the Availability Digest

www.availabilitydigest.com

DDoS Attacks on the Rise

April 2013

A DDoS attack causes a massive amount of traffic to be sent to a web site in an attempt to disable it. The web site is so overwhelmed by the malicious traffic that it cannot respond to legitimate requests and is effectively down.

Prolexic, a firm that provides DDoS attack mitigation services,[1] publishes a monthly report that summarizes DDoS activity for the quarter and compares it to past periods. It has found that DDoS activity in 2012 is more than 50% greater than it was in 2011.

Prolexic manages a Security Operations Center (SOC) staffed by DDoS experts who monitor the traffic entering a customer's web site. If malicious activity is suspected, the Prolexic staff will alert the customer and will provide recommendations for thwarting the attack. If the attack cannot be fended off by the customer taking advantage of his firewalls, intrusion-detection appliances, and other defenses, Prolexic will reroute the traffic to one of its four worldwide scrubbing data centers. There, the malicious traffic will be filtered out; and clean traffic will be returned to the customer.

Prolexic detects and blocks between ten and eighty DDoS attacks every day for its customers. The volume of attacks and their sizes continue to increase. Prolexic mitigated more attacks in the first quarter of 2012 than it did in all of 2011. The norm of 10 gigabit per second (gbps) attacks has grown to over 50 gbps. A recent attack on Spamhaus exceed 300 gbps.[2]

In this article, we review Prolexic's findings as published in its fourth quarter, 2012, report.[3]

DDoS Attack Statistics

2012 saw a marked increase in the number of attacks and their sizes against Prolexic customers. Prolexic mitigated seven high-bandwidth attacks exceeding 50 gbps attacks in 2012. The number of attacks in the fourth quarter of 2012 was the highest ever recorded by Prolexic. The number of attacks in 2012 represented a 53% increase over the attacks in 2011.

Attacks in general lasted for more than a day. The average attack duration was 32 hours. Several attacks lasted several days.

Attacks ranged across a variety of industries, including financial services, e-commerce, software-as-a-service (SaaS), energy, and even ISPs. There was no decline in the level of attacks on any industry.

[1] Prolexic – A DDoS Mitigation Services Company, *Availability Digest*; April 2013.
http://www.availabilitydigest.com/public_articles/0804/prolexic.pdf

[2] History's Largest DDoS Attack?, *Availability Digest*; April 2013.
http://www.availabilitydigest.com/public_articles/0804/spamhaus.pdf

[3] Prolexic Quarterly Global DDoS Attack Report, *Prolexic White Paper*; 2013.

© 2013 Sombers Associates, Inc., and W. H. Highleyman

DDoS Attack Vectors

There are several ways in which a DDoS attack can be carried out.[4] Each vector (the method used to assault the computer system or network) attacks a specific layer in the Internet protocol suite.

Attacks against Layer 3 (Internet) and Layer 4 (Transport) were favored. They accounted for 75% of all attacks. SYN floods were the most popular attack. In a SYN flood, a connection request is sent to the victim and then is not completed, causing an exhaustion of resources required to make further connections. UDP floods (see *itsoknoproblembro*, described below) and ICMP floods (typically pings) were also common.

Level 7 attacks included GET and POST floods, in which bogus requests are sent to read data from the web site or to post data (such as forms) to it.

Countries of Origin

During the fourth quarter of 2012, the top ten countries generating DDoS attacks and their contributions to these attacks are as follows:

China	55.4%
Germany	9.1%
India	8.8%
Egypt	5.7%
Pakistan	4.3%
Indonesia	3.6%
Turkey	3.6%
Thailand	3.5%
France	3.3%
United States	2.7%

This represents a marked decrease in DDoS activity originating in the United States, perhaps due to law-enforcement activities.

DNS Reflection Attacks

A significant change in strategy was reflected in the increasing use of DNS reflection attacks. A DNS reflection attack is staged by the attacker sending DNS requests to a DNS server with a spoofed source address. The source address is set to that of the victim's system. Therefore, the DNS responses are returned to the victim.

This is a particularly vicious attack since there is about a 100:1 ratio between the size of the DNS request message (about 30 bytes) and the size of the DNS response message (about 3,000 bytes). Therefore, an attacker need only generate 1% of the traffic with which he wishes to bombard his victim.

In the case of the Spamhaus attack referenced above, DNS reflection was used to generate an unprecedented attack of 300 gbps. The attacker only had to generate 3 gbps, a trivial amount for a botnet of modest size.

DNS reflection attacks depend upon the existence of *DNS open resolvers*. In the early days of the Internet, a DNS server would respond to any request for a URL-to-IP translation, regardless of its source. This was later determined to be a security hole, and provisions were made to close the resolvers so that they would only respond to requests from their administrative domains or from other DNS servers.

[4] Anatomy of a DDoS Attack, *Availability Digest*; April 2013.
http://www.availabilitydigest.com/public_articles/0804/ddos_anatomy.pdf

© 2013 Sombers Associates, Inc., and W. H. Highleyman

However, system administrators are not incentivized to add this task to their otherwise busy schedules. The result is that there are still 27 million open resolvers on the Internet. Even worse, the IP addresses of all of these systems have been published.

The popularity of this attack vector has been enhanced by many publicly available toolkits designed to engineer such attacks. The most popular toolkit is *itsoknoproblembro* (think "its ok no problem bro"). This toolkit infects servers to create a high-bandwidth botnet. The infection finds its way into servers via vulnerabilities in such popular applications an Joomla, WordPress, AWStats, Plesk, cPanel, phpMyFaQ, and others. Itsoknoproblembro played a role in most of the larger attacks.

Itsoknoproblembro inserts an encrypted payload indx.php into a web site's main file, index.php. Index.php is the default file that is executed when a web site is accessed via its URL. The infecting file, indx.php, allows the server to become a bot in a large DDoS botnet army that can now launch multiple types of DDoS attacks simultaneously. Indx.php allows the command and control server to upload files and shells of malicious code into the real index.php file. They are then executed when the web site is accessed. The malicious code acts as a PHP eval script, which is very dangerous because it allows execution of arbitrary PHP code. It allows hackers to maintain persistent infections on compromised hosts even when the malicious files are discovered and removed.

There is an active battle between attackers and researchers. As attackers determine that malware-detection facilities are targeting itsoknoproblembro, they change its signatures to evade detection. For instance, over a period of a few weeks, the file name of the infection changed from indx.php to inedx.php, then to configic.php, and back again.

Prolexic has published an itsoknoproblembro threat advisory containing detailed mitigation rules for the threat.[5] The threat advisory contains:

- Details on how the toolkit operates and how it has evolved.
- Analysis of the toolkit files.
- Profiles of 11 different attack signatures with detailed rules for DDoS mitigation.
- Detection rules to identify infected web servers (bRobots).
- A free log analysis tool (BroLog.py) that can be used to pinpoint which scripts were accessed, by what IP address, and for what DDoS targets to aid sanitization efforts

Mitigating DDoS Attacks

There are three ways to deal with DDoS attacks:

- Filter the attack by looking for attack signatures.
- Distribute the attack over a large number of servers dedicated to DDoS attack mitigation.
- Take down the botnet.

Taking down botnets requires international cooperation. Initially, the botnet takedown rate was quite high as they were easily disabled in the U.S. and Europe. Now, however, the takedown rate has reached a steady state as new botnets are added as fast as existing ones are closed down. Botnet takedown has become more complex as there are fewer botnets per ISP. More ISPs have to be contacted across regions and languages, and there is no guarantee of cooperation. Expect to see a significant growth of botnets in the future.

[5] itsoknoproblembro DDoS Threat Advisory
http://www.prolexic.com/knowledge-center-ddos-threat-advisory-itsok.html

© 2013 Sombers Associates, Inc., and W. H. Highleyman

Summary

DDoS attacks are on the rise. They have become more frequent and are gaining in size. Toolkits such as itsoknoproblembro are bringing sophisticated DDoS technology to more and more hackers.

Companies must plan for unexpected DDoS attacks because they are not going to go away.

© 2013 Sombers Associates, Inc., and W. H. Highleyman