Threats

Threats

- Danger that might exploit a vulnerability to breach security and cause harm
- Internal threats
- External threats
- Viruses and computer worms are threats caused by intentional, malicious, insider’s human actions that can cause high level of information and resources destruction.
- Terrorism and political warfare are caused by intentional, malicious, outsider’s human actions.
- Passwords change, failing to log off before leaving a workstation, careless discarding of sensitive information are malicious accidental insider human actions

Threats

- Sabotage, data theft, data destruction and spoofing attacks are threats caused by human outsider intentional agents. They caused malicious damage like the corruption of data.
- Wildfire, flooding, earthquakes and tidal waves are caused by accidental external natural phenomena and allow serious impacts like destruction end corruption of data and resources.

Malicious Programs

- Virus
  - Maicious program attached to a program or file
  - Range in severity
  - Cannot infected unless open or run the malicious program
  - Cannot run without a human action
- Worm
  - Similar to virus by design
  - Capability to travel without human action
  - Capability to replicate itself
- Trojan Horse
  - Appears to be a useful software
  - Cause damage once installed or run in computer
  - Create backdoors

Phishing

- Social engineering attack
- Technique by creating a similar web page with the original one with some modifications
- Steals user data including login information, credit card details
- It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.
- The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information
- Often used to gain a foothold in corporate or governmental networks as a part of a larger attack such as APT

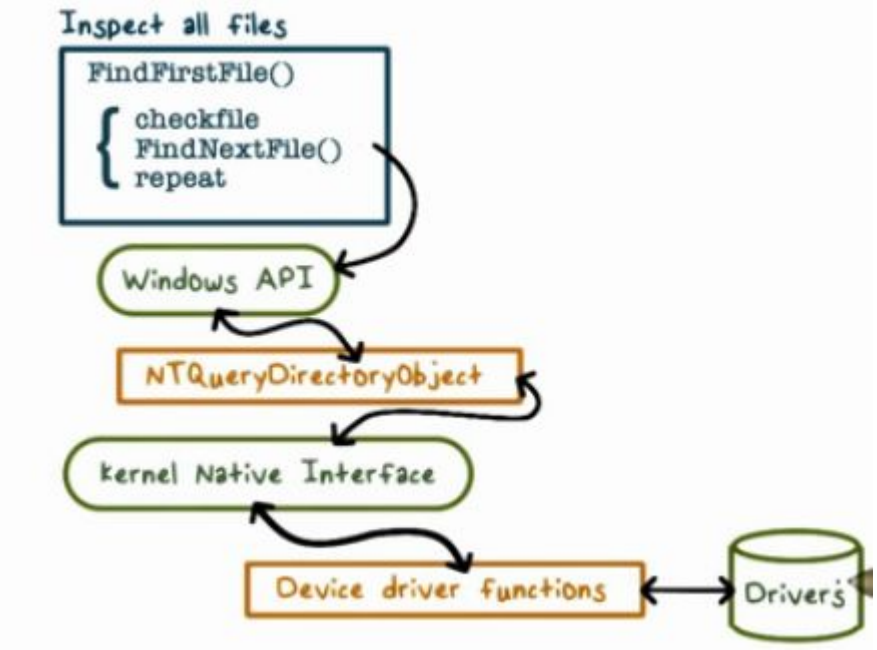
Types of Phishing

- Spear phishing attacks
  - Directed specific individual or company
- Whaling attacks
  - Type of spear phishing attack
  - Specifically target senior executives in an organisation
- Pharming
  - Depends on DNS cache poisoning to redirect users from legitimate site to fraudulent site
  - Email contain either a link or attachment
  - Users previosly delivered legimitate email and done modifications
- Voice phishing
  - Occurs over voice communication media

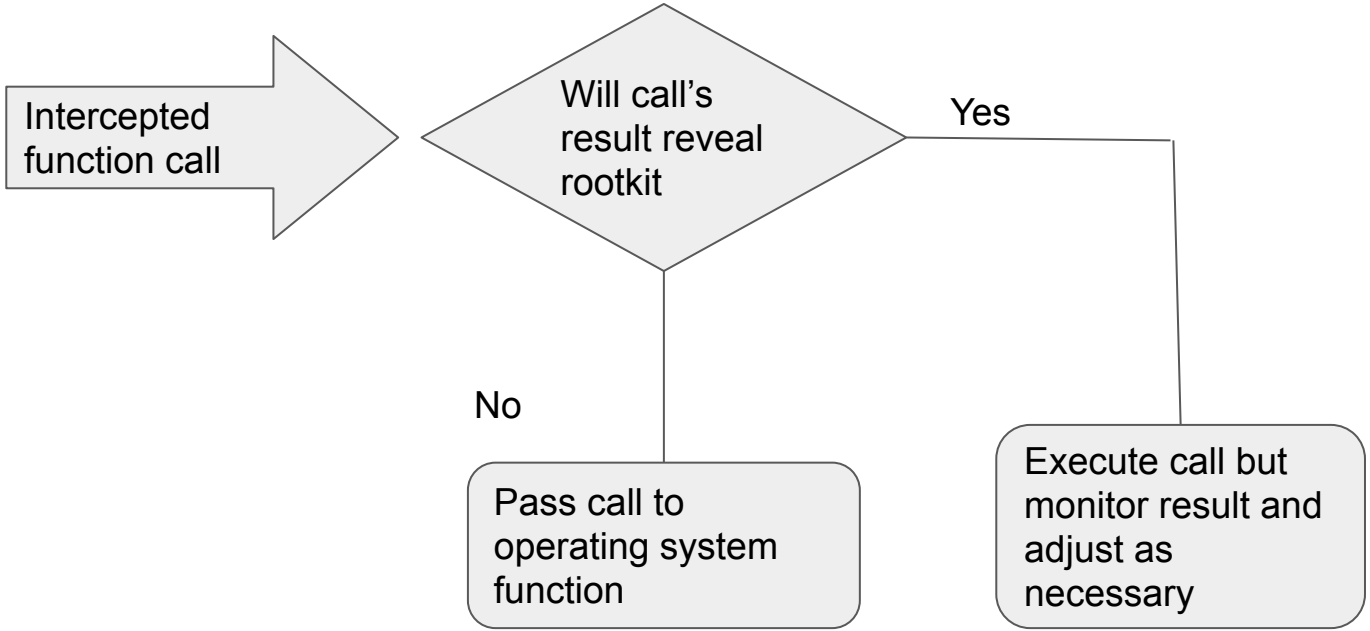
Rootkit

- Set of softwares that have root privilege
- Resides in OS and is persistent
- Modifies OS code and data structure
- Hide it from user (e.g. not listed in ls or ps command)

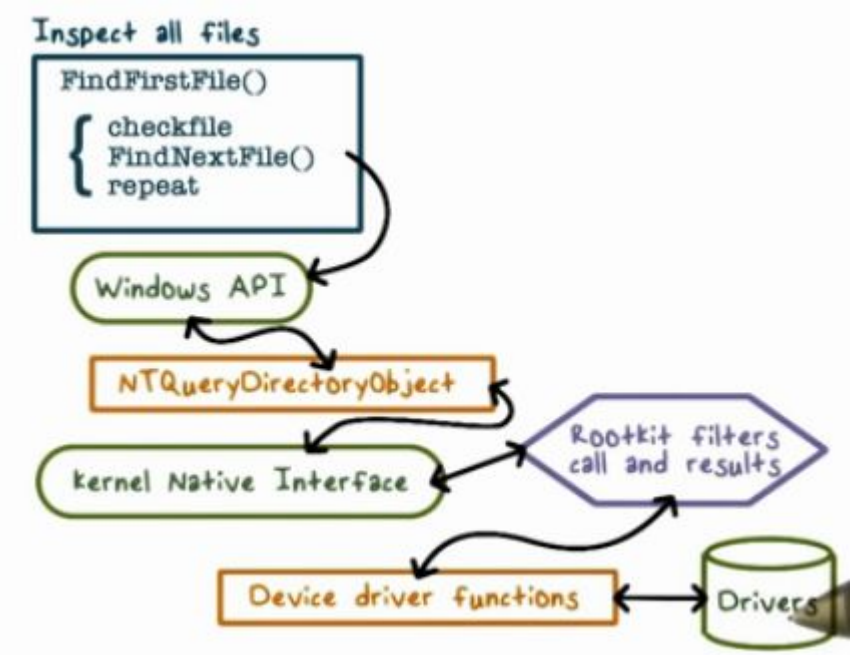
ls command


Inspect all files
FindFirstFile()
checkfile
FindNextFile()
repeat
Windows API
NTQueryDirectoryObject
kernel Native Interface
Device driver functions
Drivers

Rootkit


Intercepted function call
Will call's result reveal rootkit
Yes
No
Pass call to operating system function
Execute call but monitor result and adjust as necessary

Modified ls operation



Botnets

- Collection of interconnected devices that are infected and controlled by a common type of malware
- Bots - infected devices
- Deploy botnets onto computers through a trojan horse
- Can cause denial of service attack