IT3789 Cyber Security Attack & Defence

L12 – Maintaining Access

WITH KNOWLEDGE COMES RESPONSIBILITY

Maintaining Access

Trojans & Backdoors

Virus & Worms

RootKit

Convert Channels

Trojan – What is it?

- A malware disguised as a benign program and appears to perform a desirable function for the user.
- Actually designed to allow a hacker remote access to a target computer system and perform operations.
- Is not self-replicating (unlike viruses & worms).

Trojan - What are the damages?

- Operations which could be performed by a hacker on a target computer system includes:
  - Use of the machine as part of a Botnet
    - e.g. To perform distributed denial-of-service (DDoS) attacks
  - Data theft
    - e.g. passwords, security codes, credit card information
  - Installation of software (including other malware)
  - Download/Upload files
  - Manipulate files (Deletion/modification)
  - Run commands remotely
  - Keystroke logging
  - Viewing the user's screen
  - Cause system crashes or slowdown
  - Restart or shutdown infected machines

Backdoor

- A program that a hacker installs on target system to allow access to the system at anytime he requires.
- A backdoor can be embedded within a Trojan.
- The key is to get into the backdoor undetected.
  - Hacker must investigate the system to find services that are running.
  - e.g. Adding a new service in Windows operating system with an inconspicuous name or services that is disabled or needs to be activated manually.

Maintaining Access

Trojans & Backdoors

Virus & Worms

RootKit

Convert Channels

Viruses & Worms

- Once a system is infected, the system is modified to allow a hacker to access system.
- Viruses and worms are usually carriers of Trojans and backdoors.
  - Allows malicious codes such as Trojans and backdoors to be transmitted from system to system.

Viruses & Worms

- Viruses and worms are form of malicious software.
- A virus infects another executable and uses it as a carrier program to spread itself.
  - Virus codes are injected into a benign program.
  - Virus spread when the program executes.
- A worm does not need a carrier program and can self-replicate and spread itself from system to system.

Maintaining Access

Trojans & Backdoors

Virus & Worms

RootKit

Convert Channels

RootKit

- A collection of tools/programs that allow the attacker to mask intrusion.
  - Typically hide files, processes, network connections, blocks of memory and Windows Registry entries.
- RootKit cannot elevate an attacker's privileges before it is installed on the target system.
  - Installation requires the intruder to have root or administrator access.

Five Types of Rootkits

1. Hardware/Firmware
   - Uses device or platform firmware to create a persistent malware image.
2. Hypervisor Level
   - Work by modifying the boot sequence of the machine to load themselves as a hypervisor (virtual machine monitor) under the original operating system.
3. Kernel Level
   - Add additional code and/or replace portions of an operating system, including both the kernel and associated device drivers.

Five Types of Rootkits

4. Library Level
   - Commonly patch or replace system calls with versions that hide information about the attacker.
   - They can be hidden in code libraries, dynamic link library etc.
5. Application Level
   - Replace regular application binaries.
   - May modify the behavior of existing applications using hooks, patches, injected code, or other means.

Maintaining Access

Trojans & Backdoors

Virus & Worms

RootKit

Convert Channels

Encrypted Tunnels

- After a system has been compromised, any activity over remote connection can be detected.
- Setting up encrypted tunnels will prevent detection.
  - e.g. A SSH tunnel allows a hacker to push malware and additional exploits onto the victim machine without being detected as traffic are encrypted.

SSH Tunneling

Local Port-forwarding

- Connections from the SSH client are forwarded via the SSH server, then to a destination server.

Remote Port-forwarding

- Connections from the SSH server are forwarded via the SSH client, then to a destination server.

Dynamic Port-forwarding

- Connections from various programs are forwarded via the SSH client, then via the SSH server, and finally to several destination servers.

Maintaining Access

Trojans & Backdoors

Virus & Worms

RootKit

- Type of RootKits
- Sample RootKit Activities

Encrypted Tunnels & Port Redirection

- SSH Tunneling
- Other Tunnel Options