F21AN Individual Report - DNS Amplification Attack

The implications of a DNS Amplification attack, like any Distributed Denial of Service (DDoS), can be wide ranging. This report will lay out the effects of such an attack, which any victim (industry, end-user, or society) may have to deal with, accounting for the nature of the attack and any mitigation that has been put in place.

The most immediate danger is to a web server, which can be forced offline because a malicious attack is filling its bandwidth. While a web server is unavailable, a 502 gateway error is shown to clients. This attack is particularly dangerous against any individual or industry that is running an e-commerce platform, and repairing a web server after a Domain Name System (DNS) amplification attack can take time and money. In the event a victim does not know what has happened to their service; little, to no, mitigation has been put in place; or no backup of the data has been taken, a software developer may need to be hired to rebuild the website from scratch. This will cost the individual or company yet more time and money. A sites Search Engine Optimisation (SEO) index could also be badly affected if a DNS Amplification attack continues for an extended period of time[1].

During or after a DNS amplification attack, a victim's server may be rendered more vulnerable to other forms of attack - which could go unnoticed by a victim while they work on getting their service back online. This includes taking anti-virus systems out of action, making it easier for a hacker to find an access point to otherwise secure areas of a server. These follow-up attacks will not always come from the same source as the requests that formed the DNS Amplification attack, a hacker will know how to ensure their anonymity and use multiple IP address to attack your site[2].

Forms of extortion may be used against a victim industry, end-user, or society in conjunction with a DNS amplification attack as such attacks could cause the loss of, or be run in conjunction with, the stealing of, sensitive or confidential data. Victims of such ransomware would, in some cases, receive a ransom note prior to the attack which demands payment in exchange for the attacker not launching the attack in the near future. Another scenario could see the ransom note arriving while the initial DDoS flood from the attack takes place - as a warning that the attacker expects payment. If data containing sensitive or confidential data is destroyed or stolen this also may have a legal impact upon the victim of the attack[2].

In conclusion there is a wide range of effects that any DDoS, and more specifically a DNS Amplification attack, can have upon an industry, end-user or society. These can include financial, legal and data losses which a company will need to mitigate sufficiently against. With these attacks becoming ever larger and more prevalent[3], it is important that the potential victims understand what they are, the forms they take and how they can be mitigated if they are to protect their enterprises.

References

[1] Sachdeva, M., Singh, G., Kumar, K. and Singh, K., 2010. Measuring impact of ddos attacks on web services.

[2] Chadd, A., 2018. DDoS attacks: past, present and future. *Network Security*, *2018*(7), pp.13-15.

[3] Vlajic, N. and Zhou, D., 2018. IoT as a land of opportunity for DDoS hackers. *Computer*, *51*(7), pp.26-34.