July, 2009 South Korea and US DDoS Attacks

Arbor Networks ASERT Team
July 10, 2009

Background

Beginning on July 4, 2009, we began seeing a series of DDoS attacks against US government, US commercial, South Korean government and South Korean commercial websites. These attacks were from a previously unknown botnet. The bots are configured to attack a pre-defined set of targets and have been updated using a configuration file to attack new targets, as well.

This report provides an overview of the malware and DDoS attacks and is designed to be used in conjunction with other reports from US-CERT, KrCERT, and other analysis teams. This report was generated using internally performed analysis and also with data shared by third parties.

Distribution: Limited
For Arbor Networks Customer or specified use only.

Document ID: dcc8b4d0246dff94ae33d73b9bf5a11a

Signature Traffic

Infected systems will be seen sending HTTP requests with the string:

```
HTTP/1.1 GET /china/dns?
```

The following HTTP user agent strings will be used in the HTTP DDoS:

```
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6; .NET CLR
2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)

Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0;
GTB6; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR
3.5.30729)

Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.20)
Gecko/20081217 Firefox/2.0.0.20 (.NET CLR 3.5.30729)

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0;
GTB6; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR
3.5.30729)
```

Two of those user agent strings are legitimately seen with browsers but the other two are distinct for the bot's forged HTTP headers. Additional headers seen in the malware include:

```
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword, application/x-
ms-application, application/x-ms-xbap, application/vnd.ms-
xpsdocument, application/xaml+xml, */*

Accept-Language: ko

UA-CPU: x86

Accept-Encoding: gzip, deflate

Content-Length: 0

Connection: Keep-Alive
```

Any or all of these headers may be present in an HTTP request. Simple HTTP request rate monitoring via TMS can be used to detect the bots' activities. Note that some of these headers alone do not indicate a bot's presence.

DDoS Attack Characteristics and Mitigation Strategies

We have observed the following DDoS attack traffic in the wild:

UDP port 80 flood

This is a trivial attack to stop for affected websites. Simply deny all UDP port 80 traffic to the websites. This traffic may be source spoofed.

ICMP Echo Request flood

This can be rate limited to the victim and may also be source spoofed.

IP protocol 0 flood

This can be rate limited to the victim and may also be source spoofed.

TCP SYN flood to port 80

This can be rate limited to the victim and may also be source spoofed. Arbor TMS SYN authentication countermeasures may also be used.

HTTP GET request flood to '/'

This affects the websites listed above. Request rate limiting can be used to defeat the attack. We have seen websites use HTTP 302 redirects to detect bots as they will not follow the redirect; Arbor TMS HTTP authentication countermeasures may also be used. Once bots are identified they can be filtered.

Proactive Deployment of Infrastructure and Server Configuration Best Current Practices

There are a number of industry best current practices (BCPs) which should be proactively deployed by network operators responsible for Internet-facing infrastructure and properties; organizations which had implemented these BCPs prior to this particular round of attacks were far better equipped to detect, classify, traceback, and mitigate the attack traffic than those who had not done previously done so.

Network Infrastructure BCPs

Interface ACLs (iACLs) should be employed at the relevant network edges (peering/transit, customer aggregation edge, etc.) to protect the network infrastructure itself; additional service-specific sections should be used to restrict traffic destined for

Internet-facing servers to the ports and protocols associated with the services and applications on those servers.

The use of IP protocol 0 in this attack is notable as a common mechanism used by attackers to bypass ACLs that only contain policy statements relating to common protocols such as TCP, UDP, and ICMP; there are 254 valid Internet protocols, and irrelevant protocols should be filtered at the edges via ACLs.

Additional network infrastructure BCPs such as control- and management-plane self protection mechanisms should also be deployed.

All network infrastructure devices should be accessible only via designated management hosts, and this access should be facilitated via a dedicated out-of-band (OOB) management network. During high-impact DDoS attacks, a dedicated management network ensures that devices can be managed irrespective of conditions on the production network, and also ensures that vital mechanisms such as flow telemetry and SNMP are uninterrupted, which assures continuing visibility into attack traffic during an incident.

Flow telemetry such as Cisco NetFlow, Juniper cflowd, and sFlow should be enabled at all network edges, and exported into a collection/analysis system. Arbor Peakflow SP provides flow-based anomaly-detection capabilities, allowing detection, classification, and traceback of attack traffic.

Source-based remotely-triggered blackholing (S/RTBH) is a powerful reaction technique which allows tens or even hundreds of thousands of attacking source IPs (classified via flow analysis, logfiles, etc.) to be rapidly blackholed based upon their source addresses. S/RTBH leverages BGP as a control-plane mechanism to instantaneously signal edge devices to start dropping attack traffic. Arbor Peakflow SP can serve as the trigger for S/RTBH.

Reverse-proxy caching in front of Internet-facing Web properties allows for scaling of capacity as well as a policy control point which enables filtering of layer-7 application protocol traffic; in this particular instance, reverse-proxy cache HTTP header-based filtering based upon the identified attacking bot user-agent strings allows mitigation of the HTTP GET attack component.

Host BCPs

Public-facing servers should be configured in a hardened manner, with unnecessary services disabled, OOB management access, service-specific configuration hardening, IP stack tuning, and other relevant mechanisms. Stateless on-server filtering via tcpwrappers is a useful policy-enforcement mechanism; for Web servers, Apache modules such as mod_security and mod_evasive bring additional capabilities.

The deployment of stateful firewalls or other inspection devices such as IDS/IPS in front of Internet-facing servers is contraindicated; as each incoming connection to Internet-facing servers is by definition unsolicited, the stateful inspection adds nothing to the security posture of the servers, and serves to weaken their ability to withstand DDoS traffic due to the limited state-table size of even the largest/fastest firewalls and IDS/IPS on the market today. During this particular attack, Web application firewalls in front of targeted servers were observed to fail while receiving relatively low amounts of attack traffic, thereby enabling the DDoS to succeed in making the servers unavailable with little effort on the part of the attacker. The Arbor TMS can be deployed to protect the DNS infrastructure in the same fashion as the Web servers.

Load-balancers also instantiate state which renders the real servers behind the load-balancers more vulnerable to DDoS; during this attack, load-balancers were observed to fail due to state exhaustion as a result of the attack traffic. S/RTBH, reverse-proxy caches, and intelligent DDoS mitigation via the Arbor TMS can be utilized to protect the load-balancer and the real servers behind it.

DNS infrastructure should be deployed in a modular, bulkheaded architecture, with separation of functions such as authoritative servers, internal resolvers, external resolvers, caching-only resolvers, etc., and should be scaled appropriately by employing techniques such as IPv4 anycasting. During this attack, it does not appear that DNS was directly targeted; however, DNS lookups for targeted domains were observed to intermittently fail, probably as a result of large amounts of queries for sites in these domains by both legitimate users attempting to access them repeatedly as well as by botted hosts resolving the target host IPs as part of the HTTP GET attack component.

Implicated Malware

The main infector malware appears to be related to the MyDoom family, specifically MyDoom A or B variants from late 2003 or early 2004. The source code is available on the underground market and was apparently modified to suit the author’s needs.

None of the samples are “packed” (compressed to expand at run-time, a popular technique to thwart static analysis) and none of them display anti-AV or anti-analysis armoring.

The South Korean antivirus firm AhnLab provided all of the following malware samples to the security research community. We have not been able to independently verify that this is a complete set of malcode, although we have seen these samples behave as bots in the lab. The malware samples we have been investigating have the following MD5 hashes:

```
04a3552a78ed2f8dc8dc9a77ee9eb281
06C105D0D4AD7F63EB3ADE6810C1DD47
0f394734c65d44915060b36a0b1a972d
1CBA81FEA0F34511C026E77CFA1F0EF6
1cba81fea0f34511c026e77cfa1f0ef6
3711AE663975041E0F2958A6226D9660
445BDE29CEB233A301A70AD8E66F4CC4
4b834eadab00115c65f3563fd1dd299a
```

```
50C97BF514643D9E60980985DB0908CA
5FBD592AE4704045EEC712C5AEBB6419
6350758b6248476523905721 8bd81d9e
65ba85102aaec5daf021f9bfb9cddd16
6623E51595C0076755C29C00846C4EB2
6FDDB7E59C4977AD173C1D8F2A86E8BE
6e5b00560a3c5bb92dfacb3766d6d7bc
70483D481EC1C9CB3F8221829C7A67FF
84C9C342CE1AA25CA58DD7F4E06857DD
8520911EB8F7AD6E822D7E57EE63321A
90550F6692F3255C78E5C5B3DEF6B970
93322e3614babd2f36131d604fb42905
9b08939834b2fe265ebaedccebd3d470
A34981AC5B0DAA12C9F11525DED3FFBB
F2F8347F30B6EC8276B02D4A45AA8C01
bcb69c1bab27f53a0223e255d9b60d87
e199d5c70745c363b734f499a3e065a9
```

Key pieces of malware are used to start the process and may be the initial infection tools. They are all related to the MyDoom source code base and include:

```
MD5: 0f394734c65d44915060b36a0b1a972d VTotal
SHA1: 426bc6bb3704441e5804d75ad020706f06b3db5d
File type: application/x-ms-dos-executable
File size: 374651 bytes
```

This sample attempts to install itself as “wmiconf”, the “WMI Performance Configuration” service. Infected users will see this service with the description “Configures and manages performance library information from WMI HiPerf providers.” On execution this program will create the following files:

```
C:\DOCUME~1\Username\LOCALS~1\Temp\_S1.tmp
C:\WINDOWS\system32\wmiconf.dll
C:\DOCUME~1\ Username \LOCALS~1\Temp\_S5.tmp
C:\WINDOWS\system32\wpcap.dll
C:\DOCUME~1\ Username \LOCALS~1\Temp\_S9.tmp
C:\WINDOWS\system32\Packet.dll
C:\DOCUME~1\ Username \LOCALS~1\Temp\2733_appcompat.txt
```

The related key sample is:

```
MD5: 1cba81fea0f34511c026e77cfa1f0ef6
SHA1: 007d3c2820c41b7abdadda3b84a07355ebaef358
File type: application/x-ms-dos-executable
File size: 88064 bytes
```

This sample attempts to install itself as the “mstimer” service, which is described on an infected PC as “Maintains date and time synchronization on all clients and server in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.”. This file will create similar files and launch the attacks in a manner similar to the file above.

Another key related file is:

```
MD5: 93322e3614babd2f36131d604fb42905
SHA1: 3f8ed8a0a8be604f68b01a8d44df81e743b23a34
File type: application/x-ms-dos-executable
File size: 45056 bytes
```

This program does not behave similarly to the other files above but is related to MyDoom. This program appears to try to spread over email.

Identified Command and Control Servers

Third parties have identified the following command and control servers and ports: 213.33.116.41:53 216.199.83.203:80 213.23.243.210:443. These servers are in the US, Germany and Austria and are, to the best of our knowledge, under investigation by law enforcement teams.

Botnet Composition

Third parties have identified approximately 130,000 active bots through attack log examinations. Over 95% of the bots are from South Korean IP addresses. Another third party who has infiltrated one of the command and control servers has identified approximately 200,000 bots in the network.

Initial Infection Point

At this time we are not able to identify how the systems became infected with the malware. We are examining common attacks on clients such as drive by downloads, email propagations, or peer-to-peer network poisoning. We have not yet reached any conclusions with this investigation.

We believe that the infection vector struck Korean language users, which would account for the great concentration of South Korean users in the botnet.

Attack Targets

The attack tools have targets embedded in some files but will also receive updated target lists.

The samples with MD5 hashes 6e5b00560a3c5bb92dfacb3766d6d7bc and e199d5c70745c363b734f499a3e065a9 has the following targets embedded in the malcode for UDP and HTTP flood attacks:

```
www.voanews.com
www.yahoo.com
www.defenselink.mil
www.nyse.com
www.nasdaq.com
www.site-by-site.com
www.marketwatch.com
finance.yahoo.com
www.usauctionslive.com
www.usbank.com
www.amazon.com
```

The sample with the hash 9b08939834b2fe265ebaedccebd3d470 embeds the following targets for DDoS attacks

```
evisaforms.state.gov
www.faa.gov
www.whitehouse.gov
```

Configuration files have been used (in NLS format) to reconfigure the bots' floods. The command file with the MD5 checksum 4b834eadab00115c65f3563fd1dd299a specified the following targets:

```
www.president.go.kr
www.mnd.go.kr
www.mofat.go.kr
www.assembly.go.kr
www.usfk.mil
blog.naver.com
mail.naver.com
banking.nonghyup.com
ezbank.shinhan.com
ebank.keb.co.kr
www.hannara.or.kr
www.chosun.com
www.auction.co.kr
www.whitehouse.gov
www.faa.gov
www.dhs.gov
www.state.gov
www.voanews.com
www.defenselink.mil
www.nyse.com
www.nasdaq.com
finance.yahoo.com
www.usauctionslive.com
www.usbank.com
www.washingtonpost.com
www.ustreas.gov
```

With the help of AhnLab, we have seen the following configuration files and attack targets specified:

2009/07/05 02:00 ~ 2009/07/05 14:00

```
www.whitehouse.gov
whitehouse.gov
www.faa.gov
faa.gov
evisaforms.state.gov
```

2009/07/05 22:00 ~ 2009/07/06 07:00

```
www.whitehouse.gov
www.faa.gov
www.ustreas.gov
www.dhs.gov
www.state.gov
www.dot.gov
www.ftc.gov
www.nsa.gov
www.usps.gov
www.voa.gov
www.yahoo.com
www.defenselink.mil
travel.state.gov
www.nyse.com
www.nasdaq.com
www.site-by-site.com
www.marketwatch.com
finance.yahoo.com
www.usauctionslive.com
www.usbank.com
www.amazon.com
```

2009/07/05 22:00 ~ 2009/07/06 18:00

```
www.whitehouse.gov
www.faa.gov
www.ustreas.gov
www.dhs.gov
www.state.gov
www.dot.gov
www.ftc.gov
www.nsa.gov
www.usps.gov
www.voanews.com
www.yahoo.com
www.defenselink.mil
```

```
travel.state.gov
www.nyse.com
www.nasdaq.com
www.site-by-site.com
www.marketwatch.com
finance.yahoo.com
www.usauctionslive.com
www.usbank.com
www.amazon.com
```

2009/07/07 18:00 ~ 2009/07/08 18:00

```
www.president.go.kr
www.mnd.go.kr
www.mofat.go.kr
www.assembly.go.kr
www.usfk.mil
blog.naver.com
mail.naver.com
banking.nonghyup.com
ezbank.shinhan.com
ebank.keb.co.kr
www.hannara.or.kr
www.chosun.com
www.auction.co.kr
```

2009/07/07 21:00 ~ 2009/07/08 07:00

```
www.whitehouse.gov
www.faa.gov
www.dhs.gov
www.state.gov
www.voanews.com
www.defenselink.mil
www.nyse.com
www.nasdaq.com
finance.yahoo.com
www.usauctionslive.com
www.usbank.com
www.washingtonpost.com
www.ustreas.gov
```

2009/07/08 18:00 ~ 2009/07/09 18:00

```
www.mnd.go.kr
www.president.go.kr
www.ncsc.go.kr
mail.naver.com
mail.daum.net
mail.paran.com
www.auction.co.kr
www.ibk.co.kr
www.hanabank.com
www.wooribank.com
www.altools.co.kr
www.ahnlab.com
www.usfk.mil
www.egov.go.kr
```

2009/07/09 18:00 ~ 2009/07/10 18:00

```
mail.naver.com
mail.daum.net
mail.paran.com
www.egov.go.kr
www.kbstar.com
www.chosun.com
www.auction.co.kr
```

Attack Rates and Durations

The Arbor ATLAS system, which collects data from Arbor Peakflow SP monitors around the world, has identified some of the attacks in the wild. We have observed packet rates of between 50,000 and 100,000 packets per second in TCP floods and bandwidth rates of 25Mbps to 50Mbps in many cases. Attacks lasted several hours in these cases.

We have received reports from third parties of attacks in this set with sizes three orders of magnitude larger, approximately 25Gbps. We cannot confirm this at this time.

Self Destruct Mechanism

The malware will download the file “flash.gif” from a number of websites. This file may have the MD5 hash f5c6b935e47b6a8da4c5337f8dc84f76. The file is actually a Windows EXE file with a small, minimal JPEG header prepended. This header is stripped off and then the EXE is launched. If the system date is July 10, 2009, key files are compressed and the original files are deleted. This malware also destroys the PCs Master Boot Record (MBR) and renders the system unbootable.

Users who may be infected should take the following steps to prevent such destruction:

1. Boot the PC in “safe mode”
2. Set the system clock to before July 10, 2009
3. Run freshly installed AV
4. Reboot
5. Restore the system clock to the correct date

Additional Information

Readers may find the following URLs helpful for additional information.

http://maxoverpro.tistory.com/
http://www.krcert.or.kr/secureNoticeView.do?num=342&seq=-1
http://isc.sans.org/diary.html?storyid=6748
http://www.kisa.or.kr/main.jsp
http://api.v.daum.net/open/related_news?news_id=3606586&display_type=widget&skin=1&frameContents=both