




Million Dollar Home Page DDoS

Version 1.1

2006-01-16



Executive Overview

An Internet phenomenon, the "Million Dollar Homepage" has been targeted by a distributed denial of service attack (DDoS). Sandvine has determined that this attack is sourced from computers located on residential Internet service provider networks that have been compromised by malware to collectively form a botnet.

A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for legitimate users of the targeted system. The flood of incoming messages to the target system forces it to shut down as the rate at which it receives service requests is greater than its capacity to deliver service. As a result, legitimate users of the system are denied service; their requests lost in the noise. From Figure 1, a Netcraft measurement of the Million Dollar Homepage site performance, we can see that this particular site is globally unavailable for particular periods, implying that all of the outage is due to the server itself.

The nature of the attack is a connection-flood, in which each attacking machine opens a connection to the victim and issues a separate request. These requests cause the victim to maintain a crippling amount of state memory (to timeout each connection, whether it successfully connected or not). The victim also maintains memory in the socket buffer as each TCP connection goes through the TCP FIN_WAIT etc. tear down phase. The attack also causes a significant amount of CPU and network resources to be consumed, as the Apache (web server) back-end must be scheduled for each connection. This approach is different than a traditional SYN-flood attack since the attacker is listening and will accept a response, but nevertheless has the same overall affect.

Because of the very distributed nature of the attack it is not possible to detect the sources and place an access control list (ACL) on the router or firewall in front of the victim.

Sandvine has determined that the most likely bot responsible for this attack was 'Sicklebot'. All 5 of the hosts examined in detail contained the Sicklebot signature.

Sandvine estimates that there are approximately 23000 hosts participating in this attack.

Attack dissection

Sandvine's Security Operations Services team provides security services for networks covering a broad swath of the residential Internet space. Consequently, the insight into global traffic serves as a network telescope of unprecedented scope. One of the primary values of this telescope is that it does not rely on 'black space' as, for example, the CAIDA telescope (<http://www.caida.org/analysis/security/telescope/>) does, but instead is seeing the traffic of real live subscribers. This allows the telescope to see a sourced DDoS attack, rather than just the destination of address scans.

Utilizing Sandvine's network telescope, the ongoing attack on the 'Million Dollar Homepage' was examined, revealing a number of and the following information found.

Sandvine cross-correlated its measurements of the DDoS attack times against Netcraft's performance metrics for the site, as shown below in Figure 1.

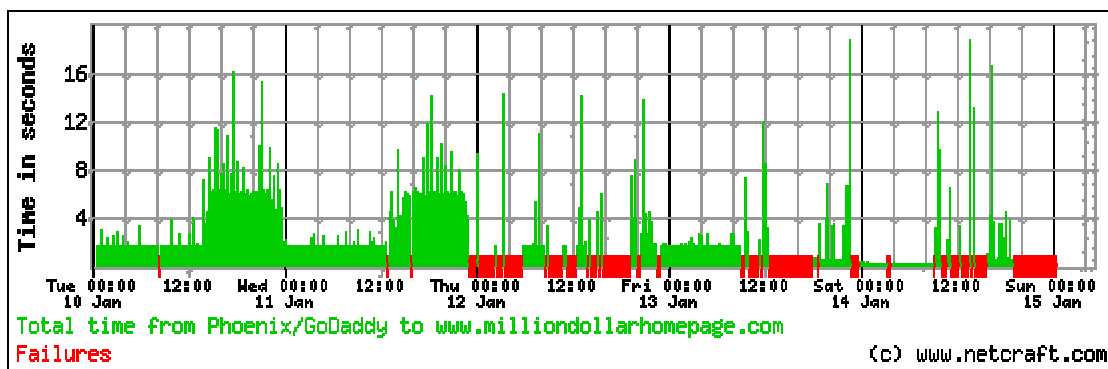


Figure 1: Netcraft measurement of www.milliondollarhomepage.com performance

Analysis techniques

For the purposes of this dissection, 50 attackers from six different Internet service providers were examined in detail. These six Internet service providers comprise approximately 5 million residential Internet subscribers.

Sandvine's Attack Traffic Mitigation feature running on the Sandvine PTS 8210 was used to detect the attackers and to provide packet captures for analysis. The captured files were analyzed offline by Sandvine's Security Operations Services team.

A low-detail examination of the 50 attackers revealed that they all exhibited similar behavior; consequently, detailed analysis was performed on only five, as these would be sufficiently representative of the entire attack base.

A compounding affect is that usually, when a host has a vulnerability that allows it to be exploited, there may be multiple exploits present. This reality can make it difficult to identify which specific Trojan is causing the undesired behaviour.

Initial examination, all 50 hosts

It appears that there are two different concurrent types of attacks manifesting, although it is possible that these attacks are the result of a single Trojan agent. The captured SYN have 2 characteristics: WIN=16384, and WIN=<random> with MSS=1460 and WS=random. The random window chosen appears to be constant for a given attacker, but different from attacker to attacker. Figure 2 and Figure 3, below, depict this behavior.

Time	Source	Destination	Protocol	Info
14:48:04.298	51.127	69.26.178.167	TCP	1312 > 80 [SYN] Seq=2075273403 Ack=0 win=16384 Len=0
14:48:04.302	51.127	69.26.178.167	TCP	1579 > 80 [SYN] Seq=2277326790 Ack=0 win=16384 Len=0
14:48:04.308	51.127	69.26.178.167	TCP	1436 > 80 [SYN] Seq=2698404831 Ack=0 win=16384 Len=0
14:48:04.746	51.127	69.26.178.167	TCP	1905 > 80 [SYN] Seq=3640502022 Ack=0 win=16384 Len=0
14:48:04.757	51.127	69.26.178.167	TCP	1998 > 80 [SYN] Seq=1127423292 Ack=0 win=16384 Len=0
14:48:04.762	51.127	69.26.178.167	TCP	1733 > 80 [SYN] Seq=4051097215 Ack=0 win=16384 Len=0
14:48:05.038	51.127	69.26.178.167	TCP	2268 > 80 [SYN] Seq=2321144408 Ack=0 win=64240 Len=0 MSS=1460
14:48:05.277	51.127	69.26.178.167	TCP	1132 > 80 [SYN] Seq=4106806481 Ack=0 win=16384 Len=0
14:48:05.283	51.127	69.26.178.167	TCP	1210 > 80 [SYN] Seq=1596545842 Ack=0 win=16384 Len=0
14:48:05.287	51.127	69.26.178.167	TCP	1991 > 80 [SYN] Seq=1134054049 Ack=0 win=16384 Len=0
14:48:05.931	51.127	69.26.178.167	TCP	1086 > 80 [SYN] Seq=3021326110 Ack=0 win=16384 Len=0
14:48:05.941	51.127	69.26.178.167	TCP	1717 > 80 [SYN] Seq=3298943658 Ack=0 win=16384 Len=0
14:48:05.945	51.127	69.26.178.167	TCP	1696 > 80 [SYN] Seq=2235346757 Ack=0 win=16384 Len=0
14:48:06.353	51.127	69.26.178.167	TCP	2281 > 80 [SYN] Seq=2319678757 Ack=0 win=64240 Len=0 MSS=1460
14:48:06.359	51.127	69.26.178.167	TCP	2280 > 80 [SYN] Seq=2319621667 Ack=0 win=64240 Len=0 MSS=1460
14:48:06.588	51.127	69.26.178.167	TCP	2283 > 80 [SYN] Seq=2319849561 Ack=0 win=64240 Len=0 MSS=1460
14:48:06.592	51.127	69.26.178.167	TCP	2282 > 80 [SYN] Seq=2319784948 Ack=0 win=64240 Len=0 MSS=1460
14:48:06.597	51.127	69.26.178.167	TCP	1131 > 80 [SYN] Seq=199639279 Ack=0 win=16384 Len=0
14:48:06.602	51.127	69.26.178.167	TCP	1754 > 80 [SYN] Seq=1755228583 Ack=0 win=16384 Len=0

Figure 2: TCP window options, site 1

No. -	Time	Source	Destination	Protocol	Info
3326	10:38:29.473	16.147	69.26.178.167	TCP	44323 > 80 [SYN] Seq=202010149 Ack=0 win=16384 Len=0
3327	10:38:29.481	16.147	69.26.178.167	TCP	1307 > 80 [SYN] Seq=3251502289 Ack=0 win=16384 Len=0
3328	10:38:29.481	16.147	69.26.178.167	TCP	1648 > 80 [SYN] Seq=3694140725 Ack=0 win=16384 Len=0
3329	10:38:29.529	16.147	69.26.178.167	TCP	3470 > 80 [SYN] Seq=241214632 Ack=0 win=5168 Len=0 MSS=1460 WS=3
3330	10:38:29.577	16.147	69.26.178.167	TCP	1741 > 80 [SYN] Seq=3533314207 Ack=0 win=16384 Len=0

Figure 3: TCP window options, site 2

We can infer from Figure 4 that the attacker is using the Windows TCP stack, rather than hand-crafting the packets. This conclusion is based upon the fact that the unanswered packet 2525 on source port 61214 is later re-transmitted. It is unlikely an attacker would bother to perform a re-transmission, since this activity would provide no additional value to the attack.

The same figure also suggests that the attacker is threaded, as there are two sequences of source ports interleaved. For example, we observe that source

port 61212 is used, then 61214, then 61213. This interleave factor implies that at least two threads of execution are being used by the malware behind the attack.

No. -	Time	Source	Destination	Protocol	Info
2524	16:16:13.453	.61.238	69.26.178.167	TCP	61212 > 80 [SYN] Seq=511998664 Ack=0 win=65535 Len=0 MSS=1460
2525	16:16:13.798	.61.238	69.26.178.167	TCP	61214 > 80 [SYN] Seq=3940999570 Ack=0 win=65535 Len=0 MSS=1460
2526	16:16:14.547	.61.238	69.26.178.167	TCP	61213 > 80 [SYN] Seq=870957854 Ack=0 win=65535 Len=0 MSS=1460
2527	16:16:16.083	.61.238	69.26.178.167	TCP	61210 > 80 [SYN] Seq=1356369765 Ack=0 win=65535 Len=0 MSS=1460
2528	16:16:16.959	.61.238	69.26.178.167	TCP	61214 > 80 [SYN] Seq=3940999570 Ack=0 win=65535 Len=0 MSS=1460
2529	16:16:18.237	.61.238	69.26.178.167	TCP	61215 > 80 [SYN] Seq=3568931892 Ack=0 win=65535 Len=0 MSS=1460

Figure 4: port sequence number

The use of Gnutella (and the commercial variant, Morpheus) was detected on a number of the attacking machines. While this observation by no means implicates these applications as the source of infection, peer-to-peer (P2P) networks are a well-known avenue utilized by authors and distributors of malicious applications.

Figure 5, below, indicates that the attacker is periodically looking up the IP address of the victim. By implementing frequent DNS look-ups, the attacker bypasses the common mitigation strategy of changing IP address, used by DoS targets. As a historical example, one of the strategies the 'Blaster' worm used was to launch a denial of service attack on microsoftupdate.com. However, the Blaster worm cached the IP address of this site, allowing Microsoft to change it. In the attack against milliondollarhomepage.com, the Trojan responsible is using the same DNS lookup a valid client must use, so the victim will not be able to simply change the IP.

No. -	Time	Source	Destination	Protocol	Info
234	16:30:06.080			DNS	standard query A milliondollarhomepage.com
235	16:30:06.094			DNS	standard query response A 69.26.178.167

Figure 5: DNS lookup

The Security Operations Services team also observed that the attacker is periodically sending illegal TCP packets to the victim. It is unknown why this might occur. The packet included below in Figure 6 is shown to have both SYN and FIN set, which is not common. This packet also has an illegal TCP header length.

No. -	Time	Source	Destination	Protocol	Info
2856	16:58:45.543		69.26.178.167	TCP	4818 > 80 [FIN, SYN, PSH, ACK] Seq=0 Ack=1879244799 win=0, bogus TCP header length (16, must be at least 20)

Figure 6: Illegal TCP message

Control

HTTP

For control purposes, it is very common for web servers to have well known URL's that are periodically polled. These web servers are themselves typically unwitting participants that are victims of a vulnerability exploit. By controlling botnets in this manner, the botnet master engages in misdirection and makes it more difficult to track down the culprit.

For controlling the attack against milliondollarhomepage.com, some of the affected hosts are periodically fetching a URL with user-agent 'SickleBot'. One of the captured requests is shown below.

```
GET /Galleries/java/45/stat.php?id=1020880659&v=1.0 HTTP/1.1
User-Agent: SickleBot
Host: gernhardts.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Sat, 14 Jan 2006 21:43:18 GMT
Server: Apache/1.3.33 (Unix) mod_log_bytes/0.3 FrontPage/5.0.2.2635
PHP/4.3.11 mod_ssl/2.8.22 OpenSSL/0.9.7c
X-Powered-By: PHP/4.3.11
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

eG1/ZwEGf2R4eHwBBn9/dWIBBn5keHh8LDUsYVWgYGVjYmhjYGBtfmRjYWl8bWtpIm9jYQE
Gfn91Yiw/LGF1YGB1Y2JoY2BgbX5kY2FpfG1raSJvY2EBBm==
```

The site 'gernhardts.com' is likely acting as an unwitting intermediary. Registered in 2001, the site is hosted by 'ipowerweb.com'. This host is running FreeBSD 4.x and is used to host multiple different web pages. The zombies engaging in the attack against milliondollarhomepage.com are checking back with this site approximately every 10 minutes.

IRC

It is very common for botnets to be controlled via an IRC channel. The use of an IRC channel was detected on several of the attacking hosts for this particular attack. Figure 7 shows the general chatter going back and forth between the attacker and the IRC server 'irc.easyshe1lz.com'. Note that this

activity does not necessarily imply that 'easysHELLz.com' is knowingly involved with the attack, or for that matter involved at all.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	66.252.7.195	66.252.7.195	IRC	Response
2	0.278669	66.252.7.195	66.252.7.195	TCP	60166 > 6667 [ACK] Seq=2843485177 Ack=1539739686 win=65535 Len=0
3	1.485564	66.252.7.195	66.252.7.195	IRC	Response
4	1.810629	66.252.7.195	66.252.7.195	TCP	60166 > 6667 [ACK] Seq=2843485177 Ack=1539739758 win=65463 Len=0
5	3.324953	66.252.7.195	66.252.7.195	IRC	Response
6	3.358908	66.252.7.195	66.252.7.195	IRC	Request
7	3.376133	66.252.7.195	66.252.7.195	TCP	6667 > 60166 [ACK] Seq=1539739827 Ack=2843485441 win=17256 Len=0
8	4.268071	66.252.7.195	66.252.7.195	IRC	Response

Figure 7: IRC channel control

Speed of attack

Each attacker is sending approximately 1.8 to 20 connection attempts per second, and is consuming a bandwidth from 2000 bits per second to 32000 bits per second. While these levels of traffic may not seem extreme, in this type of attack each attacker doesn't need to generate a very high rate of traffic - the vast number of attackers will very quickly add up to a crippling amount of data.

Furthermore, it is usually beneficial to generate a low rate from a large quantity of hosts since this is much more difficult to detect and mitigate. Sending huge quantities of data from a relative handful of hosts will raise many alarm bells, whereas a much more distributed approach can go unnoticed by those hosts and networks unwittingly engaged in the attack.

Other attacks from and to attacking hosts

Windows popup spam

The client is also being sent Windows Messenger 'popup' spam, as shown below in Figure 8. This spam will cause a message to pop-up on the user's screen, generally reporting some problem and asking the user to perform some action to remedy the problem. Unsophisticated subscribers will often follow this type of instruction, which can result in their machine being compromised. The particular host that is sending this message to our attacker is located in China, part of "China Network Communications Group Corporation". The web site it references, which will, if visited, infect the subscriber's computer, is registered to "China Mobile Communications Corporation - jiangsu", and was created October 9, 2005. The web site performs a

```
<meta http-equiv="refresh"
content="2;url=http://www.registryupdate.com/affil/idevaffiliate.php?id
=109">
```

which has the affect of sending the user to www.registryupdate.com

No.	Time	Source	Destination	Protocol	Info
0060	da 87 00 00 00 01 00	00 00 00 00 00 00 00	00 00 00 00 00 00 00	TCP	4458 > 80 [SYN] Seq=1257
0070	ff ff ff ff 77 01 00 00	00 00 10 00 00 00 00	00 00 10 00 00 00 00		..K.I.V... ..K.I.V..
0080	00 00 10 00 00 53 59	53 54 45 4d 00 00 00	00 00 00 00 00 00 00	W... ..
0090	00 00 00 00 00 10 00	00 00 00 00 00 00 00	00 00 00 00 00 10 00	SY STEM...
00a0	00 00 41 4c 45 52 54 00	00 00 00 00 00 00 00	00 00 00 00 00 00 00		..ALERT.
00b0	00 00 33 01 00 00 00 00	00 00 33 01 00 00 53 54	00 00 33 01 00 00 53 54		..3..... ..3...ST
00c0	4f 50 21 20 57 49 4e 44	4f 57 53 20 52 45 51 55	OP! WIND OWS REQU		
00d0	49 52 45 53 20 49 4d 4d	45 44 49 41 54 45 20 41	IRES IMM EDIATE A		
00e0	54 54 45 4e 54 49 4f 4e	2e 0a 0a 57 69 6e 64 6f	TTENTION ...windo		
00f0	77 73 20 68 61 73 20 66	6f 75 6e 64 20 35 35 20	ws has f ound 55		
0100	43 72 69 74 69 63 61 6c	20 53 79 73 74 65 6d 20	Critical System		
0110	45 72 72 6f 72 73 2e 0a	0a 54 6f 20 66 69 78 20	Errors.. .To fix		
0120	74 68 65 20 65 72 72 6f	72 73 20 70 6c 65 61 73	the erro rs pleas		
0130	65 20 64 6f 20 74 68 65	20 66 6f 6c 6c 6f 77 69	e do the followi		
0140	6e 67 3a 0a 0a 31 2e 20	44 6f 77 6e 6c 6f 61 64	ng:..1. Download		
0150	20 52 65 67 69 73 74 72	79 20 55 70 64 61 74 65	Registr y Update		
0160	20 66 72 6f 6d 3a 20 77	77 77 2e 66 69 78 2d 6d	from: w ww.fix-m		
0170	73 2e 63 6f 6d 0a 32 2e	20 49 6e 73 74 61 6c 6c	s.com.2. Install		
0180	20 52 65 67 69 73 74 72	79 20 55 70 64 61 74 65	Registr y Update		
0190	0a 33 2e 20 52 75 6e 20	52 65 67 69 73 74 72 79	.3. Run Registry		
01a0	20 55 70 64 61 74 65 0a	34 2e 20 52 65 62 6f 6f	Update. 4. Reboo		
01b0	74 20 79 6f 75 72 20 63	6f 6d 70 75 74 65 72 0a	t your c omputer.		
01c0	0a 46 41 49 4c 55 52 45	20 54 4f 20 41 43 54 20	.FAILURE TO ACT		
01d0	4e 4f 57 20 4d 41 59 20	4c 45 41 44 20 54 4f 20	NOW MAY LEAD TO		
01e0	53 59 53 54 45 4d 20 46	41 49 4c 55 52 45 21 0a	SYSTEM F AILURE!.		
01f0	00		.		

Figure 8: Windows messenger popup spam

The 'www.registryupdate.com' web site is registered in Panama.

We can see that some of the hosts are also actively trying to find and exploit other hosts, implying that they have more than one piece of active malware. In Figure 9, we can see this host is trying to attack a random host on port 445. Multiple Microsoft vulnerabilities exist on this port, and numerous worm families have exploited it. The most common vulnerability is the MS LSASS vulnerability (MS04-011). Sandvine's Security Operations Services team recommends to customers that they outright block this port.

No. -	Time	Source	Destination	Protocol	Info
1566	16:42:44.696	69.26.178.167	82.212.47.4	TCP	4404 > 80 [SYN] Seq=964746132 Ack=0 win=65535 Len=0 MSS=1460
1567	16:42:47.480	82.212.47.4	82.212.47.4	TCP	4517 > 445 [SYN] Seq=4230323850 Ack=0 win=53760 Len=0 MSS=1436 WS=3 TSV=0 TSER=0

Figure 9: Port 445 attack

HTTP sent

Although due to the attack's success, most attack connection attempts failed, a few connections did make it through. A sample request is shown below:

```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, application/vnd.ms-excel,
application/msword, */*
Accept-Language: ru
Accept-Encoding: gzip, deflate
Referer: milliondollarhomepage.com
User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600
Host: milliondollarhomepage.com
Connection: close

HTTP/1.1 200 OK
Date: Sat, 14 Jan 2006 20:55:53 GMT
Server: Apache/1.3.33 (Unix) mod_auth_passthrough/1.8 mod_log_bytes/1.2
mod_bwlimited/1.4 PHP/4.3.11 FrontPage/5.0.2.2635
Last-Modified: Fri, 13 Jan 2006 18:08:15 GMT
ETag: "14000c-97-43c7eca6"
Accept-Ranges: bytes
Content-Length: 151
Connection: close
Content-Type: text/html

<html>
<head>
<script type="text/javascript">
<!--
window.location = "http://www.milliondollarhomepage.com/index.php"
//-->
</script>
</head>

</html>
```

This request is interesting for a number of reasons:

- The user-supplied language is 'ru', which means Russian. The attacker in this case is a PC in the United States. Statistically speaking, the odds of a randomly-selected PC in the United States operating a Russian version of Windows is unlikely. While by no means an outright conclusion, this characteristic could imply that the attacker originates from a Russian speaking country. Historically, a large percentage of Internet attacks originate from Eastern European nations.

- The use of the 'Microsoft-WebDAV-MiniRedir/5.1.2600' user-agent implies that this malware might be exploiting the MS03-007 vulnerability, or a newer version of it.
(<http://www.microsoft.com/technet/security/bulletin/MS03-007.msp>)
- The 'Host' is spoofed to be the victim itself.
- The 'Referer' is similarly spoofed.
- The attacker is using the TCP stack rather than sending specifically crafted SYN packets.

The packets themselves also contain some information. We can see in Figure 10 that the connection is torn down by the attacker prematurely: when the victim sends back a FIN, the attacker sends a RST, implying it has already closed the connection. This suggests that the attacker opened the connection, sent the GET request, and then closed the connection almost immediately without regard for the response.

No. -	Time	Source	Destination	Protocol	Info
26731	15:45:38.100	69.26.178.167	69.26.178.167	TCP	1830 > 80 [SYN, ACK] Seq=3574582384 Ack=0 Win=16384 Len=0 MSS=1460
26733	15:45:38.224	69.26.178.167	24.55.29.200	TCP	80 > 1830 [SYN, ACK] Seq=1425602268 Ack=3574582385 Win=5840 Len=0 MSS=1460
26734	15:45:38.237	69.26.178.167	69.26.178.167	TCP	1830 > 80 [ACK] Seq=3574582385 Ack=1425602269 Win=17520 Len=0
26735	15:45:38.244	69.26.178.167	69.26.178.167	HTTP	GET / HTTP/1.1
26796	15:45:41.208	69.26.178.167	69.26.178.167	HTTP	GET / HTTP/1.1
26830	15:45:42.238	69.26.178.167	69.26.178.167	TCP	1830 > 80 [FIN, ACK] Seq=3574582736 Ack=1425602269 Win=17520 Len=0
27116	15:45:47.228	69.26.178.167	69.26.178.167	HTTP	GET / HTTP/1.1
27136	15:45:47.316	69.26.178.167	24.55.29.200	HTTP	HTTP/1.1 200 OK (text/html)
27137	15:45:47.316	69.26.178.167	24.55.29.200	TCP	80 > 1830 [FIN, ACK] Seq=1425602760 Ack=3574582737 Win=6432 Len=0
27139	15:45:47.334	69.26.178.167	69.26.178.167	TCP	1830 > 80 [RST, ACK] Seq=3574582737 Ack=1425602760 Win=0 Len=0

Figure 10: TCP analysis of web packets