radware

Pre-Attack Planning Causes
Successful DoS/DDoS Attacks
Research Brief

radware ert

Pre-attack Planning

A famous quote by Alexander Graham Bell states that “before anything else, preparation is the key to success.” Unfortunately, it appears that attackers launching DoS/DDoS attacks are increasingly embracing this line of thought and investing efforts in the pre-attack phase.

Rather than ‘naively’ selecting a target and ‘carelessly’ launching an attack, more and more attackers carefully prepare their strategy; they closely study their potential targets, gather information about their vulnerabilities, and determine the best attack vectors to be used. Attackers will even conduct dry test runs to evaluate the effectiveness of their selected attack vectors prior to a full-scale launch. Such pre-attack planning and detailed preparation dramatically increases the potency and success rate of attacks. It is part of the overall imbalance between attackers and defenders sketched in the opening of this report.

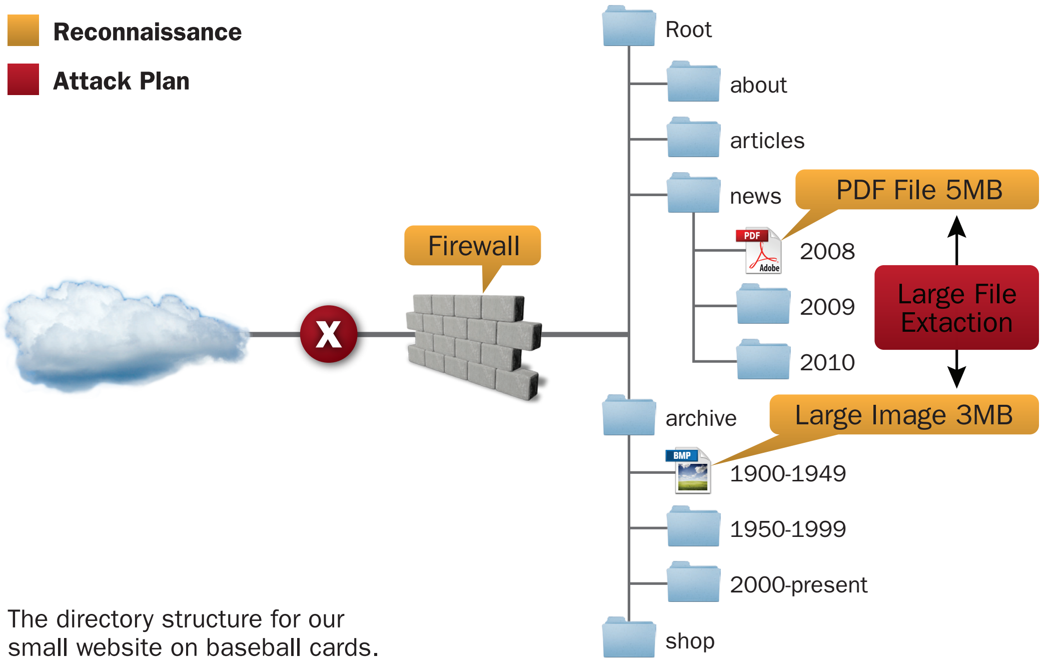
Reconnaissance – Identifying Vulnerabilities

During the pre-attack phase attackers conduct reconnaissance, with the goal identifying weak spots that provide the best opportunity for an attack.

For example, attackers look for resource- intensive activities of the target server, such as large image files or large PDF documents. After identifying such files on the target server, attackers can launch an HTTP GET flood attack that saturates the upstream Internet pipe by repeatedly requesting these large files.

Case study I – Upstream Pipe Saturation

A DoS attack handled by the ERT team involved a large financial institute and HTTP GET flood of large files. The attackers clearly studied the site prior to the attack and focused on two large files hosted on the web server - a BMP image and a PDF document, each with a 5MB file size. By sending simultaneous download requests for these files using an HTTP GET flood, the attackers were able to saturate the upstream Internet pipe of the financial institute and cause a DoS.

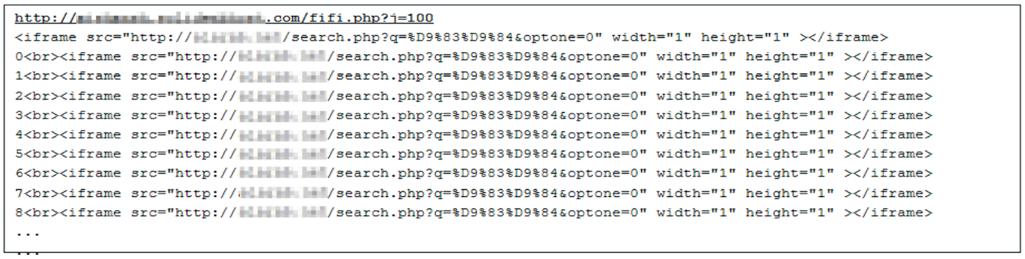


The directory structure for our small website on baseball cards.

Attackers may also look for dynamic pages that involve resource intensive tasks such as long or blocking queries to the database. Sending many requests for these pages leads to high CPU and consumption of other resources, this eventually brings down the target server and causes DoS.

Case study II – Exploiting Search Engine Vulnerability
One case handled by Radware'sERT involved an attack that exploited the vulnerability of a web site using a search engine backend. Having studied the target site, the attacker concluded that search results were not cached, meaning the server would run the same query again and again. This design involved high consumption of CPU resources.

The attack was launched by injecting iFrames in another compromised website, which pointed to the target website search URL. This reflective type of attack generated requests that peaked to about 12 requests per second - to the point where the target server CPU was exhausted. The screen capture below shows the iFrame source URLs redirecting traffic to the attacked site.



```
http://[redacted].com/fifi.php?j=100
<iframe src="http://[redacted]/search.php?q=%D9%83%D9%84&optone=0" width="1" height="1" ></iframe>
0<br><iframe src="http://[redacted]/search.php?q=%D9%83%D9%84&optone=0" width="1" height="1" ></iframe>
1<br><iframe src="http://[redacted]/search.php?q=%D9%83%D9%84&optone=0" width="1" height="1" ></iframe>
2<br><iframe src="http://[redacted]/search.php?q=%D9%83%D9%84&optone=0" width="1" height="1" ></iframe>
3<br><iframe src="http://[redacted]/search.php?q=%D9%83%D9%84&optone=0" width="1" height="1" ></iframe>
4<br><iframe src="http://[redacted]/search.php?q=%D9%83%D9%84&optone=0" width="1" height="1" ></iframe>
5<br><iframe src="http://[redacted]/search.php?q=%D9%83%D9%84&optone=0" width="1" height="1" ></iframe>
6<br><iframe src="http://[redacted]/search.php?q=%D9%83%D9%84&optone=0" width="1" height="1" ></iframe>
7<br><iframe src="http://[redacted]/search.php?q=%D9%83%D9%84&optone=0" width="1" height="1" ></iframe>
8<br><iframe src="http://[redacted]/search.php?q=%D9%83%D9%84&optone=0" width="1" height="1" ></iframe>
...
...
```

Attackers may also use the pre-attack phase to outline an ongoing attack plan, consisting of different attack vectors that can be switched during the attack, in the event that a specific attack vector is blocked by dynamic or static signatures.

'Dry Run' - Using Tools to Test Reconnaissance Findings
Another method used by attackers is launching a limited, dry run 'test attack' in order to check the validity of their plan and select the best method. For instance, assuming the attacker spotted a weakness in the form of large image files and heavy dynamic pages. The attacker may test vectors affecting the CPU and upstream bandwidth, to determine which vector yields the best results.

Once attackers have learned the victim's site and determined the attack vectors and strategy, they often use tools to test their findings and maximize the attack.

High Orbit Ion Cannon (HOIC) is one example. Offering multi-threading and multiple target capabilities, it is often the tool of choice for attackers planning to launch a massive HTTP flood attack. Attackers can use HOIC to launch an attack that simultaneously targets multiple URLs hosted by the same server. Such an asymmetric attack can be launched from one or more machines.

The HOIC tool also supports a configuration script, which attackers sometimes distribute to a wide audience prior to the attack. This essentially enables a single skilled attacker to plan and 'mastermind' the attack, and then be joined by many others.

To summarize, using DoS/DDoS tools attackers can test the valuable insight they gained during the planning phase, conduct dry test runs and maximize their attack capabilities.

Looking Deeper – Inspecting Networking Layers
The more advanced attackers perform a deep analysis of their target, including network implementation, web server application and the TCP stack.

Such attackers may conduct an extensive exploration of the target site behavior, such as testing the HTTP web server support of GET and POST methods, the caching mechanism, support of incomplete requests, HTTP pipelining (multiple HTTP requests in one packet), etc.

Attackers will then check if the TCP stack is hardened enough. They may use application layer protocols like HTTP to post a long request, checking if and when the server times out the connection, and whether the server can be forced to keep the connection alive. The attacker maps the server response on each parameter in the TCP stack, hoping to find a weak link such as bad timeout configurations.

Putting all this data together, the attacker gains an exhaustive grasp of the destination site architecture and its security devices (firewalls, IDS, IPS), and can determine the best method for bringing the target service down. For example, the attacker can launch an attack that combines a pipelined HTTP 'GET' attack on a large PNG file with a random parameter to bypass CDN and caching.

Deep Attack Reconnaissance – An Example
By testing servers' timeouts an attacker may optimize a Simultaneous Connection Flood, making it difficult for detection. The concept of such an attack is opening numerous connections until the server is depleted of resources for new connections. To make this work, the attack has to "maintain" each connection, and send at least one packet within the expiration time set by the server.

Most tools will simply send at least one packet every second to maintain the connection. However, deep reconnaissance will enable 'tailoring' the attack to the specific behavior of a site. The attacker first studies the connection timeout of the server; for example, if the timeout is 1 minute, the attacker will send a new packet every 59 seconds. With this knowledge of the TCP continuous ACK server timeout, the attacker will keep probing the server at the appropriate intervals to keep the connections alive.

Such knowledge might be translated into an efficient attack that generates much less traffic but has the same DoS effect. In addition to consuming less resources from the attacker- it has a much lower detection footprint, and can pass under the radar of the target without being discovered.

Summary

The extensive pre-attack preparation and planning conducted by attackers has a dramatic effect on the results and dynamic of DoS/DDoS attacks. Attackers are well-prepared and launch attacks that directly target the weakest spots, and can dynamically switch between attack vectors in response to the reaction of their target.

© 2013 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners.