DDoS Attack Tools

A Survey of the Toolkits, Apps and Services Used Today to Launch DDoS Attacks

Table of Contents

Introduction

This whitepaper is for security and networking professionals charged with protecting their networks against the debilitating effects of Distributed Denial of Service (DDoS) attacks.

In this paper, we define and classify current DDoS threats and outline, with examples, the toolkits, apps and services used to perpetrate them, with details about how our solution provides a defense.

Overview

DDoS attacks are on the rise with a growth rate of over 50% per year. If they haven't reached your business' online borders yet, it may not be long before they do. Every Internet site and service is at risk -- whether by prank, hacktivism, revenge, or cyber crime and cyber espionage. And half of DDoS targets are also victims of "smokescreening" where the DDoS attack is a diversion to steal money, customer data or intellectual property.

Attacks are in the news elevating the awareness of bad actors such as Anonymous, LulzSec and now Lizard Squad to near celebrity status. Although the largest sector hit is the enterprise, the high-profile victims we hear about most are in media and entertainment or government.

Unreported are the thousands of businesses under attack each and every day. According to a study commissioned by Incapsula, 45% of respondents said that their organization suffered a DDoS attack at some point in the past year, with organizations of 500 or more employees more likely to be hit. Respondents estimated the cost of a successful DDoS attack at $5,000 to $100,000 per hour, with the average pegged at $40,000 per hour. Organizations that suffered DDoS attacks also had to deal with nonfinancial consequences, such as loss of customer trust and perhaps smokescreening.

All companies are potential targets because launching an attack has never been easier. A clear trend is the change in attacker profile. DDoS attacks are no longer the purview of networking gurus; they can now be carried out by any ordinary citizen with a grudge.

DoS and DDoS Attacks

Denial of Service (DoS) attacks attempt to make a network service unavailable to its users. Unlike hacking, which can be damaging, DoS attacks simply block things up. A DoS attack can happen at the lower network layers by flooding the interface with too much traffic, or it can happen with less but more specialized traffic at layer 7 to consume computational resources, which ultimately yields the same effect.

A single attacker with a strong enough machine and big enough pipe can take down a small site, but to go big game hunting, the attacker must launch a Distributed Denial of Service (DDoS) attack, which employs many smaller computational devices, collectively known as a botnet. The attackers manage the botnet through a Command and Control Center, while remaining hidden behind several proxies.

Botnets generally start their "alter ego" lives sending spam. Once discovered, they are converted and further monetized by renting them to second-tier attackers to launch DDoS attacks. These consist of servers, desktops, laptops, mobile phones and now, with the advent of the Internet of Things, smart machines. Their power comes from aggregating smaller packet streams to larger and larger traffic rates, all destined for the victim's IP address.

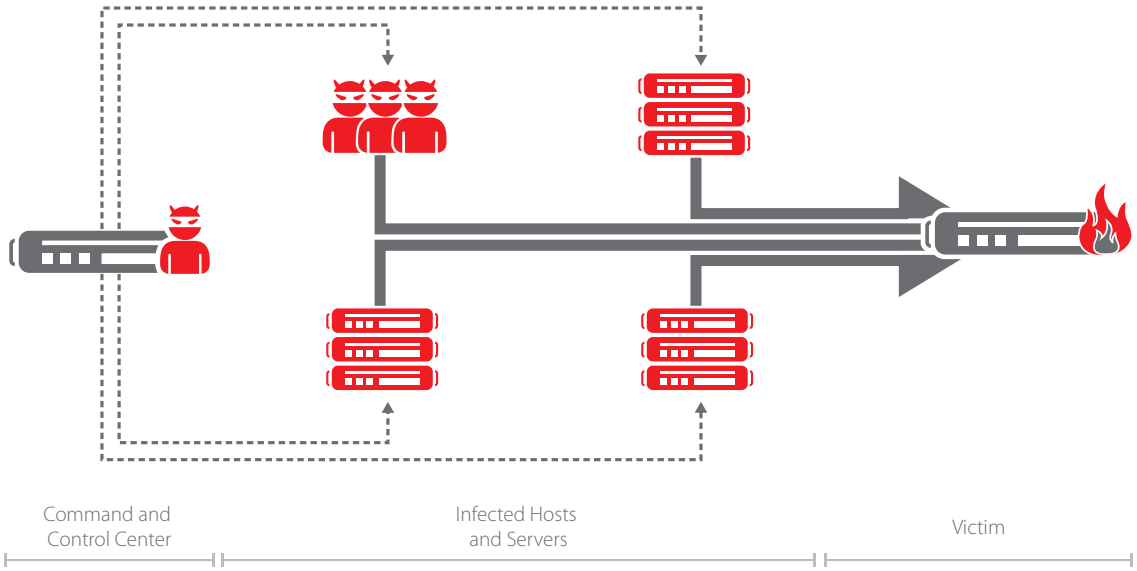

Figure 1: How a DDoS attack builds up

DDoS Attack Types

Such attacks are generally divided into three categories:

Volumetric attacks, such as DNS, NTP or CHARGEN amplification attacks, are aimed at flooding and saturating a victim's network connection, thus rendering services unavailable. Amplification attacks use bots that send requests with a fake or "spoofed" IP address (the victim's IP address) to a service such as a DNS server, which sends a response much larger than the request to the victim's IP address. All of these responses, coming from many usually unpatched or poorly configured computing devices, accumulate to large bandwidth traffic destined for the victim.

Network protocol attacks, such as SYN floods, ping of death and IP anomalies, are aimed at exhausting a victim's protocol stack so it cannot respond to legitimate traffic. A SYN flood attack, for example, takes advantage of the fact that a server reserves resources for uncompleted connection requests. Eventually the server times out the connection and frees up the reserved resources, but if these requests happen at a high enough rate, the server's resources are depleted and thus cannot respond to legitimate requests.

Application-layer attacks seek to overload resources upon which an application is running. Low-and-slow HTTP POST, HTTP GET flood or SSL-based attacks do not require high volumes of data – even 50 to 100 requests/second is often enough to consume all resources of the application's support framework, eventually overwhelming it. Unlike with volumetric attacks, application attacks cannot use spoofed IP addresses to hide their source; instead, they hijack hosting environments and Internet-connected devices.

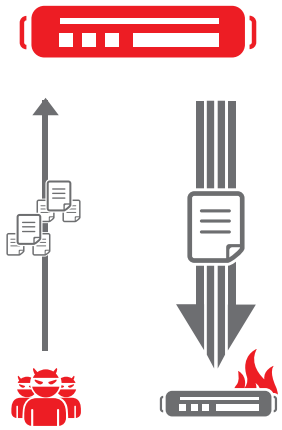

Figure 2: An amplification attack abuses online services such as DNS or NTP to increase the data size to the victim

How to Launch an Attack

The DDoS arsenal is broad and accommodating to any attacker's networking skills and budget. Tools and apps are available to attack with a single system soldier or to build a botnet to unleash an army. An attack might also direct the mercenary bot armies of others via online DDoS services.

Tools

Commercial tools for DDoS attacks are nothing new and are readily available on hacking forums. What is new is the fact that many of the toolkits now have GUIs to "point and click" their attacks. Here's a sample of some of the most popular:

- **Cythosia**: Supports SYN flooding, UDP flooding and HTTP flooding, and is highly customizable.
- **Spike:** Runs on Windows but can also execute commands on Linux and ARM-based Linux devices, recruiting from a larger pool of Internet capable devices.
- **The High Orbit Ion Cannon (HOIC):** Follow-up to the Low Orbit Ion Cannon (LOIC) made famous by the Anonymous hacking collective, HOIC spawns multiple, simultaneous attacks at different webpages on the same site. It is free and available in open source.
- **Dirt Jumper Family:** A favorite used against multiplayer gaming sites and often used as a distraction to engage in identity theft and fraud of customer accounts. Over the years, Dirt Jumper has morphed into Simple, September, Khan, Pandora, the Di BoTNet and finally Drive. It relies on HTTP flood, SYN flood and POST flood to do its damage.
- **Itsoknoproblembro (Brodos):** Threatens web content management systems by infecting servers with malicious PHP scripts. The attacks include POST, GET, TCP and UDP floods, with and without proxies, including a so-called Kamikaze GET flood script that can repeatedly relaunch automated DoS attacks.
- **Darkness (Optima):** Performs DDoS attacks, steals passwords and uses infected machines for traffic tunneling (as proxy servers). Copies can be purchased from various underground online forums for as low as $450. It most commonly uses HTTP floods, ICMP floods, SYN floods and UDP floods as its weapons of choice.
- **Storm**: The Storm kit INFECTS Windows XP (and newer) machines. Once the PC is infected, it establishes remote administration (RAT) capabilities. The kit comes preprogrammed to launch four types of DDoS attacks at once, including, UDP, TCP and ICMP floods.

Apps

For the attacker on the go, mobile phone apps provide great destructive convenience. And by mobile phones, we mean Android phones (iOS and Windows Phone are but a rounding error when counting the total number of handsets affected).

Phones are generally infected through installer hijacking malware, clandestinely replacing the app to be installed with a zombie-infected app.

Of course the real threat is in their numbers. A single contemporary phone may be able to temporarily take down a small website, but a herd of zombie smartphones are a real threat to any service.

Popular apps include:

- **MobileLOIC**: Sends a flood of TCP/UDP packets
- **AnDOSid DoS tool for Android**: Performs an HTTP POST flood attack

Services

The largest armies that attack with the most bandwidth, highest velocity and longest duration come from DDoS as a Service (DDoSaaS) operators. Known as "stressers" or "booters," these websites offer low-cost, on-demand attacks to stress test "your website" – but of course the target is never verified.

Easily outgunning PC tools and phone apps, DDoS services do all the work for you. They launch the attacks of your choice against the target of your choice for as long you specify, and this is conveniently controlled by a simple web interface. Below is the most notorious of these with examples of others that are available.

Lizard Squad

Famous for its PSN and Xbox Live Christmas attack, Lizard Squad offers a number of packages to "stress test" a server for a couple of minutes to several hours. As soon as one attack is over, another can be launched, provided you're within the same billing cycle. Monthly bitcoin fees range from $2.99 for up to 100 seconds of stressing to $130 for 30,000 seconds (8 hours).

The marketing copy reads, "Welcome to LizardStresser, brought to you by Lizard Squad. This booter is famous for taking down some of the world's largest gaming networks such as Xbox Live, Playstation Network, Jagex, BattleNet, League of Legends and many more! With this stresser, you wield the power to launch some of the world's largest denial of service attacks."

As is often the case, Lizard Squad is a second tier player that cloned the code of another stressor, in this case Titanium Stressor. Lizard Squad simply added a new frontend with a dash of high-profile marketing, to monetize its stolen cache.

The Rest

Unfortunately, Lizard Squad is not alone. The marketplace offers many competitive services, including those from Joomla, Network Stresser, Power Stresser, Str3ssed, Signal Stresser, Titanium Stresser, Hazebooter, IP Stresser, Iddos and Legion.

Solutions

Existing security solutions such as firewalls and intrusion prevention systems (IPS) are not up to the task of protecting against many of today's large scale and sophisticated attacks. For network operators, a new, complementary security solution is required to detect and mitigate all classes of DDoS attacks, simultaneously. And it is critical that a mitigation solution can easily be inserted into the existing network architecture, so that the network remains prepared for imminent DDoS threats.

The A10 Networks® Thunder TPS™ line of Threat Protection Systems ensures business continuity by providing high-performance, network-wide protection against DDoS attacks, and it defends against the volumetric and application-level attacks with the greatest flexibility and scalability.

Conclusion

DDoS attacks are not going away. In fact, they are growing at an unprecedented rate in frequency, volume, velocity, duration and sophistication as the assortment of attack options grows. Whether a PC toolkit, a mobile app or a DDoS service, there is now an attack tool to meet every skill level and budget. Network operators must respond to protect their investments and the investments of their customers. Existing security solutions such as firewalls and intrusion prevention systems (IPS) are vulnerable to volumetric state-based attacks and simply incapable of protecting against application-layer attacks. A new, complementary security solution is required to detect and mitigate all classes of DDoS attacks.

A10 Thunder TPS provides high-performance, network-wide protection against DDoS attacks. It enables service availability against a variety of volumetric, protocol, resource and more sophisticated application attacks to protect the business against negative financial consequences and loss of customer trust.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-WP-21124-EN-01
June 2015

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.