Module-3 Assignment: Delivery System

Nawaraj Khatiwada

ECE-529 Intro to Technical Cybersecurity

Prof. Dr. Lamb

Spring 2024

Introduction

In cybersecurity, Penetration testing is the process of gaining unauthorized access to a target system using flaws or vulnerabilities, which are frequently made possible by techniques like taking advantage of malvertising, software bugs, configuration errors, or social engineering techniques like phishing. Using exploit kits to automate the exploitation process or distributing malicious payloads via techniques like malvertising may also be used during this phase. Delivery is the process of delivering malicious payloads to their intended target. This is typically done by means of email attachments, compromised websites, or USB drives. The different parts of cyber-attacks, which involve things like phishing, exploit kits, and malvertising, are very important. They need strong defenses to stop hackers from getting in and to lower the chances of bad code causing harm.

Objectives

The hypothetical objective of this paper is to provide an overview of the purpose of delivering a delivery system's architecture for a payload. We'll look at given two scenarios where a rootkit is to be delivered. We'll examine methods for opposing the delivery systems after they've been designed. This involves talking about payload delivery detection and prevention strategies. We'll also look at specific countermeasures to reduce the threat that the delivery systems pose.

Methodology

Scenario I:

To deliver a rootkit into an IoT device in my professor's house, given that professor uses an older Windows installation and a single subnet for both wired and Wi-Fi connections, and suggestion for countermeasure, here's a detailed plan:

1. Delivery Methods
   - Malvertising: The plan involves creating deceptive ads that look harmless and placing them on websites that professors often visit. These ads, appearing legitimate, would contain links leading to exploiting kits or phishing pages with the goal of delivering a harmful rootkit. The process includes where actual ad networks are hacked, or malicious code is added to online advertisements that appear on the professor's frequently visited websites. When professors interact with these ads, they would be redirected to websites hosting exploit kits or phishing pages. The rootkit payload is then delivered through automatic downloads, known as drive-by downloads, initiated during the interaction with the malicious ad.
   - Exploit Kits: The plan entails using an exploit kit to attack vulnerabilities in outdated software which has been loaded on professor’s Windows system. This is done by making the professor visit a website where the exploit kit resides, usually through phishing emails, malicious links or websites that have been compromised. The exploit kit searches them automatically for weaknesses, and if it finds any the rootkit payload is delivered to professor’s device. The payload delivered to the victim is then further propagated via drive-by downloads prompted by exploitation of vulnerabilities identified on devices.

- Social Engineering: This plan includes emails or messages to trick professors into clicking on a link or downloading an attachment that contains the rootkit payload, social engineering techniques are added to the attack in this strategy. This is done by creating phishing emails or messages that look like they come from reliable sources or that present appealing offers to get the target to interact with the malicious content. When a victim interacts with the malicious link or attachment, drive-by downloads that are automatically started because of their interaction with the misleading content are used to deliver the rootkit payload.

2. Countermeasures
   - Ad Blocking: Use browser extensions or ad-blocking software to prevent unwanted advertisements from showing while browsing. By setting up these tools to block known malicious websites and filter out suspicious ads based on their content or behavior, we can improve online security and protect ourselves from malvertising campaigns.
   - Software Update: The professor's Windows system and all installed apps must be updated with the most recent security patches on a regular basis to protect against vulnerabilities that exploit kits take advantage of. This can be done by setting up a patch management system, or by turning on automatic updates for both the operating system and software programs.
   - Install a PI-Hole: Pi-hole filters out malicious advertisements and defenses users from malvertising campaigns by acting as a network-level ad blocker. Pi-hole can also filter out suspicious ads and block known malicious domains, which improves online security.

- Security Awareness Training: It is important to inform the professor about the risks involved in clicking on suspicious links and downloading attachments from unknown sources. This can be done by holding frequent security awareness training sessions that go over subjects like incident reporting protocols, safe browsing practices, and phishing awareness and make sure they stay alert to potential threats and improve their overall awareness of cybersecurity.

Scenario II:

To deliver a rootkit and crack contained passwords resident on an IoT device in a lab, which uses an old SSH daemon built around libssh, we need to design a delivery system and exfiltration method. The detail plan is explained below:

1. Delivery of Rootkit

   To deliver a rootkit we can use methods like exploiting SSH Vulnerabilities and use of social engineering. exploiting SSH vulnerabilities involves gaining unauthorized access to Internet of Things devices by taking advantage of known flaws in out-of-date SSH daemons, especially those that use the libssh library. Avoiding authentication, vulnerabilities in libssh allow us to run arbitrary commands on the device. Also, social engineering techniques exploit SSH vulnerabilities to gain unauthorized access to the targeted IoT device by tricking us into opening malicious attachments or links through convincing phishing emails or messages.

2. Installation of Rootkit

   Installing the rootkit on the IoT device will allow us to take control of it permanently once unauthorized access has been gained. The rootkit can be made to avoid being discovered by security measures and give us remote access capabilities.

3. Exfiltration of Passwords

Extraction of password hash from the IoT device can be done once control over it has been established. System files or memory can be used as sources for this data to be gathered by the rootkit. After that, we use password cracking methods to extract the passwords from the hashes, such as dictionary attacks or brute force attacks, rainbow tables, Metasploit. This involves methodically attempting different password combinations until the right one is discovered.

The final step is to exfiltrate the successfully cracked passwords. This data is sent to a remote server that they own. To avoid detection, we could cover up the data within genuine network traffic or utilize encrypted communication channels, which would make it more difficult for security systems to detect and stop malicious activity. Overall, this process allows us to gain unauthorized access to systems using compromised passwords.

Discussion and Conclusion

The paper discusses the hypothetical goal of delivering the rootkit into an IoT device in professor's house also exfiltrate the passwords from the compromised device. Through comprehensive analysis and scenarios, paper suggests how crucial it is to put strong countermeasures in place to thwart these kinds of attacks. The discussion highlights the need for a comprehensive strategy that includes software updates, network-level complete security tools like Pi-hole, and ad blocking in addition to awareness training to enable users to identify and help counter possible threats. The study also highlights how important it is to continuously monitor and modify cybersecurity procedures to stay ahead of developing attack vectors and mitigate increasingly dangerous attacks. Through the adoption of comprehensive cybersecurity approach, which is guided by the ideas discussed here, anyone can enhance the security of their digital environments against malicious cyberattacks and maintain the integrity and usefulness of their data and systems.