denial of service attacks over a coffee

Business Services

orange™

editorial

Denial-of-service (DoS) attacks are among the least understood of IT security threats. For some users, they're a threat against which firewalls are all but helpless. For others, they're an especially practical way to block access to a website. Still others will say that they're nothing new under the sun: DoS attacks are as old as the Internet itself and have to be taken into account in advance, as with any virus threat.

Actually, everyone is right. From a technical standpoint, launching a DoS attack is easy. Protecting against these attacks is a challenge. The key is not to react to a DoS attack, but to act before such an attack even occurs. This booklet, or "blog book", collects a group of blog posts that pursue a common goal: to increase our understanding of DoS attacks and learn how to protect against them.

Jean-François Audenard

content

launching a denial of service attack for $200

by Jean-François Audenard

I've written on this topic before. With a little motivation, practically anyone can launch a distributed denial-of-service (DDoS) attack to take out a website (or an entire website hosting platform).

And it's not very expensive. For $200 (according to a blog post published by Damballa, a company specializing in detecting and combating botnets) it's possible to rent a network of 80,000-120,000 zombie machines for 24 hours. According to the (believable) figures listed on the site, you can launch attacks between 10 Gbps and 100 Gbps: enough to cause a lot of problems.

If you're skeptical about what these DDoS "vendors" are capable of, no worries. Some will let you try out the service free for three minutes to give you an all-powerful "I rule the Web" rush. Key the evil mastermind music…

the article online
http://oran.ge/S3pJVF

a newly available testing service for DDoS attacks

by Jean-François Audenard

Among the plethora of threats an IT security professional must guard against, distributed denial-of-service (DDoS) attacks are a special case. They make it very hard to **test the proper functioning of response mechanisms.**

During a DDoS attack, an attacker sends a synchronized flood of packets to overload the target's servers or network access. It's hard to produce a strong enough stream of attacks (which is relatively doable for testing purposes), but it's also especially difficult to generate the necessary distributed traffic from several thousand sources.

how to prevent these attacks

When setting up a prevention system for DDoS attacks, it can be important to test the system "live," to avoid any mishaps during a real attack.

The Blitz Distributed Testing Service meets all of these needs. Using this service, it is theoretically possible to purchase "windows of opportunity" during which you can launch a DDoS attack from 5,000 to 10,000 different sources (the United States government probably uses a service of this type to test its systems' resistance against this type of threat).

“DDoS challenges will increase”

warning

good to know

It's a good idea to test the system "live", thus avoiding any potential mishaps during a real attack.

This service is a commercial "white hat" or "legal" version of the managed services already available in criminal circles.

what conclusions can we draw?

- the development of a more complete toolkit like this one means that **DDoS challenges will increase** and that an associated ecosystem is emerging around them
- improved testing tools will help validate service offers and filtering equipment more objectively
- let's get past the silence surrounding DDoS: precursors like SATAN and MetaSploit have helped even the playing field in terms of tools available to defenders

the article online

http://oran.ge/TyIKRJ

the battle against DDoS attacks: our experience (part 1)

by Jean-François Audenard

Aside from a few altered dates, locations, and names of various parties involved, all the information presented here is fact.

I would like to extend a special thanks to Emmanuel Besson and Pierre Ansel from Orange Labs for all of the information they provided: without them, we wouldn't have this blog post!
Now let's dive right into the heart of the matter. It all started in May 2008.

late May 2008: the attack begins

Operations teams at an Orange subsidiary outside France alert the Group's security teams: **several distributed denial-of-service (DDoS) attacks** have struck the corporate website of one of the subsidiary's major customers, causing repeated unavailability of services hosted for legitimate users. At the same time, two other attacks target infrastructure services, notably the local DNS service.

The Group's security experts quickly assemble a crisis team. First, it gathers as much information as possible on the origin, nature, and targets of the attack. Next, it prepares and quickly enacts measures that limit the **damage caused by the cyber-attack**, or even possibly eliminate the threat.

The crisis team sets the following two priorities:

1. completely **identify** the attack: this means tracing the attack to try to find its origin, or at least the peering points where it entered the infrastructure to target the customer
2. evaluate the means available to stop the attack. Three solutions are taken into consideration:
    - work with the Internet service providers (ISPs) conveying the attack (black hole filtering technique) to **block** traffic previously identified as located closest to sources
    - **strengthen** local defenses by changing the parameters of some firewalls or tightening attacked server configurations
    - provide the local subsidiary with complementary active probes to **analyze** and block the attack

a week later:
first countermeasures

Thanks to detection resources placed on the international networks, **the three IP addresses targeted by the attack are identified**, along with no fewer than 16 core routers relaying the traffic involved in the attack, seven peering points and as many partner operators.

The team immediately contacts the partner operators, asks them to trace the origins of the attack and apply their blocking mechanisms, if available.

At the same time, operations teams launch a **black hol**e for one of the addresses targeted by the attack. In short, this technique consists of modifying the network infrastructure’s routing configurations so that every router trashes all incoming traffic intended for a given IP address. This seems to eliminate the first element of the attack.

Meanwhile, with the help of Group security experts, **local teams reconfigure the firewalls** protecting their DNS infrastructure and managing to block the second element of the attack.

However, the last element of the DDoS attack targeting the end customer remains, since the previous two solutions aren't applicable in this case. Experts suggest using a traffic Cleaning Center solution developed through their work and that specifically counters DDoS attacks.

good to know

The fundamental difficulty with DDoS attacks lies in their apparent legitimacy, as malicious requests use "authorized" ports and produce packets that appear "well-formed".

flashback: the decisive solution

The proposed solution makes it possible to manipulate traffic so as to clean it in real-time using **intelligent filtering** functions.

The fundamental difficulty with DDoS attacks lies in their apparent legitimacy, as malicious requests use "authorized" ports and produce packets that appear "well-formed". For this reason, firewalls and other Intrusion Prevention Systems (IPS) prove ineffective against the majority of DDoS attacks.

The experts' model optimizes the use of "selective sorting" algorithms for traffic (so it can run at several Gbps). Positioned so as to cut off the influx directed toward the victim, it only admits the purified and legitimate portion to the machine.

With this system, it's possible to protect several critical services that are simultaneously attacked. In fact, the definition of a protected service can be very broad (a whole section of traffic) or more targeted, and even very specific (certain types of requests directed to a given machine). Of course, the module comes equipped with an interface for **real-time monitoring** and rapid changes in protection settings.

For these reasons, the subsidiary requests this technology to protect its customers under attack.

early June 2008: the attack stops

Once the attack has ended, the crisis team approves the experimental launch of the Cleaning Center, which goes into effect in mid-July. It's positioned in "monitoring" mode at the subsidiary's peering points and receives the traffic intended for all the local operator's customers who had requested protection.

Local teams receive training so they can activate the "protection" mode in case of a new attack.

Have the attackers stopped? No. As you'll soon see, they attack again!

the article online
http://oran.ge/QVLkuN

the battle against DDoS attacks: our experience (part 2)

by Jean-François Audenard

In the part one of this article, a Cleaning Center had been deployed against the attacks at the Orange subsidiary's network connection points.

Posted behind their fortifications, the teams in charge of the service platforms waited for a possible new round of attacks. What strategy would the attacker use? Would the cleaning system withstand the new attacks?

It started all over again in July 2008.

late July 2008: the saga continues

The attack targeting the end customer surges again, first with two 40-minute volleys of server saturation targeted by a **SYN flood**. However, this ends very quickly.

Next, multiple sources begin a coordinated effort to open (too) many connections on one of the Orange subsidiary's messaging servers. The Cleaning Center module then goes into "protection" mode.

Immediately, **the illegitimate connections are filtered out**. Realizing the failure of their efforts, the aggressors change their tactics and manage to open an apparently "legitimate"

warning

“it’s vital to detect and block the majority of usurped addresses used by a pirate” connection. As soon as they succeed, they use the connection to flood the server with requests.

The module then changes its protection mode by filtering out the malicious source address. Almost six hours later, the attack ceases. Though disruptive, the attack was not very strong. In fact, it never reached a rate of more than 1,000 packets per second.

good to know

For DDoS attacks, the defense arsenal is varied and it's imperative to know how to effectively use both the simplest and the most sophisticated techniques.

early August 2008: a new, more elaborate attempt

The Cleaning Center detects a barrage of **80,000 packets per second** targeting the original address of a customer that had received multiple attacks since July. Operations teams are alerted, but the attack quickly dies out. It was only a trial round.

Less than two hours later, the pirates renew their first attack with the same intensity. But this time it lasts. **The customer's website crashes once again** due to the massive load received by the attack.

The team decides to activate filtering by shifting the module from "monitoring" to "protection" mode. The client server's protection is now activated.

The Cleaning Center immediately begins to filter the attack. It detects and **blocks the majority of spoofed addresses** used by the pirate to launch a massive influx of simultaneous requests to open connections on the targeted web server.

Less than ten minutes after the start of the offensive, the attackers notice that their efforts are fruitless. They cease fire but reconfigure their botnet. The attack picks up again at a rate of 80,000 packets per second. It is **automatically filtered**. Three minutes later, the pirates pad their original attack (SYN flood) with a massive influx of HTTP GET requests directed at the same web server. This attack (GET flood) comes from 97 machines (members of the botnet coordinated by the pirates), increasing fire to 175,000 packets per second.

The “Cleaning Center” then adapts its protection to filter these new malicious requests.

the battle comes to an end

After nearly 40 minutes of fighting, **the attack ends**. The pirates no doubt recognize **the failure of their attempt**. The customer is now protected, and the attackers’ malicious intentions are neutralized by the Cleaning Center’s protection, positioned ahead of the target.

Taking advantage of the Cleaning Center’s onboard capture and storage features, the system updates the list of machines involved in the attack and manages to locate them. Unbeknownst to their legitimate owners, these machines had been wrapped into the botnet by the pirates.

For the most part, the machines are located in China and Korea. After a more in-depth analysis conducted the following day, Orange Labs experts detect and extract one additional address of a machine acting strangely. It had repeatedly tested the website’s availability just before, during, and up to 4 minutes after the attack. Had we found our culprit?

conclusion

The success of this operation demonstrates the critical necessity to protect against distributed denial-of-service (DDoS) attacks by quickly mobilizing network experts and utilizing adapted, innovative, powerful tools. In this pseudo-arms race, **the defense arsenal is varied**. It’s imperative to know how to effectively use both the simplest and the most sophisticated techniques.

Again, hats off and my thanks to Emmanuel Besson and Pierre Ansel from Orange Labs for the high-quality content of this blog post!

the article online
http://oran.ge/QVNdYI

about the author

Jean-François Audenard

Within Orange Business Services, I'm in charge of securing our cloud computing solutions and services. I'm the passionate kind and only look at things this way: no 50/50 for me, I'm an engaged and engaging blogger, I like to go off the beaten track. Sincerity is my tone and optimism and voluntarism my two engines

Our blog :
http://blogs.orange-business.com/connecting-technology/

Document available for download at :
http://knowledge-center.orange-business.com/

Edited by Orange Business Services
13.11.2012

France Télécom – 78, rue Olivier de Serres, 75015 Paris, France – SA au capital de 10 595 541 532 – 380 129 866 RCS Paris – Document non contractuel – juin 2012

Business
Services

orange™