A brief overview of the current threat landscape

Amy Lawson-Gunkel

31 August 2019

Details

An attacker’s objective has remained consistent throughout the evolution of cybersecurity; the attacker is driven to “compromise the confidentiality, integrity or availability of the computer or information stored on it” (Cybersecurity for Small Business: Introduction to Cyberthreats). Their assets could include but is not limited to: their data, their websites, or their own employees. Although the objective has continued to be the same, the means of obtaining these results has changed; new techniques are being developed and executed on a constant basis.

Threats can come from both inside and outside of the organization; a best practice would be to identify potential risks and attempt to mitigate them. A few forms of common cyberattacks include: advanced persistent threats, distributed denial of service, inside attacks, and malware.

The simpler of these four common attacks would be a distributed denial of service (DDoS) and an inside attack. A distributed denial of service attack can be executed by a novice script kiddie, who is not even aware of the full amount of damage they will ensue by running their executable. An insider attack can come from a current or previous employee who deliberately use their credentials in an unauthorized manner to obtain information above their privilege.

The more complex attacks, of the four previously listed, are the advanced persistent threats and malware. Advance persistent threats (APTs) are comprised of five different stages; because of the complexity of these stages, APTs are harder to detect and take longer to execute. The five stages of an advanced persistent threat are as follows: reconnaissance, incursion, discovery, capture, and exfiltration. To describe this better, APTs involve researching the targeted network, depositing the malware, determining how the network is being defended, retrieving the data, and “exploiting captured information” (Cybersecurity for Small Business: introduction to Cyberthreats). The other threat, malware, comes in many forms, such as “viruses, spyware, worms, ransomware, Trojan horses and keylloggers” (Cybersecurity for Small Business: introduction to Cyberthreats).

References

(n.d.). Tutorial 2: Introduction to Cyberthreats. Retrieved from <https://www.sbir.gov/tutorials/cyber-security/tutorial-2#>

National Institute of Standards and Technology. (2018, April 16). 01b - NIST\_Improving Cybersecurity.pdf. Retrieved from <https://drive.google.com/file/d/1wPp9kofp-gdlu3NAisszeM8d8ko1djF1/view>