Science Writing

Author's Name

Name of Institution

Course

Date

Attacks Used the Internet Against Itself to Clog Traffic

Article info: John Markoff, Nicole Perlroth: Attacks Used Internet Against Itself to Clog Traffic, The New York Times, 2013.

Introduction

In their article, *Attacks Used Internet Against Itself to Clog Traffic*, Markoff and Perlroth,(2013) state that there has been an increase of cyber attacks in recent times. This costs the victims millions of dollars, as it could shut down an entire business. The article states how black hat activity occurs and how to stop them.

How the Attacks Occurred

Cyber assaults are distasteful actions to change, interrupt, mislead, humiliate, or destroy computer systems. The main aim is to hinder or construe a significant activity that depends on the Internet (Schiller, 2010). The author says that stopping the attacks is not an easy task. The recent fronts succeeded due to both the worst and best aspects of the extensive global Internet network (Markoff & Perlroth, 2013).The Internet is open to manipulation being that it is not a closely regulated platform for communication. The way communication servers are configured makes them vulnerable to assaults. The most recent attacks showed how huge the problem has become. On Tuesday, February 21st of this year, a group discontented Spamhaus; this is an association, which distributes names of spammers to providers of e-mails (Markoff & Perlroth, 2013).

To infiltrate, the assailants used botnet-infected computers controlled by a remote to attack the primary website of Spamhaus. Afterwards, the Internet servers used by CloudFlare, Silicon Company were hired by Spamhaus to redirect its front. The author states that the attacks are successful due to the infected

computers exploiting Internet routing software so that Internet servers return the answers of the requests made for a data sent concurrently by a hefty set of computers.

Spamhaus and Cloudflare's servers answered the requests and were fooled into distributing data to the attackers. As the servers responded by sending quite a large block of information, they accelerated the attack. Data flow grew from ten billion bits the first week to three hundred billion bits for every second the following week, causing message errors and delays among millions of people across the Internet community (Markoff & Perlroth, 2013). After nine days, the black hats changed their tactics. They realized they would not be able to disable CloudFlare any longer. They aimed at the networks connected to CloudFlare and penetrated computer servers, which provide the network's establishment. They also attacked organizations within Amsterdam, London, Frankfurt, and Hong Kong that dealt with Internet exchanges. They did not cut out the Internet, except they made it slow down.

The attackers continued changing targets, stopping and starting the fronts over nine days. The black hat activities succeeded due to the blend of loopholes, complex, and poor configurations of Internet routing equipments. The attack could not have succeeded if all the organizations affected would have checked whether the outgoing information packets were being sent by the company or to the organization by customers (Markoff & Perlroth, 2013). Few companies counter-check outgoing information to determine whether or not their customers sent it.

How to Dissuade the Attacks

The authors state that, since the year 2000, the fundamental principles of shielding ourselves from cyber attacks has been extensively documented. In the same year, a voluntary group of Internet and communication engineers laid down the rules of the best practices to encourage Internet organizations and companies to get used to overcoming a hazard identified as “IP Address Spoofing”, where the attacker can conceal a fake address at the back which is critical for the success of DDoS(denial-of-service) attacks (Markoff & Perlroth, 2013). The rules were put in a document called BCP 38, and are followed by a limited number of small companies. The Internet security of late did name and ashame operators of open, misconfigured servers to try to shut them down (Markoff & Perlroth, 2013). This did pay off, as some companies dropped off the list in the last five months.

The weakness of the Internet is that it is made of many of autonomous computers, making it susceptible to enduring threats. The authors state that, if black hats had started the assault from one computer, it might have been subdued. When the source of the attack is from one source, it is easier to counter than when it is from many sources (Markoff & Perlroth, 2013). They also say that it is prudent to teach system operators to configure their networks.

Other Sources

Security concerns of the Internet have been expressed by security engineers to encourage companies, organizations, and individuals with Internet connections to take a number of essential and potentially pricey changes to their operations like implementing new protocols in network equipment to enhance security for Internet communications (Stiennon, 2010). Patching vulnerabilities in UNIX systems, frequently updating antivirus software, and intrusion detection software, all help (Garber, 2000). In the year 2010, the department of energy of the U.S.

funded Siemens Corporate Technology's research team to bring split regional systems under a universal security framework that could be adapted to the needs of any automation on the power grid system, thus creating protection against intruders. Another way of stopping the assaults is the use of the principle of separation that entails enforcement of entrance policy limitations on the users and resources in a computing environment (Amoroso & Amoroso, 2012).

Conclusion

Cyber attacks are still the main threat facing a computing atmosphere (Schiller & Phd, 2010). Network operators need to be educated on how to configure their servers to prevent attacks (Markoff & Perlroth, 2013). Organizations should make it a norm of checking whether outgoing data comes from the customers to reduce assaults (Schiller & Phd, 2010). Companies and organizations should avoid using unconfigured servers. Individuals and companies should be ready to make expensive choices in strengthening their security systems to counter these black hat attacks (Markoff & Perlroth, 2013).

References

Amoroso, E. G., & Amoroso, E. (2012). Cyber Attacks. Amsterdam: Elsevier.

Garber, L. (2000, April 7th). New York Times. Retrieved April 1st, 2013, from Denial-of-Service Attacks Rip the Internet: http://www.sciencedirect.com/science/article/pii/S1389128603004250

Markoff, J., & Perlroth, N. (2013, March 27th). Attacks Used the Internet Against Itself to Clog Traffic. Retrieved March 01/04/2013, 2013, from New York Times : http://www.nytimes.com/2013/03/28/technology/attacks-on-spamhaus-used-internet-against-itself.html?pagewanted=1&_r=2&ref=technology

Schiller (2010). Cyber Attacks and Protection. New York : CreateSpace.

Stiennon, R. (2010). Surviving Cyber War. Lanham: Government Institutes.