Can Recent Attacks Really Threaten Internet Availability?

ENISA is recommending that Internet network providers implement long-known traffic filtering techniques, which could have countered a major cyber incident that hit services across western Europe last Month (March 2013) [1].

The incident was an attack mounted against the non-profit organisation Spamhaus [2], leading to noticeable delays for internet users mostly in the UK, Germany and other parts of Western Europe. Spamhaus, which is based in Geneva and London, contributes to the fight against spam by providing a service that enables operators of email servers to check if a sender's email server is known to be sending unsolicited commercial email. Although no clear evidence exists, the attack on Spamhaus is generally attributed to a hosting provider who was flagged as a spam sender by Spamhaus.

This incident highlights some important vulnerabilities of the internet infrastructure, but at the same time also demonstrate its inherent resilience.

DNS Amplification and Open Resolvers

The attack on Spamhaus was dubbed by online media as the biggest Distributed Denial of Service (DDoS) attack ever seen [3]. Spamhaus started experiencing a significant DDoS attack on its servers on 16th March. The attack spanned a period of more than one week and happened in three phases: first, the attack was directed at Spamhaus, then at CloudFlare, a service provider contracted by Spamhaus to deal with the attack, and finally at CloudFlare's network providers. In this last stage of the attack, the enormous amount of traffic generated by the attack caused problems at the London Internet Exchange.

The technique used for the DDoS attack is by no means new. The method used by the attackers to generate the traffic directed at the Spamhaus network, DNS amplification, has been known for many years. It is made possible by the fact that today it is still possible for most internet-connected hosts to send IP packets with forged ("spoofed") source addresses.

Another factor contributing to the size of the DDoS attack is the large number of so-called "open recursive resolvers" in the internet. Open resolvers are Domain Name Service (DNS) servers which answer all requests sent to them, not just those related to the DNS domain for which they are authoritative resolvers. Open resolvers can be misused to amplify DDoS attacks [4].

Unfortunately, even today many network providers have not implemented a set of recommendations (called BCP38 [5]), which has been around for almost 13 years. If the available recommendations were implemented by all networks, traffic filtering on border routers would block such attacks. A similar set of recommendations for operators of DNS servers (called BCP140 [10]), which could help reduce the number of servers that can be misused for DNS amplification attacks, was published in 2008.

However, today there are still thousands of servers that can be abused for this kind of attacks.

BGP Hijacking

At the same time as the DDoS attack, Spamhaus was also attacked using Border Gateway Protocol (BGP) route hijacking [6]. The aim of this particular attack was to hijack legitimate queries away from Spamhaus's servers in order to disrupt their operation and reputation reporting so that every IP address on the internet was regarded as a source of spam [7].

The BGP is used by network operators to exchange information about the reachability of blocks of internet addresses. BGP hijackings can be accidental, but can also be used by attackers in various ways to disrupt or intercept a network's traffic, essentially by pretending to provide a faster way to reach the victim's network.

Lessons Learned

When looking at this incident, the question arises as to how much any particular geographical area or economic sector depends on certain network operators, internet exchanges, or physical infrastructure.

There are a number of lessons that can be learned from this incident:

- While the incident didn't affect the internet on a global scale, the effects on a local scale were rather noticeable. It therefore serves as a reminder that while the internet overall can be considered resilient, it cannot be taken for granted that this is also true for the local part of the Internet infrastructure serving a particular region, or country.
- Even disputes between private, non-state actors can have important effects on internet infrastructure, due to the high degree of interconnections and the cross-border nature of the internet.
- Attacks are increasing in size. While the largest publicly reported DDoS attack up to 2012 had been around 100 Gigabits of data per second, the March 2013 attack on Spamhaus reached a size of more than 300 Gigabits per second [8].
- At this size of attacks, the capacity of commercial internet exchanges, which normally have very high availability/capacity infrastructure, can be exhausted.
- Currently there exists no widely agreed scheme to assess the impact of the factors that played a role in the attack, or of incidents related to the physical layer of the internet infrastructure. This makes it difficult to assess the associated risks.

It is also interesting to note that despite the size of the DDoS attack, there is no clear evidence as to its originators. For the BGP route hijacking, the situation is different because the corresponding route announcements are made "in public" and were recorded [6].

Recommendations by ENISA

The interdependencies of various components forming the foundations of the internet infrastructure, such as cables, datacentres, network operators, internet exchanges, are still not completely understood. The recent incident shows that there are still many steps that can be taken even in the short term, to improve the resilience of the internet infrastructure.

- Operators serving as upstream or transit providers to end-customer networks should implement BCP38 [5].
- Operators of DNS servers should check whether their servers can be misused in DNS amplification attacks and should implement BCP140 [10].
- Operators of internet exchange points should consider that their infrastructure might be attacked directly and make sure that they have appropriate security measures in place.

ENISA will continue to investigate the area of network interconnections with the aim of providing policymakers, telecommunications regulators, cyber security agencies and network operators in European Union Member States with recommendations on how issues related to the resilience of the internet infrastructure in Europe can be addressed.

For further information on the resilience aspects of the internet interconnection ecosystem see also ENISA's Inter-X report [11] and the Computer Emergency Response Team Austria's blog [12].

References

[1] Spamhaus DDoS grows to Internet-threatening size http://arstechnica.com/security/2013/03/spamhaus-ddos-grows-to-internet-threatening-size/
[2] Spamhaus project http://www.spamhaus.org/
[3] Global internet slows after 'biggest attack in history' http://www.bbc.co.uk/news/technology-21954636
[4] Open DNS Resolvers Center Stage in Massive DDoS Attacks http://threatpost.com/en_us/blogs/open-dns-resolvers-center-stage-massive-ddos-attacks-032813
[5] Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing http://tools.ietf.org/html/bcp38
[6] Looking at the spamhaus DDOS from a BGP perspective http://www.bgpmon.net/looking-at-the-spamhouse-ddos-from-a-bgp-perspective/
[7] Spam? Not Spam? Tracking a hijacked Spamhaus IP https://greenhost.nl/2013/03/21/spam-not-spam-tracking-hijacked-spamhaus-ip/
[8] Putting the Spamhaus DDoS attack into perspective http://www.arbornetworks.com/corporate/blog/4813-putting-the-spamhouse-ddos-attack-in-perspective
[9] 'Biggest ever' Internet attack is indeed huge, but it isn't global http://venturebeat.com/2013/03/27/biggest-ever-internet-attack-is-indeed-huge-but-not-global/
[10] Preventing Use of Recursive Nameservers in Reflector Attacks http://tools.ietf.org/html/bcp140
[11] Inter-X: Resilience of the Internet Interconnection Ecosystem http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x
[12] Lessons from the Stophaus/CloudFlare/Spamhaus DDoS for ISPs http://www.cert.at/services/blog/20130328190708-815_en.html

Flash Note produced by: Thomas Haeberlen, Expert in Network and Information Security, and Rossella Mattioli, Security and Resilience of Communication Networks Officer, ENISA