigation of computer-related offenses including offenses involving computer intrusions, distributed denial of service attacks and other malicious computer activity.

**DEFINITION OF TECHNICAL TERMS**

8. I know, based on my training and experience, the following:

a. An Internet Protocol Address (or simply an "IP address") is a unique numeric address used by computers to communicate on a network such as the Internet. An IP address is comprised of a series of four numbers, separated by periods (e.g., 121.56.97.178) and a unique number is assigned to every computer or device connected to the Internet. An IP address is necessary so that Internet traffic sent from and directed to that computer or device may be properly routed from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses.

b. A Uniform Resource Locator ("URL") is the global address of a web site on the World Wide Web. The first part of the address indicates what protocol to use, and the second part identifies either the Internet Protocol address or the domain name where the resource is located. An example of a URL is "http://www.msnbc.msn.com/.

c. Internet Relay Chat ("IRC") is a network of computers connected through the Internet that allows users to communicate (or chat) with others in real time. IRC users utilize specialized client software to use the service and can access a "channel" which is administered by one or more "operators" or "ops." IRC channels are sometimes dedicated to a topic and are identified by a pound sign and a description of the topic such as "#newyorkjets."

d. The term "bot" is derived from the word "robot" and commonly refers to a software program that performs repetitive functions, such as indexing information on the Internet. Bots have been created to perform tasks automatically on IRC servers and the term is also used to refer to computers that have been infected with a program used to control or launch attacks on other computers.

e. A "Botnet" is a network of bots that are commonly used to control or attack computer systems. Botnets are created by gaining unauthorized access to computers on the Internet and infecting those computers with a particular bot program. The botnet is then controlled by a user, often through the use of a specified IRC channel. Bots are also inserted into vulnerable computer systems similar to a computer virus or worm which propagates throughout the Internet. The unsuspecting infected or compromised computers are often referred to as "zombies" or "drones" and are used in distributed denial of service attacks.

f. Worm: A worm is a program that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down. Unlike a virus, a worm needs little or no human assistance to spread.

g. A "Distributed Denial of Service Attack" (or "DDOS attack") is a type of malicious computer activity by which an attacker causes a network of computers to "flood" a victim computer with large amounts of data or specific commands. As a result, the victim computer is unable to handle legitimate network traffic and legitimate users are denied the services of the computer. Depending on the type and strength of the DDOS attack, the victim computer and its network may become completely disabled and unable to perform its intended function without significant repair. (Attached as Exhibit A, is a diagram describing a typical botnet and DDOS attack).

h. Shell Account: A "Shell Account" is an account on a server computer that allows the client to log in from the Internet and utilize resources physically located on that machine such as a powerful CPU, expanded memory, or a particular operating system. These accounts are often used as a "portal" through which users can then access the Internet, because the hostname and IP address associated with that user is then linked to the server, and not their own personal computer. These services are often used by individuals who want to access IRC channels with some degree of anonymity.

i. Virtual host: Often abbreviated as "vhost;" a virtual host is a provider of web services that include server functions and Internet connectivity.

j. DNS: Short for "Domain Name Service," a computer protocol which translates a domain name to an Internet Protocol address. This service is provided by Domain Name Servers on the Internet, so that when a user types in www.cybercrime.gov for example, they are connected to the correct website. This prevents the user from having to type in the complex numbers of the IP address.

k. Dynamic DNS: A method of keeping a domain name linked to a changing IP address. Most well-known e-commerce sites have a static IP address, but since the DNS protocol is a system which refreshes information on a regular basis, a dynamic DNS service provider will update DNS tables whenever the user changes IP address.

l. Synflood: A particular type of denial of service whereby the attacking computer (also known as "the client") initiates contact with the target computer (typically a server) by sending a "synchronous" or "syn" packet. The target computer acknowledges that the client computer wants to communicate with a "synchronous-acknowledgment" or "syn-ack" packet and then awaits further instructions. This protocol is part of the normal exchange of data. A Synflood occurs when the attacking computers send the "syn" to initiate communication, but do not send any additional data. The targeted server will wait for some specified period of time before disconnecting; however, when that lag time is combined with a flood of "syn" packets from attacking computers, it overwhelms the server's ability to honor legitimate requests. The Synflood can be targeted against any service offered by a server.

m. "HTTPflood": A variation of a Denial of Service attack where the attacking computers flood a web server with valid requests for a web page using the HyperText Tranfer Protocol (HTTP). HTTP is the protocol used to provide web pages and generally operates on port 80 of a server. Each attacking computer will ask again and again, many times a second, for a page it has already received. Because the computer is tied up providing the page to attacking computers, it cannot provide it to legitimate computers.

## **STATEMENT OF PROBABLE CAUSE**

9. On October 15, 2003 and on numerous subsequent occasions, SA Panico interviewed Jeff Shapiro and Michael Adberg, owners and operators of Weaknees.Com ("Weaknees"). During the interview, Shapiro and Adberg told SA Panico the following:

a. Weaknees sells and upgrades personal digital video recorders (“DVRs”) including the popular “TIVO” DVR that is used by home entertainment consumers. Weaknees is an e-commerce business that relies on sales from its website www.weaknees.com. Weaknees generates over 99% of its $3 million in annual revenues from its website. I know, based on my training and experience, that computers that provide web services, such as the Weaknees.Com website, are “protected computers” that are used in interstate and foreign commerce and communication.

b. Weaknees and its employees are based in Los Angeles, California, although its website is hosted by a third-party web hosting company.

c. On or about October 6, 2003, Weaknees’ website came under attack by an overwhelming volume of data requests known as a “Syn-flood” in which computers on the Internet made contact with the Weaknees server, but never completed any connections. This caused the resources of the Weaknees server to be tied up waiting for a request for data, and therefore rendered unavailable to legitimate users on the Internet for approximately 12 hours.

d. At the time of the DDOS attacks, Weaknees was paying Lexiconn, a web hosting company located in Connecticut, to host the Weaknees.Com website. On October 10, 2003, Weaknees suffered another DDOS attack that was so severe that it began affecting service to other Lexiconn customers. As a result, Lexiconn dropped Weaknees as a customer.

e. After Weaknees’ service was terminated by Lexiconn, Adberg and Shapiro hired Rackspace.Com ("Rackspace"), a large, nation-wide web hosting company to host its website at a significant increase in cost. The DDOS attacks, however, continued and increased in volume and severity. Weaknees.Com essentially became unavailable for approximately two weeks. Rackspace employees determined that the cause of the disruption was a DDOS attack from numerous computers on the Internet. Over time, the attack changed to adjust to countermeasures that Weaknees and its web hosting companies attempted. In particular, a DDOS attack beginning on or around October 14, 2003 involved repeated requests by computers on the Internet for image files from the Weaknees website (this would later become known as the "HTTPflood" attack). The number and frequency of the requests consumed the amount of available bandwidth and again prevented legitimate users from accessing the Weaknees.Com website. Over time, Rackspace has been able to mitigate the attacks and allow Weaknees to maintain a web presence. The last attack against Weaknees occurred on November 14, 2003.

f. Adberg and SA Panico reviewed computer logs showing the activity on the Weaknees.Com website during a portion of the DDOS attacks. In addition, I reviewed the logs and learned that a visitor had navigated the web site on October 15 and several subsequent occasions. The user appeared to be conducting reconnaissance log looking for large image files contained within the web server files. These image files were the same files requested by the attacking computers during the concurrent attack on the Weaknees web server. A sophisticated computer user would realize that large image files take longer to download, and hence are more likely to tie up system resources. The logs revealed the IP address of the computer that had conducted the reconnaissance.

g. Adberg and Shapiro stated that they had learned that one of their strategic partners, RapidSatellite.Com, was also under constant DDOS attack during this same time period. Rapid Satellite is a reseller of satellite television systems; Weaknees upgrades the personal digital video recorders (DVR) that come with the satellite television system at an additional cost to the customer.

h. Adberg and Shapiro indicated that they had recently had a business conflict with Jay Echouafni, the owner of Orbit Communication Corps, another satellite television reseller. Adberg and Shapiro indicated that they had an acrimonious relationship with Echouafni after a deal to become strategic business partners fell through.

i. Weaknees estimated that the DDOS attacks that occurred from October 6, 2003 to November 14, 2003 have caused close to $200,000 in losses to the company for, among other items, the response costs related to the attacks, damage assessments, and lost revenues resulting from the unavailability of the Weaknees website.

10. On October 20, 2003 and October 24, 2003, SA Panico spoke to Jeff Nelson, a network engineer and "DoS mitigation expert" for Rackspace. Nelson confirmed that www.weaknees.com had been the victim of a large DDOS attack. On October 15 and 16, 2003, the attack took the form of a large number of computers across the Internet "flooding" the web server with valid requests for the webpage and certain items from the webpage (the "HTTPflood"). Weaknees had purchased special filtering/intrusion detection software, which generated a number of "logfiles." That data included the IP addresses of some of the attacking computers.

11. After reviewing the IP addresses provided by Nelson, SA Panico was able to determine that one of the computers attacking Weaknees.Com was physically located in Los Angeles, California. SA Panico retrieved that computer and, with the assistance of specially trained computer forensic examiners, made a copy of the hard drive. The forensic examiner

notified SA Panico that the Norton Antivirus software program on his review machine identified the virus/worm as "W32.HLLW.Gaobot."

12. SA Panico searched the Symantec Anti-Virus Website using the name of the worm found on the infected machine. SA Panico learned that the "Gaobot" worm was also known as "Agobot," and that the worm inserted trojan executable programs into the "System 32" folder of the Windows operating system. He also learned that the executive programs could allow an attacker to control the computer remotely. Symantec reported that the worm caused an infected computer to connect to an IRC server to receive commands from an attacker. Furthermore, the worm located CD keys for popular video games that may be stored on the victim's hard drive. The possession of a CD "key" would allow a user to play pirated games on Internet games servers.

13. On October 17, 2003, Nick Molina, the owner of RapidSatellite.Com, was interviewed by FBI SA Michelle Meredith of the Miami Field Office. SA Panico has read SA Meredith's summary report (known as an FD-302) of this interview, and has had numerous phone conversations with SA Meredith concerning this investigation. Panico also spoke to Molina directly on several occasions, the last being on July 27, 2004. Molina provided SA Panico and SA Meredith the following information:

a. RapidSatellite.Com is a subsidiary of WebClick Concepts located in Miami Beach, Florida and is a reseller of satellite television systems. The RapidSatellite.Com website produces 95% of the revenue for WebClick Concepts.

b. On October 6, 2003, RapidSatellite.Com was the victim of a "Synflood" DDOS attack on its web server, which at the time was hosted by Datapipe. According to SA Panico, Datapipe has its corporate offices in New Jersey and a satellite office in Mountain View, California.

c. After the Synflood attack Rapid Satellite transferred some of its web site content to Speedera, a content delivery provider, in an effort to mitigate some of the Synflood attacks. Essentially, customers who visited Rapid Satellite's website were re-directed by the Domain Name Service to the Speedera network to receive some of the data they requested. Because Speedera possessed greater bandwidth, shifting some of the client requests to the larger network theoretically should have eased some of the burden on Datapipe**.**

d. From October 9 through October 10, 2003, however, Rapid Satellite was adversely affected by a massive DDOS attack on Speedera's DNS servers. Eventually, Rapid Satellite was forced to move again to Akamai, a larger web hosting company with even greater bandwidth. Molina was required to pay $10,000 in emergency funds to move the Rapid Satellite website to Akamai while under attack.

e. While hosted at Akamai, Rapid Satellite was targeted by yet another DDOS attack on or about October 14, 2003. This attack took the form of an HTTPflood, where the attacking computers repeatedly requested the Rapid Satellite home page and also invoked the "search" function available on the home page. These actions quickly used up the server's resources.

f. Molina estimated that Rapid Satellites's losses from the attacks was approximately $300,000.

g. During Meredith's initial interview, Molina stated that Jay Echouafni, whose company was a competitor of Rapid Satellite, had called him several times during the DDOS attacks offering to host Rapid Satellite on his own network for $5,000 per month.

14. On November 12, 2003, SA Panico interviewed Eric Swildens, Chief Technology Officer of Speedera Networks ("Speedera") in Mountain View, California, and he told me the following:

a. Speedera is a web hosting company which hosted some of the content for the RapidSatellite.Com website. Swildens advised SA Panico that Speedera was the victim of a large DDOS attack on October 10, 2003. The attack began shortly after Rapid Satellite had moved its content from its prior web server located at Datapipe. The attack was targeted at the Domain Name Servers of Speedera, which are shared by all of Speedera's clients.

b. The attack was so severe that it disrupted service for Speedera's other customers for nearly an hour. At the time, Speedera hosted numerous customers including the website for the U.S. Department of Homeland Security and Amazon.Com. Because of the volume of Speedera's business and the prestige of its clients, Speedera estimated that the attack caused a loss of approximately $1 million.

15. On April 21, 2004, SA Panico received an email message from Swildens indicating that a number of affected customers of Speedera were located in Los Angeles, California including a company known as "Ultramercial."

16. On July 27, 2004, SA Panico spoke to Jim Smith, the Chief Technology Officer of Ultramercial, which is located in Los Angeles. Ultramercial sells advertising on the Internet and has the graphical content of its webpage provided by Speedera. Smith told SA Panico that October 10, 2003 was the slowest day of the month for the company and that the advertising traffic was 32% below average. Smith indicated that company records showed that 10,000 "hits" were lost to the company on that day representing approximately $2,000 in lost revenue.

17. After the interview of Adberg and Shapiro, SA Panico determined that the IP

address of the computer used by the intruder to conduct the reconnaissance of Weaknees.Com on October 15, 2003 was owned by Unixcon.Net. SA Panico subsequently contacted Unixcon.Net and interviewed it's owner/operator, Gene De Roule, on November 12, 2003. De Roule told SA Panico the following:

a. Unixcon was a shell hosting company located in Mountain View, California. One of its administrators was an individual known as LEE WALKER, who was a resident of the United Kingdom. WALKER also was a "security consultant" for the company. De Roule corroborated that a user on the Unixcon system had visited the Weaknees.Com website on October 15, 2003. The user account had the name "DODOL" but the account had been paid for using a stolen credit card number and the account had been terminated within a month of its activation.

18. SA Panico also received information from a Confidential Source ("CS") who told him that LEE WALKER of Unixcon.Net used nicknamed "sorCe". The CS advised SA Panico that WALKER had engaged in DDOS attacks on the Internet and provided a logfile of an attack as corroboration.

19. SA Panico reviewed the logfile which appeared to be a record of an IRC conversation between "sorCe" and "Setient" in which sorCe threatened to attack Setient. Setient's connection to the chat room was then interrupted. SA Panico told me that based on his training and experience, he knows that DDOS attacks can cause a user's connection to an IRC channel to be interrupted.

20. SA Panico was able to further corroborate the information received from the CS. SA Panico learned that Ronald Cotoni, who uses the nickname "Setient," had been interviewed by FBI agents on March 7, 2003. During that interview, Cotoni stated that LEE WALKER,

utilizing the nickname “sorCe,” had conducted a DDOS attack against him. Furthermore, Cotoni was able to provide WALKER’s home address in the United Kingdom.

21. On January 7, 2004, the CS provided additional information to SA Panico that indicated WALKER was controlling his zombie computers from an IRC Server located on the CIT/FOONET network at IP address 66.252.1.222. WALKER had apparently infected computers across the Internet with a worm called “Agobot.” Once infected, these computers would then automatically connect to the IRC server at FOONET, and await further instructions from WALKER.

22. SA Panico learned that FOONET is a nickname for CREATIVE INTERNET TECHNIQUES, (“CIT”) an Internet business that hosts servers for e-commerce, IRC, games networks and other users of the Internet. SA Panico utilized a publicly available database to determine that the IP address 66.252.1.222 was assigned to CIT. Furthermore, SA Panico learned that other Special Agents in the FBI had ongoing investigations in which CIT was hosting the servers involved.

23. On or about December 7, 2003, SA Panico spoke to FBI SA E.J. Hilbert of the Los Angeles Field Office. SA Hilbert told SA Panico that he had been conducting an investigation into a target whose computer was hosted at CIT. SA Hilbert indicated that he had a number of contacts with PAUL GARRETT ASHLEY, and advised that ASHLEY owned and operated CIT. SA Hilbert also indicated that CIT’s servers and network were physically located in the basement of ASHLEY’s residence in Ohio.

24. On February 11, 2004, SA Panico was present during an interview of LEE GRAHAM WALKER, conducted by the London Metropolitan Police Service, Computer Crime Unit ("MET-CCU") in London, England. The interview was conducted following the search of

WALKER's residence by law enforcement authorities in the United Kingdom. During the search, WALKER'S computer was seized as evidence. SA Panico was again present on July 10, 2004 when WALKER was re-interviewed by detectives of the MET-CCU in the presence of an attorney. WALKER had been read his rights prior to both interviews. During the interviews, WALKER provided the following information:

a. WALKER had used the nicknames "sorCe" and "fight." WALKER had developed a close relationship with PAUL ASHLEY while WALKER was the system administrator for Unixcon, which was hosted by CIT/FOONET. Eventually, WALKER began to do work for ASHLEY, mostly "security consulting." WALKER explained this to mean that he would track down the origin of DDOS attacks against the CIT/FOONET network. Furthermore, WALKER claimed that he had conducted a number of DDOS attacks at ASHLEY's request within the past year, and that the attacks were usually directed against hackers who had attacked CIT/FOONET.

b. WALKER admitted that he had conducted a DDOS attack against Weaknees.Com and RapidSatellite.Com. WALKER stated that he had used a DDOS botnet that he controlled from an IRC channel on a server located at CIT/FOONET. This botnet was created by infecting between 5,000 to 10,000 computers across the Internet with a worm called "Agobot," which was developed by an individual nicknamed "AGO," who then provided it to WALKER for his use. AGO had access to the IRC control channel and knew that WALKER was using the zombie computers for DDOS attacks. WALKER also stated that ASHLEY knew that this botnet was being controlled from CIT/FOONET.

c. WALKER stated that he conducted the attacks against Weaknees and Rapid Satellite at the direction of ASHLEY, the owner and network administrator of

CIT/FOONET. ASHLEY had provided the URL's of the two websites to WALKER over an instant messenger program. WALKER had "cut and pasted" these names into a "notepad" file so that he would be able to recall them later when he accessed the botnet control channel. ASHLEY told WALKER that the victims of the DDOS attacks had been bothering one of ASHLEY's other clients and that the victims were business competitors of that client.

d. WALKER stated that the "HTTPflood" attack that was conducted was an innovation developed by AGO specifically for WALKER. WALKER indicated that such a specially-designed attack was necessary against large webhosting companies like Akamai that had the money and technical savvy to filter less sophisticated attacks. WALKER stated that he had used the "DODOL" shell account on Unixcon to conduct the reconnaissance of the Weaknees website, and that he had directed the zombies to request the large image files from the website.

e. WALKER stated that the domain name for the bot server was initially "bots.unixcon.net" and later became "bunghole.mysqld.com." WALKER and AGO used a domain name instead of an IP address for the IRC control server so that they could change the IP address of the server without having to update every zombie computer. Zombies would do a DNS query for "bunghole.mysqld.com" which would automatically translate to whatever IP address the channel was then assigned to.

f. Access to the botnet control channel was controlled by AGO and WALKER, and required special login procedures.

25. The London-Metropolitan Police Service, Computer Crime Unit provided SA Panico a forensic image of LEE WALKER's computer, which was seized during a search of WALKER's residence in the United Kingdom on February 11, 2004. Forensically trained

computer personnel, using commercially available software, prepared these computers for SA Panico's review. SA Panico reviewed the computer and advised me that he had found the following pertinent computer files:

a. A file called "–ussians.txt" which contained the following text:

".DDOS.synflood www.rapidsatellite.com 30000 0 80 –s"

".DDOS synflood www.rapidsatellite.com 30000 0 80 –s"

b. A file named "hitlist.txt" that contained the URLs of a number of websites.

c. A number of "initialization" files which were used to configure the IRC client program that WALKER was using to access the IRC control channel. In a folder named "BOT1," an initialization file called "servers.ini" held the text "SERVER:66.252.1.220." One of the IP addresses for CIT is 66.252.1.222 provided by CS. I know from my training and experience, that internet service providers such as CIT, often have control of a range of similar IP addresses.

d. SA Panico found a logfile named "#Agobot3" which appeared to be a log of an IRC control channel for the botnet. The logfile showed a number of zombies reporting in with the text: "Found Half-Life CDKey" followed by a string of numbers and/or letters characteristic of a video game key.

26. I know based on my training and experience, one of the properties of the Agobot worm as specified by Symantec, was that it harvests CD keys from video games such as the popular Half-Life video game. As mentioned above, only individuals with knowledge of the special login procedures for the botnet control channel would have been able to make this logfile.

27. On February 14, 2004, agents of the FBI executed a federal search warrant for,

among other items, the computers of CIT/FOONET, located at the residence of PAUL ASHLEY in Powell, Ohio. During the execution of the warrant, ASHLEY agreed to be interviewed and voluntarily told SA Panico the following:

a. ASHLEY admitted that he had instructed LEE WALKER to launch DDOS attacks against Rapid Satellite and another company whose name he recalled as "Weakness." ASHLEY further admitted that he knew other individuals who had the ability to launch DDOS attacks. ASHLEY named JOSHUA SCHICHTEL, also known as “EMP,” and JONATHAN HALL, also known as “RAIN” and “CODES DOT OBS,” as two of the individuals who had conducted attacks at his request. ASHLEY stated that he had provided HALL**,** SCHICHTEL and WALKER with the web server names for the victims of the attacks.

b. ASHLEY stated that WALKER had hosted his botnet control channel on a CIT/FOONET server that ASHLEY had provided for him, during the time the attacks were carried out.

c. ASHLEY stated that he had ordered the DDOS attacks at the request of Jay Echouafni, who was then a customer of CIT/FOONET. Echouafni had told ASHLEY that the two companies had stolen content from his website for use in their websites, and that they were conducting a DDOS attack on him. Echouafni had paid ASHLEY $1,000 for conducting the DDOS attacks and transmitted the funds to ASHLEY’s PayPal account.

d. Echouafni had purchased CIT/FOONET from ASHLEY in or around December of 2003. ASHLEY stated that he remained as the network administrator for a salary of $120,000 per year.

28. On March 18, 2004, the FBI executed a search at the home of JONATHAN DAVID HALL at his residence in Metairie, Louisiana. SA Panico and I subsequently

interviewed HALL at the FBI office in New Orleans, Louisiana. HALL signed a written waiver of his Miranda rights and told us the following:

a. HALL is an employee of CIT/FOONET.

b. HALL has compromised a number of computers on the Internet since 1997. HALL became friendly with PAUL ASHLEY in 2002 and assisted ASHLEY by tracking down the sources of DDOS attacks launched against CIT/FOONET.

c. When CIT was purchased by Jay Echouafni, Echouafni hired HALL to perform “security’ for CIT/FOONET. ASHLEY contacted HALL and ask HALL to “test the lines” or “consult” on various websites. HALL understood this to mean that he was to launch DDOS attacks on the specified website. Initially, HALL believed these websites were hosted at CIT and that he was testing the CIT network to see if it could withstand attack. Eventually, however, he learned that he was attacking websites that were outside of the CIT network

d. HALL recalled that ASHLEY had requested that he attack Weaknees and Rapid Satellite. In late 2003 or early 2004, ASHLEY provided the URLs for those companies over AOL Instant Messenger (“AIM”). ASHLEY had specifically told HALL to “nail” Weaknees.

e. HALL attempted to attack these sites with his botnet, but was later informed by ASHLEY that his bots had not been effective in taking down the websites. HALL surmised that he had not issued the commands to the bot network properly; he recalled that he had “cut and pasted” the URLs into the IRC control channel, but that perhaps he had not logged on properly, so the bots ignored his commands. ASHLEY subsequently told HALL that he would get “Lee” to do it instead.

f. In February 2004, Echouafni contacted HALL and asked him to “consult” the web site for Expert Satellite. At Echouafni's request, HALL launched a synflood attack against Expert Satellite. Echouafni contacted HALL on a number of occasions to inform HALL when the website was back on line, and implored him to continue attacking, by saying that he was disappointed with the "consulting." Echouafni also implied that HALL would be fired if he did not launch the attacks. At the time, HALL understood Echouafni to be the owner of CIT/FOONET.

g. After the FBI had searched CIT/FOONET, Echouafni contacted HALL and asked HALL to call him back on a payphone. Echouafni informed HALL that HALL was a target of the FBI investigation and that HALL should "do some housecleaning," which HALL understood to mean that he should remove any evidence from his home.

29. On February 25, 2004, SA Panico interviewed Michael Reich, the Chief Technology Officer of Expert Satellite. Reich told SA Panico the following:

a. During the week of February 6 through February 12, 2004, Expert Satellite was the victim of a DDOS attack that made their website unavailable. Reich was told by Expert Satellite's web hosting company that the attack was a Synflood. Expert Satellite initially attempted to mitigate the attack by using specialized software called "syn-cookies," but the attacker re-doubled his efforts, and sent so much data traffic to the web server that Reich eventually just had to pull the plug on the computer.

b. Expert Satellite moved their web server to a larger and more expensive hosting company, Rackspace, on February 12, 2004. Only with Rackspace's assistance was the company able to regain their web presence.

c. Reich estimated that Expert Satellite suffered $400,000 in lost revenue, labor, and costs due to the attacks.

30. On May 10, 2004, and on a number of subsequent occasions, SA Panico and I interviewed JOSHUA SCHICHTEL near his home in Chandler, Arizona. Special Agent E.J. Hilbert had interviewed SCHICHTEL previously on February 19, 2004, and provided to SA Panico his written summary (FD-302) of the interview. In his interviews, SCHICHTEL provided the following information:

a. SCHICHTEL used the nickname "EMP" and “Emperor of the Net” and operated a web and shell hosting company known as Concepthosting. One of Concepthosting’s servers was located on CIT/FOONET. SCHICHTEL had been active on the Internet and is technically sophisticated. He is conversant in the means of creating and controlling botnets, and had utilized botnets in the past. SCHICHTEL admitted that he was well known in the hacker community.

b. SCHICHTEL originally met ASHLEY when he was the administrator for an Internet company that was hosted on CIT/FOONET. Eventually, SCHICHTEL began helping ASHLEY track down hackers who were launching DDOS attacks on CIT/FOONET clients. SCHICHTEL would do this by finding the attacking zombies, hacking into them and determining what IRC channel the zombie was connecting to for its instructions. In return, ASHLEY provided SCHICHTEL with a server on CIT/FOONET at a reduced cost.

c. ASHLEY asked SCHICHTEL to attack the websites for Rapid Satellite and Weaknees in October of 2003. SCHICHTEL recalled a chat session that he had with ASHLEY in which ASHLEY told him that he was tasking two other individuals to attack the websites as well. SCHICHTEL recalled that one of these individuals may have been named “Lee.” SCHICHTEL recalled that ASHLEY told him that one of the other hackers had a botnet of 50,000 computers. ASHLEY was intent on keeping the sites down for a long time, and told

SCHICHTEL that he was doing so on behalf of one of his clients.

d. Using his botnet of approximately 3,000 compromised computers, SCHICHTEL launched a Synflood attack against the webserver of RapidSatellite.Com, but it seemed to be ineffective. ASHLEY contacted SCHICHTEL on AOL Instant Messenger on a number of occasions and was disappointed that the websites were still active.
Because SCHICHTEL did not want to lose his server on CIT/FOONET, SCHICHTEL told ASHLEY that he was attacking the websites when, in fact, he was not.

e. Instead, SCHICHTEL contacted RICHARD ROBY, who used the nickname "Krashed." SCHICHTEL knew that ROBY had a botnet and the capability to launch DDOS attacks. SCHICHTEL promised ROBY a shell account on the Concepthosting server if ROBY would launch a DDOS attack against Rapid Satellite. ROBY agreed to do so.

31. On April 27, 2004, SA Panico reviewed files from JOSHUA SCHICHTEL's computer. SCHICHTEL had previously provided an image of his computer's hard drive to SA Hilbert, who provided it to SA Panico. SA Panico told me he found the following pertinent files on SCHICHTEL's computer:

a. SA Panico found a number of files that appeared to be logs of AIM chats between SCHICHTEL, using the nickname "CIT Joshua," and someone using the nickname "yourfoo." On a log dated October 7, 2003, "yourfoo" asked CIT JOSHUA to conduct a DDOS attack on www.rapidsatellite.com and www.rapidsatelite.com, stating, "both need to permanently… disappear." Later in the chat, "yourfoo" added www.weaknees.com. Yourfoo promised SCHICHTEL a "box" or server. Yourfoo admonished SCHICHTEL: "u gotta keep ane (sic) eye on it…cuz they could null route the ip and change the dns…and it would be back up." When CIT JOSHUA asked, "what did they do to you?" Yourfoo replied, "fucking with us…well, a customer." During an interview with SCHICHTEL, SA Panico showed SCHICHTEL this log. SCHICHTEL confirmed that the chat had taken place on the date appearing on the log and that PAUL ASHLEY was "yourfoo."

b. SA Panico found additional AIM chat logs dated October 8, 2003 and October 15, 2003 between ASHLEY, again using the nickname "yourfoo," and SCHICHTEL. In both logs, ASHLEY implored SCHICHTEL to keep the websites off of the Internet. In the October 8 log, ASHLEY said, "destroy it..heheh." After SCHICHTEL told him that the company had changed IPs six times, and that "we've gone th [sic] like three or four boxes," ASHLEY responded, "HEHEH..THAT'S OK…just keep fucking it." On October 15, 2003, ASHLEY notified SCHICHTEL that the site was moved to Akamai, and suggested to SCHICHTEL, "can u make a spoofed dns flooder that does massive dns requests…we can roast the akamai name servers." ASHLEY explained to SCHICHTEL how the DNS flooder worked.

c. SA Panico also found a file that was a log of an AIM chat that SCHICHTEL had with "KRASHEDKOMP" dated October 8, 2003. During this chat, SCHICHTEL asked KRASHEDKOMP to attack the e-commerce websites of www.rapidsatellite.com and provided KRASHEDKOMP with the IP address for the website. In return, KRASHED received a shell account and virtual hosting for free. After some initial trouble with his botnet, KRASHED stated, "I'm hitten (sic) it now." The log then shows the following:

> "KrashedKomp (1:33:06 PM): (16:33:22) (Bianca55) SynFlooding: 204.251.10.215 port: 80 delay: 5 times:9999999.
>
> (16:33:22) (Robbie31) SynFlooding: 204.251.10.215 port: 80 delay: 5 times:9999999.
>
> (16:33:22) (tpype) SynFlooding: 204.251.10.215 port: 80 delay: 5 times:9999999.

```
(16:33:22)  (JOHN32) SynFlooding: 204.251.10.215 port: 80 delay: 5 times:9999999.
(16:33:22)  (griwj) SynFlooding: 204.251.10.215 port: 80 delay: 5 times:9999999.
(16:33:22)  (Browser63) SynFlooding: 204.251.10.215 port: 80 delay: 5 times:9999999.
(16:33:22)  (kqavms) SynFlooding: 204.251.10.215 port: 80 delay: 5 times:9999999.
(16:33:22)  (Jason36) SynFlooding: 204.251.10.215 port: 80 delay: 5 times:9999999.
(16:33:22)  (andrew61) SynFlooding: 204.251.10.215 port: 80 delay: 5 times:9999999.
KrashedKomp (1:33:16 PM): i am hitten with all i have now”
```

32. Based on my training and experience and the opinion of SA Panico, it appears that KRASHEDKOMP had cut and pasted a portion of the log from the IRC control channel of zombie computers that were attacking RapidSatellite.Com. SCHICHTEL was shown this logfile and confirmed its authenticity, identifying KRASHEDKOMP as another alias of KRASHED. SCHICHTEL recalled that he had asked for KRASHED’s assistance in attacking these websites because he knew from their prior interactions, that KRASHED would not hestitate to engage in this type of malicious computer activity.

33. On June 17, 2004, SA Panico and I interviewed RICHARD ROBY at his residence in Celina, Ohio contemporaneously with the execution of a federal search warrant at his residence. ROBY voluntarily provided the following information:

a. ROBY stated that he used the nicknames “KRASHED,” “KRASHEDKOMP,” and “DRAGONFLY.”

b. After being shown the AIM chat log dated October 8, 2003 that had been retrieved from SCHICHTEL’s computer, ROBY confirmed that it appeared to be an authentic chat between himself and someone he identified as “EMP.”

c. At the time of the attack, ROBY was using a botnet comprised of 15,000 compromised computers that had been created by a friend, nicknamed "JZ." ROBY had used this botnet on a number of occasions to launch DDOS attacks. ROBY explained that the botnet was created by infecting computers with a variant of the "Spybot" worm. ROBY is certain that the logfile shown to him by agents is a "cut and paste" excerpt of that botnet because, as he explained to us, zombies on that botnet would report to channels with names like "(Robbie31)" and "(Jason36)." This was a peculiar characteristic of that variant of Spybot; it would take the name that the user had given the computer and append random numbers to it.

d. ROBY stated that he did not check to see if the website was down, because he knew that the botnet that he was using was very powerful and if he hit something, "it went down." ROBY knew that it was powerful from using it on previous occasions.

e. ROBY admitted that he had released the "Agobot" worm onto the Internet. In the fall of 2003, ROBY obtained a "C" programming language version of the "Agobot" code, and compiled it with configuration parameters which allowed him to control the bot network it created. ROBY no longer had control of the botnet, and could not recall whether he had used that botnet for any additional attacks against Rapid Satellite.

34. On March 25, 2004, SA Panico interviewed Quentin Olwell, Chief Financial Officer of Global Satellite, previously known as Mavcomm. Olwell told SA Panico the following:

a. Mavcomm/Global Satellite is a satellite television reseller located in Aliso Viejo, California. Olwell met Jay Echouafni in late January of 2004 when Mavcomm was negotiating with Echouafni to develop management software for their expansion into the e-commerce forum. Previously, Mavcomm did most of their sales through traditional telephone marketing. Echouafni had his own satellite television business, Orbit Satellite, which used this specialized software.

b. Echouafni stayed in California for several weeks, working with the staff and network technology at Mavcomm to get the e-commerce site operational. During that period of time, Echouafni used the offices of Olwell and some of the other officers of the company.

c. Olwell was present when Echouafni attempted to visit his Orbit Satellite website. Echouafni discovered that a pop-up advertisement for a competitor, Expert Satellite, was running over his website. Echouafni became irate.

d. The next day, Olwell noticed that Expert Satellite's website was unavailable on the Internet. Olwell joked with Echouafni about Echouafni taking the website down, and Echouafni became angry, throwing a plastic tray at Olwell. Echouafni told Olwell, "Don't you ever tell anybody about this."

e. Later in the day, Expert Satellite's website was back on the Internet. During a meeting with Echouafni, Olwell observed Echouafni sending AIM messages to someone about "consulting our friend." Echouafni had also previously told Olwell about a security consultant named "Paul." Olwell believed that Echouafni was in contact with Paul on the day of the attack against Expert Satellite.

35. On August 25, 2004 a federal grand jury in Los Angeles returned a five-count indictment against Echouafni alleging multiple conspiracies to attack Weaknees, Rapid Satellite, and ExpertSatellite and violations of 18 U.S.C. § 1030(a)(5)(A)(i). It is believed that Echouafni has fled the United States and is currently a fugitive.

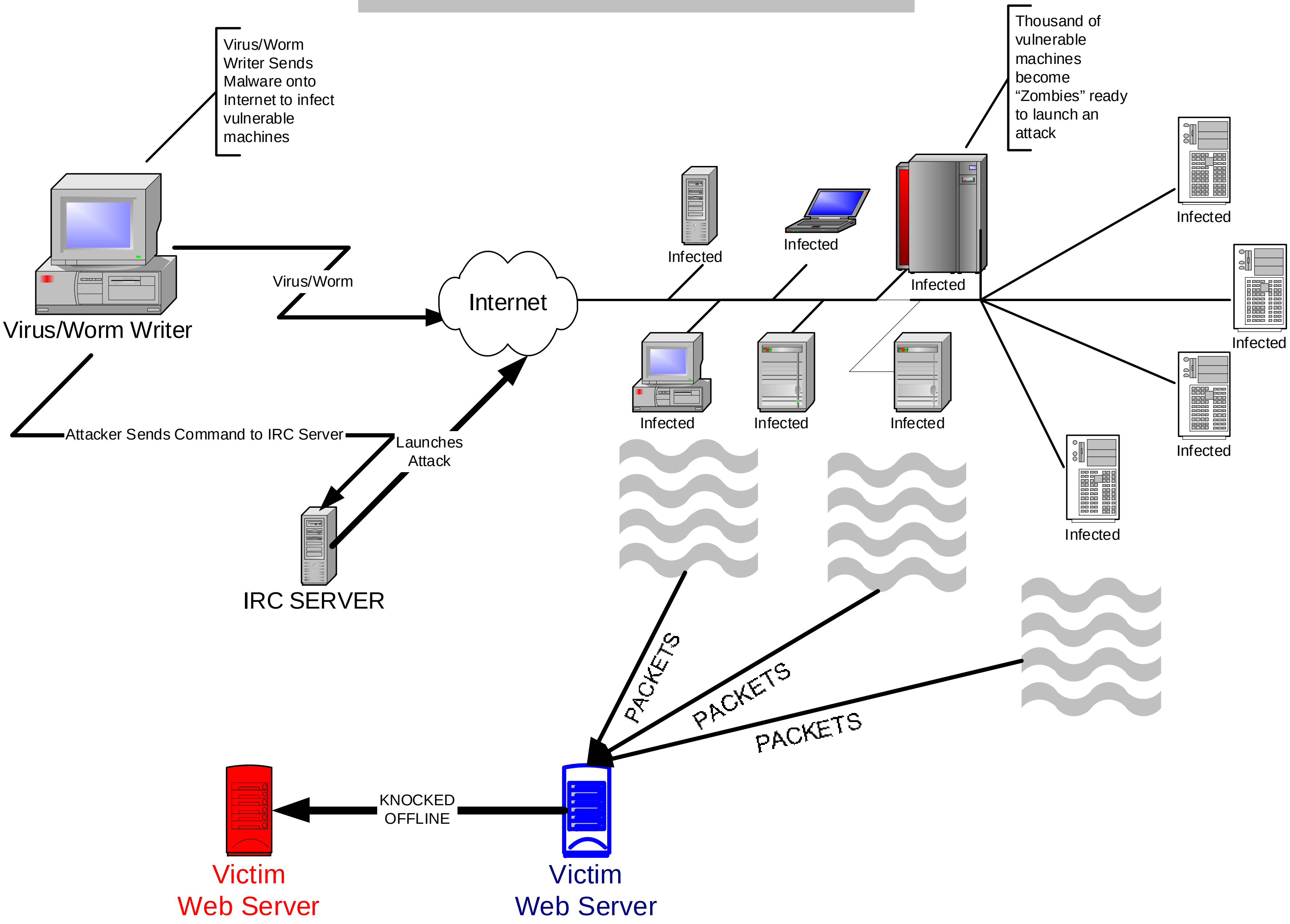
36. Based on the foregoing, I believe there is probable cause to believe that PAUL GARRETT ASHLEY, LEE GRAHAM WALKER, JONATHAN DAVID HALL, JOSHUA JAMES SCHICHTEL, and RICHARD ROBY have violated 18 U.S.C. § 371, Conspiracy, and 18 U.S.C. §§ 1030(a)(5)(A)(i), 2, Knowingly Causing Damage to a Protected Computer.

____________________________________
Cameron Malin, Special Agent FBI

Subscribed and sworn to before
me this _____ day of August, 2004

____________________________________
UNITED STATES MAGISTRATE JUDGE

# Distributed Denial of Service Attack



Virus/Worm Writer Sends Malware onto Internet to infect vulnerable machines

Thousand of vulnerable machines become "Zombies" ready to launch an attack

EXHIBIT A

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

October 2003, Grand Jury

| | |
|---|---|
| UNITED STATES OF AMERICA,<br>Plaintiff,<br>v.<br>JAY R. ECHOUAFNI,<br>a.k.a. Saad Echouafni,<br>Defendant. | Case No. CR 04-704(A)<br>FIRST SUPERSEDING INDICTMENT<br>[18 U.S.C. § 371: Conspiracy; 18 U.S.C. §§ 1030(a)(5)(A)(i) and 2: Aiding and Abetting the Transmission of a Code, Information, Program or Command to a Protected Computer] |

The Grand Jury charges:

INTRODUCTION

At all times pertinent to this indictment:

1. Defendant JAY R. ECHOUAFNI, also known as ("a.k.a.") Saad Echouafni, was the owner and Chief Executive Officer of Orbit Communication Corporation, a Massachusetts corporation based in Sudbury, Massachusetts. Orbit Communication Corp. provided home satellite systems to customers through its website, www.orbitsat.com, and its sales department.

AA:aa

2. Weaknees was an online business based in Los Angeles, California that sold and upgraded personal digital video recorders (“DVRs”) including “TIVO” and other DVRs. Weaknees sold its products through its website on the Internet, www.weaknees.com. Weaknees had a strategic alliance with Rapid Satellite.

3. Rapid Satellite was an online business owned by WebClick Concepts Inc. in Miami, Florida. Rapid Satellite sold home satellite television systems to customers through its website, www.rapidsatellite.com, and sales department. Rapid Satellite was a competitor of Orbit Communication Corp.

4. Expert Satellite was an online business based in Worcester, Massachussetts that sold home satellite television systems to customers through its website and sales department. Expert’s website, www.expertsatellite.com, was available to customers over the Internet. Expert Satellite was a competitor of Orbit Communication Corp.

5. Creative Internet Techniques, Inc. (“CIT”) was an Internet Service Provider based in Powell, Ohio owned by defendant ECHOUAFNI. CIT ran a network known as “Foonet” that provided web hosting and other computer services to customers.

6. An unindicted co-conspirator in Powell, Ohio was the prior owner and systems administrator of CIT and Foonet and, as set forth below, was involved in the conspiracies to attack Weaknees, Rapid Satellite and Expert Satellite.

7. An unindicted co-conspirator in Metairie, Louisiana was an employee of CIT with experience in launching attacks on computer systems and, as set forth below, was involved in the conspiracies

to attack Weaknees, Rapid Satellite and Expert Satellite.

8. An unindicted co-conspirator in Celina, Ohio was a computer user with experience in launching computer attacks and, as set forth below, was involved in the conspiracy to attack Weaknees and Rapid Satellite.

9. An unindicted co-conspirator in the United Kingdom was a computer user with experience in launching computer attacks and, as set forth below, was involved in the conspiracy to attack Weaknees and Rapid Satellite.

10. An unindicted co-conspirator in Chandler, Arizona was a computer user with experience in launching computer attacks and, as set forth below, was involved in the conspiracy to attack Weaknees and Rapid Satellite.

11. At all pertinent times, the computers and web-hosting services of Foonet, Weaknees, Rapid Satellite and Expert Satellite were used in interstate and foreign commerce and communication.

Computer Terminology

12. A distributed denial of service ("DDOS") attack is a type of malicious computer activity where an attacker causes a network of compromised computers to "flood" a victim computer with large amounts of data or specified computer commands.  A DDOS attack typically renders the victim computer unable to handle legitimate network traffic and often the victim computer will be unable to perform its intended function and legitimate users are denied the services of the computer.  Depending on the type and intensity of the DDOS attack, the victim computer and its network may become completely disabled and require significant repair.

13. A “SynFlood” is a type of DDOS attack where a computer or network of computers send a large number of “Syn” data packets to a targeted computer. Syn packets are sent by a computer that is requesting a connection with a destination computer. A SynFlood typically involves thousands of compromised computers in a botnet that flood a computer system on the Internet with “Syn” packets containing false source information. The flood of Syn packets cause the victimized computer to use all of its resources to respond to the requests and render it unable to handle legitimate traffic.

14. An “HttpFlood” is a type of DDOS attack where a computer or network of computers send a large number of Hyper Text Transfer Protocol (“HTTP”) requests to a targeted web server.

15. The term "bot" is derived from the word "robot" and commonly refers to a software program that performs repetitive functions, such as indexing information on the Internet. Bots have been created to perform tasks automatically on IRC servers and the term is also used to refer to computers that have been infected with a program used to control or launch DDOS attacks against other computers.

16. A "botnet" is typically a network of computers infected with bots that are used to control or attack computer systems. Botnets are often created by spreading a computer virus or worm that propagates throughout the Internet, gains unauthorized access to computers on the Internet and infects the system with a particular bot program. The botnet is then controlled by a user, often through the use of a specified IRC channel. A botnet can

consist of tens of thousands of infected computers. The unsuspecting infected or compromised computers are often referred to as "zombies" or "drones" and are used in DDOS attacks.

17. Internet Relay Chat ("IRC") is a network of computers connected through the Internet that allows users to communicate (or chat) with others in real time. IRC users utilize specialized client software to use the service and can access a "channel" which is administered by one or more "operators" or "ops." IRC channels are sometimes dedicated to a topic and are identified by a pound sign and a description of the topic such as "#miamidolphins." IRC channels are also used to control botnets that are used to launch DDOS attacks.

//

//

COUNT ONE

[18 U.S.C. § 371]

18. The grand jury re-alleges and incorporates all of the introductory allegations set forth in paragraphs 1 through 17.

OBJECT OF THE CONSPIRACY

19. Beginning on an unknown date, and continuing through on or about February 16, 2004, in Los Angeles County, within the Central District of California, and elsewhere, defendant JAY R. ECHOUAFNI, a.k.a. Saad Echouafni, and others known and unknown to the grand jury, conspired and agreed with each other to knowingly transmit a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss aggregating more than $5,000, in violation of 18 U.S.C. § 1030(a)(5)(A)(i).

MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED

20. The object of the conspiracy was to be accomplished as follows:

a. Defendant ECHOUAFNI would contact an unindicted co-conspirator and order the co-conspirator to launch an attack against the web sites Weaknees.Com and RapidSatellite.Com to make them inaccessible on the Internet.

b. The co-conspirator would contact other co-conspirators and coordinate the DDOS attacks against the particular web site.

c. The co-conspirators would access a botnet that they had access to or controlled and caused the botnet to launch DDOS attacks against the web site making it inaccessible to legitimate users on the Internet.

OVERT ACTS

21. In furtherance of the conspiracy and to accomplish the object of the conspiracy, defendant ECHOUAFNI and others known and unknown to the grand jury, committed various overt acts within the Central District of California and elsewhere, including the following:

a. On or about October 6, 2003, defendant ECHOUAFNI contacted an unindicted co-conspirator in Powell, Ohio and discussed launching an attack against Weaknees.Com and Rapid Satellite.

b. On or about October 6, 2003, the unindicted co-conspirator in Powell, Ohio contacted another co-conspirator in the United Kingdom and instructed him to launch a DDOS attack against Weaknees.Com and RapidSatellite.Com, competitors of Orbit Communication Corp.

c. On or about October 6, 2003, the co-conspirators launched SynFlood DDOS attacks against Weaknees.Com and RapidSatellite.Com.

d. After the Synflood attacks successfully knocked the web sites offline, defendant ECHOUAFNI contacted the co-conspirator in Powell, Ohio and stated "You guys did a good job."

e. On or about October 6, 2003, defendant ECHOUAFNI paid the co-conspirator in Powell, Ohio $1,000 through the PayPal online payment system.

f. On or about October 7, 2003, the co-conspirator in Powell, Ohio contacted the co-conspirator in Chandler, Arizona to request that he conduct a DDOS attack on Weaknees and Rapid Satellite.

g. On or about October 8, 2003, the co-conspirator in Powell, Ohio contacted the co-conspirator in Chandler, Arizona to discuss the continuing attacks on Weaknees and Rapid Satellite.

h. On or about October 8, 2003, the co-conspirator in Chandler, Arizona contacted the co-conspirator in Celina, Ohio and directed him to launch a DDOS attack against Rapid Satellite.

i. On or about October 10, 2003, the co-conspirators launched a series of DDOS attacks against the Domain Name Servers for the companies hosting the Weaknees.Com and RapidSatellite.Com web sites.

j. On or about October 10, 2003, defendant ECHOUAFNI paid the co-conspirator in Powell, Ohio $1,000 via PayPal.

k. On or about October 11, 2003, the co-conspirator in Powell, Ohio transferred $900 to a co-conspirator in England via PayPal.

l. On or about October 14, 2003, the co-conspirators launched HttpFlood DDOS attacks against Weaknees.Com and RapidSatellite.Com.

m. In or about October 2003, defendant ECHOUAFNI contacted Rapid Satellite's owner and offered to host Rapid Satellite's web site for $5,000 a month.

n. In or about December 2003, defendant ECHOUAFNI offered to purchase CIT Inc. and pay the co-conspirator in Powell, Ohio $120,000 a year as a systems administrator.

o. After federal agents executed a search of CIT, defendant ECHOUAFNI contacted a co-conspirator in Metairie, Louisiana to inform him that he was under investigation by the Federal Bureau of Investigation and advised the co-conspirator to conduct “some housecleaning.”

//

//

## COUNT TWO

## [18 U.S.C. §§ 1030(a)(5)(A)(i) and 2]

Beginning on or about October 6, 2003 and continuing through on or about October 16, 2003, within the Central District of California, within Los Angeles County and elsewhere, defendant JAY R. ECHOUAFNI, a.k.a. Saad Echouafni, aided, abetted, counseled, commanded, induced and procured the knowing transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, namely, defendant ECHOUAFNI aided and abetted the launching of distributed denial of service attacks against the protected computers of Weaknees.com, and as a result of such conduct, caused loss during a one-year period aggregating at least $5,000 in value.

COUNT THREE

[18 U.S.C. §§ 1030(a)(5)(A)(i) and 2]

Beginning on or about October 6, 2003 and continuing through on or about October 16, 2003, within the Central District of California, within Orange County and elsewhere, defendant JAY R. ECHOUAFNI, a.k.a. Saad Echouafni, aided, abetted, counseled, commanded, induced and procured the knowing transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, namely, defendant ECHOUAFNI aided and abetted the launching of distributed denial of service attacks against the protected computers of RAPIDSATELLITE.COM, and as a result of such conduct, caused loss during a one-year period aggregating at least $5,000 in value.

COUNT FOUR

[18 U.S.C. § 371]

The grand jury re-alleges and incorporates all of the introductory allegations set forth in paragraphs 1 through 17.

OBJECT OF THE CONSPIRACY

22. Beginning on an unknown date, and continuing through on or about February 16, 2004, in Los Angeles County, within the Central District of California, and elsewhere, defendant JAY R. ECHOUAFNI, a.k.a. Saad Echouafni, and others known and unknown to the grand jury, conspired and agreed with each other to knowingly transmit a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss aggregating more than $5,000, in violation of 18 U.S.C. § 1030(a)(5)(A)(i).

MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED

23. The object of the conspiracy was to be accomplished as follows:

a. Defendant ECHOUAFNI would contact an unindicted co-conspirator and order the co-conspirator to launch an attack against the web site of Expert Satellite to make it inaccessible on the Internet.

b. The co-conspirator would contact other co-conspirators and coordinate the DDOS attacks against the particular web site.

c. The co-conspirators would access a botnet that they had access to or controlled and caused the botnet to launch DDOS attacks against the web site making it inaccessible to legitimate users on the Internet.

OVERT ACTS

24. In furtherance of the conspiracy and to accomplish the object of the conspiracy, defendant ECHOUAFNI and others known and unknown to the grand jury, committed various overt acts within the Central District of California and elsewhere, including the following:

25. On or about February 6, 2004, defendant ECHOUAFNI ordered the co-conspirator in Powell, Ohio to launch an attack against the web site for Expert Satellite.

26. In or about February 2004, the co-conspirator in Powell, Ohio asked others to launch attacks on the web site for Expert Satellite.

27. From February 6, 2004 through February 12, 2004, defendant made repeated requests of the unindicted co-conspirator in Metairie, Louisiana to launch DDOS attacks against Expert Satellite to keep Expert Satellite's website inaccessible to customers on the Internet.

28. From February 6, 2004 through February 12, 2004, an unindicted co-conspirator launched DDOS attacks against Expert Satellite's web site to prevent customers from accessing the site.

29. On or about February 15, 2004, defendant ECHOUAFNI contacted a co-conspirator in Metairie, Louisiana to inform him that he was under investigation by the Federal Bureau of Investigation and advised the co-conspirator to conduct "some housecleaning."

## COUNT FIVE

## [18 U.S.C. §§ 1030(a)(5)(A)(i) and 2]

Beginning on or about February 5, 2004 and continuing through on or about February 12, 2004, within the Central District of California, within Orange County and elsewhere, defendant JAY R. ECHOUAFNI, a.k.a. Saad Echouafni, aided, abetted, counseled, commanded, induced and procured the knowing transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, namely, defendant ECHOUAFNI aided and abetted the launching of distributed denial of service attacks against the protected computers of EXPERTSATELLITE.COM, and as a result of such conduct, caused loss during a one-year period aggregating at least $5,000 in value.

## ADDITIONAL ALLEGATIONS

The grand jury further alleges:

30. The loss resulting from defendant’s conduct, the jointly undertaken criminal activity, and the reasonably foreseeable acts of the co-conspirators in furtherance of the conspiracy, as alleged in Count One, was more than $120,000.

31. The loss resulting from defendant’s conduct, the jointly undertaken criminal activity, and the reasonably foreseeable acts of others, as alleged in Count Two, was more than $70,000.

32. The loss resulting from defendant’s conduct, the jointly undertaken criminal activity, and the reasonably foreseeable acts of others, as alleged in Count Three, was more than $70,000.

33. The loss resulting from defendant’s conduct, the jointly undertaken criminal activity, and the reasonably foreseeable acts of the co-conspirators in furtherance of the conspiracy, as alleged in Count Four, was more than $120,000.

34. The loss resulting from defendant’s conduct, the jointly undertaken criminal activity, and the reasonably foreseeable acts of others, as alleged in Count Five, was more than $120,000.

35. The offenses charged in Counts One through Five of the Indictment involved sophisticated means, that is, especially complex or intricate offense conduct pertaining to the execution or concealment of the offenses, including the propagation of viruses and worms, the use of compromised computers, and the launching of sophisticated computer attacks against computer networks.

f. A substantial part of the scheme charged in Counts One, Two and Three were committed from outside the United States by an unindicted co-conspirator in the United Kingdom and by compromised computers located outside the United States.

g. Defendant ECHOUAFNI was an organizer and leader of the criminal activity charged in Counts One through Five and the underlying conduct involved more than five participants. Defendant ECHOUAFNI ordered the attacks against business competitors of Orbit Communication Corp. and paid his employees for the attacks.

A TRUE BILL

_____________________
FOREPERSON

DEBRA W. YANG
United States Attorney

SALLY MELOCH
Assistant United States Attorney
Acting Chief, Criminal Division

ARIF ALIKHAN
Assistant United States Attorney
Chief, Cyber and Intellectual Property Crimes Section