Denial-of-service attack or DDos

Refusal of service attacks are planned to make a machine or network resource inaccessible to its expecting clients. Attackers can deny service to individual victims, such as by purposely entering a wrong password enough consecutive times to cause the victim’s account to be bolted, or they may overload the capabilities of a machine or arrange and block all clients at once. Whereas a arrange attack from a single IP address can be blocked by including a modern firewall run the show, numerous forms of distributed denial of benefit assaults are possible, where the attack comes from a huge number of points and guarding is much more difficult. Such attacks can start from the zombie computers of a botnet or from extend of other possible techniques, including reflection and enhancement assaults, where innocent systems are tricked into sending traffic to the victims where systems that have not been sanitized are tricked into sending traffic to the victims, infecting them by a malware or sending them to a different website, where their information can be easily stolen.

According to Cisco data “This kind of attacks are becoming more common from 2018 attacks run around 7.9 million but is predicted that by 2023 would be around 15 million.” (Cisco 2020)

The most recent attack of this kind was “The google attack 2020” on October 16,2020. It was discovered by Google’s Threat Analyst group or TAG is the group in charge with in google company to work to protect against these threats. The UDP amplification attack sourced out of several Chinese ISPs and it remains the largest bandwidth attack in 2020.

Mounted from three Chinese ISPs, the attack on thousands of Google’s IP addresses lasted for six months and peaked at a breath-taking 2.5Tbps! Damian Menscher, a Security Reliability Engineer at Google, wrote:

The attacker used several networks to spoof 167 Mpps (millions of packets per second) to 180,000 exposed CLDAP, DNS, and SMTP servers, which would then send large responses to us. This **demonstrates the volumes a well-resourced attacker can achieve:** This was four times larger than the record-breaking 623 Gbps attack from the Mirai botnet a year earlier. ( <https://www.a10networks.com/blog/5-most-famous-ddos-attacks/>)

Social engineering and Malware

Social engineering, in the context of computer security, aims to convince a user to disclose secrets such as passwords, card numbers, address, emails, or gran physical access, by, for example impersonating a senior executive, bank, a contractor, or a customer. This generally involves exploiting peoples trust and relying on their cognitive biases. A common scam involves emails sent to accounting and finance departments personnel, impersonating their CEO and urgently requesting some action. In early 2016, the FBI reported that such “business email compromise” scams had cost US businesses mor than 2 billion in about two years.

In May 2016, the Milwaukee Bucks NBA team was the victim of this type of cyber scam. Yahoo! Sports reported that the Milwaukee Bucks fell victim to a spoofed email scam. Names, addresses, Social Security numbers, compensation information and dates of birth of the players were unknowingly sent to a hacker and created a massive security issue for the team.

The perpetrator impersonating the team’s president Peter Feigin resulting in the handover of all the team’s employees’ 2015 W-2 tax forms.

I think this kind of attack is harder to prevent because in order to install a malware or infect a server or a computer. Social Engineering counts on human error to attack the company. Training is important to help different segments of the organization work effectively or work against effectiveness towards information security within an organization.

But social engineering is not the only way that the NBA has been in risk for private and financial information has been expose. Malware software that is install on a computer an leak any information, such as personal information, business information and password, can give control of the system to attacker, and can corrupt or delete data permanently. A famous example is what happen to National Basketball Association (NBA) in middle of April of 2021. The hacker group Babuk claimed to have stolen 500 GB of confidential data concerning the Huston Rockets. Babuk warned that these confidential documents, including financial infor and contracts, would be made public if their demands were not me. (https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php).