Justin Ciocoi

Feb. 15, 2024

CSCI 400 Textbook Notes

Chapter 6: Malicious Software

6.1: Types of Malware

- NIST defines **malware** as a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim

- The below table illustrates some common malware terminology

Name	Description
Advanced persistent threat	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack Kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanisms that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system then to import a larger malware package.
Drive-by download	An attack using code in a compromised web site that exploits a browser vulnerability to attack a client system when the site is viewed.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Coded inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act.
Macro Virus	A type of virus that uses macro or scripting code, typically embedded in a document, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Mobile Code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.

Name	Description
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Spammer Programs	Used to send large volumes of unwanted e-mail.
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data and/or network traffic; or by scanning files on the system for sensitive information.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
Virus	Malware that, when executed, tries to replicate itself into other executable machine or script code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network, usually by exploiting software vulnerabilities in the target system.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.

- **Classification of Malware**
    - Can be classified in terms of method of propagation, or payloads executed

6.2: Advanced Persistent Threats (APTs)

- Advanced Persistent Threats (APTs) are well resourced and consistent application of intrusion technologies and malware
- Usually, APTs are attributed to state-sponsored organizations due to the high amount of resources necessary to carry one out
- They are named as a result of the following characteristics
    - *Advanced*, since attackers will use a wide variety of technologies and even develop custom malware if necessary

    - *Persistent*, since the attack will occur over an extended period of time in order to maximize the chances of success
    - *Threats*, since the attacks pose a high threat to the organizations being attacked
    -

6.3-6.5: Propagation

- Malware propagation can occur in a variety of ways
    - Infection of existing content by viruses that is subsequently spread to other systems
    - Exploit of software vulnerabilities by worms or drive-by-downloads to allow the malware to replicate
    - Social engineering attacks that convince users to bypass security mechanisms to install Trojans or to respond to phishing attacks
- Malware payloads could take on the following forms
    - Corruption of system files or data
    - Theft of service/make the system a zombie agent of attack as part of a botnet
    - Theft of system information or keylogging
    - Stealthing its presence on the system
- **Attack Kits**
    - Initially malware could only be possessed by individuals with high levels of technical skill due to the technical knowledge needed in software development
    - Now, toolkits exist that can be purchased and utilized by novice to launch attacks
    - Toolkits are known as crimeware and several examples exist
        - Zeus
        - Angler
- While in the past, attacks came mostly from individuals, modern attacks are often launched by more organized and resource rich threat actors such as nation states, organized crime groups, and large corporations

- These types of threat actors make way for advanced persistent threats (APTs) where well resourced intrusion campaigns are launched typically by state sponsored organizations
- **Viruses**
    - A virus is a piece of software that infects programs
    - It will modify the program to include a copy of the virus
    - When attached to an executable, a virus is able to do anything that program is allowed to do
    - Viruses are specific to both operating system and hardware
    - A virus is composed of the following
        - Infection mechanisms, or the means by which a virus spreads
        - A trigger, or condition that determines when the payload is activated
        - A payload, which may involve damage or benign but noticeable activity
- **Worms**
    - A worm is a program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
    - Worms generally exploit software vulnerabilities in client or server programs
    - Worms can use network connections to spread from system to system
    - Worms can also spread through shared media
    - Worms can propagate in the following ways

Mechanism	Description
Electronic mail or instant messenger facility	Worm e-mails a copy of itself to other systems. Sends itself as an attachment via an instant message service.
File sharing	Creates a copy of itself or infects a file as a virus on removable media.
Remote execution capability	Worm executes a copy of itself on another system.
Remote file access or transfer capability	Worm uses a remote file access or transfer service to copy itself from one system to the other.
Remote login capability	Worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other.

- This is a table of recent worm attacks

Malware	Year	Description
Melissa	1998	E-mail worm. First to include virus, worm and Trojan in one package.
Code Red	July 2001	Exploited Microsoft IIS bug. Probes random IP addresses. Consumes significant Internet capacity when active.
Code Red II	August 2001	Also targeted Microsoft IIS. Installs a backdoor for access.
Nimda	September 2001	Had worm, virus and mobile code characteristics. Spread using e-mail, Windows shares, Web servers, Web clients, backdoors.
SQL Slammer	Early 2003	Exploited a buffer overflow vulnerability in SQL server. Compact and spread rapidly.
Sobig.F	Late 2003	Exploited open proxy servers to turn infected machines into spam engines.
Mydoom	2004	Mass-mailing e-mail worm. Installed a backdoor in infected machines.
Warezov	2006	Creates executables in system directories. Sends itself as an e-mail attachment. Can disable security related products.
Conficker (Downadup)	November 2008	Exploits a Windows buffer overflow vulnerability. Most widespread infection since SQL Slammer.
Stuxnet	2010	Restricted rate of spread to reduce chance of detection. Targeted industrial systems.

- **Spam**
  - Spam refers to unsolicited bulk email sent by an attacker
  - Some reasons for spam is
    - Phishing attacks
    - Whaling attacks
    - Social Engineering Attacks

        - Trojan Horse Installation

- **Trojan Horses**
    - A Trojan Horse is a piece of malware that masquerades as a legitimate piece of software, either as a malware obscured by that software, or as a malicious portion of that software itself
    - A Trojan Horse falls into one of three models
        - Continuing to perform the original program's function and additionally performing a separate malicious activity
        - Modifying that function such that it will carry out some malicious activity
        - Performing a malicious function that replaces the function of the original program altogether
- **Drive-By Downloads** exploit browser and plugin vulnerabilities in order to download malware from an attacker's webpage without the user's knowledge or consent
- A **Watering Hole Attack** is a drive-by download where the patterns of desired targets is analyzed to find commonly visited webpages and attempt to identify vulnerabilities in these webpages
- **Malvertising** exploits browser vulnerabilities in order to infect user systems with malware when the attacker's advertisement is displayed on a webpage
- **Clickjacking**
    - This is also known as a UI redress attack
    - This attack allows an attacker to collect clicks of an infected users machine
    - In a similar manner, keystrokes can be logged by an attacker in order to steal passwords and other sensitive information

6.6-6.9: Payload

- The next area of concern is what the malware will do on a system once it has propagated and become active
- This action that will be taken is known as the malware's **payload**, and can come in a variety of ways

- **System Corruption**
    - *Data Destruction and Ransomware*
        - Often, the destruction of data is the goal of malware
        - Sometimes, instead of destroying data outright, malware will claim to hold data ransom until a ransom is paid to the attacker
    - *Real-World Damage*
        - Payloads may also cause damage to physical equipment
        - Means of achieving real world damage include things like rewriting BIOS code to alter the boot sequence of the system
    - *Logic Bomb* which refers to a malware who's payload remains inactive until some predetermined condition is met
- **Zombies and Bots**
    - This category of payload redirects a system's computational or network resources such that they can be used by an attacker in an attack
    - When an attacker has a network of infected computers, or **bots**, it is referred to as a **botnet**
    - There are a variety of uses for botnets, including
        - DDoS attacks
        - Spamming
        - Traffic Sniffing
        - Keylogging
        - Spreading New Malware
        - Installing Advertisement Add-Ons
        - Attacking IRC Chat Networks
        - Manipulating Online Polls/Games
- **Information Theft**

    - *Keyloggers and Spyware*
        - Login credentials are typically sent using encryption schemes which protects them from being captured by monitoring packet traffic
        - Keyloggers bypass this protection by directly capturing the keystrokes entered by a user and sending them to the attacker, thus giving the attacker access to unencrypted login credentials that have been entered via a user's keyboard
    - *Phishing and Identity Theft*
        - Phishing attacks present a user with a legitimate looking login site, but one that will send the entered credentials to an attacker rather than the desired entity
        - This usually happens in the form of a spam email that redirects a user to a malicious login page
        - **Spear phishing** refers to sending out mass phishing emails with the expectation that only a few will succeed
- **Backdoors**, which open up channels by which attackers will be able to re-enter the system or network in the future
- **Rootkits**, which are a set of hidden programs maintaining covert access to the system, giving an attacker administrative privileges

6.10: Countermeasures

- The most ideal solution to the threat of malware is prevention, which has four main elements
    - Policy
    - Awareness
    - Vulnerability Mitigation
    - Threat Mitigation
- If prevention fails to stop malware, then several mitigation techniques may be used
    - Detection
    - Identification
    - Removal

- **Anti-Virus Software** has gone through a number of iterations
    - **Simple Scanners** were the first generation, and required a malware signature to detect malware and was limited to the detection of known malware packages
    - **Heuristic Scanners** which use heuristic rules to search for instances of probable malware
    - **Activity Traps** where memory resident programs identify malware based on its actions rather than the structure of the program itself
    - **Full Featured Protection**, where a variety of packages are used to implement all of the above methods of malware detection
- **Sandbox Analysis**
    - Potentially malicious code should always first be run in an emulated sandbox or on a virtual machine
    - This allows the code to be executed in a controlled environment and enables easier detection of malware