Arbor Special Report

DDoS Attack Tools and Best-Practices for Defense

ARBOR NETWORKS

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for enterprise and service provider networks. Arbor's proven solutions help grow and protect our customers' networks, businesses and brands. Arbor's unparalleled, privileged relationships with worldwide service providers and global network operators provide unequalled insight into and perspective on Internet security and traffic trends via ATLAS®—a unique collaborative effort with 100+ network operators across the globe sharing real-time security, traffic and routing information that informs numerous business decisions. For technical insight into the latest security threats and Internet traffic trends, please visit our Web site at www.arbornetworks.com and our blog at asert.arbornetworks.com.

Table of Contents

Overview

In many respects, the Internet underground economy functions in ways that are similar to legitimate sectors of the IT industry. In both, we see continuous research and development that create a self sustaining cycle of growth and innovation. In particular, there has been an explosion of DDoS attack tools and services that enable anyone with an Internet connection and a grievance to launch crippling attacks.

The emergence of ubiquitous DDoS attack tools and services is evidence of a thriving underground economy that is finding new applications and markets for denial of service. These include basic one-on one attack tools that internet gamers use to take rivals offline to more complex, opt-in tools that hactivists use to take down websites. Commercial DDoS services and blended attack tools are also used as part of well planned attacks in order to cloak the theft of high value information.

Arbor's Security Engineering & Response Team (ASERT) have investigated and catalogued a large number of these tools and services. The work of finding, tracking and analyzing attack tools is critical to developing effective defenses, which is a primary mission of the ASERT team.

This article provides an overview of a number of these tools in order to raise awareness of the diversity of attack options and to provide a window into the underground DDoS economy itself. The range of attack motivations, targets, techniques and commercial attack services are evidence of the size and scope of the problem. Other Arbor research such as the *Worldwide Infrastructure Security Report* provides direct information on the impact of this underground economy as carriers and enterprises report on the size, frequency and types of attacks they are experiencing on their networks.

The risk of DDoS attack has increased in tandem with the proliferation of DDoS attack tools and services. Personnel responsible for IT security need to understand the extent, scope and fast evolving nature of the problem in order to make informed decisions. IT decision makers need to understand what is at risk and the steps that are needed to mitigate those risks. This paper concludes by describing best practices for addressing the problem, consisting of a layered defense approach that combines in-cloud and purpose-built, on-premise protection.

Visual Examples of DDoS Attack Tools and Services

A variety of popular DDoS attack tools have received a fair amount of attention by the security research community, but other lower-profile attack tools have been developed in the last few years. This report provides a review of both well-known and lesser-known attack tools in use today. These include single user flooding tools, small host booters, shell booters, Remote Access Trojans (RATs) with flooding capabilities, simple DDoS bots, complex DDoS bots and some commercial DDoS services. Many types of threats can be blended into any given tool to make it more attractive and financially lucrative.

Professionally coded bots with a variety of stealthy attributes and corresponding commercial flooding services pose a severe DDoS threat to enterprises and network providers. Small projects coded by amateurs pose less of a threat. However, many of the small-time "host booters" profiled here—typically designed to flood a single gaming user's IP address and knock that user out of the game—often have Remote Access Trojan (RAT) functionality. This functionality enables these simple flooding tools to steal passwords, download and execute other malware, sniff keystrokes and perform other malicious activities. Such simple tools do more than threaten confidentiality. Arbor's ASERT team has seen them take down enterprise-class firewalls from either side of the firewall due to state-table exhaustion.

At the other end of the spectrum, commercial DDoS services are running at full speed, with a variety of service offerings readily available. While there are numerous motives for DDoS such as revenge, extortion and protest, many commercial DDoS services emphasize their value as a competitive weapon to take rival businesses offline. More troubling is the recently reported distracting use of DDoS to flood networks after a financial theft via a banking Trojan-giving the thieves extended access to the loot. Within this diverse landscape, Arbor is aware of many ongoing attacks from large, widely distributed DDoS botnets.

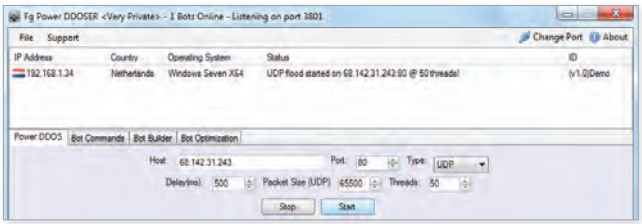
This section of the report includes descriptions and control-panel screenshots of over 40 DDoS threats. It begins with the simpler threats, moves to the intermediate threats, and then covers the more complex and advanced bots and botnets. It concludes with examples of various commercial DDoS service offerings.

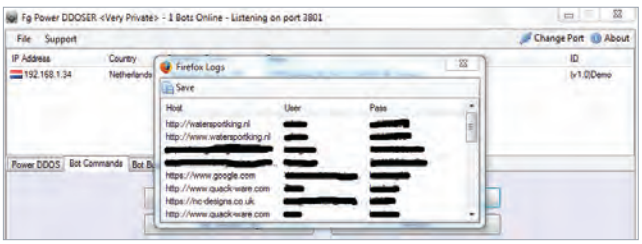
Simple DDoS Threats

Many of the attack tools listed in this section are "host booter" tools used by internet gamers to take rival gamers offline. However, many of these tools can also be used to steal passwords and have been known to cause firewalls to crash. These types of tools are also used by "hacktivists" in carrying out opt-in attacks that have become so common.

Fg Power DDOSER

This tool is primarily a "host booter" aimed at giving unscrupulous gamers an advantage by flooding opponents with traffic. HTTP flooding capabilities may be effective at bringing down unprotected Web sites as well. A Firefox password stealer is also included, which can be very deadly as people reuse passwords all the time.



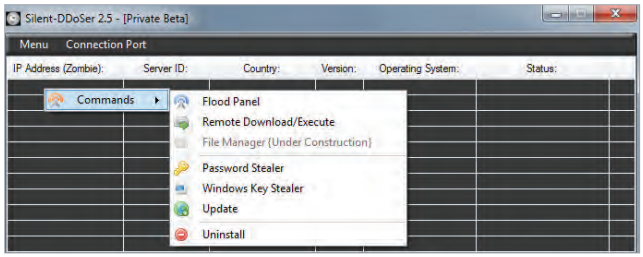


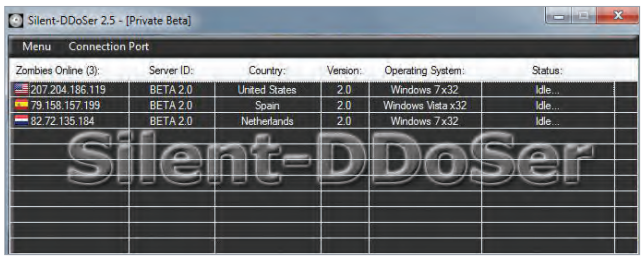
GB DDoSeR v3

This tool is advertised as a booter and delivers a TCP or UDP stream of characters of the attacker's choice towards a victim IP/host and port. This simple bot is written in Visual Basic.

Silent-DDoSer

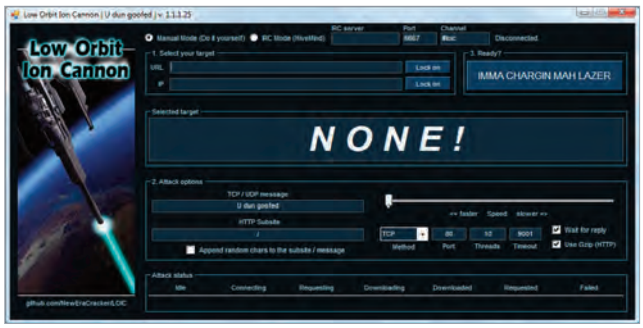
This Visual Basic tool offers attack types "UDP," "SYN" and "HTTP." All appear to send a basic user-specified flood string. Silent-DDoSer utilizes triple-DES and RC4 encryption, IPv6 capabilities and password-stealing functions.





Low Orbit Ion Cannon (LOIC)

One of the original opt-in tools used by the "hacktivist" community. Unlike many of the tools in this section these opt-in tools are used to perpetrate coordinated attacks. LOIC has numerous variants and successors.



Drop-Dead DDoS

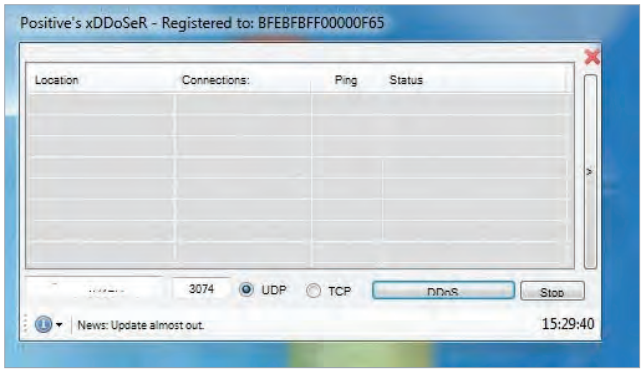
This tool is one example of a Runescaper booter. The opportunity to make real-world money through the virtual economies of gaming worlds may have helped make such tools popular.

D.NET DDoSeR

This tool is again aimed at the Runescape audience, but also features SYN and HTTP flooding. The floods in this case are just poorly formed garbage characters randomly generated. This particular screenshot only has one connected bot.

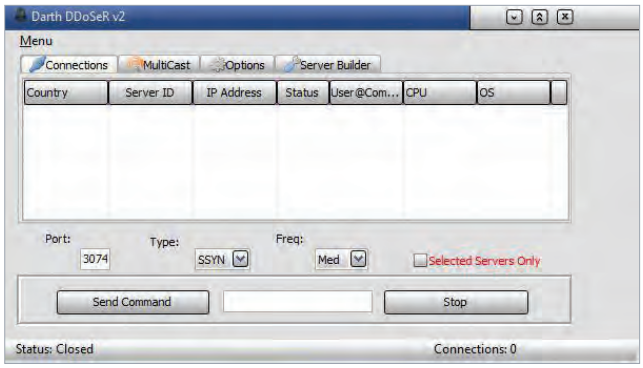
Positive's xDDoSeR

Like anything flooding port 3074, this is an Xbox booter application, designed to boot users off to generate an unfair advantage. This particular screenshot shows no connected bots.



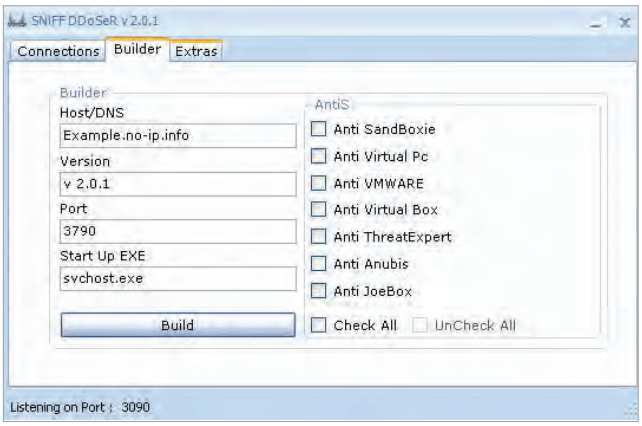
Darth DDoSeR v2

Here is another tool aimed at Xbox booting, at least in this screenshot. The flood in this case looks like a "SSYN" type, which is slightly different than many other host booters that appear to use UDP by default.



Positive's xDDoSeR

Like anything flooding port 3074, this is an Xbox booter application, designed to boot users off to generate an unfair advantage. This particular screenshot shows no connected bots.

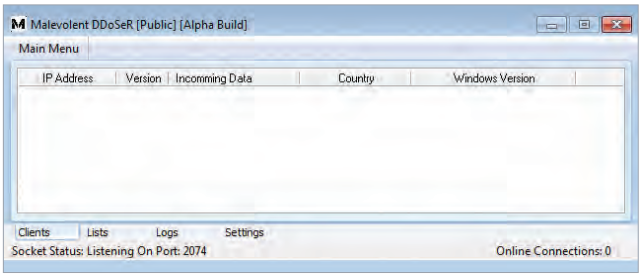


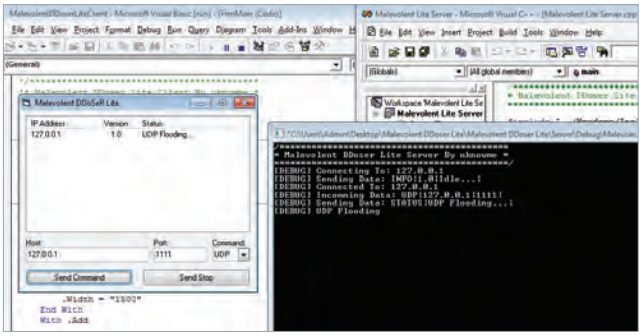
Net-Weave

Net-Weave is one of the many bots that appeared in the extensive ASERT malware collection in mid-2011. It is a booter/bot and backdoor written in .NET. It features the typical array of malware functionality including download and execute, USB spreading capabilities, TCP connection exhaustion flood, UDP flood and a basic port 80 flood instantiated with a .NET socket call.

Malevolent DDoSeR

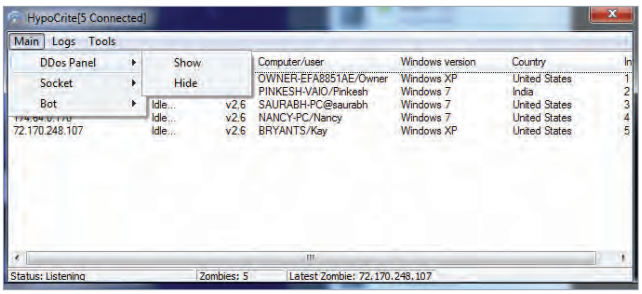
The source code for a version of this leaked some time back. The server is written in C++, and the client is written in Visual Basic. It appears to offer only download and execute and UDP flooding attacks. Shown below are a server screenshot and a developer's viewpoint screenshot, obtained from various forums.





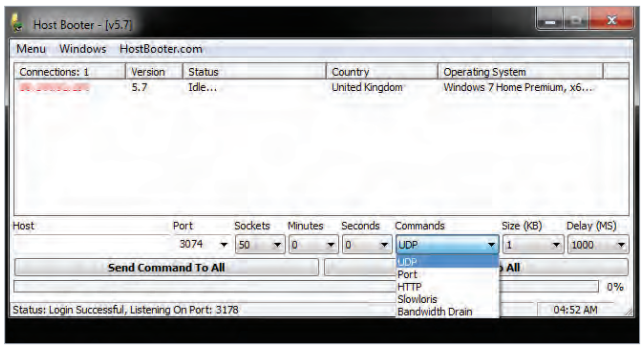
HypoCrite

HypoCrite is a Visual Basic host booter apparently on version 4. It offers the ability to steal MSN passwords, in addition to basic flooding capabilities.



Host Booter v5.7

This booter features several flooding attacks including the popular Slowloris attack style.



The features are listed as:

- UDP (UDP flood)
- Port (floods a port with attack traffic)
- HTTP (for Web sites)
- Slowloris (for Web sites)
- Bandwidth Drain (put a direct link for a .exe or any other file)
- Send Command to All/Send Stop to All (execute or end your command)
- Ports: 25/80/445/3074/27015 (ports you can choose from; you can use your own)
- Sockets: [1-250] (how many sockets you will use)
- Seconds: [1-60] (how many seconds you wish your attack to be enabled for)
- Minutes: [1-59] (how many minutes you wish your attack to be enabled for)
- Size (KB) Packet Size for UDP
- Delay (MS) Time (between sending a packet)
- Connect (MS) (reconnect sockets)
- Timeout (MS) (connection timeout)

AlbaDDoS

It appears that the author of this DDoS tool is also involved in defacing Web sites.

Good Bye v3.0

The Good-Bye tools appear to be simple HTTP flooding tools that have no DDoS or botnet capability.

Manta d0s v1.0

The author of this tool, Puridee, has also written multiple other tools including the “Good-Bye” DoS tool.

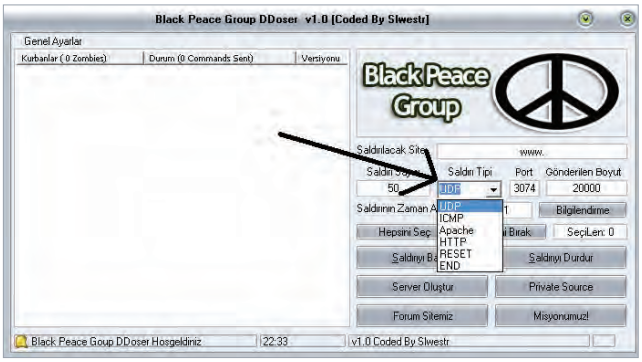
Good Bye v5.0

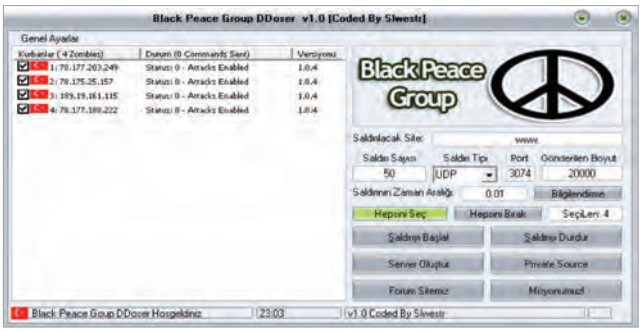
Intermediate DDoS Threats

Unlike the one-on-one attack tools in the previous section, most of the tools listed in this section make use of compromised web applications to launch attacks from multiple sources (DDoS).

Black Peace Group DDoser

This tool is of Turkish origin and features several attack types as seen in the first picture. The second picture shows four zombies enlisted and awaiting commands.



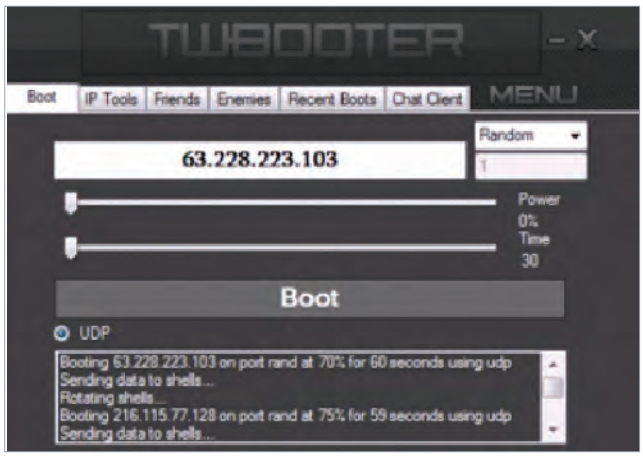


PHPDoS

PHPDoS is a "shell booter" that utilizes hijacked Web applications to perform flooding attacks. While shell booters have been well-documented in the past, they typically leverage a number of compromised Web applications where an attacker has installed a PHP webshell. Sometimes, these webshells may exist on high-bandwidth networks, which can amplify the force of the attack significantly. Private webshells are worth more, and lists of webshells can be purchased. Some generic webshells are x32, greenshell, PsYChOTiiC, shell, mouss, Supershell, venom, atomic, and many others. There are other shells specifically created for DDoS, such as ddos.php. Of course, a webshell can be named anything, but these names are common.

TWBOOTER

TWBOOTER is another "shell booter." This screenshot shows 235 shells online and a UDP flood taking place on random target ports. An update from about a year ago says, "Releasing twBooter Web Version today! Might have slowloris and http tonight, but I'll be releasing without." Incidentally, someone using the nickname "twbooter" was seen selling flooding services via chat.

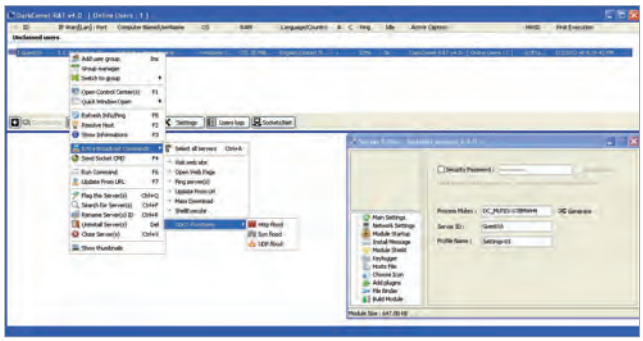


Gray Pigeon RAT

This is a screenshot from the Gray Pigeon Remote Access Trojan (RAT). In this screenshot, the attacker appears to have three bots online, but has filtered the list to show only bots from Beijing, China. Gray Pigeon is well-known for its RAT capabilities, but it also has DDoS features as well. Many DDoS bots use Chinese language sets and operate from within the Chinese IP address space. Some of these have been profiled by ASERT's Jeff Edwards in the past. A great deal of code-sharing takes place among the Chinese DDoS bot families that ASERT has analyzed. While Gray Pigeon can be used for DDoS, its main danger lies in its RAT functionality. Trojans such as Gray Pigeon have been used for serious data theft and espionage style attacks.

DarkComet RAT, aka 'Fynloski'

DarkComet is freeware and easily available to anyone. While it features a variety of flooding types, these are an afterthought compared to its main Remote Access Trojan functions, which are significant. The binaries for this threat are often called Fynloski.

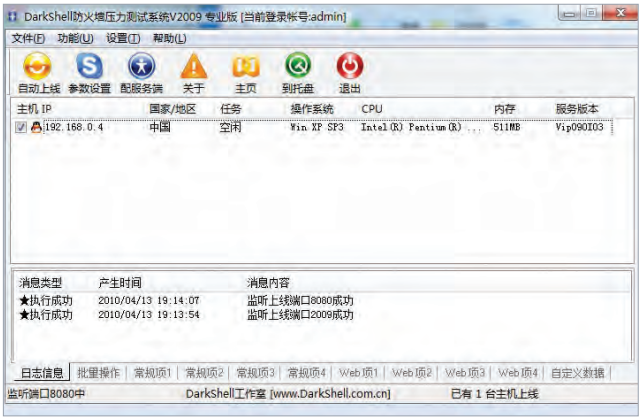


MP-DDoser v1.3

MP-DDoser is a relatively new threat, coming to ASERT's attention in December, 2011. It supports UDP, TCP connection flood and HTTP attacks. Marketing materials and the GUI for this bot claim that it supports a slowloris style attack. Despite these claims, ASERT analysis indicates that the slowloris attack does not function.

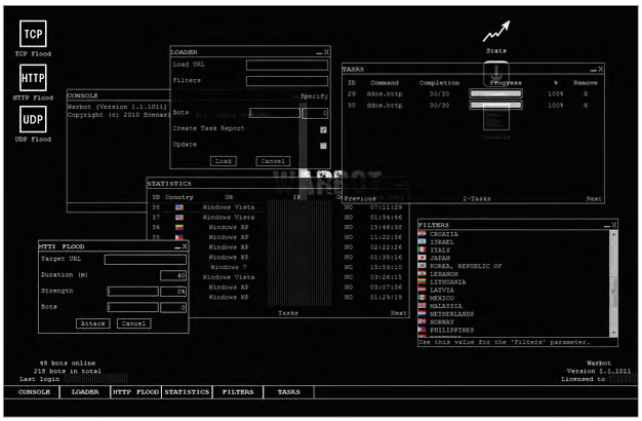
DarkShell

Darkshell is popular among the Chinese DDoS bot families and features a variety of attack types. Included are three distinct HTTP attacks, two types of TCP flooding attacks, two UDP floods, an ICMP flood, a SYN flood, TCP connection exhaustion and TCP idle attack types. For extensive details on the Darkshell bot, please see the excellent analysis by ASERT's Jeff Edwards at ddos.arbornetworks.com/2011/01/darkshell-a-ddos-bot-targetting-vendors-of-industrial-food-processing-equipment/.



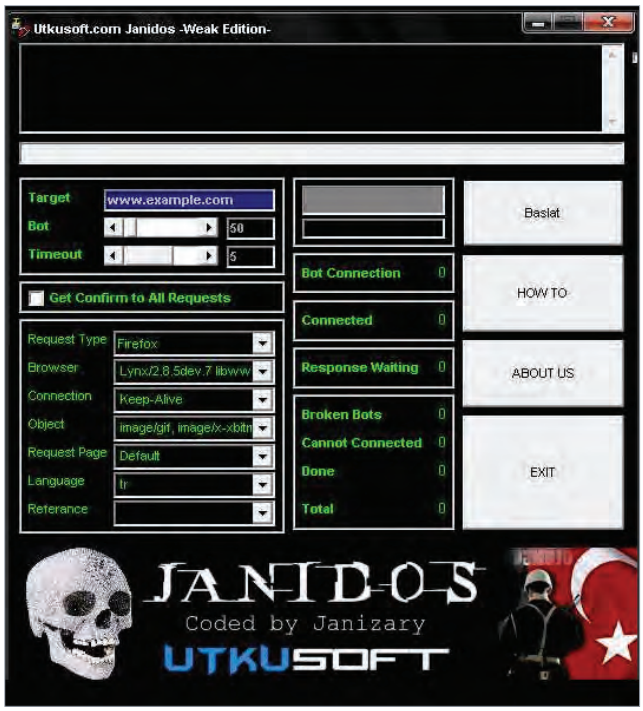
Warbot

This is the warbot Web-based control panel. Commands are ddos.http (seen here), ddos.tcp and ddos.udp.



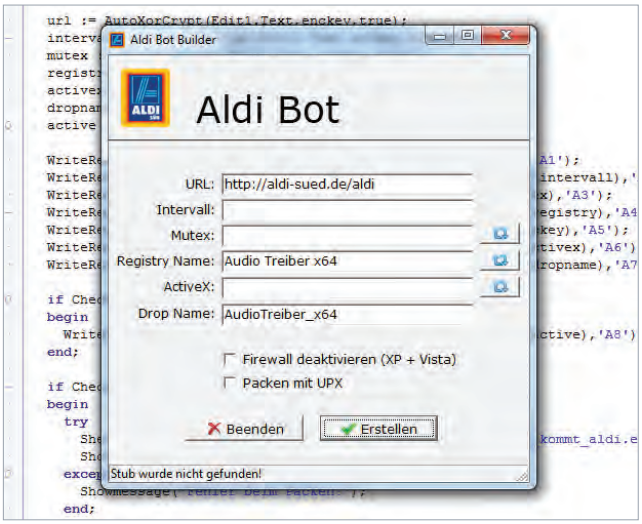
Janidos

Without a license key, Janidos runs as a "weak edition." This version offers the opportunity to toggle through a variety of User-Agent values during an HTTP DDoS attack. Like the BlackPeace DDoSer, Janidos appears to be of Turkish origin.



Aldi Bot

This is an inexpensive bot that showed up in late 2011. It was interesting to see InfinityBot downloaded and executed from one Aldi Bot node that ASERT was analyzing. Some forums suggest that Aldi Bot is not very good quality. For more information about Aldi Bot, please see an analysis and write-up at ddos.arbornetworks.com/2011/10/ddos-aldi-bot/.

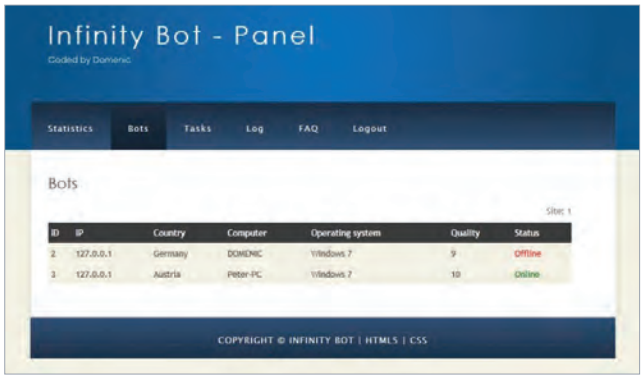


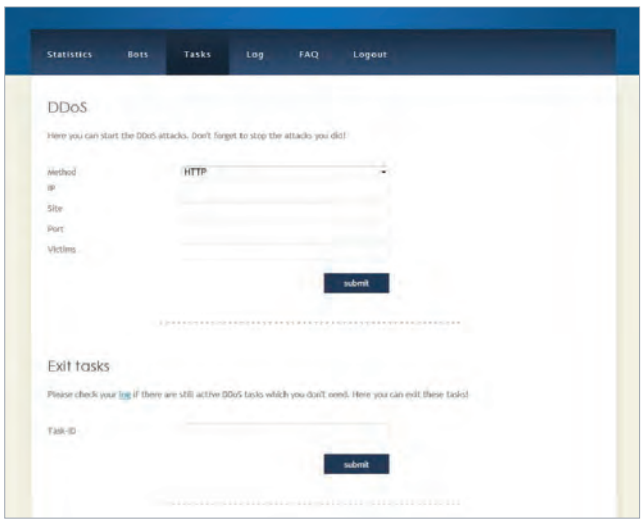
Advanced Bots and Botnets

These attack tools are advanced in terms of their ability to infect targeted systems, the resilience of the command and control infrastructure and the ability to launch multithreaded and multivector attacks. These tools form the basis of many of the largest botnets and are used by many commercial DDoS services.

Infinity Bot

Infinity Bot was seen being downloaded in the wild by an Aldi Bot instance in September, 2011. A demonstration video posted October 4, 2011, on YouTube shows Infinity Bot being used to DDoS the Pentagon Web site. The video also shows approximately 15,000 bots on the botnet, with the highest concentration of bots being in Germany, the Netherlands, Austria and Switzerland.



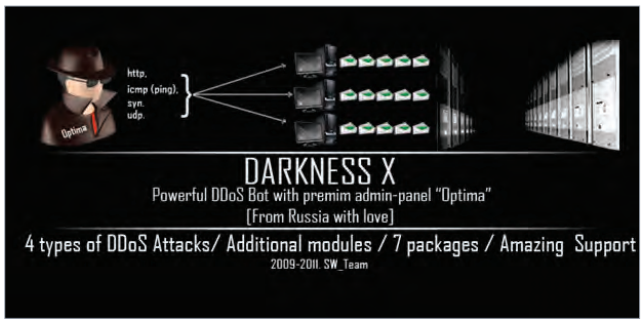


N0PE

The n0pe bot is written in .NET. Here is a screenshot of the control panel that demonstrates its attack types. N0pe appears to be Russian in origin.

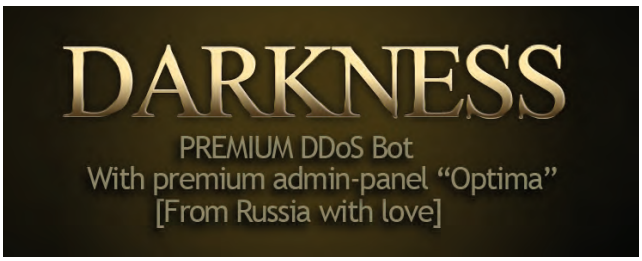
Darkness X

Darkness X is the 10th version (10a being the latest) of the Darkness bot. The following advertising graphic was used in various forums. Prices have been seen ranging from $499 to $999, depending upon what features are requested. Darkness X includes newly developed plug-in architecture.



Darkness (Prior to Darkness X)

This is a banner used to advertise the Russian Darkness bot. Darkness connects to a back-end called Optima. Darkness appears to be popular and used in commercial DDoS services.



Optima—Darkness X Control Panel

The Optima control panel for Darkness X (aka "Destination Darkness Outcast System & Optima control panel") has been explored in other forums and looks something like this as of October, 2011.

Dedal

Dedal has been mentioned in Russian underground forums describing commercial DDoS services. Dedal has been seen to utilize three types of attack—TCP, UDP and HTTP GET. The HTTP GET attack looks very similar to another bot, implying code-sharing or swiping.

Russkill

Russkill is another Russian bot that has undergone some evolution and is commonly mentioned in commercial botnet service advertisements. Russkill appears to have evolved into the Dirt Jumper.

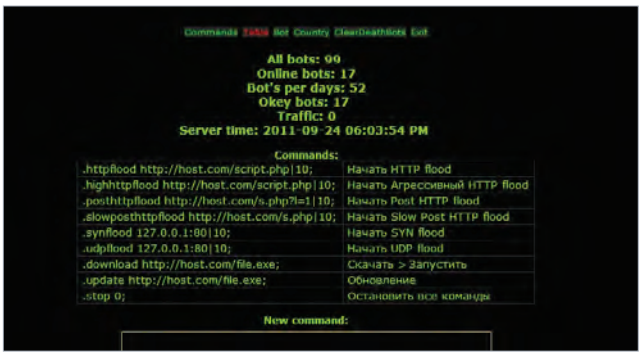
Dirt Jumper

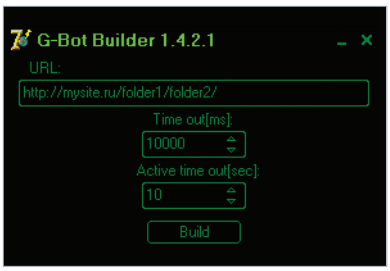
Dirt Jumper continues its popularity in the underground DDoS service economy. Dirt Jumper attacks have been widespread. See ddos.arbornetworks.com/2011/08/dirt-jumper-caught/ for a full write-up of this version of Dirt Jumper, and also see the excellent blog entry by DeepEnd Research for a write-up of Dirt Jumper version 3, aka "September" at www.deependresearch.org/2011/10/dirt-jumper-ddos-bot-new-versions-new.html.

Dirt Jumper v3, aka 'September'

G-Bot, aka 'Piranha' and 'DroopTroop'

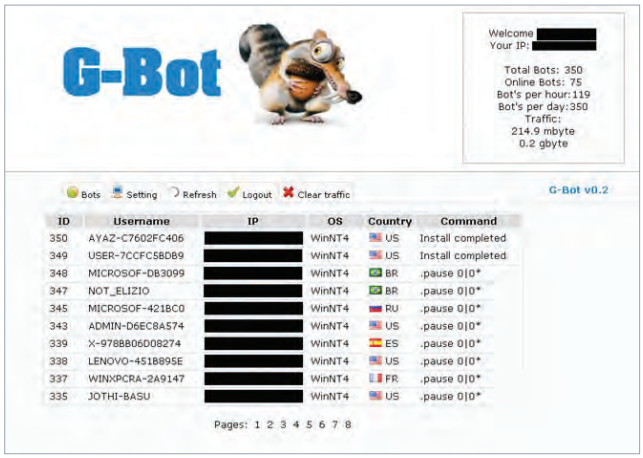
G-Bot has been mentioned many times in various forums in 2011 and seems to be a popular Russian bot. There are indicators that it is used in the commercial DDoS market. It appears that version 2.0 is probably the newest. Around July of 2011, G-Bot source code and customer lists were apparently sold by "westside" to "night." Development stats are currently unknown. Various versions of the Web panel and other artifacts are displayed here. G-Bot is also known as DroopTroop.



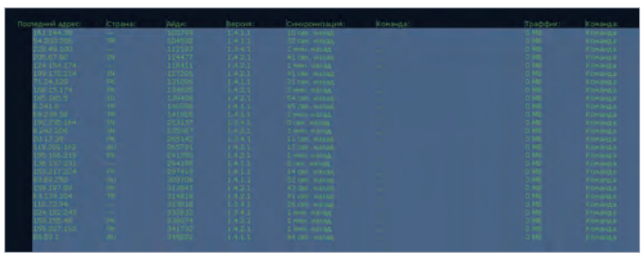


G-Bot Bot List Screenshot

First an older version, then a newer.

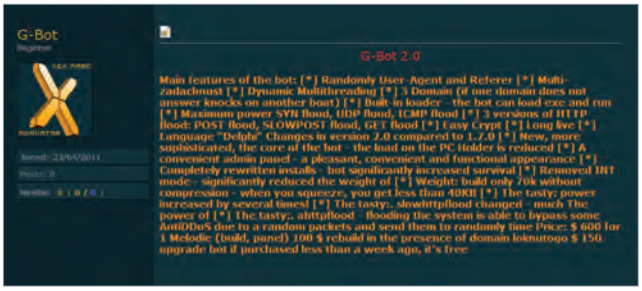


The second screenshot appears to be from somewhere around January of 2011, and shows the (obscured) IP addresses of infected hosts, country and version of G-Bot installed on the host, mostly version 1.4.



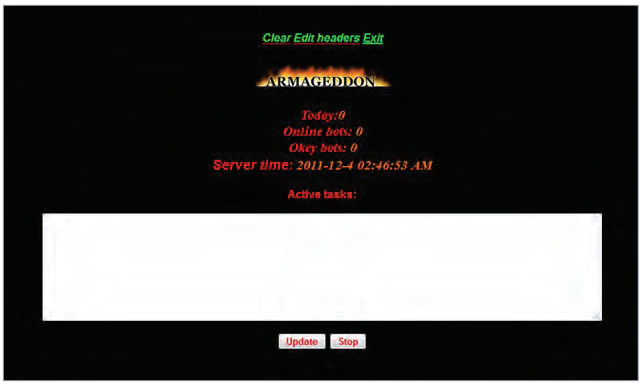
G-Bot Advertisement for Version 2.0

A leaked version of G-Bot v1.7 comes with a small .exe encoder and a builder.



Armageddon

The Russian Armageddon bot increased in popularity in mid to late 2011. It has been positioned as a competitor to Dirt Jumper, G-Bot, Darkness/Optima and DeDal. Recent versions of Armageddon allow greater control of attack traffic from within the Web panel Command & Control, and also claim to have an "Anti-DDoS" attack style that is said to bypass various anti-DDoS defenses. Additionally, DoS attacks against specific Apache vulnerabilities have been discussed. Armageddon has been observed performing many attacks including politically motivated attacks in Russia, attacks towards online betting sites, attacks towards forums advertising competing DDoS bot products and more. While Armageddon is heavily involved in HTTP attacks, it has also been seen targeting other services such as Remote Desktop, FTP and SSH.



Commercial DDoS Services

Many of the attack tools listed above are available for sale, enabling the buyer to perpetrate attacks on their own. Commercial DDoS services enable a buyer to attack a target without the risk of being caught perpetrating an attack from their own PC. More importantly, these services can bring to bear large scale botnets that have the power to bring down the infrastructure of even the largest enterprises. Such services are easily found on the Internet and offer features such as tiered pricing and free trials. Transactions are anonymous.

Unique DDoS Service

WildDDOS

OXIA DDoS Service

Death ddos Service

504 Gateway DDoS Tools

FireDDoS

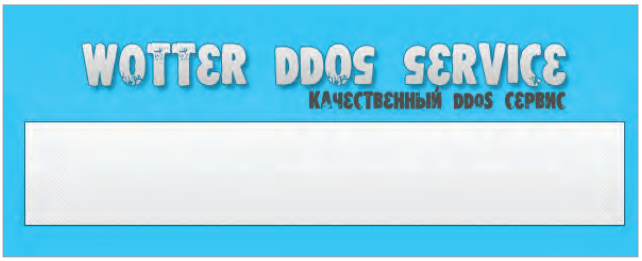
DDoS4Fun

DDoS-SeRVIS

NoName

Beer DDoS

Wotter DDoS Service



Totoro

IceDDoS

500 Internal DDoS Service

A Best Practice Approach to DDoS Defense

As the scope of overall security threats and the assets at risk become broader, security managers face some difficult decisions. It is uneconomical and impractical to protect against all threats. Decisions regarding how much to spend on security and where to allocate spending requires a business-based approach that factors in potential losses and the risk that those losses will occur.

The key questions are:

- What are the threats?
- What assets are at risk?
- What is the value of those assets?
- What is the probability of loss with/without a given security investment?
- What is the risk tolerance of the organization for each potential loss? For example, there may be a very low tolerance for catastrophic loss even if the loss expectancy (loss amount multiplied by loss probability) is lower than the expectancy of other losses.

The explosion in DDoS attack tools, hactivism and DDoS services for hire and the attack trends reported in industry surveys point to the following: the probability any given enterprise will experience business impacting DDoS attacks is going up, and the scope of assets vulnerable to attack (the "attack surface") is broadening. We are seeing DDoS used as part of an attack strategy for stealing intellectual property, credential theft and destroying company reputation.

Every enterprise should make its own risk assessment with regards to this threat but the trends are clear and there are several well publicized examples that illustrate how DDoS can become a catastrophic event for an unprepared enterprise.

As previously summarized there are best practice approaches for making security investment decisions. There are also best practices for how to deploy those investments. With respect to DDoS protection, best practices derive from understanding the scope of attacks and their targets. DDoS attacks use techniques ranging from network-layer to the application-layer protocols. These attacks target different elements of the infrastructure. As a result, protection is needed for each of those elements:

Bandwidth Protection

The first targets of vulnerability are the network links connecting the enterprise to the Internet. Enterprises generally have on the order of several hundred Mbps to several Gbps of bandwidth. DDoS attacks as large as 100 Gbps have been recorded and attacks of 10 Gbps are common. In short, attackers can easily summon the resources to overwhelm the bandwidth capacity of even the largest enterprises. These bandwidth flood attacks can only be mitigated upstream from the enterprise—in the provider network or in the cloud. As a result, enterprises need protection services from their ISP or a cloud based MSSP to prevent simple bandwidth flood attacks from saturating their links to the Internet.

Perimeter Protection

The enterprise network perimeter generally consists of some or all of the following security and access devices: router, firewall, IPS, load balancer, application acceleration, and/or web application firewall. These devices are highly "stateful"—that is they perform their core functions by tracking every incoming and outgoing session. This session tracking characteristic is what enables these devices to determine the context of every incoming and outgoing packet and apply the appropriate policy whether that be a firewall rule, redirection to the most highly available server, or delivering cached content, compression, etc. There are numerous connection-oriented attacks that exploit the stateful nature of these devices and attack tools have become more sophisticated in using blended and stealthy techniques to defeat the simple DDoS detections built in to those devices. The majority of network operators in industry surveys have reported perimeter device failures due to DDoS. As a result, protections are needed in front of the perimeter that can both detect and block connection-oriented attacks before the attacks degrade or bring down those devices.

Application Protection

In recent years there has been a dramatic increase in layer 7 (or application-layer) attacks. These are highly effective because they require much less overall traffic than flood- or connection-based attacks and so they can escape detection by tools that use behavioral and baselining techniques. A single or small number of attackers can bring down critical services even in large enterprise data centers. That is why this form of attack is often favored by hactivist groups such as Anonymous. As a result a DDoS protection system is needed that quickly detects both single threaded and blended application-level attacks based not only on behavioral and baselining techniques but also signature techniques which are typically the best way to quickly detect and stop these attacks.

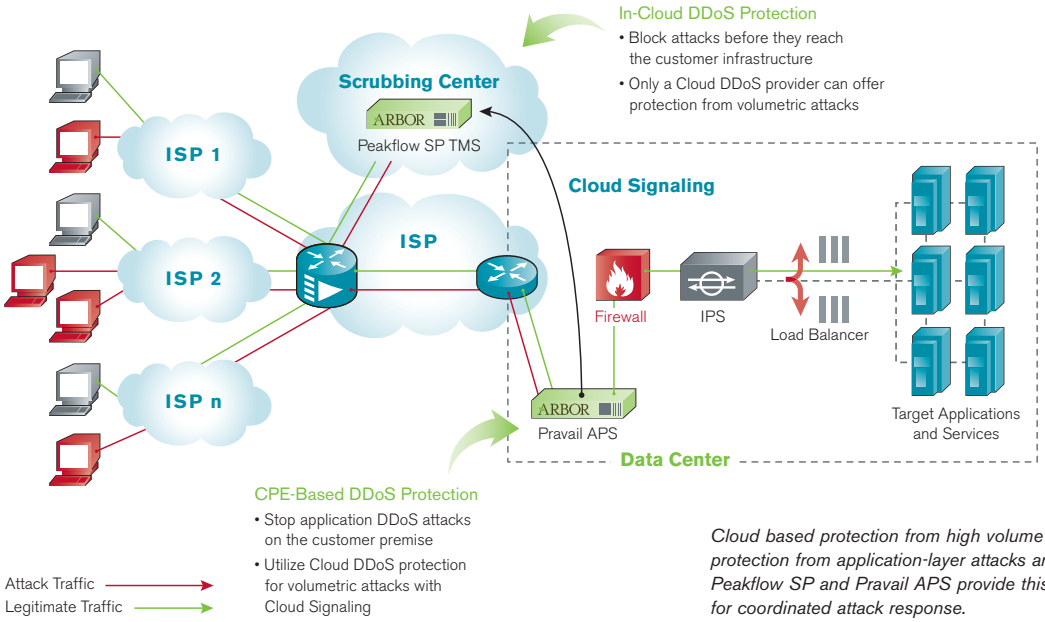
Putting It All Together

Arbor believes that optimal protection against DDoS attacks is achieved through a combination of on-premise and in-cloud protection. In-cloud protection is needed to address high-volume flood attacks. On-premise protection is needed to detect and block state-based and application-level attacks. Cloud-based DDoS services are unable to detect many such attacks before the data center infrastructure or services are degraded.

Finally, in-cloud and on-premise protections should be coordinated. Attackers often use blended methods and will vary attack methods and traffic volumes if the initial attempts are thwarted. Working with its Internet service provider (ISP) and managed security services provider (MSSP) customers, Arbor has developed a techology called Cloud Signaling℠ that facilitates both customer-edge mitigation of application-layer attacks and upstream mitigation of high-bandwidth attacks in an automated and real-time manner.

Cloud Signaling technology is an efficient and integrated way of bridging the enterprise data center to the service provider cloud. It connects the on-premise Pravail™ Availability Protection System (APS) appliance with the cloud-based Peakflow® SP solution that powers more than 50 DDoS managed security service offerings. Cloud Signaling helps to ensure the availability of enterprise data center infrastructures and speed time-to-mitigation for DDoS attacks. A best practices DDoS defense architecture is shown below.

For more technical insight into the latest security threats, Internet traffic trends and Cloud Signaling, please visit our Web site at www.arbornetworks.com and our blog at ddos.arbor.net.



Cloud based protection from high volume flood attacks and premises-based protection from application-layer attacks are needed for full protection. Arbor's Peakflow SP and Pravail APS provide this protection with Cloud Signaling for coordinated attack response.

Corporate Headquarters

6 Omni Way
Chelmsford, Massachusetts 01824

Toll Free USA +1 866 212 7267
T +1 978 703 6600
F +1 978 250 1905

Europe

T +44 207 127 8147

Asia Pacific

T +65 6299 0695

www.arbornetworks.com

ARBOR® NETWORKS

SR/DDOSTOOLS/EN/0512