FOUNDATIONS IN IT SECURITY: GETTING INTO A SYSTEM

COMPUTER SYSTEMS SECURITY

GORDON | REYNOLDS (2019)

TODAY ….

Today we will overview varies methods used to gain access to a system:

- Stopping Imposters
- Getting in the Backdoor
- Buffer Overflow
- Exploiting the Unknown

GORDON | REYNOLDS (2019)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: OVERVIEW

OVERVIEW

- Today, computer systems are under a constant barrage of attacks with hackers trying to gain access to computer systems.
- In this lecture we will consider,
  - Stopping the imposters
  - Getting in the Backdoor
  - Buffer Overflows
  - Exploiting the unknown

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: STOPPING IMPOSTERS

GORDON | REYNOLDS (2018)

STOPPING IMPOSTERS

- A common way to try and gain access to a system is with the aid of Malware, such as a Trojan.
- Trojan
  - A program that appears innocent but is designed to cause some malicious activity or provide a backdoor to a system.
  - It impersonates something else.

GORDON | REYNOLDS (2018)

STOPPING IMPOSTERS

A comparison of method :

- **Worms & Botnets** propagate without any transport agent.
- **Viruses** require a transport agent, such as an email attachment, to get into a system.
- **Ransomware** uses social engineering to trick users into clicking a link that releases that malware.
- **Trojans** use a wrapper that hides the malware beneath.
- **Trojan variants**, such as multi-function or modular trojans, can perform different functions such as stealing passwords, embedding a rootkit or lunching ransomware.

GORDON | REYNOLDS (2018)

STOPPING IMPOSTERS

- Malware is typically downloaded along side free utilities, apps and games.
- Malicious Website Lookup
  - https://zeltser.com/lookup-malicious-websites/
- Malware Removal
  - https://www.bleepingcomputer.com/tutorials/how-to-remove-a-trojan-virus-worm-or-malware/

GORDON | REYNOLDS (2018)

STOPPING IMPOSTERS

- Good Practice
  - Don't download free programs
  - Think before you click
  - Use anti-malware protection

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: GETTING IN THE BACKDOOR

GETTING IN THE BACKDOOR

- A backdoor is a means to access a computer system that bypasses the system's customary security mechanisms.
- Attackers often use backdoors that they detect or install themselves as part of an exploit.

GORDON | REYNOLDS (2018)

GETTING IN THE BACKDOOR

RootKits

- A rootkit is a collection of programs that can infiltrate a computer system.
- Once a computer system is infiltrated, a rootkit can:
  - Create a backdoor
  - Remain undetected
  - Take control of the system
- Rootkits have been around for decades providing backdoor access into hosts.

GORDON | REYNOLDS (2018)

GETTING IN THE BACKDOOR

- An attacker can use a root kit to gain access to a system and then remain undetected for months or even years.
- Hackers use rootkits to:
  - Monitor Users:
    - Gather intelligence
    - Monitor keystrokes and send information back to a server.
  - Based on the information collected, an attacker can
    - Drill further into a network
    - Leave a logicbomb which can trigger an attack

GORDON | REYNOLDS (2018)

GETTING IN THE BACKDOOR

- Getting a RootKit
  - Lure someone to a website where they can become a victim of a clickjacking attack.
  - Deliver a Trojan via a phishing attack.
  - Obtaining a username and password so they can get into a system to conceal a rootkit.
  - Embedding a rootkit on a removable flash device.

GORDON | REYNOLDS (2018)

GETTING IN THE BACKDOOR

- A RootKit is not a virus and may not have an identifiable signature, so it is able to avoid detection.
- As a result, RootKits are very hard to detect and difficult to remove.

GORDON | REYNOLDS (2018)

GETTING IN THE BACKDOOR

- Good Practice:
  - Strong Passwords
  - Think before you click
  - Use strong spam filters
  - Use anti-malware protection
  - Patch and update when prompted

GORDON | REYNOLDS (2018)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: BUFFER OVERFLOW

BUFFER OVERFLOW

- A buffer overflow is a software vulnerability that allows a process to put more data into a buffer than it can hold.
- A hacker can use this to launch an attack and install malware, spyware or a rootkit on a system.

BUFFER OVERFLOW

- Buffers are areas in memory that are created to hold a finite amount of data.
  - The extra information can overflow and overwrite into adjacent buffers

GORDON | REYNOLDS (2018)

BUFFER OVERFLOW

- Hackers design attacks to take advantage of this vulnerability.
- They write programs to overflow into other areas on the system.
- Possible results of a buffer overflow includes:
  - Core dump
  - System Crash
  - Security Vulnerabilities
- Buffer overflows are common, see software errors blow
  - https://www.sans.org/top25-software-errors/#cat2

GORDON | REYNOLDS (2018)

BUFFER OVERFLOW

- Good Practice:
  - Make sure data execution prevention is active on your system
  - Microsoft does have software to manage this
  - Think before you click
  - Strong spam filters
  - Use browser security

GORDON | REYNOLDS (2018)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: EXPLOITING THE UNKNOWN

GORDON | REYNOLDS (2018)

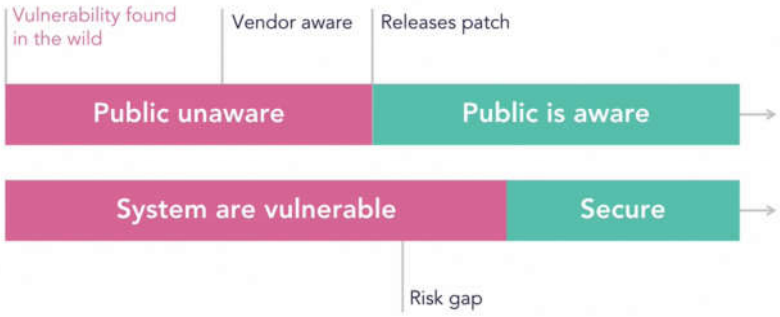
EXPLOITING THE UNKNOWN

- A Zero-Day-Attack takes advantage of a software vulnerability that is unknown or undisclosed by the vendor
- There are a constant barrage of attacks
- Many options are available to protect a system, however, to stop incoming malicious activity, firstly, it must be possible to identify a threat.

- Kaspersky Cyber Map
  - https://cybermap.kaspersky.com/

GORDON | REYNOLDS (2018)

EXPLOITING THE UNKNOWN



GORDON | REYNOLDS (2018)

EXPLOITING THE UNKNOWN

- Anti-malware Protection
  - Malware signatures are used in pattern-based detection and help stop malware
  - The major disadvantage in this type of detection, is that it can not detect unknown attacks.
    - That is, there are no signatures available to use to for detection
  - The one threat that will propose a significant risk to an organisation is a **zero-day-attack**.

GORDON | REYNOLDS (2018)

EXPLOITING THE UNKNOWN

- Best practice:
  - Use anomaly/profile based detection
    - Monitors virus/malware 'like' behaviour
    - Helps detects new and previously unpublished attacks such as zero-day
  - When browsing,
    - Think before you click
    - Apply Updates as required
    - Use tools such as SmartScreen Filter
      - MS cloud-based protection against phishing and malware

GORDON | REYNOLDS (2018)

SUMMARY ….

Today we overviewed varies methods used to gain access to a system:

- Stopping Imposters
- Getting in the Backdoor
- Buffer Overflow
- Exploiting the Unknown

GORDON | REYNOLDS (2019)