the Availability Digest

www.availabilitydigest.com

Prolexic – a DDoS Mitigation Service Provider

April 2013

Prolexic (www.prolexic.com) is a firm that focuses solely on mitigating Distributed Denial of Service (DDoS) attacks. Headquartered in Hollywood, Florida, Prolexic was founded in 2003 and become the first company to offer cloud-based DDoS mitigation services. Many companies – ISPs, telcos, Content Distribution Networks, DNS service providers, and others – offer these services on their platforms but only as an adjunct to their normal business activities. Prolexic is unique in that its data centers are dedicated solely to DDoS attack mitigation.

Prolexic has grown rapidly since its founding. Within one year, it had one hundred customers. In 2005, it was named among the top 100 privately held companies. It has experienced a compound annual growth rate of 45%. This growth rate is commensurate with the growth in DDoS attacks. In the first quarter of 2012, Prolexic mitigated more attacks then it did in all of 2011. Prolexic claims to mitigate ten to eighty attacks per day.

Prolexic employs a layered defense against DDoS attacks to block attack attempts and to keep legitimate traffic flowing. It uses experts to analyze traffic and to identify malicious traffic and its signatures. It develops defenses against new and changing attack signatures in real time. It provides emergency bandwidth through its scrubbing centers to allow a customer to weather an attack.

What is a DDoS Attack?

A denial-of-service (DoS) attack is intended to bring the Internet-facing services of a company to its knees by sending so much malicious traffic to it that it does not have the resources to respond to legitimate traffic. In effect, so far as users are concerned, the web site is down.

In a DoS attack, a single computer attempts to generate sufficient traffic to achieve this goal. However, a DoS attack by a single system faces two problems:

- The attacking system is unlikely to be able to generate enough traffic to seriously affect its victim.
- It is easy to identify the attacking system and to block traffic from it (and perhaps to take felony action against it under the laws of many countries).

Enter a Distributed Denial of Service (DDoS) attack. In a DDoS attack, a *botnet* of hundreds, thousands, or more infected PCs (the *bots*), controlled by one or more command and control servers, generates millions of messages per second directed at the victim server. This is enough traffic to seriously impact even the largest of systems. Furthermore, the IP address of the attacker is hidden by the botnet, and the IP addresses of the bots can be *spoofed* so that it is impossible to identify the attackers and block their traffic.

Botnets have now matured to the point that extremely large botnets are created by volunteers who offer their PCs for political reasons. Furthermore, botnets of PC systems are being superseded by botnets of massive infected servers. A server can generate a thousand times as much malicious traffic as a PC.[1]

Botnets can now be rented from cybercriminals rather inexpensively. A botnet containing 100,000 bots can be rented for $200 per day.

An excellent example of a successful DDoS attack is the series of attacks against major U.S. banks in late 2012 by an Islamic hactivist group incensed at the objectionable YouTube video, "Innocence of Muslims." Their attacks, occurring in September and December, disabled the online portals of several banks for a day or more each. The group vows that it will continue its attacks until the video is removed from the Internet.[2]

Mitigating a DDoS Attack

Combating a determined DDoS attack is a very difficult proposition. Firewalls and intrusion prevention appliances can be successful for small attacks measured in the few gigabit-per-second (gbps) range, but get overwhelmed at higher rates. DDoS attacks that generate 50 to 100 gbps are becoming more common. In 2012, Prolexic mitigated seven attacks that exceeded 50 gbps.

At these high data rates, the only effective defense for a company is to route its traffic to a DDoS mitigation network. These are networks of large data centers that can handle the traffic load, scrub the attacked data to remove malicious traffic, and reroute the good traffic back to the company.

The Prolexic DDoS Mitigation Strategy

Prolexic combats DDoS attacks through two mechanisms:

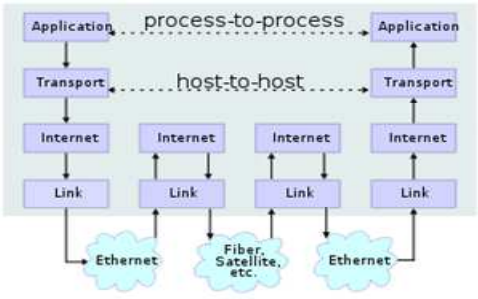
- It monitors a client's traffic via its Security Operations Center (SOC). DDoS specialists watch for traffic patterns that might signal an attack and provide real-time instructions to the client's IT staff as to what steps to take to thwart the attack.

- If the attack becomes excessive, the client's traffic is routed to the Prolexic DDoS mitigation network for scrubbing so that the client's systems receive only clean traffic. Prolexic manages four large data centers around the world for scrubbing – one in London, one in Hong Kong, one in California, and one in Virginia. Currently, a scrubbing center can handle 800 gbps of traffic. However, with the increasing size of DDoS attacks, Prolexic is making ongoing investments in its scrubbing centers to increase their capacity so as to stay ahead of DDoS hackers.

The Internet Protocol Layers

The Internet protocol stack comprises four layers:

- The Application layer provides communications between applications (such as FTP and SMTP).
- The Transport layer establishes communications between two hosts (TCP, UDP)



Wikipedia – Internet protocol suite

[1] An excellent resource for those new to DDoS attacks is the Prolexic white paper, The Executive Guide to DDoS.
[2] Islamic Hactivists Attack U.S. Banks, *Availability Digest*; October 2012.
http://www.availabilitydigest.com/public_articles/0710/bank_attacks.pdf
DDoS Attacks on U.S. Banks Continue, *Availability Digest*; January 2013.
http://www.availabilitydigest.com/public_articles/0801/more_bank_attacks.pdf

- The Internet layer forwards datagrams from one network to another (IP).
- The Network layer implements the local network (Ethernet, Fibre Channel).

DDoS attacks are made against the Application, Transport, and Internet layers. Application layer attacks (Level 7 attacks) attempt to overwhelm a host's processing capacity by invoking application functions on a massive scale. Transport layer and Internet Layer attacks (Level 4 and Level 3 attacks) attempt to overwhelm the routers, switches, firewalls, and hubs in the host's local network (its Intranet). There are also Volumetric attacks that attempt to use up the Internet bandwidth feeding the host.

DDoS Monitoring

Prolexic monitors traffic through a client's system with its DDoS experts located in the Prolexic Security Operations Center (SOC). Monitoring services are provided for Level 3, 4, and 7 attacks.

Many attacks are orchestrated by live hackers. As a consequence, the characteristics of an attack can change in real time during the attack. Mitigation strategies must react in real time to keep up with the hackers. The Prolexic SOC supplants its automated tools for attack monitoring with human experience.

Prolexic monitoring services include:

PLXfbm (flow-based monitoring provides early detection and notification of Level 3 and Level 4 DDoS attacks by directly monitoring customer edge routers without the need to insert additional hardware components into the traffic flow. It is these edge routers that are the gateway into the customer's system for malicious traffic.


Prolexic Security Operations Center

The PLXfbm service looks for anomalies in volumetric traffic flow through the routers at the Level 3 and Level 4 layers. This information is sent to the SOC where experienced technicians use flow-based monitoring tools to detect DDoS attacks. In the event of a suspected attack, a recommended action plan is provided to the client. This action plan may include a recommendation for immediate protection by rerouting traffic through the Prolexic DDoS mitigation network.

PLXfbm detects several types of attacks, including TCP abuse, UDP floods, and ICMP floods. Attacks are typically identified within fifteen minutes.

PLXabm (application-based monitoring) provides real-time monitoring of application level (Level 7) attacks. These attacks cause the greatest financial devastation to online businesses. PLXabm generates Layer 7 behaviour analysis and alerts via an onsite appliance to enable Prolexic technicians in the SOC to pinpoint exactly from where the DDoS attack is coming, even as signatures (known malicious code blocks) change. There is no additional hardware inserted into the traffic flow.

Prolexic's onsite PLXabm appliance collects the data and sends it back to Prolexic's SOC, where alerts, long-term statistical metrics, baselines, and forensic sets are created. Once a DDoS vector and attacker behaviour are determined, the PLXabm appliance is configured to automatically send attacker information back to Prolexic to mitigate in the cloud.

PLXabm detects application-layer GET and POST floods that attempt to issue these commands to application processes.

DDoS Mitigation

Prolexic's mitigation services route client traffic through Prolexic's closest scrubbing center and return clean data to the client's systems. Data flow is monitored by Prolexic mitigation experts who identify, analyze, and remove malicious traffic, allowing only legitimate traffic to flow through the scrubbing center back to the customer. If the attacker changes signatures, the mitigation experts will detect them immediately with Prolexic's proprietary monitoring tools and take defensive action until all DDoS activity ends.

During mitigation, outgoing customer traffic flows directly to the Internet. A scrubbing center can mitigate DDoS attacks up to 200 gbps.

There are three mechanisms to reroute traffic to a scrubbing center:

PLXproxy uses the customer's DNS server to reroute traffic. The customer's DNS entries are changed to redirect selected URLs to the Prolexic scrubbing center. Virtual IP addresses (VIPs) are advertised from each of the Prolexic scrubbing centers to allow automatic routing of malicious or clean traffic to the optimum scrubbing center. The scrubbing centers are ready to accept traffic immediately.

PLXrouted reroutes traffic at the interface of the client's local network with the Internet. The Generic Route Encapsulation protocol (GRE) is used to construct virtual connections to the client's routers, enabling Prolexic routers and client routers to "see" each other as directly connected via a tunnel. The Border Gateway Protocol (BGP) is used to communicate network advertisements from the client site to Prolexic. These network advertisements are used to activate and deactivate the service as needed.

PLXconnect delivers Prolexic's mitigation services via a direct physical connection to a scrubbing center. PLXconnect provides a higher throughput with lower latency than the other mitigation options. Connections can carry up to 10 gbps of traffic.

Other Services

PLXsert (Prolexic Security Engineering and Response Team) analyzes global DDoS attack data to understand the sources and attributes of DDoS attacks around the world. PLXsert distributes this data to custmers in several ways:

- It releases quarterly global DDoS attack reports.
- It issues DDoS threat advisories when appropriate.
- It maintains an IP reputational database identifying and detailing active botnets.
- It delivers data forensics to Prolexic customers as an optional subscription service.

PLXplanner asks the customer a series of in-depth questions about its IT and networking environment. It offers tips and advice along the way, and ends up with a report that the customer can use to evaluate its DDoS protection strategy. It provides the customer a path forward to take proactive protective steps if necessary.

PLXpatrol provides a global snapshot of current DDoS activity via its Attack Tracker display. It shows from where attacks against Prolexic clients are originating, and ranks the countries that have originated the most attacks against Prolexic customers over the last 24 hours and since 2009.

Mitigation SLAs

Prolexic provides SLAs for both the time that it takes to identify an attack and the time that it takes to mitigate the attack. For instance, its mitigation SLA provides the following time guarantees:

Attack Type	Time to mitigate SLA (minutes)
UDP/ICMP Floods	5
SYN Floods	5
TCP Flag Abuses	5
GET/POST Floods	20
DNS Reflection	10
DNS Attack	10

Mitigation Subscription

Prolexic provides it mitigation services on a subscription basis. The subscription fee is based on the customer's network topology and the amount of data it handles. It there is an attack, the mitigation services are covered by the subscription fee. There are no additional fees.

Summary

Not only are DDoS attacks here to stay, they are getting bigger and more frequent. In a recent report, Gartner stated:[3]

> "DDoS mitigation services should be a standard part of business continuity/disaster recovery planning and be included in all Internet service procurements when the business depends on the availability of Internet connectivity. Any Internet-enabled application that requires guaranteed levels of availability should employ DDoS protection to meet those requirements."

Companies must be prepared for the unexpected DDoS attack. Mitigation services such as those from Prolexic are perhaps the ultimate defense.

[3] Hype Cycle for Infrastructure protection, 2011, *Gartner White Paper*; August 10, 2011.