ZiaSpace Productions
463 Fourth Avenue, Suite #3R
Brooklyn, NY 11263
718.499.5531
http://www.ziaspace.com/
elaine@ziaspace.com
john@ziaspace.com

This document contains information regarding the distributed denial of service (DDoS) attacks which have been directed at ZiaSpace Productions servers. Information in this document is to be used for the purpose of aiding in the apprehension and conviction of the attacker(s).

Unless otherwise noted, all times are in EST (GMT-5), and all usernames correspond to users on the server reva.sixgirls.org.

ZiaSpace Productions is an Internet hosting business owned by Elaine Walker and John Klos. It is our intention that all of the assets that constitute Sixgirls Computing Labs, which has been operated as a DBA, be brought into ZiaSpace Productions when we register the business as a corporation.

The servers discussed in this document are reva.sixgirls.org and andromeda.ziaspace.com. Sixgirls Computing Labs is the name for the community of programmers, developers, and computing enthusiasts who share a common server, which is reva.sixgirls.org.

reva.sixgirls.org, or reva, primarily exists as a public access server used for programming, development, static web hosting, email, and other community activities. Hosting and shell accounts are offered for free for non-profit and open source / free software projects. Reva also performs backup DNS and email for andromeda.ziaspace.com, and stores MySQL databases for several large web sites which are run on andromeda.ziaspace.com.

andromeda.ziaspace.com or andromeda, primarily exists as a for-profit Internet server, offering shell accounts, email, static, dynamic, and SSL encrypted web hosting, and development environments for various languages, such as Java, Perl, php, c, c++, and more.

Reva is a unique server; it employs a Motorola m68060 processor, which makes it attractive to developers who wish to confirm that their code will work on this alternative processor architecture. It is, by contemporary measures, not a fast machine, and the ethernet is only 10 mbps. However, its unique features, unique and efficient design, and its “classic” appeal make it a very popular machine. There are currently 200 users on reva, and reva serves approximately 150 domains. It serves approximately 200 gigabytes of Internet traffic a month.

However, reva’s speed and 10 mbps connection puts it at a disadvantage when it comes to attacks. Andromeda, with 5 times the clock speed and a 100 mbps connection, is much more resistant to attacks. Note that to put things into perspective, one should understand that reva can handle the full-time traffic of four T1s. This is not a trivial amount of traffic, but relative to the amount of traffic that has been used in these attacks, it is insignificant.

When referring to UnixCon or unixcon.net, we are referring to the company that is called UnixCon, which is short for Unix Connections. They are based out of Mountain View, California, and their primary business is offering shell accounts for people who wish to use IRC (Internet Relay Chat). The attacker, we believe, is one of the administrators of UnixCon who goes by the username sorce (sorce@unixcon.net) and the IRC handle sorCe. sorce@unixcon.net is listed on unixcon.net’s web site as one of the systems administrators. His first name is Lee.

Following is a timeframe of events. Some of the times have been approximated where exact data is not available.

1-January-2003: User setient on reva (Ron Cotoni) and another user, psytek (from webiest.com) join an IRC (Internet Relay Chat) channel #unixcon on mclean.va.us.undernet.org to ask for UnixCon to return psytek's handle. (In IRC, people can register a handle for long-term use; apparently the UnixCon people "stole" psytek's handle and would not give it back). This was at around 5:01am (GMT-6, or 6:01am EST). They waited for a UnixCon administrator to log in; sorCe logged in at approximately 8:52am (GMT-6, or 9:52am EST).

At approximately 2:14pm (GMT-6, or 3:14pm EST), sorCe and psytek start chatting about psytek's handle; sorCe was not helpful, and basically told psytek that he was out of luck. User setient started saying things which aggravated sorCe. At 2:28pm (GMT-6, or 3:28pm EST), setient's connection to the Internet is flooded with traffic, and he has to connect using another Internet connection. Shortly after he connects again, that line is flooded with traffic as well (at 2:30pm GMT-6, or 3:30pm).

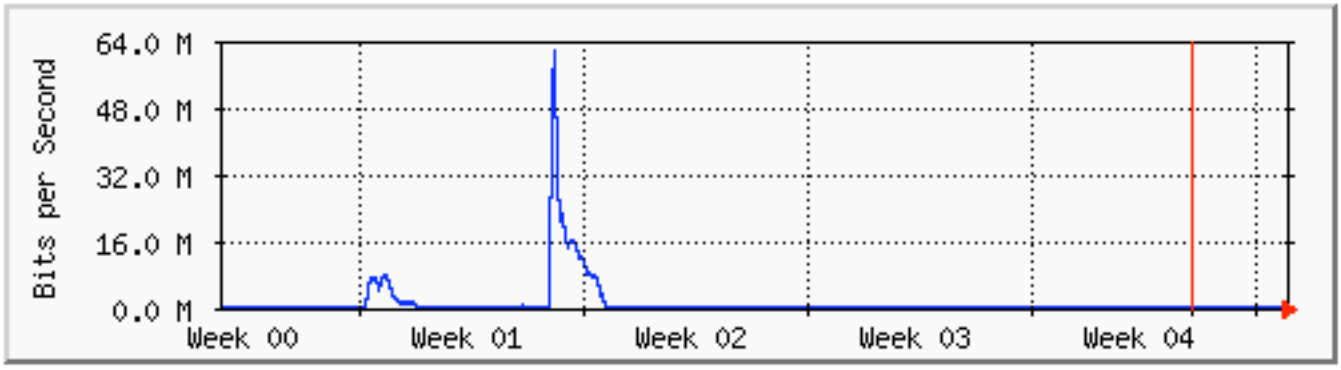
See logfile logs/irc_1_jan_2003 for the full IRC log of this event.

6-January-2003: User setient antagonises user sorCe again on IRC; because setient is connecting to the IRC channel using his shell account on reva.sixgirls.org, reva becomes the focus of a distributed denial of service attack. Because Elaine Walker and John Klos were in Arizona at the time of this attack, reva was rebooted because it was mistakenly believed that it may have become unresponsive because of a sysem crash. After some further diagnosis, it became apparent that the system was in fact still working, but unable to communicate. Reva's connection to the Internet was then disconnected, and that connection was physically plugged into an extra ethernet port on andromeda. Andromeda was then configured remotely to assume the IP address of reva and to forward traffic from reva's IP address to reva via a crossover cable that had been used for private, secure communications between the two machines.

Although we do not have useful IRC logs, andromeda kept count of the number of packets which were handled by the ethernet device which was handling reva's Internet connection. The number of incoming packets handled between the time when andromeda started handling reva's traffic and the daily system report, run at 3:15am 7-Jan-2003, was 412770800. The number of packets which actually constituted legitimate traffic was 2191399, or one half of one percent of all of the packets.

Note that this attack is shown in the following MRTG graph at the beginning of Week 01. The traffic did not average more than 7 mbps or so due to the fact that this graph measures the actual traffic exchanged with the machine, and during most of the attack the connection was plugged into a 10 mbps ethernet port.

`Monthly' Graph (2 Hour Average)



Max In:1088.3 kb/s (1.1%) Average In: 347.0 kb/s (0.3%) Current In:0.0 b/s (0.0%)
Max Out:61.9 Mb/s (61.9%) Average Out:2846.2 kb/s (2.8%) Current Out:0.0 b/s (0.0%)

12-January-2003: Again, setient joins IRC channels which sorCe frequents, and another attack begins. This attack is directed at setient's cable modem, at another server, durga.indira.net, on which setient has an account, and at reva.sixgirls.org. Because reva is protected by andromeda, andromeda becomes unavailable as the attack escalates. The upstream provider for the ZiaSpace machines indicates that the traffic peaked at 150 mbps.The graph above shows this as a spike at the end of Week 1. Note that the graph above represents averages of intervals of two hours; the attack sustained an average of 61.9 mbps for two hours. Traffic indicates that the attack started modestly, and was intensified when the initial attack did not appear to stop traffic to reva.

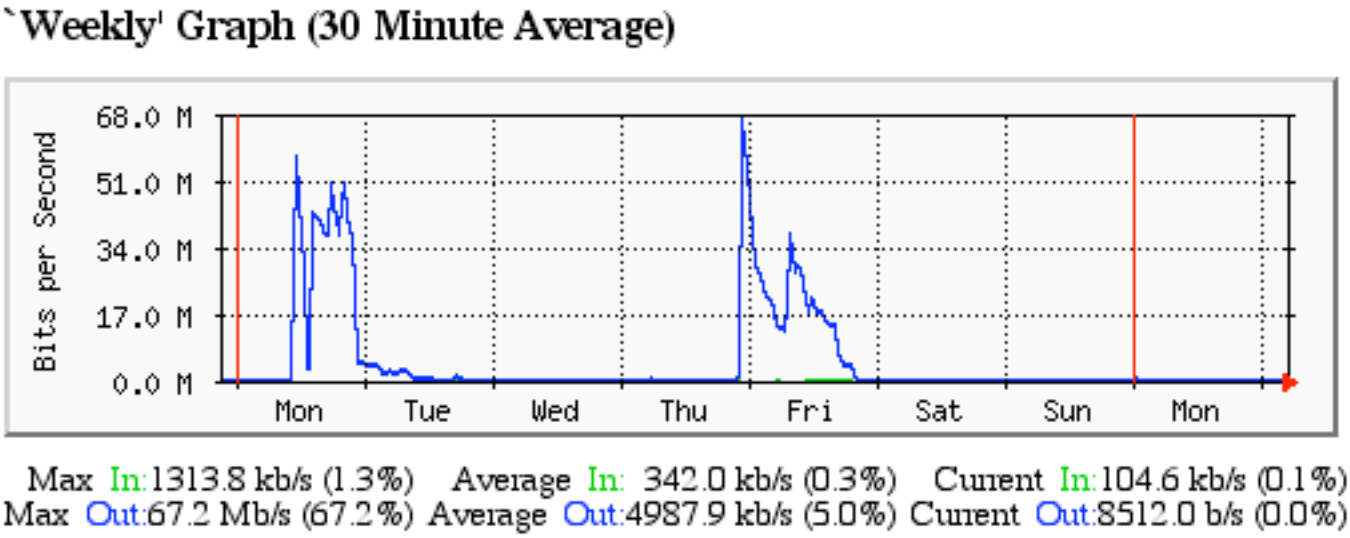
This attack causes both andromeda and reva to be unavailable through almost all of Sunday until early Monday. Andromeda became available again after the attack tapered down to somewhere between 30 and 40 mbps.

27-January-2003: The situation is pretty much the same as before; however, setient has arranged to have a friend "lurk" in an IRC channel which they both believe is used to control the machines which perform the attack. This proves to be correct, as the IRC logs of that channel show that at 9:22am (GMT-6, or 10:22am EST), sorCe logs into that channel, and, minutes later, at 9:25am (GMT-6, or 10:25am EST) approximately 1564 unique "zombies" are told to attack setient, as can be seen by the 11,308 lines in the IRC log which read like this:

```
[09:25] <Rql3qo1> setient the goblin boy with no pubes.
```

Furthermore, the times in the IRC log directly correspond with the graph showing the attack on reva. Please see the data for Monday on the following graph.

The IRC logs for the 27-January-2003 can be found in logs/irc_attack_27_jan_2003



30-January-2003: Another attack begins at 10:00pm as seen in the graph above. No new information is gained during this attack.

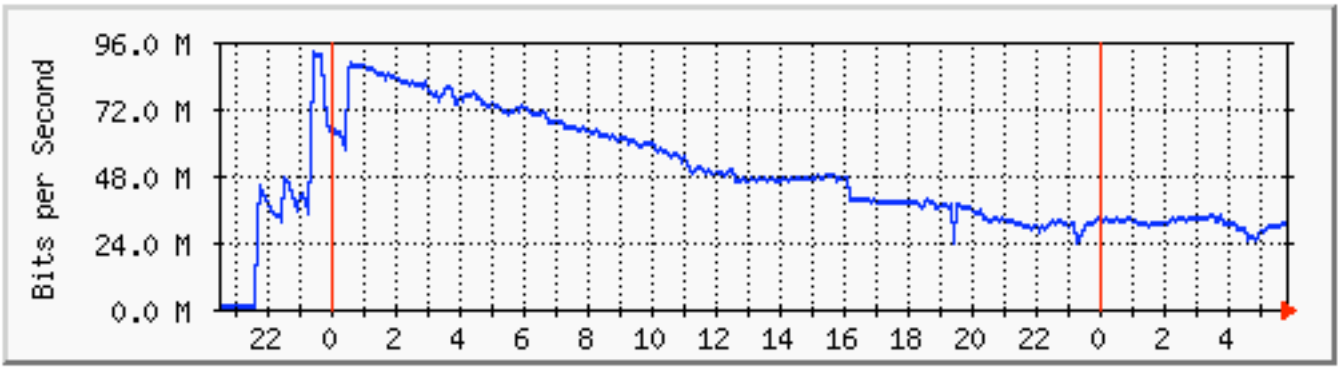
2-February-2003: Another attack begins at approximately 9:45pm. When the attack does not appear to be effective because reva is still accessible to the Internet, the attack intensifies. The upstream provider informs ZiaSpace that the attack reached 200 mbps, and that if any future attacks happen with increased bandwidth, reva may be removed from the Internet until the attack stops.

Importantly, though, someone at UnixCon attempts to gather information about setient and about psytek, and also about the root and toor users, during a slower period of the attack. That can be seen in these examples:

```
Feb  3 00:25:40 reva fingerd[23005]: query from 203.167.115.82: setient
Feb  3 00:34:01 reva fingerd[23094]: query from public1-bolt1-4-
cust103.oldh.broadband.ntl.com: setient
Feb  3 01:19:30 reva fingerd[23431]: query from noc.unixcon.net: setient
```

The full logs of the finger events can be found in logs/finger_log and in logs/authlog_log.

`Daily' Graph (5 Minute Average)



Max In: 964.2 kb/s (1.0%) Average In: 172.4 kb/s (0.2%) Current In: 120.5 kb/s (0.1%)
Max Out:92.5 Mb/s (92.5%) Average Out:48.3 Mb/s (48.3%) Current Out:30.6 Mb/s (30.6%)

This graph shows the latest attack which started on 2-February-2003, and is ongoing as of now (the morning of 4-February-2003).

Details of the attack

The attacks have been carefully examined. All of the significant traffic consists of SYN packets with spoofed source IPs. Due to the fact that the source IPs all end in 0.0, packet filtering based on a reverse subnet mask (0.0.0.0/0.0.255.255) has proven to be very effective. Packet rates of up to 70,000 packets a second have been counted; our machines cannot handle more than that at this time.

At first, it was believed that the only way that someone could control the amount of bandwidth that was directed at the ZiaSpace machines was to "own" a fleet of up to or more than 1,000 Windows computers on modestly fast broadband connections throughout the world. This guess proved correct when the IRC logs showing a list of the "zombies" was captured; an nmap of each IP address in that list has consistently shown that each machine is a Windows machine with certain ports open which would normally not be open on a non-infected machine. We are in the process of talking with the administrators of some of the networks which provide Internet connections to infected machines, and we hope that a willing victim of this infection will allow us to dissect the zombie on her/his system.

Furthermore, several of the machines are behind Linux and BSD firewalls, which implies that the agent of infection used was either an email virus, a trojan which was installed with some other software, or an infected web site which allowed the download and installation of this trojan by well known security flaws in Microsoft's Internet Explorer. We are in contact with the admins of at least one of those firewalls, and we are hopeful that they will cooperate in examining data being communicated between the zombie and the controlling channel.

Evaluation

It has been pointed out to us that many people have been victim to attacks by sorCe and/or other people associated with UnixCon. Attempts were made by several administrators of other machines to talk with the administrators of UnixCon. User setient tried, along with Indira, the administrator of durga.indira.net, to contact the owner of UnixCon, Gene De Roule, but to no avail; not only did Gene indicate that he was unwilling to investigate claims of attacks orchestrated by sorCe, he led setient and Indira to believe that sorCe lives in Malaysia, and that nothing could be done to stop sorCe even if he were behind the attacks.

It is the belief of ZiaSpace that Gene De Roule knows about these activities. Even if Gene is not taking an active part in the attacks, he is making resources available to sorCe which facilitate these attacks. We believe that Gene De Roule is responsible for the actions of an agent of his company, and is criminally negligent in ignoring requests to investigate these attacks.

Other evidence clearly shows that sorCe has a committed hatred of setient. sorCe has even directly physically threatened setient, and this threat should be taken seriously considering how much energy sorCe has already expended attacking any place where setient has an account.

This is an excerpt from the IRC logs from logs/irc_31_jan_2003 (note that the original log has ANSI escape sequences, so it has been converted and saved as logs/irc_31_jan_2003.rtf as well):

```
[sorCe(sorce@ppp-63.151.206.197.noc11.unixcon.net)] lol
[sorCe(sorce@ppp-63.151.206.197.noc11.unixcon.net)] you are still talking like a spaz
[sorCe(sorce@ppp-63.151.206.197.noc11.unixcon.net)] who has a big head
[sorCe(sorce@ppp-63.151.206.197.noc11.unixcon.net)] goblin boy
[sorCe(sorce@ppp-63.151.206.197.noc11.unixcon.net)] it will get u fucked one day
[sorCe(sorce@ppp-63.151.206.197.noc11.unixcon.net)] u will piss someone off
[msg(sorCe)] nope it won't
[sorCe(sorce@ppp-63.151.206.197.noc11.unixcon.net)] who will come round and cut you up
```

Losses

ZiaSpace Productions has lost significant revenue because of these attacks. None of ZiaSpace's clients will be charged for hosting for the month of January because of the significant amount of downtile that they experienced. Elaine Walker and John Klos also incurred lost revenue directly attributable to the attacks. Consulting work was lined up for both of them in Arizona; that trip was cut short and the consulting jobs lost as a result of the first attack. Over a hundred and fifty hours of billable time has been spent by both Elaine and John during the month of January which was directly related to the attacks: time was spent distributing services to backup servers to minimise the effects of later attacks, time was spent researching more efficient ways to block the traffic and money was spent on expensive equipment to take the place of andromeda as a firewall, and time was spent collecting and examining data regarding the attacks. ZiaSpace Productions owes the upstream provider money to pay for the bandwidth used during the attacks. Finally, clients' faith in ZiaSpace Productions is diminished, which devalues our company.

Sample of SYN flood traffic:

```
02:17:58.928587 151.223.0.0.1303 > 66.250.131.180.21830: S 1012006912:1012006912(0) win 16384
02:17:58.928789 41.220.0.0.1561 > 66.250.131.180.15135: S 1890385920:1890385920(0) win 16384
02:17:58.928970 41.225.0.0.1368 > 66.250.131.180.15135: S 1289027584:1289027584(0) win 16384
02:17:58.928994 102.168.0.0.1341 > 66.250.131.180.4911: S 1831993344:1831993344(0) win 16384
02:17:58.929339 41.221.0.0.1667 > 66.250.131.180.15135: S 151322624:151322624(0) win 16384
02:17:58.929360 168.139.0.0.1800 > 66.250.131.180.30980: S 907935744:907935744(0) win 16384
02:17:58.929368 41.203.0.0.1754 > 66.250.131.180.15135: S 423428096:423428096(0) win 16384
02:17:58.929378 19.250.0.0.1373 > 66.250.131.180.16813: S 1381367808:1381367808(0) win 16384
02:17:58.929386 168.138.0.0.1519 > 66.250.131.180.30980: S 862453760:862453760(0) win 16384
02:17:58.929610 65.213.70.42.6667 > 66.250.131.180.49943: P 374478608:374478723(115) ack 866780397 win
17520
02:17:58.929623 41.226.0.0.1162 > 66.250.131.180.15135: S 1692794880:1692794880(0) win 16384
02:17:58.929633 132.40.0.0.1246 > 66.250.131.180.4655: S 507183104:507183104(0) win 16384
02:17:58.929972 41.228.0.0.1341 > 66.250.131.180.15135: S 1366622208:1366622208(0) win 16384
02:17:58.930241 245.167.0.0.1000 > 66.250.131.180.23866: S 1705508864:1705508864(0) win 16384
02:17:58.930510 41.205.0.0.1135 > 66.250.131.180.15135: S 1444151296:1444151296(0) win 16384
02:17:58.930774 41.230.0.0.1199 > 66.250.131.180.15135: S 1005649920:1005649920(0) win 16384
02:17:58.930818 162.233.0.0.1599 > 66.250.131.180.14474: S 1758396416:1758396416(0) win 16384
02:17:58.930874 41.231.0.0.1711 > 66.250.131.180.15135: S 1570045952:1570045952(0) win 16384
02:17:58.930922 61.85.72.178.65158 > 66.250.131.180.13969: S 1137770496:1137770496(0) win 16384
02:17:58.930960 168.147.0.0.1347 > 66.250.131.180.30980: S 1083834368:1083834368(0) win 16384
02:17:58.930973 168.142.0.0.1334 > 66.250.131.180.30980: S 25755648:25755648(0) win 16384
02:17:58.931217 168.148.0.0.1701 > 66.250.131.180.30980: S 2007564288:2007564288(0) win 16384
02:17:58.931273 168.143.0.0.1666 > 66.250.131.180.30980: S 842072064:842072064(0) win 16384
02:17:58.931288 41.232.0.0.1139 > 66.250.131.180.15135: S 699727872:699727872(0) win 16384
02:17:58.931295 245.230.0.0.1187 > 66.250.131.180.23866: S 2052456448:2052456448(0) win 16384
02:17:58.931384 151.224.0.0.1214 > 66.250.131.180.21830: S 2082209792:2082209792(0) win 16384
02:17:58.931645 41.233.0.0.1149 > 66.250.131.180.15135: S 1565130752:1565130752(0) win 16384
02:17:58.931658 41.207.0.0.1133 > 66.250.131.180.15135: S 1123287040:1123287040(0) win 16384
02:17:58.931876 133.23.0.0.1725 > 66.250.131.180.5242: S 1923219456:1923219456(0) win 16384
02:17:58.932202 168.151.0.0.1046 > 66.250.131.180.30980: S 400556032:400556032(0) win 16384
02:17:58.932349 41.235.0.0.1325 > 66.250.131.180.15135: S 865402880:865402880(0) win 16384
```

All of the attack traffick is from spoofed IP addresses, such as 151.223.0.0, and the port numbers that they try to reach do not provide well know services, such as ftp, ssh, http, or DNS.

Logs of samples of the attack are available in these locations:
38 seconds worth of traffic from 6-January-2003: logs/dump_6_jan_2003_1
Approximately three and a half hours from 6-January-2003: logs/dump_6_jan_2003_2
Seven minutes worth of traffic from 28-January-2003: logs/dump_28_jan_2003