OPEN ACCESS Freely available online

Journal of Defense Management

Commentary

Short Note on Cyber Security

Sherin K*

Department of Military Science, Walden University, Washington, USA

DESCRIPTION

Cyber security is the application of the technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks.

Common cyber threats

Backdoors: Backdoors allow remote the access to the computers or systems without the users' knowledge.

Formjacking: Formjacking is the process of inserting malicious JavaScript code into the online payment forms to reap customers' card details.

Cryptojacking: Cryptojacking is the malicious installation of cryptocurrency–which is a software. This software illegally harnesses the victim's processing power to mine for cryptocurrency.

DDoS attacks: Distributed Denial-Of-Service attacks attempt to disrupt the normal web traffic and take targeted websites offline by the flooding systems, servers or networks with more requests than they can handle, causing them to crash.

DNS poisoning attacks: DNS (Domain Name System) poisoning attacks to compromise DNS to redirect traffic to the malicious sites. Affected sites are not 'hacked' themselves.

Malware

Malware is the broad term used to describe any file or program intended to harm or disrupt a computer. This includes:
Botnet software: Botnet software is designed to interrupt to pollute large numbers of Internet-connected devices. Some botnets include millions of compromised machines, each using a relatively small amount of processing power. This means it can be difficult to detect this type of the malware, even when the botnet is running.

Ransomware attack: Ransomware is a form of the malware that encrypts the victims' information and demands the payment in return for the decryption key. Paying a ransom does not necessarily guarantee that you will be able to recover the encrypted data.

RATs: RATs (Remote-Access Trojans) are malware that installs the backdoors on the targeted systems to give remote access and/or administrative control to the malicious users.

Rootkits and bootkits: Rootkits comprise several malicious payloads, such as keyloggers, RATs and viruses, allowing attackers remote access to the targeted machines. Bootkits are a type of the rootkit that can infect start-up code – the software that loads before the operating system.

Spyware: Spyware is a form of the malware used to illicitly monitor a user's computer activity and to harvest the personal information.

Trojan: A Trojan is a type of the malware that disguises itself as legitimate software but performs the malicious activity when executed.

Viruses and worms: A computer virus is a piece of the malicious code that is installed without the user's knowledge. Viruses can replicate and spread to the other computers by attaching themselves to other computer files.

Common cyber attacks

Botnets: Botnets are the large networks of compromised computers, whose processing power is used without the user's knowledge to carry out the criminal activity. This can include distributing spam or phishing emails or carrying out the Distributed Denial-of-Service (DDoS) attacks.

Drive-by downloads: Drive-by downloads install the malware when victims visit a compromised or malicious website. They don't rely on the unsuspecting users taking action, such as clicking the malicious email attachments or links, to infect them.

Exploits and exploit kits: An exploit is a piece of the malicious code that can compromise security vulnerability. Many have been advanced by the security services. Exploit kits are the collections of multiple exploits. Available for rent on the dark web, they are enable unskilled criminals to automate attacks on known vulnerabilities.

Correspondence to: Sherin K, Department of Military Science, Walden University, Washington, USA, E-mail: Sherin.k.@edu

Received: 01-Mar-2022, Manuscript No. JDFM-22-16946; **Editor assigned:** 04-Mar-2022, PreQC No. JDFM-22-16946 (PQ); **Reviewed:** 18-Mar-2022, QC No. JDFM-22-16946; **Revised:** 24-Mar-2022, Manuscript No. JDFM-22-16946 (R); **Published:** 31-Mar-2022, DOI: 10.35248/ 2167-0374.22.12.230

Citation: Sherin K (2022) Short Note on Cyber Security. J Defense Manag. 12: 230.

MITM attacks: A MITM (Man-In-The-Middle) attack occurs when a criminal hacker inserts themselves between a device and the server to intercept the communications that can then be read and/or to be altered. MITM attacks frequently happen when a user logs on to an insecure public Wi-Fi network. Attackers may insert themselves between a visitor's device and the network. The user will then unknowingly pass the information through the attacker.

Phishing attacks: Phishing is a method of the social engineering used to trick people into the exposing sensitive or confidential information, often *via* email. Not always easy to distinguish from the genuine messages, these scams can inflict enormous damage on the organisations.