Malware Threats Glossary

Created By: Natisha Stiles, Teaching Assistant

1. **Anti-Malware** - is a software solution that helps protect a PC or system from malware.
2. **Batch File** - This is a file that is used to run commands and perform tasks.
3. **Cache** - Stored data for future use.
4. **CISO** - Chief Information Security Officer
5. **Delivery** - The method in which malware gets to its target.
6. **Denial of Service Attack** - **DOS** - This type of attack happens when the resources of a system are used up preventing further access to that system.
7. **Encapsulation** - is enclosing the data or code into a single unit. This is done to hide the details or inner workings of a program that the user does not need to know.
8. **Encryption** - Converting information into a binary format to prevent unauthorized access.
9. **Fork Bomb Attack** - This attack is performed when a process is opened repeatedly. This continues until all resources on the machine have been exhausted.
10. **HTTPS** - Secure Hyper Text Transfer Protocol is the protocol used for secure web communications.
11. **Infiltrate** - The act of entering a system when not authorized to do so.
12. **Insider Threat** - is “defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems (as cited in Combating the Insider Threat, 2014).
13. **Malware** - Malicious software that includes viruses, worms, and trojans.
14. **Malvertising** - is advertising used for the delivery of malware.
15. **Operating System** - The software that runs on a computer which is used to control basic tasks and processes, as well as giving a user the ability to access programs and user peripherals like the keyboard and mouse.
16. **Pentesting** - or penetration testing, is the simulation of various cyber attacks against a computer system or network.

17. **Phishing** - The attempt to obtain information from an individual through deceptive e-mails that are disguised as coming from a legitimate company or someone you may know.
18. **Ransomware** - This type of malware encrypts files so the attacker can demand payment, primarily in a crypto currency, before decrypting the files.
19. **RAT** - Random Access Trojan
20. **Self-propagating** - The ability to spread itself.
21. **Self-replicating** - The ability to copy itself.
22. **Trojan** - This is a type of virus that is disguised as a legitimate program with a hidden action.
23. **USB Drop Attack** - This is an attack that happens when a random USB device or SD card with malware is dropped in a random location. An unknowing person will pick up the device or card and put it in their own system which then becomes infected with the malware.
24. **Virtual Box** - Virtualization software provided by Oracle that is used to run one or more virtual machines.
25. **Virtual Machine** - A machine that can run an operating system utilizing virtualization software.
26. **Virus** - Malicious software that needs a host to run and is attached to files; some types include boot sector, ransomware, shell virus, polymorphic, and macro viruses.
27. **Virus** - **Boot Sector Virus** - is a virus that is launched during the boot sequence.
28. **Virus** - **Macro Virus** - A virus that is run via macros such as within Excel or Word docs.
29. **Virus** - **Polymorphic Virus** - A virus that changes its code so it is hard for signature based anti-virus to find it.
30. **Virus** - **Ransomware** - This type of malware encrypts files so the attacker can demand payment, primarily in a crypto currency, before decrypting the files.
31. **Virus - Shell Virus** - Encapsulating the virus code. [See encapsulation]
32. **Virus** - **Wanna Cry Virus** - A ransomware virus that encrypts the files and starts a countdown timer. The attacker threatens to delete the files at the end of the timer if they are not paid via the Bitcoin crypto currency.
33. **Worm** - This is a self-propagating piece of code that is able to spread itself to other hosts on a network.

Combating the Insider Threat [PDF]. (2014, May 4). NCCIC/US-CERT.