# 2009 年 7 月韩美 DDoS 攻击分析报告

Arbor 网络 ASERT 小组
2009 年 7 月 10 日

## 相关背景

2009 年 7 月 4 日以来，韩美部分重要政府和商业网站遭受到一系列未知木马病毒 DDoS（分布式拒绝服务）的攻击。此次攻击预先设定了一系列目标并对目标进行不断更新。

本分析报告可以让用户对此次木马病毒及恶意软件攻击事件有所了解，并可以结合其它机构（US-CERT, KrCERT 等）的分析报告对攻击事件有整体了解。本分析报告用于为三方数据共享做攻击推演。

## 病毒流量样本

被感染系统将发送一个 HTTP 请求字符串：

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

下面的 HTTP 用户代理字符串将被用于 HTTP DDoS 攻击代码中:

```
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 CLR3.5.30729)
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 CLR3.5.30729)
```

其中两种浏览器请求是合法操作,但其余两个包含伪装木马病毒，来控制 HTTP 标头。此恶意软件发送的两个 HTTP 请求如下:

```
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/xms-
application, application/x-ms-xbap, application/vnd.msxpsdocument,
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 requestrate 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.

所有这些标头（header）可能存储在一个 HTTP 请求中，通过简单的 HTTP 流量流向分析设备可检测类似的僵尸(bot)活动。但是这些请求 Header 并不一定意味着僵尸的存在。

## DDoS 的攻击特点和减灾战略

在互联网上我们已经检测到以下的 DDoS 攻击流量：

**UDP80 端口溢出**

对于受攻击的网站来说，这是一个普通的攻击。简单的拒绝此网站所有 UDP 80 端口流量，病毒可能利用这些流量进行伪装。

**ICMP 回应请求溢出**

这个攻击可能是感染网站的正常请求流量,也可能会是欺骗。

**IP protocol 0 flood**

这个攻击可能是感染网站的正常请求流量,也可能会是欺骗。

**TCP 80 端口同步溢出**

这个攻击可能是感染网站的正常请求流量,也可能会是欺骗。Arbor TMS SYS 可以检测到这类攻击.

**HTTP GET request flood to '/'**

这种将影响上列网站。请求限制速率可以用来打败攻击。我们已经看到网站使用 HTTP 302 来探测木马病毒，因为他们不会重新认证,Arbor TMS SYS 可以检测到这类攻击，我们一旦确定病毒，立即执行过滤操作。

## 积极部署基础设施和服务器 配置最好设施

有一些行业应该执行桥接控制协议，网络运营商应负责定制互联网基础设施设备，实施了桥接控制协议的机构对此类攻击应准备优秀装备进行检测，分类，追踪，疏通并缓减攻击。

**网络基础设施桥接控制协议**

接口访问控制列表（ iACLs ）应部署在相关的网络边界处（对等/穿越，客户聚集节点等），以保护网络自身基础设施;额外的服务细节部分应当用来限制目的为互联网的服务器上与业务相关的端口以和协议，以及这些服务器上的应用。

值得注意的是，IP 0 协议在攻击中被攻击者作为一个通用机制使用，用来避开只包含策略描述与普通协议（如 TCP，UDP，ICMP）有关的 ACL；网络中有 254 种合法的 IP 协议， 同时不相关的协议应在网络边界处通过的 ACL 进行过滤 。

其他额外的网络基础架构 BCP，如控制和管理平面、自保护机制，也应该进行部署。

登录所有网络基础架构设备应该只能通过指定的管理主机，同时登录操作应易于通过专用的带外管理网络进行操作。在一个严重的 DDoS 攻击发生时，一个专门的管理网络在忽略产品本身网络的条件下可确保设备可管理，同时也应该确保例如“流动”监测和 SNMP 等重要机制不被中断，保证在攻击发生时攻击流量的连续可视化。

“流”监测技术，如 Cisco NetFlow、Juniper cflowd 和 sFlow 应该开启在全部网络边界处，同时发送到一个采集/分析系统。Arbor Peakflow SP 系统提供的基于“流”的异常检测功能，允许对攻击流量进行检测、分类和追溯。

基于源的远程触发黑洞机制 （S / RTBH ）是一种强大的响应技术，允许基于其源地址将数万、甚至数以十万计的攻击源 IP 地址（通过“流”分析或记录文件进行归类）迅速地被置于黑洞中。

作为控制平面机制，S/RTBH 提高桥接控制协议，利用瞬间信号边缘设备开始减缓攻击流量。同时，Arbor 高锋速流 SP 可触发 S/RTBH

互联网的反向代理缓存可以进行解压缩放以及控制政策点，能够过滤 7 层协议;在这一特定情况下，以反向代理缓存 HTTP 为基础的过滤器根据木马病毒攻击字符串来缓解的 HTTP GET 攻击的部分组成。

**Host BCPs**

公共服务器应该配置稳定，去除了冗长服务，管理了带外数据权限，硬化了特定服务器配置，调整了网络协议，以及其他有关程序。无国界的服务器过滤器 viatcpwrappers 是一个有效的程序执行器，为模块文件如安全请求和规避风险等的网络服务器带来额外的执行能力。
在 Internet 前沿服务器设置防火墙或其他检查设备是应被禁止的，如入侵检测系统/入侵防御软件;以防止任何来源不清的互联网连接。

# 有关的恶意软件

主要传染恶意软件似乎与 MyDoom 系列软件息息相关，尤其是在 04 年年初开发的 MyDoom

中的变种 A 程序和变种 B 程序。来源码在市场上随处可得，明显它已被改进，用来满足客户需求。

没有一个病毒的感染是经过“压缩的”，（指：一种流行技术通过瞬间解压扩张，来破坏数据分析体系），它们即不携带防病毒软件，也没有防破解软件。

以下恶意软件攻击案例是由韩国防病毒公司 AhnLab 提供给国家安全局。我们现今还不能确定这是一整套的病毒代码，但我们仍在实验室进行这方面的研究工作。这些包含 MD5 检查文件恶意软件正在调查中。

04a3552a78ed2f8dc8dc9a77ee9eb281
06C105D0D4AD7F63EB3ADE6810C1DD47
0f394734c65d44915060b36a0b1a972d
1CBA81FEA0F34511C026E77CFA1F0EF6
1cba81fea0f34511c026e77cfa1f0ef6
3711AE663975041E0F2958A6226D9660
445BDE29CEB233A301A70AD8E66F4CC4
4b834eadab00115c65f3563fd1dd299a
50C97BF514643D9E60980985DB0908CA
5FBD592AE4704045EEC712C5AEBB6419
6350758b62484765239057218bd81d9e
65ba85102aaec5daf021f9bfb9cddd16
6623E51595C0076755C29C00846C4EB2
6FDDB7E59C4977AD173C1D8F2A86E8BE
6e5b00560a3c5bb92dfacb3766d6d7bc
70483D481EC1C9CB3F8221829C7A67FF
84C9C342CE1AA25CA58DD7F4E06857DD
8520911EB8F7AD6E822D7E57EE63321A
90550F6692F3255C78E5C5B3DEF6B970
93322e3614babd2f36131d604fb42905
9b08939834b2fe265ebaedccebd3d470
A34981AC5B0DAA12C9F11525DED3FFBB
F2F8347F30B6EC8276B02D4A45AA8C01
bcb69c1bab27f53a0223e255d9b60d87
e199d5c70745c363b734f499a3e065a9

恶意软件的主要部分都会引发病毒的传染，或可能它们就是最初的传染源。它们都以 MyDoom 源代码为基础并包括：

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

上面这个例子把“WMICONF”作为 WMI 性能配置器安装进程序，被感染用户将会看到来自“此信息来自 HiPer 供应商的配置和管理性能库”一行解释。执行以上操作将导出下列文件：

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

相似例子为：

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

上面这个例子一旦把“MSTIMER”安装进程序,被感染的个人电脑将显示：保持所有客户端和服务器的日期和时间同步。若上述操作中断，数据和时间将不可得。若禁止操作，任何相关程序将被迫停止。这个文件将制造更多类似文件以相同方式对以上文件发起攻击。

另一个相关案例是：

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

此程序与上述程序性质相同，但带有 MyDoom 病毒。病毒将通过邮件扩散到整个网络。

## 明确命令和控制伺服器

三方已确定了连续命令，控制伺服器和端口：213.33.116.41:53 216.199.83.203:80 213.23.243.210:443.这些伺服器在美国，德国，奥地利耳熟能详，现在正在法律调查中。

**木马病毒组成**

三方已确定了约 13 万个变种木马病毒，它们试图攻击网络日志。95%的病毒来自韩国网站。另一个受感染的控制和伺服器已经传播了约 20 万个病毒。

**最初感染源**

现在我们还不能判断系统是如何被传染恶意病毒的。我们正检查客户端收到的相同攻击，如通过下载，邮件，或点对点网络传播的。现在调查还未有进展。

我们认为韩国受到了矢量感染，通过这种方式韩国用户大范围的感染上了木马病毒。

**攻击目标**

攻击目标嵌入这些文件中，但也会不断更新目标列表。

在以下两个 MD5 检查文件 6e5b00560a3c5bb92dfacb3766d6d7bc 和 e199d5c70745c363b734f499a3e065a9 中，病毒代码规定目标，横扫 UDP 和 HTTP 地址。

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

这是 MD5 检查文件 9b08939834b2fe265ebaedccebd3d470 遭受 DDos 病毒攻击的例子。

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

以上是木马病毒以含 MD5 校验文件 4b834eadab00115c65f3563fd1dd299a 为指定目标的攻击代码。此配置文件通过 NLS 形式受到木马感染。

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

在 AhnLab 的帮助下，我们看到下面的配置文件和攻击目标指明：

**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

## 攻击频率和持续时间

Arbor Atlas 系统收集的数据来自 Arbor Peakflow 监测点，确定了一些攻击。在许多攻击的时候，我们注意到 packet rates 保持在 5 万至 10 万包中的 TCPTCP floods 和带宽率每秒钟 25MB 至 50Mbps。在这些情况下袭击持续了几个小时。

## 自毁机制

恶意软件将从一些网站上下载文件“ flash.gif ”。该文件可能有 MD5 校验文件 f5c6b935e47b6a8da4c5337f8dc84f76 。该文件实际上是一个 Windows EXE 文件，标题被拿掉了，然后 EXE 文件启动了。如果系统日期是 2009 年 7 月 10 日，关键的压缩文件和原来的文件就被删除。该恶意软件还摧毁了电脑主引导记录（MBR），并使该系统无法启动。

可能感染的用户应采取以下措施来防止这种破坏行为：

1 .启动电脑在“安全模式”
2 .设置系统时钟在 2009 年 7 月 10 号
3 .行新安装的 AV
4 .重新启动
5 .恢复系统时钟，以正确的日期

## 其他信息

读者可能会发现下在面的网址找到补充资料。

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