CSC8101 Penetration Testing

Assignment 1

Created by: Deep Shah

Student ID: U1137064

Date: 26th March 2022

Question 4: Answer the following.

a) What can eLiTeWrap do?
b) Explain how eLiTeWrap can be justified as a malware.
c) Briefly describe two ways to deliver a malware to a target system.
d) Evaluate the features of eLiTeWrap and justify if it is a better than average malware or not.

Solution:

a) What can eLiTeWrap do?

Answer: Elite wrap is a program that combines two programs, one hidden and the other not. As a result, it would be simple to merge the virus with it. a puzzle game or a social media software, for example. The game or application would only be visible to the end user, but when it ran, it would launch the virus (easttom, 2018).

Files can be extracted automatically into a temporary directory from which they can be manipulated by other applications in the pack file or on the user's machine. Programs (both internal and external) can be launched in plain view or hidden from the user.

b) Explain how eLiTeWrap can be justified as a malware.

Answer: The insertion of an attacker vector and a payload is the basic definition of malware.

eLiTe Wrap can connect any two programs. Anyone may use a tool like this to attach a virus or malware to a seemingly harmless product like a attractive application. As a result, a big number of users will inadvertently download what they think is a free and attractive application and install virus on their own systems. The Trojan horse components are illustrated by this method of hiding the virus in another form

Therefore, the payload is the virus file, and the attack vector is the program in which the virus is hidden. As a result, Elite wrap can be classified as malware (easttom, 2018).

c) Briefly describe two ways to deliver a malware to a target system.

Answer: The two ways to deliver the malware are:

I. Downloads from suspicious websites
II. Viruses in Email Attachments

I. Downloads from suspicious websites.

A malicious website is one that tries to install software (a wide term for anything that might slow down your computer, steal personal information, or, in the worst-case scenario, take total control of your system) on it. In most circumstances, you will be required to act; but, in the event of a drive-by download, the website will attempt to install software on your computer without first obtaining your consent. In addition, fraudulent websites can look to be legitimate. On rare occasions, they may ask you to install software that your computer appears to need.

II. Viruses from suspicious websites.

An email virus is harmful code that is disseminated in email messages and can be triggered when a user opens an email attachment, clicks on a link in an email message, or interacts with the infected email message in any other manner.
Most email viruses propagate by sending a malicious message or attachment to everyone in the victim's contact book. Viruses may be packaged and delivered in a variety of ways. Recipients may also find it difficult to detect individual email messages carrying malware, since these communications represent a significant amount of effort on the part of the malicious actor to make the email look as if it came from a recognized and trustworthy sender. This is especially true when phishing assaults are used to carry out corporate email compromise attacks. Phishing attacks, in which hackers send out harmful email messages that look to have been sent from approved sources such as internet search sites, social media, the victim's bank, or even coworkers and friends, are the most common causes of email infections. The attacker's goal in such instances is to deceive users into disclosing personal information such the victim's complete names and addresses, usernames, passwords, credit card details, or Social Security numbers.

d) Evaluate the features of eLiTeWrap and justify if it is a better than average malware or not.

Answer: As we discuss above elitewrap is a tool that combines two programs, one hidden and the other not. As a result, it would be simple to merge the virus with it.

Features: It is possible to extract programs from the pack file without having to launch them. Unlike many EXE wrappers, files can be extracted automatically into a temporary directory from which they can be manipulated by other applications in the pack file or on the user's machine. Programs in the pack file and on the user's, computer can be launched automatically.
eLiTeWrap, unlike many self-extractor applications, can launch any number of programs contained in the pack file or already installed on the user's system. Programs (both internal and external) can be launched in plain view or concealed from the user. Programs that do not require user interaction can be started without the user's knowledge. Programs can be launched in a synchronous or asynchronous manner. Script files may be created to automate the production of pack files, and the pack file can be programmed to wait for a program to finish before the remainder of the files are processed. (eLiTe, 2020)

As a result, elitewrap's claim of being better than normal malware.

Though, in most cases, modern antivirus software or a firewall offered by an operating system such as Windows may identify the files. The reason for this is that this tool is a little outdated, and cyber security technology has progressed. However, in comparison to other common viruses, we may still consider this program to be superior and more harmful.

Bibliography

easttom, c. (2018). *Penetration Testing Fundamentals.* (M. taub, Ed.) Indianapolis, indiana, USA: Vanessa Evans.

eLiTe. (2020). *elitewrap.zp.html*. Retrieved from packet strom: https://packetstormsecurity.com/files/14593/elitewrap.zip.html