The IMDDOS Botnet: Discovery and Analysis

Damballa Threat Research

In less than four months, the Chinese IMDDOS Botnet has become one of the largest active botnets in the world.

This report details the discovery of the IMDDOS botnet, the growth and timeline, the commercial aspects of its operation, the technical components of the botnet infrastructure, the malware used, and what is currently being done to disrupt its operation.

Take Back Command-and-Control

The IMDDOS Botnet: Discovery and Analysis

Contents

Executive Overview

On March 20, 2010, a criminal organization registered a series of malicious domains signaling the birth of a new botnet; one designed to offer a commercial service for delivering Distributed Denial of Service (DDoS) attacks against any desired target. This publicly available service, hosted in China, is available for lease to anyone willing to establish an account on-line, input the domain(s) they wish to attack, and pay for the service.

The website promoting this service is called “IM DDOS”, elsewhere referred to as “I’M DDOS”.

Damballa announced the discovery of this new botnet on September 13, 2010, and has named it the IMDDOS Botnet.

A Denial of Service (DoS) attack is a technique used to overwhelm a website/domain in an effort to reduce its responsiveness, or completely eliminate its ability to respond to new connection attempts. DoS attacks have been used to ‘take down’ political sites, abuse sites, commercial business websites and even military command centers as part of a coordinated targeted campaign.

A *Distributed* Denial of Service (DDoS) attack utilizes multiple PCs or servers to initiate a coordinated attack against a targeted system. Obviously, the more assets involved in the attack, the larger the flood of requests and data that can be targeted at the victim. To create a very large army of assets that can launch these DDoS attacks, botnets are used to rally and command unwitting victim machines into participating in the attacks. The criminals establish the botnet by installing malicious software (malware) on to unwitting victim machines (hosts). The infected hosts are rallied and then instructed to launch a coordinated DDoS attack against the victim of choice. In this manner, thousands or tens of thousands of unwitting hosts can simultaneously flood a list of targeted systems - rendering even the most robust websites or web applications unable to respond to legitimate customer requests.

The risk to enterprise networks containing victim machines that have successfully rallied to the botnet is that the enterprise is unwittingly participating in attacks on unknown victims, and that malware capable of a variety of criminal attacks has penetrated the enterprise. For ISPs and their customers, it represents a tremendous drain on network and computing resources, which can result in poor network performance and significant loss of otherwise revenue-generating bandwidth.

The newly uncovered IMDDOS Botnet is a commercial DDoS service. The botnet, throughout the Damballa period of study, grew large very quickly. Following testing by the crminal operators back in April 2010, it reached a production peak activity by the second week of August of 25,000 unique Recursive DNS (RDNS) lookups per hour attempting to resolve to the botnet’s command-and-control (CnC) servers.

This paper details the growth of the IMDDOS Botnet, the commercial aspects of its operation, the technical components of the botnet infrastructure, how it was discovered, and what has been done to disrupt its operation.

The Growth of the IMDDOS Botnet

The origination of this particular botnet appears to date back to March 20, 2010, when the original domain names were registered. Looking into the growth of the botnet we note that during the month of April there was a testing phase originating from China (Figure 1).

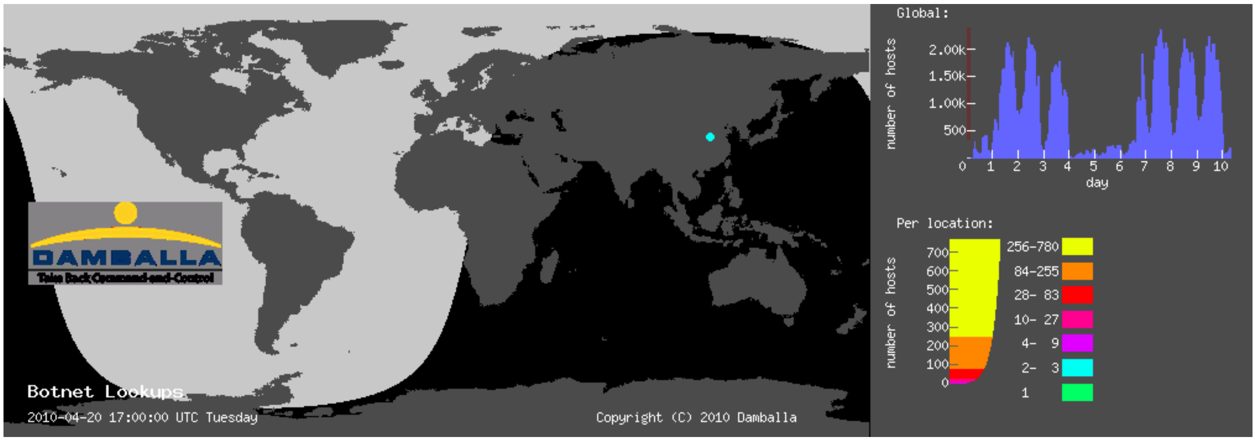


Figure 1: IMDDOS Botnet DNS Lookups for April

During the next two months the number of DNS lookups for all domain names associated with the botnet grew from 2,000 to 10,000.

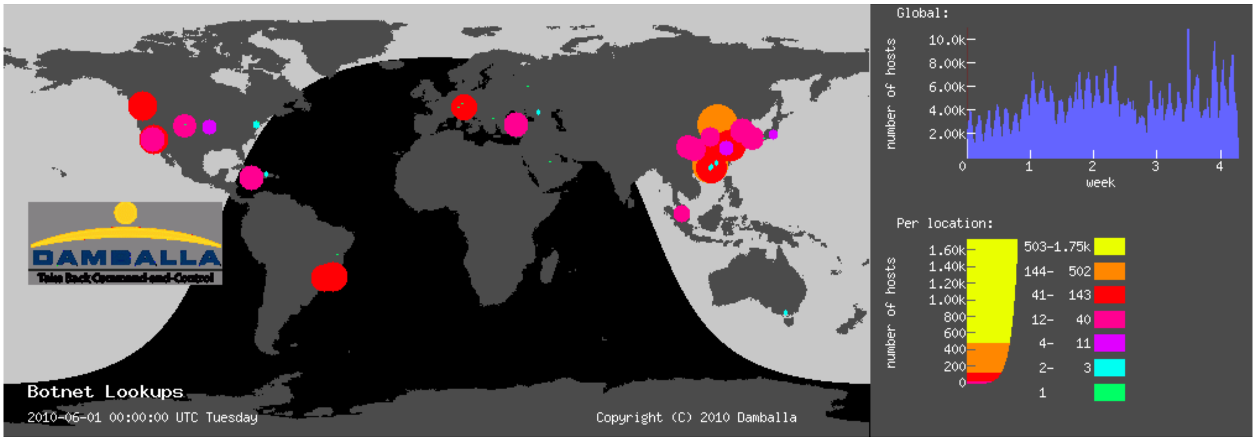


Figure 2: IMDDOS Botnet DNS Lookups for June

The botnet grew quickly as observed by the rapid increase in daily DNS lookups for all CnC domain names associated with the IMDDOS botnet. During the second week of August the botnet reached its peak with more than 25,000 unique RDNS lookups per hour cummulatively for all CnC domains (Figure 3).

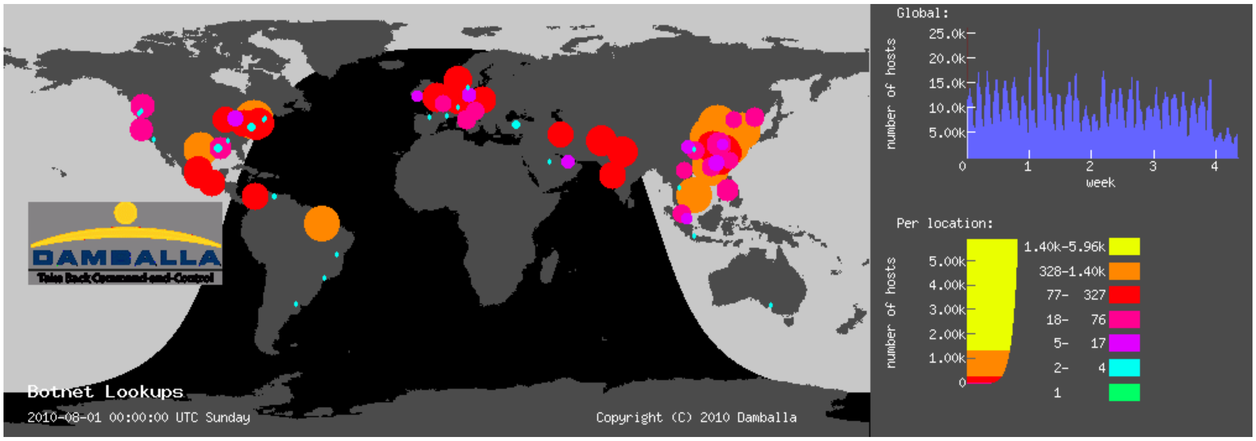


Figure 3: IMDDOS Botnet DNS Lookups for August

An animated account of the botnet activity and growth, as observed on an hourly basis since the first day the botnet became active, can be viewed at the following link:

www.damballa.com/IMDDOS

In order to provide a rough estimate of the infected population for this new botnet, its CnC activity is plotted against already known CnC domain names from other popular botnets - Mariposa, Bobax, and Virut. (Figure 4).

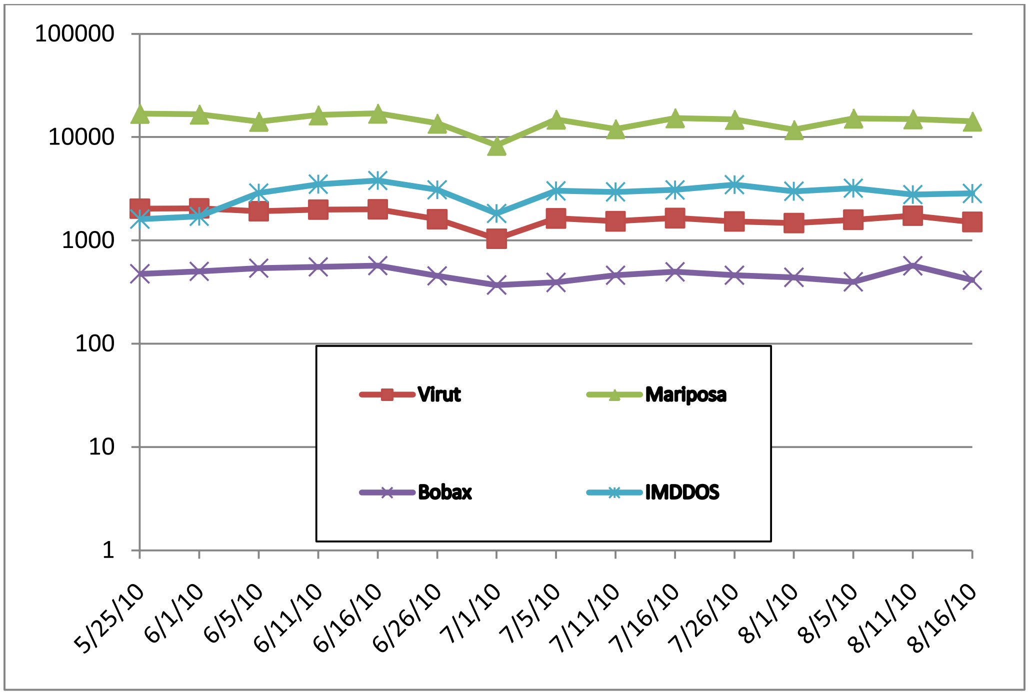


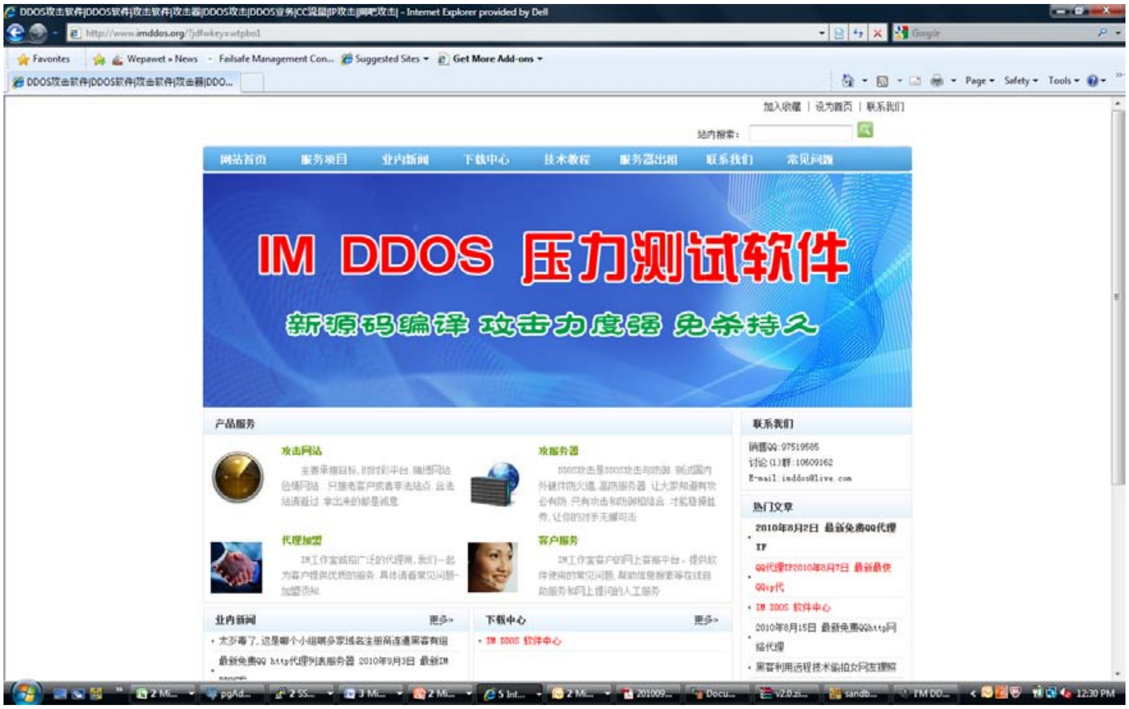
Figure 4: Volume of Unique Recursives Observed in a Daily Basis from known Domain Names for Major Botnets (Logorithmic Scale)

Figure 4 represents the number of unique hosts (recursives or simple stubs) that are looking up the most popular authority CnC domain name for the IMDDOS botnet compared with the most popular domain name from Mariposa, Bobax, and Virut.

Consistently, over this period of investigation, the primary domain name from the new botnet was looked up from the same number of recursives as the Virut Domain name (visible from the Damballa monitoring standpoint) and twice the size of the most popular Bobax domain name (visible from the Damballa monitoring standpoint). It is important to note that these numbers do not necessarily reflect the infection population for each botnet; rather, they should be used as a rough scale of comparing botnet size from DNS infrastructure perspective.

The IMDDOS Botnet Website

The investigation of the IMDDOS Botnet led Damballa researchers to a Chinese website advertising a commercally available version of the service. There is a comphensive introduction to the IMDDOS service, attack metholodgy and tools, contact info, and other details important to the potential user/customer. The website states that only non-legitimate websites, such as gambling sites, can be added to the list of attack targets.



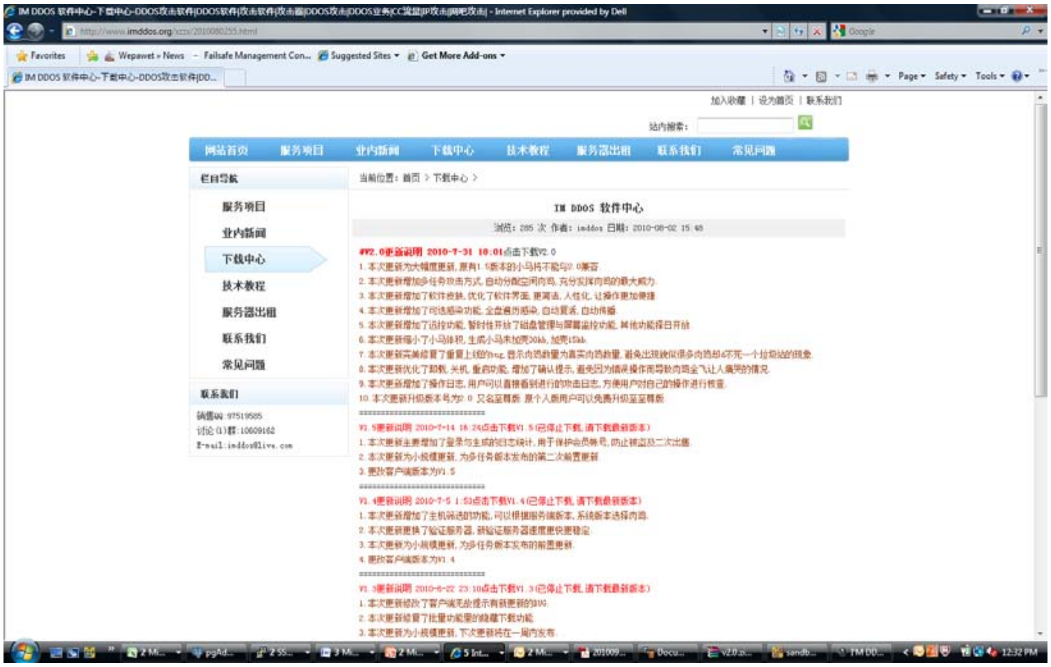
销售QQ:97519585
讨论(1)群:10609162
E-mail:imddos@live.com

- 2010年8月2日 最新免费QQ代理IP
- QQ代理IP2010年8月7日 最新最快QQip代
- IM DDOS 软件中心
- 2010年8月15日 最新免费QQhttp网络代理
- 黑客利用远程技术偷拍女网友裸照

- 太歹毒了，这是哪个小组嘛多家域名注册商连遭黑客袭击
- 最新免费QQ http代理列表服务器 2010年9月3日 最新IM

Figure 5: The main website advertising the IMDDOS Service

Figure 6 is a screen capture of the tool download page. It describes release logs for different revisions of the malware agents and supporting tool, as well as a list of the main features and functions. The latest revision is listed as V2.0, released on July 21, 2010. V2.0 has many new features including a smaller malware footprint for the infected host. Additional new features include support for new attack methods and the reassignment of spare bots. It states that the current version is not compatiable with V1.5.


IM DDOS 软件中心-下载中心-DDOS攻击软件|DDOS软件|攻击软件|攻击器|DDOS攻击|DDOS业务|CC流量|IP攻击|网吧攻击| - Internet Explorer provided by Dell
http://www.imddos.org/xzzx/2010080255.html
加入收藏 | 设为首页 | 联系我们
站内搜索:
网站首页
服务项目
业内新闻
下载中心
技术教程
服务器出租
联系我们
常见问题
栏目导航
服务项目
业内新闻
下载中心
技术教程
服务器出租
联系我们
常见问题
联系我们

销售QQ:97519585
讨论(1)群:10609162
E-mail:imddos@live.com

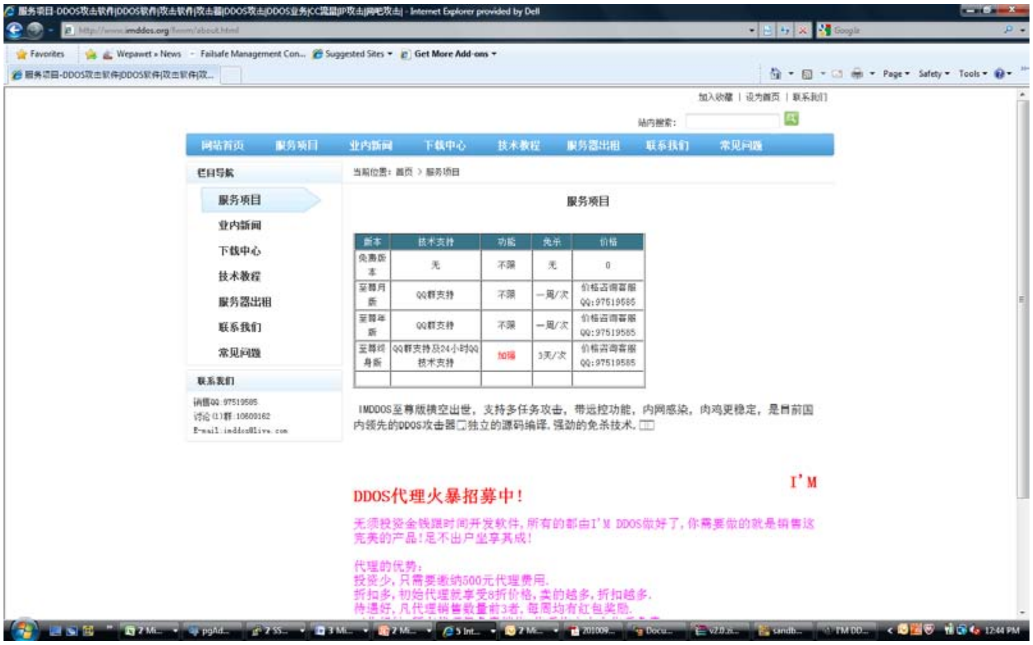
当前位置: 首页 > 下载中心 >

IM DDOS 软件中心

浏览: 285 次 作者: imddos 日期: 2010-08-02 15:48

#V2.0更新说明 2010-7-31 10:01点击下载V2.0
1. 本次更新为大幅度更新，原有1.5版本的小马将不能与2.0兼容
2. 本次更新增加多任务攻击方式，自动分配空闲肉鸡，充分发挥肉鸡的最大威力
3. 本次更新增加了软件皮肤，优化了软件界面，更简洁，人性化，让操作更加便捷
4. 本次更新增加了可选感染功能，全盘遍历感染，自动复活，自动传播
5. 本次更新增加了远控功能，暂时性开放了磁盘管理与屏幕监控功能，其他功能择日开放
6. 本次更新缩小了小马体积，生成小马未加壳30kb，加壳15kb
7. 本次更新完美修复了重复上线的bug，显示肉鸡数量为真实肉鸡数量，避免出现貌似很多肉鸡却打不死一个垃圾站的现象
8. 本次更新优化了卸载，关机，重启功能，增加了确认提示，避免因为错误操作而导致肉鸡全飞让人痛哭的情况
9. 本次更新增加了操作日志，用户可以直接看到进行的攻击日志，方便用户对自己的操作进行核查
10. 本次更新升级版本号为2.0 又名至尊版 原个人版用户可以免费升级至至尊版
==============================
V1.5更新说明 2010-7-14 16:24点击下载V1.5(已停止下载，请下载最新版本)
1. 本次更新主要增加了登录与生成的日志统计，用于保护会员帐号，防止被盗及二次出售
2. 本次更新为小规模更新，为多任务版本发布的第二次前置更新
3. 更改客户端版本为V1.5
==============================
V1.4更新说明 2010-7-5 1:53点击下载V1.4(已停止下载，请下载最新版本)
1. 本次更新增加了主机筛选的功能，可以根据服务端版本，系统版本选择肉鸡
2. 本次更新更换了验证服务器，新验证服务器速度更快更稳定
3. 本次更新为小规模更新，为多任务版本发布的前置更新
4. 更改客户端版本为V1.4
==============================
V1.3更新说明 2010-6-22 23:10点击下载V1.3(已停止下载，请下载最新版本)
1. 本次更新修改了客户端无故提示有新更新的BUG
2. 本次更新修复了批量功能里的批量下载功能
3. 本次更新为小规模更新，下次更新将在一周内发布

Figure 6: Tools Download Page


服务项目-DDOS攻击软件|DDOS软件|攻击软件|攻击器|DDOS攻击|DDOS业务|CC流量|IP攻击|网吧攻击| - Internet Explorer provided by Dell
http://www.imddos.org/fwxm/about.html
加入收藏 | 设为首页 | 联系我们
站内搜索:
网站首页
服务项目
业内新闻
下载中心
技术教程
服务器出租
联系我们
常见问题
栏目导航
服务项目
业内新闻
下载中心
技术教程
服务器出租
联系我们
常见问题
联系我们

销售QQ:97519585
讨论(1)群:10609162
E-mail:imddos@live.com

当前位置: 首页 > 服务项目

服务项目

版本	技术支持	功能	免杀	价格
免费版本	无	不限	无	0
至尊月版	QQ群支持	不限	一周/次	价格咨询客服 QQ:97519585
至尊年版	QQ群支持	不限	一周/次	价格咨询客服 QQ:97519585
至尊终身版	QQ群支持及24小时QQ技术支持	加强	3天/次	价格咨询客服 QQ:97519585

IMDDOS至尊版横空出世，支持多任务攻击，带远控功能，内网感染，肉鸡更稳定，是目前国内领先的DDOS攻击器□独立的源码编译，强劲的免杀技术。□□

I'M

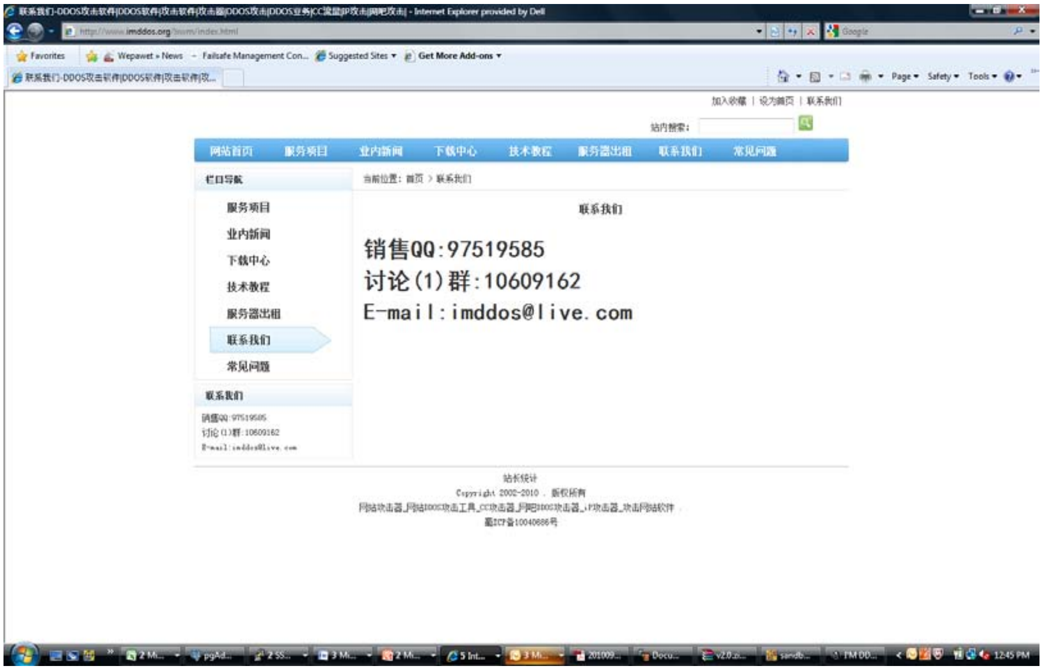
DDOS代理火暴招募中！

无须投资金钱跟时间开发软件，所有的都由I'M DDOS做好了，你需要做的就是销售这完美的产品！足不出户坐享其成！

代理的优势：
投资少，只需要缴纳500元代理费用。
折扣多，初始代理就享受8折价格，卖的越多，折扣越多。
待遇好，凡代理销售数量前3者，每周均有红包奖励。

Figure 7: The Service Model: From Free to Paid Service

IMDDOS offers different service agreements, ranging from free to paid services, as depicted in Figure 7. Besides the free service, the website does not publicly list any pricing information for the paid services. A prospective customer would need to contact customer service via the QQ service (a Chinese chat service) to a get a detailed price quote. There are three levels of paid services: monthly, annually, or lifetime. For the lifetime customers, there is 24x7 technical support. In addition, IMDDOS recruits resale agents to promote its business.



联系我们-DDOS攻击软件|DDOS软件|攻击软件|攻击器|DDOS攻击|DDOS业务|CC流量|IP攻击|网吧攻击| - Internet Explorer provided by Dell

http://www.imddos.org/

加入收藏 | 设为首页 | 联系我们

站内搜索：

网站首页 服务项目 业内新闻 下载中心 技术教程 服务器出租 联系我们 常见问题

栏目导航

服务项目
业内新闻
下载中心
技术教程
服务器出租
联系我们
常见问题

当前位置：首页 > 联系我们

联系我们

销售QQ:97519585
讨论(1)群:10609162
E-mail:imddos@live.com

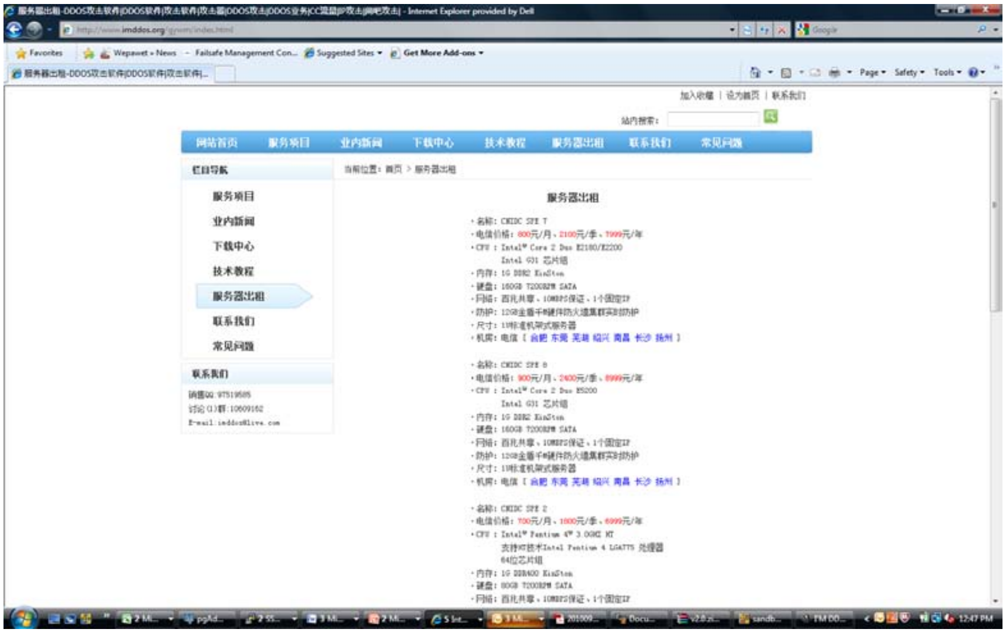
联系我们

销售QQ:97519585
讨论(1)群:10609162
E-mail:imddos@live.com

站长统计
Copyright 2002-2010 , 版权所有
网站攻击器_网站DDOS攻击工具_CC攻击器_网吧DDOS攻击器_IP攻击器_攻击网站软件
蜀ICP备10040686号

Figure 8: Contact information for support and service inquiries

Figure 8 shows IMDDOS contact info, including sales QQ number (Chinese chat service), discussion group, and email address.



服务器出租-DDOS攻击软件|DDOS软件|攻击软件|攻击器|DDOS攻击|DDOS业务|CC流量|IP攻击|网吧攻击| - Internet Explorer provided by Dell

http://www.imddos.org/

加入收藏 | 设为首页 | 联系我们

站内搜索：

网站首页 服务项目 业内新闻 下载中心 技术教程 服务器出租 联系我们 常见问题

栏目导航

服务项目
业内新闻
下载中心
技术教程
服务器出租
联系我们
常见问题

联系我们

销售QQ:97519585
讨论(1)群:10609162
E-mail:imddos@live.com

当前位置：首页 > 服务器出租

服务器出租

- 名称：CNIDC SPE 7
- 电信价格：800元/月、2100元/季、7999元/年
- CPU：Intel® Core 2 Duo E2180/E2200
  Intel G31 芯片组
- 内存：1G DDR2 KinSton
- 硬盘：160GB 7200RPM SATA
- 网络：百兆共享，10MBPS保证，1个固定IP
- 防护：12G金盾千M硬件防火墙集群实时防护
- 尺寸：1U标准机架式服务器
- 机房：电信【合肥 东莞 芜湖 绍兴 南昌 长沙 扬州】

- 名称：CNIDC SPE 8
- 电信价格：900元/月、2400元/季、8999元/年
- CPU：Intel® Core 2 Duo E5200
  Intel G31 芯片组
- 内存：1G DDR2 KinSton
- 硬盘：160GB 7200RPM SATA
- 网络：百兆共享，10MBPS保证，1个固定IP
- 防护：12G金盾千M硬件防火墙集群实时防护
- 尺寸：1U标准机架式服务器
- 机房：电信【合肥 东莞 芜湖 绍兴 南昌 长沙 扬州】

- 名称：CNIDC SPE 2
- 电信价格：700元/月、1800元/季、6999元/年
- CPU：Intel® Pentium 4® 3.0GHz HT
  支持HT技术Intel Pentium 4 LGA775 处理器
  64位芯片组
- 内存：1G DDR400 KinSton
- 硬盘：80GB 7200RPM SATA
- 网络：百兆共享，10MBPS保证，1个固定IP

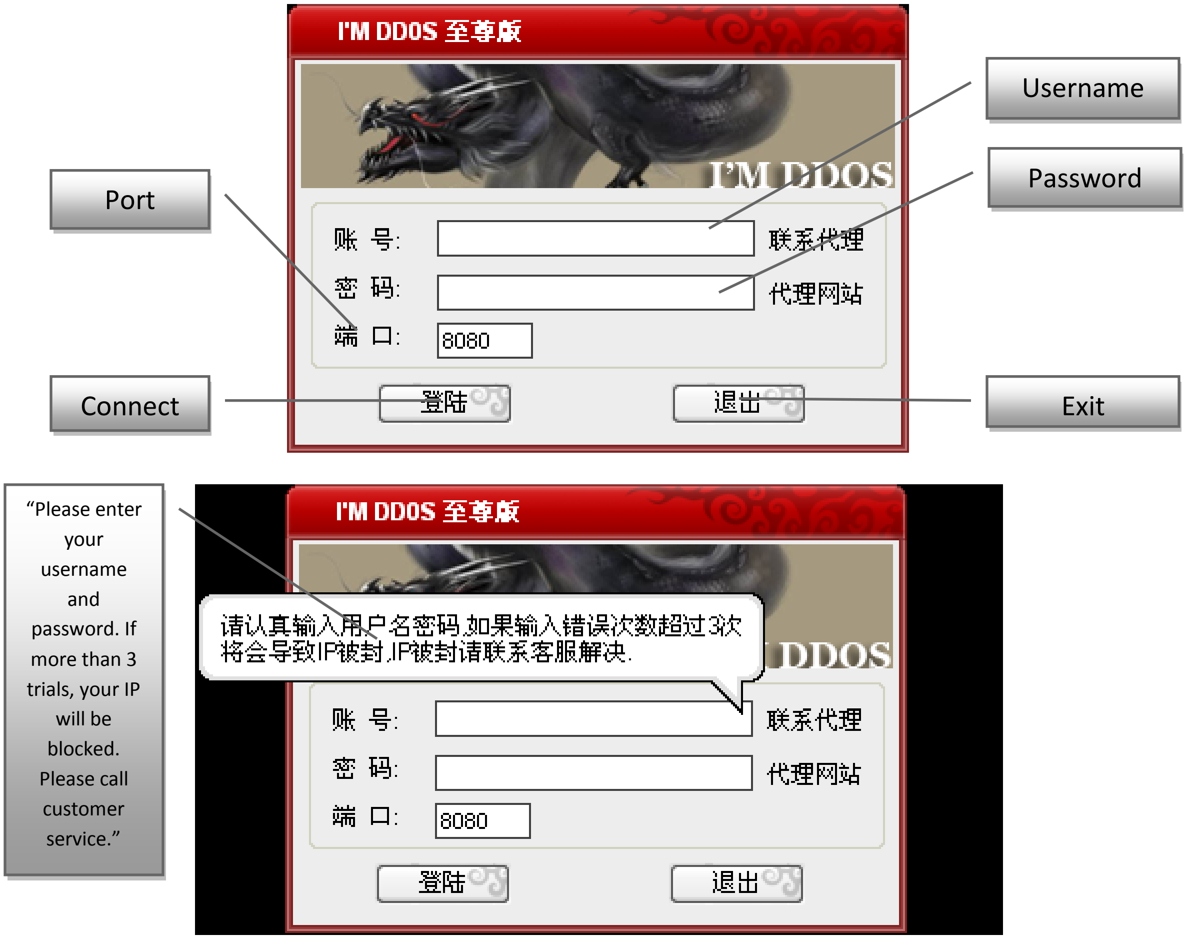
Figure 9: CnC Rental Information

IMDDOS also allows customers to rent servers from its server pool – severs are selected based on desired location, computing power, etc. Figure 9 lists the servers' specifications, price, and location.

The first version of their commercial tool that Damballa identified in the wild appeared in May of 2010. There may have been earlier tools that are still undiscovered (especially during the testing phase of the botnet).

Tool revision history:

- V2.0 – July 30, 2010
- V1.5 – July 14, 2010
- V1.4 – July 5, 2010
- V1.3 – June 22, 2010
- V1.2.2 – May 29, 2010
- V1.2 – May 20, 2010
- V1.1 – May 14, 2010



账 号:

密 码:

端 口: 8080

请认真输入用户名密码,如果输入错误次数超过3次将会导致IP被封,IP被封请联系客服解决.

"Please enter your username and password. If more than 3 trials, your IP will be blocked. Please call customer service."

Figure 10: Tool Screenshots

The tool enables the Bot Operator (the 'customer' who has rented a segment of the Botnet) to log-in to the online resource offered by the IMDDOS Service Provider.

The IMDDOS Botnet Infrastructure

The IMDDOS Botnet consists of three components:

1. IMDDOS Malware – This is the executable that infects a host PC enabling it to be part of the IMDDOS Botnet.
2. Target-List Hosting Domain (TLHD) - This is the domain that hosts the *PREDEFINED HTML* file that contains the list of domain DDoS targets. This is where the IMDDOS Malware gets the list of its DDoS target.
3. CnC Domain – This domain houses the *DDoS Control Panel* used to control the infected hosts.

The IMDDOS Malware

Our analysis of the IMDDOS Malware centers on the samples Damballa has gathered since March 2010. The samples behave in a similar fashion:

1. Infection Routine - The way it infects the system
2. Persistence - The way it sets itself up to survive boot-up
3. CnC Communication – uses IP to connect directly to the CnC Domain and TLHD

They also share similar characteristics:

1. No Rootkit Technology – The samples did not attempt to hide themselves in the file system, in memory and in the registry
2. Not Packed – The samples did not use any real-time packers
3. Plain Text Communication – The samples send information about the host PC they have infected in plain text

Judging from their host level activity, these samples appear to behave consistently across the group. The only visible differences they have relate to the User-Agent assigned of each sample (used as an ID for the malware), the PREDEFINED HTML in the TLHD containing the target domains, and the CnC they report to.

Behavior

The malware samples are typical "auto set-up" malware. This means that whenever the malware sample is executed anywhere, it can install itself on the victim host independent of any dropper or malicious installer. Once executed, the malware copies itself to the system32 folder in Windows. It renames itself into six random character filenames.

The malware then modifies the registry for it to boot during Startup by adding itself to the Service subkeys under:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

This registry path contains parameters for the device drivers, file system drivers, and Win32 service drivers.

It sets itself up as a Service with the name SafePrec<xxx>. An attempt to hide the image path is employed by converting the strings pointing to the malicious files into HEXADECIMAL. See below for an example:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SafePrecpfu – ImagePath - hex(2):43,3a,5c,57,49,4e,44,4f,57,53,5c,73,79,73,74,65,6d,33,32,5c,67,6f,65,6d,6b,61,2e,65,78,65,00,

The HEXADECIMAL when converted to ASCII yields:

C:\WINDOWS\system32\goemka.exe.

Once the malware is active as a Service under the Winlogon Process, it proceeds to do the following (Figure 11):

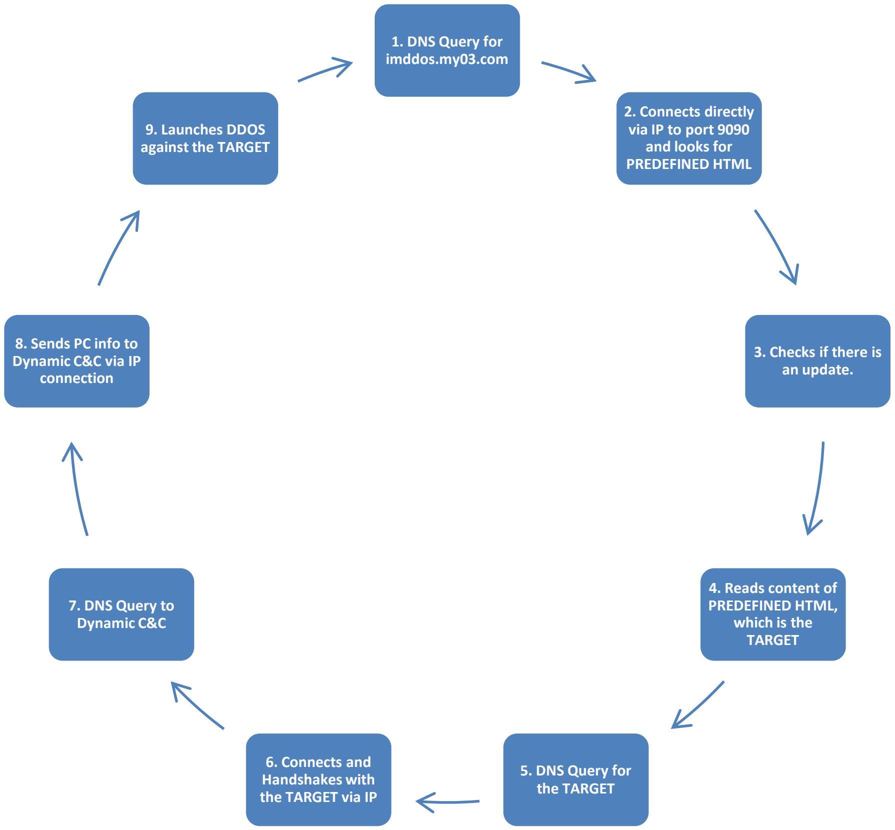

1. DNS Query for imddos.my03.com
2. Connects directly via IP to port 9090 and looks for PREDEFINED HTML
3. Checks if there is an update.
4. Reads content of PREDEFINED HTML, which is the TARGET
5. DNS Query for the TARGET
6. Connects and Handshakes with the TARGET via IP
7. DNS Query to Dynamic C&C
8. Sends PC info to Dynamic C&C via IP connection
9. Launches DDOS against the TARGET

Figure 11: The process flow of the IMDDOS Malware

The first thing it does is it attempts to connect to the TLHD, *imddos.my03.com,* where it will get the Predefined HTML containing the DDoS target (steps 1 and 2). It then checks whether there is a change in the target list (step 3). If there is no update, it then proceeds to steps 5 and 6 using its current target list in the cache. If there is an update, the malware updates its cache (step 4) and proceeds to the next step and attempts to connect to the new target (step 5 and 6). In steps 5 and 6, the malware just checks whether the target is still live, and it can connect to it.

The malware then connects to the CnC server (step 7). If the connection is successful, it sends information about the infected host to the CnC server (step 8). The infected host information is sent in plain text. The information sent includes:

- OS of the infected PC
- CPU speed
- Memory size

These parameters are then used to determine which assets will be used in any given attack based on the computing power required, etc.

The last step in its flow is the actual DDoS attack which is triggered remotely by its CnC.

Basically, it's behavioral flow is a repetitive loop. If one step is unsuccessful, it proceeds to the next. The advantage of this mechanism is that the malware does not die in the host system when a certain online resource is down. It justs attempts to connect to the online resource again and again until it is up again and then the malware will continue to function. This is also its way of checking for an updated target. The disadvantage of this is that the malware tends to be noisy both in the host level and network level. Also, it ceases to function as a DDoS agent if its online resource is down given the fact that it has no target and no CnC to trigger it. It simply becomes an executable looping endlessly checking for an online resource and nothing more.

Each cluster of malware samples has their own user-agent when it connects to its online resource as a way to identify itself to the host and CnC servers. This is one way of identifying or clustering the malware samples outside of its host-based behaviors. The most popular user-agents identified during our analysis include:

- STORMDDOS
- YTDDOS
- IAMDDOS
- i am ddos
- kav

Symptoms

The following will help in determining whether a system has been compromised. These symptoms are based on and cover only the sample sets that Damballa has available.

The presence of the following registry key:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SafePrec<xxx> – ImagePath - hex(2):43,3a,5c,57,49,4e,44,4f,57,53,5c,73,79,73,74,65,6d,33,32,5c,<xx, xx, xx, xx, xx, xx, xx, xx, xx, xx, xx>

The <xxx> varies. In the image path, the last ten hex bytes varies depending on the random file name of dropped file. It ranges from six bytes (files with no extension) to ten bytes (files with extensions). The first hex bytes when converted to ASCII represents C:\WINDOWS\system32\.

Once the HEXADECIMAL bytes have been converted to reveal the name of the dropped file, it can be found in the System32 folder of Windows.

To demonstrate the randomness of the file names, below are some examples. File names found in an infected system will differ from these. The names will depend on what can be found in the registry.

- hgprcq.exe
- iyouuq.exe
- iigmiy.exe
- uumuui.exe
- osyusk
- aqmkqm
- goemka.exe
- ccywco.exe
- kaywai.exe
- auwyqo.exe
- iykuuq.exe
- bsbnoo.exe
- cgcagc.exe
- mmuema.exe
- uuwoue.exe
- yyaoye.exe
- gkgyki.exe
- mqeymw.exe

The same file names can also be found running in memory under the Winlogon process. This is another way of telling which random file name the malware used by looking for suspicious, six random character filenames running as a service under Winlogon.

The Target List Hosting Domain (TLHD)

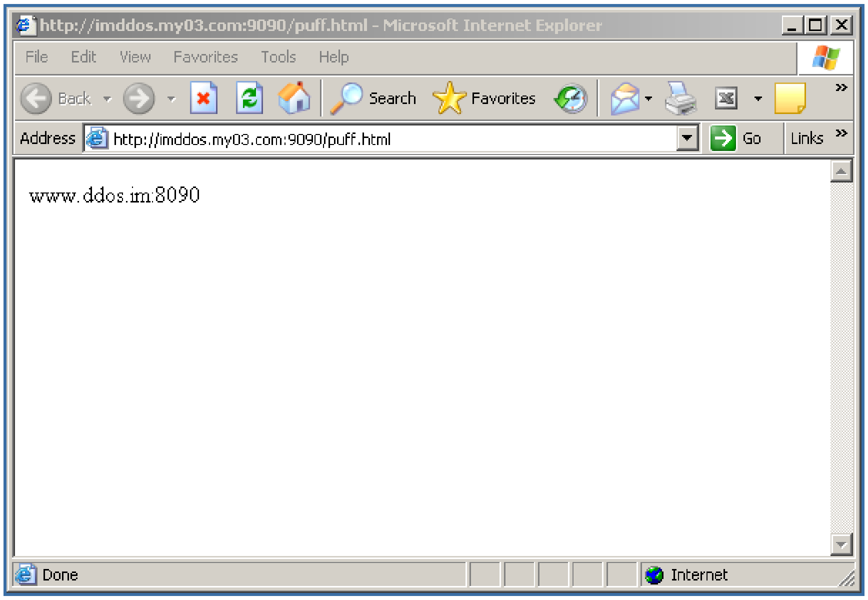
The TLHD is the domain that hosts the PREDEFINED HTML (PH) file that contains the list of targeted domains to be DD0S'd. Each malware sample contains the name of the PH. Once active, the malware goes to the TLHD, connects to TCP port 9090, and opens the PH to reveal the list of targets. The list of targets is not encrypted.

The TLHD's used by this botnet are:

- *http://imddos.my03.com:9090/ (main)*
- *http://test.dns-dns.com:9090/ (testing)*

Some of the PREDEFINED HTML captured during analysis are:

- test1.html
- 888.html
- bawang.html
- puff.html
- gesheng.html
- 090210.html
- 2764485.html
- chinawf518.html
- xiaonan888.html


http://imddos.my03.com:9090/puff.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://imddos.my03.com:9090/puff.html Go Links
Done
Internet

www.ddos.im:8090

Figure 12: Target List Hosting Domain with a Predefined HTML file named puff.html (domain shown is the domain used for testing the botnet)

CnC Domains

The CnC domain is where the control panel is hosted that enables the Bot Operator to enumerate the number of infected hosts and to send commands to them.

All but one of the CnC Domains are hosted by 3322.org, which is a popular dynamic DNS provider based in China. The only exception is *dns.ddos.im,* which appears to be used for testing purposes during the development of the IMDDOS Botnet.

The CnC Domains identified during analysis of the malware samples include the following:

- dns.ddos.im
- win2003ddos.3322.org
- woshindi.3322.org
- pk518.3322.org
- huanjue6369029.3322.org
- qq603535.3322.org
- qq188588.3322.org
- hjff.3322.org
- 198600.3322.org
- ankankan.3322.org
- yinn.3322.org

Botnet Component Relationships

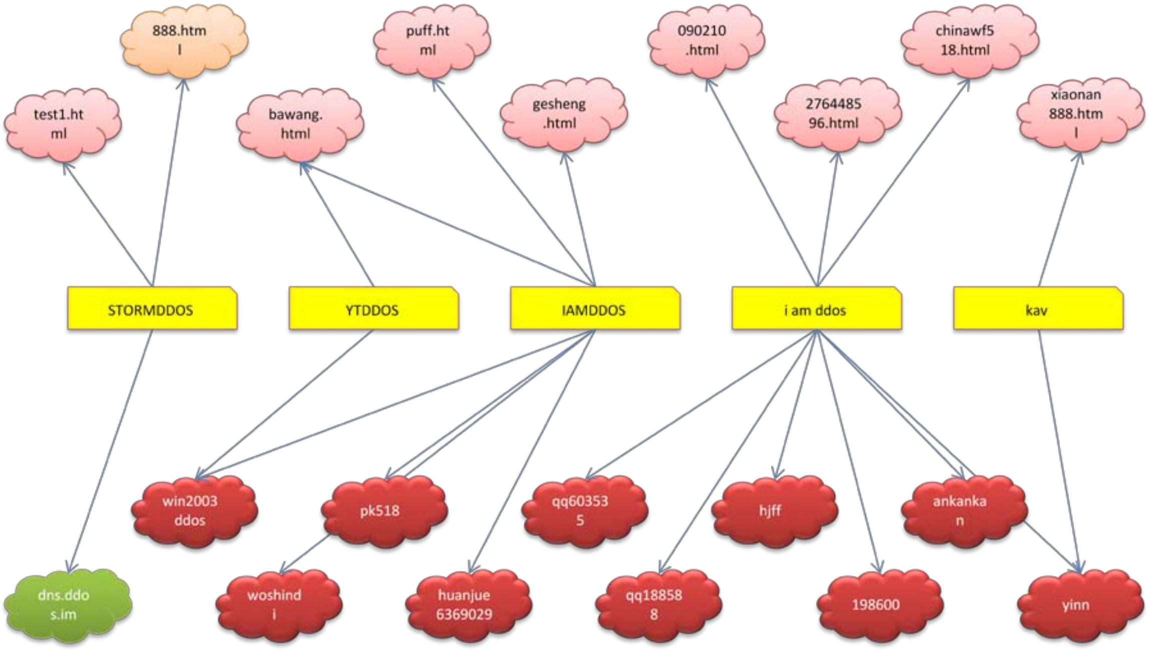


Figure 13: An example of the IMDDOS Botnet Ecosystem

Clustering the malware samples based on User-Agent and plotting them against the TLHD/PREDEFINED HTML they connect to to get their target list, and against the CnC Domain they connect to, reveals an example of the IMDDOS Botnet ecosystem.

From this example, it can be concluded that:

1. All the targets are located in one TLHD, indicating that the botnet is controlled only by one entity (bot master).
2. Since the CnC Domains are unrelated, each CnC can have it's own operator. This is typical of a "rental" infrastructure.

Given these conclusions, the IMDDOS Botnet is designed with business in mind: one entity controls the TLHD and the Predefined HTML containing target sites, while the bot master rents out a small subset of it to anyone who wishes to pay for such service - as shown, by the decoupling of the appropriate CnC domains.

This infrastructure, also gives the Bot Master some advantages over non-paying or rogue Bot Operators:

1. The Bot Master can render a certain segment of its Botnet useless by removing the Predefined HTML from the TLHD
2. The Bot Master can DDoS the actual CnC Domain of the non-paying Bot Operator by simply updating the domain target in the Predefined HTML

Potential Impact

- The actual domain names targeted by IMDDOS 'customers' for DDoS attacks are variable and are defined by the customers of the service.
- The malware activity is very 'noisy', resulting in significant malicious network traffic.
- Each malware infection, when active, initiates a constant, 'pinging' sequence to the hosting domain, CnC domains and target domains, resulting in three network requests every two seconds (approximately).
- Significant infections within enterprise and ISPs, can result in a significant drain on network resources, and for ISPs, a costly use of resources and bandwidth.
- Organizations with infected computers that launch external attacks may be identified as facilitators of the attack – having failed to adequately secure their own networks.
- Infected customers will need to wait for their AV providers to create detection signatures and removal tools to eradicate the main malware components – presuming that the IMDDOS providers do not update the installed malware components in the interim.
- In addition to the obvious intent to launch DDOS attacks, it is not clear at this time what other malicious actions the malware may have been instructed to perform.

How it Was Discovered

Damballa is the leading authority in botnets and botnet construction and their criminal operation. Damballa has a globe-spanning array of sensors, including deployments with Internet Service Providers that monitor CnC activity and malicious DNS traffic.

Damballa tracks thousands of botnet operators and their growing cache of botnets every day. Each criminal botnet building campaign is observed, analyzed, catalogued and categorized automatically using a sophisticated array of clustering and machine learning systems. As the criminal botnet operators attempt to grow the botnet, their investments and modifications to their CnC hosting infrastructure are tracked and used as markers for eventual attribution.

This discovery was made possible due to this array of Damballa DNS sensors, which provide worldwide visibility into CnC activity, combined with the understanding and quantification of statistical heuristics that could explain --- and most importantly detect early --- the malicious nature of this botnet operation.

Action Taken

As of this writing:

- Damballa Failsafe customers have been preemptively alerted to the IMDDOS Botnet. The Knowledge Base that Damballa Failsafe customers use to detect CnC activity has been updated every time a new domain has been used by the IMDDOS service provider. If the malware associated with this botnet has infected assets within their enterprise, they are being alerted to its presence and we have identified the exact assets that have been compromised.
- The proper authorities and unwitting hosts of the botnet CnC domains have been notified and all appropriate information has been shared to contain, and ultimately dismantle the botnet.

- All malware samples and domains have been shared with the security community through appropriate alerting channels.

Summary

The IMDDOS Botnet quickly became one of the rising stars among global botnets. This discovery was possible due to an array of globe-spanning Damballa network sensors and their our advances in massive-scale automated DNS analysis technologies.

This new botnet was not constructed by a casual group of hackers but rather a formally organized business that offers a fee-based commercial service. It is easily accessible and widely available to anyone who has money and motive.

As to the malware, this botnet demonstrates that unsophisticated malware can quickly spread and infect victim machines. The malware employed by the IMDDOS Botnet is simple and straightforward - yet “good enough” to thwart the default defenses of tens-of-thousands of victims.

The IMDDOS Botnet infrastructure, in terms of technology and construction, is not particularly innovative. It used well established techniques both in the implementation of its bot agents and its resource domains. But it was more successful than average in propagating quickly and offering a successful service – proving once again that well constructed social engineering campaigns can escalate infection rates dramatically.

Damballa has exhausted every effort to discover all relevant components of the botnet before issuing a public disclosure.

Dismantling botnets is a tricky business. It’s difficult, if not impossible, to have complete knowledge of all possible CnC domains in use, the infection vectors used and the intent of the malware, without illegally infiltrating the criminal organization. To completely takedown the IMDDOS Botnet, the following would need to happen:

1. Take down the TLHD – Without this, the bot agents will not get any fresh domain targets. But the Bot Operator can still issue DDoS directives to the bot clients targeting the current domain target(s) it has in its cache.
2. Take down the CnC domains – This will cut communication between the Bot Operator and the bot clients. This will effectively render the bot clients useless. They would not have a target and they would not have a directive.
3. Remove the bot agents – If undetected by AV solutions, the ***Symptoms*** section will prove useful in detecting the bot agents in the infected system.

Steps 1 and 2 require cooperation from the registrars. In cases where the registrars are uncooperative, especially those found in countries that do not have specific laws covering this category of abuse, tearing down the domains can become more difficult.

Contributors:

Manos Antonakakis, Damballa

Christopher Elisan, Damballa

Aldrich de Mata, Damballa

Erik Wu, Damballa

About Damballa, Inc.

Damballa stops crimeware threats that exploit enterprise networks for illegal activity by finding and terminating the hidden communication channels used to control breached computer systems. Damballa solutions protect companies from the devastating effects of botnets, advanced persistent threats, next generation malware, cyber crime, and insider threats. Damballa customers include major banks, manufacturers, ecommerce providers, Internet service providers, government agencies, educational organizations, and other companies typically targeted by organized cyber crime. Privately held, Damballa is headquartered in Atlanta. http://www.damballa.com.