BELTUG
Be Connected

BELTUG POSITION

BELTUG – DDoS attacks, open DNS resolvers and IP address spoofing

BELTUG urges all organisations, companies and ISPs running DNS servers to check and if necessary correct the configuration of the open DNS resolvers to prevent them from being used as an attack vector in a DDoS attack

April 2013

1 MARCH 2013: A MASSIVE DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACK

From 18 March on the Internet experienced one of the most massive distributed denial of service (DDoS) attacks in its history. Attackers targeted the Spamhaus Project website, its content provider CloudFlare and a number of Tier 1 Internet exchange points.

Spamhaus Project is a non-profit organisation dedicated to fighting spam. As such they distribute blacklists containing IP addresses of mail servers and websites suspected of acting as source of spam emails. The blacklists are distributed to ISPs and used by DNS to block access from these suspected spam sources.

The work done by the Spamhaus Project is not without controversy and as such it is no surprise its website became the target of a DDoS attack. Many feel Spamhaus is simultaneously acting as judge, jury and executioner despite the mechanisms put in place to remove legitimate systems from the blacklists and as such the Spamhaus Project website is often victim of attack.

After initiating the attack it quickly became clear to Spamhaus Project they would not be able to handle this large-scale attack alone so they contacted their content provider CloudFlare to spread the attack over a large number of data centers. The attackers then started targeting the ISPs supporting Spamhaus Project and CloudFlare and the focus of the attack shifted to a number of Tier 1 Internet exchange points such as the London, Amsterdam and Hong Kong Internet Exchanges. At the height of the attack the total bandwidth of the attack reached about 300 Gbps for an attacker input bandwidth of only 3 Gbps!

2 A FLAW IN DNS SERVERS CONFIGURATIONS

In the post-incident analysis it became quickly clear the attackers exploited a specific flaw in how many DNS servers are configured. Too many DNS servers are configured as open resolvers returning information to anyone who asks. In addition to that DNS queries allow for easy spoofing of the source IP address. In this particular incident the attacker spoofed his or her original IP

address to be the Spamhaus Project website and then asked many open resolvers for a lot of DNS database information.

3 25 MILLION OPEN DNS RESOLVERS ON THE INTERNET POSING A SIGNIFICANT THREAT

The Open DNS Resolver Project estimates that at the end of March 2013 there were about 25 million open DNS resolvers on the Internet posing a significant threat. The full listing of the open DNS resolvers can be found on the ASN website. Close scrutiny of this listing will show a number of open DNS resolvers in Belgium.

BELTUG urges all organisations, companies and ISPs running DNS servers to check and if necessary correct the configuration of the open DNS resolvers to prevent them from being used as an attack vector in a DDoS attack. Guidelines concerning the configuration of your DNS servers can be found on the Open DNS Resolver Project website. DNS servers should be configured according to the guidelines offered in RFC 5358 / BCP 140.

Since for the foreseeable future it will be impossible to eliminate all open DNS resolvers from the Internet, additional measures need to be taken to tackle the use of spoofed source IP addresses. The RFC 2827 / BCP 38 describe how ISPs can filter source addresses to eliminate spoofed addresses within the edge of their networks. Additionally, the RFC describes how filtering can be achieved by adjacent networks to protect themselves and others. This too, is a long-term solution requiring the whole Internet to cooperate. For non-ISPs the guidelines are to implement tighter lines of security around their DNS infrastructure. Specialists recommend implementing solutions that defend against all kinds of attacks without weighing your network down with latency. Solutions based on fast caches, multiple security filters, and ability to rapidly address security countermeasures are to be preferred.