Chapter 2

Attacks, Concepts and Techniques

This chapter covers the ways that cybersecurity professionals analyze what has happened after a cyberattack. It explains security software and hardware vulnerabilities and the different categories of security vulnerabilities.

The different types of malicious software (known as malware) and the symptoms of malware are discussed. The different ways that attackers can infiltrate a system is covered, as well as denial of service attacks.

Most modern cyberattacks are considered to be blended attacks. Blended attacks use multiple techniques to infiltrate and attack a system. When an attack cannot be prevented, it is the job of a cybersecurity professional to reduce the impact of that attack.

Finding Security Vulnerabilities

Security vulnerabilities are any kind of software or hardware defect. After gaining knowledge of a vulnerability, malicious users attempt to exploit it. An exploit is the term used to describe a program written to take advantage of a known vulnerability. The act of using an exploit against a vulnerability is referred to as an attack. The goal of the attack is to gain access to a system, the data it hosts or to a specific resource.

Software vulnerabilities:

Software vulnerabilities are usually introduced by errors in the operating system or application code, despite all the effort companies put into finding and patching software vulnerabilities, it is common for new vulnerabilities to surface. Microsoft, Apple, and other operating system producers release patches and updates almost every day. Application updates are also common. Applications such as web browsers, mobile apps and web servers are often updated by the companies or organizations responsible for them.

In 2015, a major vulnerability, called SYNful Knock, was discovered in Cisco IOS. This vulnerability allowed attackers to gain control of enterprise-grade routers, such as the legacy Cisco 1841, 2811, and 3825 routers. The attackers could then monitor all network communication and had the ability to infect other network devices. This vulnerability was introduced into the system when an altered IOS version was installed in the routers. To avoid this, always verify the integrity of the downloaded IOS image and limit the physical access of the equipment to authorized personnel only.

The goal of software updates is to stay current and avoid exploitation of vulnerabilities. While some companies have penetration testing teams dedicated to search, find and patch software vulnerabilities before they can get exploited, third party security researchers also specialize in finding vulnerabilities in software.

Google's Project Zero is a great example of such practice. After discovering a number of vulnerabilities in various software used by end-users, Google formed a permanent team dedicated to finding software vulnerabilities.

Hardware vulnerabilities

Hardware vulnerabilities are often introduced by hardware design flaws. RAM memory for example, is essentially capacitors installed very close to one another. It was discovered that, due to proximity, constant changes applied to one of these capacitors could influence neighbor capacitors. Based on that design flaw, an exploit called Rowhammer was created. By repeatedly rewriting memory in the same addresses, the Rowhammer exploit allows data to be retrieved from nearby address memory cells, even if the cells are protected.

Hardware vulnerabilities are specific to device models and are not generally exploited through random compromising attempts. While hardware exploits are more common in highly targeted attacks, traditional malware protection and a physical security are sufficient protection for the everyday user.

Types of Malware

Short for Malicious Software, malware is any code that can be used to steal data, bypass access controls, or cause harm to, or compromise a system. Below are a few common types of malware:

Spyware – This malware is design to track and spy on the user. Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings. Spyware often bundles itself with legitimate software or with Trojan horses.

Adware – Advertising supported software is designed to automatically deliver advertisements. Adware is often installed with some versions of software. Some adware is designed to only deliver advertisements but it is also common for adware to come with spyware.

Bot – From the word robot, a bot is malware designed to automatically perform action, usually online. While most bots are harmless, one increasing use of malicious bots are botnets. Several computers are infected with bots which are programmed to quietly wait for commands provided by the attacker.

Ransomware – This malware is designed to hold a computer system or the data it contains captive until a payment is made. Ransomware usually works by encrypting data in the computer with a key unknown to the user. Some other versions of ransomware can take advantage of specific system vulnerabilities to lock down the system. Ransomware is spread by a downloaded file or some software vulnerability.

Scareware – This is a type of malware designed to persuade the user to take a specific action based on fear. Scareware forges pop-up windows that resemble operating system dialogue windows. These windows convey forged messages stating the system is at risk or needs the execution of a

specific program to return to normal operation. In reality, no problems were assessed or detected and if the user agrees and clears the mentioned program to execute, his or her system will be infected with malware.

Rootkit – This malware is designed to modify the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely. Most rootkits take advantage of software vulnerabilities to perform privilege escalation and modify system files. It is also common for rootkits to modify system forensics and monitoring tools, making them very hard to detect. Often, a computer infected by a rootkit must be wiped and reinstalled.

Virus - A virus is malicious executable code that is attached to other executable files, often legitimate programs. Most viruses require end-user activation and can activate at a specific time or date. Viruses can be harmless and simply display a picture or they can be destructive, such as those that modify or delete data. Viruses can also be programmed to mutate to avoid detection. Most viruses are now spread by USB drives, optical disks, network shares, or email.

Trojan horse - A Trojan horse is malware that carries out malicious operations under the guise of a desired operation. This malicious code exploits the privileges of the user that runs it. Often, Trojans are found in image files, audio files or games. A Trojan horse differs from a virus because it binds itself to non-executable files.

Worms – Worms are malicious code that replicate themselves by independently exploiting vulnerabilities in networks. Worms usually slow

down networks. Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, they no longer require user participation. After a host is infected, the worm is able to spread very quickly over the network. Worms share similar patterns. They all have an enabling vulnerability, a way to propagate themselves, and they all contain a payload.

Worms are responsible for some of the most devastating attacks on the Internet. As shown in Figure 1.

in 2001 the Code Red worm had infected 658 servers. Within 19 hours, the worm had infected over 300,000 servers as shown in Figure 2.

Man-In-The-Middle (MitM) – MitM allows the attacker to take control over a device without the user's knowledge. With that level of access, the attacker can intercept and capture user information before relaying it to its intended destination. MitM attacks are widely used to steal financial information. Many malware and techniques exist to provide attackers with MitM capabilities.

Man-In-The-Mobile (MitMo) – A variation of man-in-middle, MitMo is a type of attack used to take control over a mobile device. When infected, the mobile device can be instructed to exfiltrate user-sensitive information and send it to the attackers. ZeuS, an example of an exploit with MitMo capabilities, allows attackers quietly to capture 2-step verification SMS messages sent to users.

Symptoms of Malware

Regardless of the type of malware a system has been infected with, these are common malware symptoms:

There is an increase in CPU usage.

There is a decrease in computer speed.

The computer freezes or crashes often.

There is a decrease in Web browsing speed.

There are unexplainable problems with network connections.

Files are modified.

Files are deleted.

There is a presence of unknown files, programs, or desktop icons.

There are unknown processes running.

Programs are turning off or reconfiguring themselves.

Email is being sent without the user's knowledge or consent.