The Impact of DNS Attacks

The DNS system converts readable host names to IP addresses and vice versa (Harrison, 2012). The Internet Assigned Number Authority (IANA), assigns names through the Internet Registries and logs them in a large database held on various computers. When there is an attempt to resolve a hostname, a query is made to the database and an IP address is returned. This process is at the heart of how URL’s are accessed and is the basis for how data is transmitted over the internet. Unfortunately, attacks against the DNS are on the rise (Reedy, 2013). This paper will discuss the impact of attacks on DNS and what they mean for Internet operations.

According to an article by Reedy (2013), there are 2 forms of DNS attack. The first type of DNS attack is from the outside-in, for example the denial of service (DOS) attack. In order to mitigate these attacks, the servers being attacked would need be be able to recognize false DNS queries from legitimate ones. The second type of attack is characterized as inside-out because it uses the DNS as a communication pathway to create botnets, spam, and phishing. Both of these forms of attack generate network traffic that can create latency if not take down servers entirely.

If an organization’s DNS server becomes congested with queries and goes down, the network it serves will be cut off from the rest of the Internet. This has dire consequences, as will be discussed shortly. However, it is not just the consequences of each DNS attack that is an issue. The growing number of DNS attacks itself is a growing concern. Behind HTTP attacks, DNS is the next vector being exploited by hackers, with DNS-targeted attacks increasing 216% in 2013 alone (Infoblox, 2014).

Reedy goes on to say that, “... [DNS] attacks can take 10 hours or more to resolve” (2013). If you consider the number of hours of website downtime, potential e-commerce lost and the man-hours to fix the DNS problem, the cost of DNS attacks is staggering.

DNS attacks not only “cost hundreds of thousands of dollars” (Reedy, 2013), but they also damage the reputations of the brands marketed through the websites. For example, GoDaddy, Spamhaus, and Twitter have all experienced DNS attacks in the past year and have suffered as a result. According to estimates by Forrester Research, the average cost for a 24-hour network outage when you take into account lost sales, customers, and brand name loss is $27 million dollars (Infoblox, 2014).

Considering the DNS system is at the core of Internet operations for both the individual organization and for the Internet at large, the increasing attacks targeting DNS are a serious concern. Not only are organizations harmed, but the economy that is based in the digital marketplace becomes tenuous as well. Organizations and technology personnel responsible for maintaining their web presence should not be the only people concerned about DNS attacks. The rise in DNS attacks can have a negative impact on the reliability of the Internet at large and the economies that depend on it.

References

Harrison, P. (2012). Quick HOWTO: Ch 18: Configuring DNS. Retrieved from <http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch18_:_Configuring_DNS#.VHZVHpUtBgU>

Infoblox (2014). Securing your business with DNS servers that protect themselves. Retrieved from <https://www.infoblox.com/sites/infobloxcom/files/resources/infoblox-note-secure-business-dns-servers-protect.pdf>

Reedy, S. (2013). DNS Attacks on the Rise. Retrieved from <http://www.lightreading.com/mobile/mobile-security/dns-attacks-on-the-rise/d/d-id/706866>