

Browser Malware

Learn Rank Protect vs Signature-based anomaly detection

A hosted web server on a 1Gbps link might typically see 100 requests/sec. An attacker can compromise one or more other web servers and then put hidden JavaScript (or flash) on a frequently accessed page.

Normal users browsing these these pages unwittingly download the malicious JavaScript, which directs their web browser to access the victim's web server many times.

The attacked servers cannot process the large number on incoming connections, meaning legitimate customers of those servers have a very low chance of their connections being processed.

Such attacks do not require a bot-net. They consist of a large number of connections where the attack traffic looks like legitimate traffic because it originates from non-compromised web browsers and involves each client sending only a small number of connection requests.

Anomaly-based DDoS Protection methods may detect the significant increase in number of incoming connections, but be unable to differentiate attack from legitimate traffic. Thus the attack defeats them.

IntelliGuard DPS, on the other hand, detects connection attempts exceeding limits in under one second and limits incoming connections down to a rate that the attacked web servers can handle, giving preference to prior customers of the attacked web server.

“Prolexic has also been tracking a big increase in browser based malware. These attacks require attackers to first compromise web servers, and using those web servers to embed light-weight malware written in JavaScript or Flash.” - Prolexic Zombie Report 2007 (July 2007)

