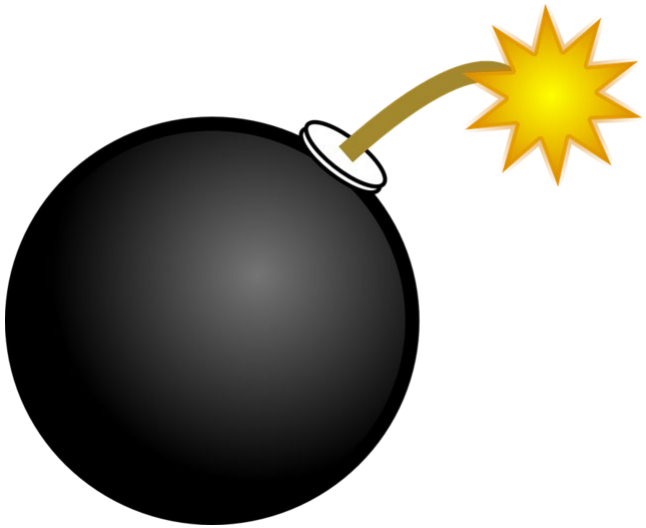
Cybersecurity

Lesson 2.4.6 – Logic Bombs & Rootkits

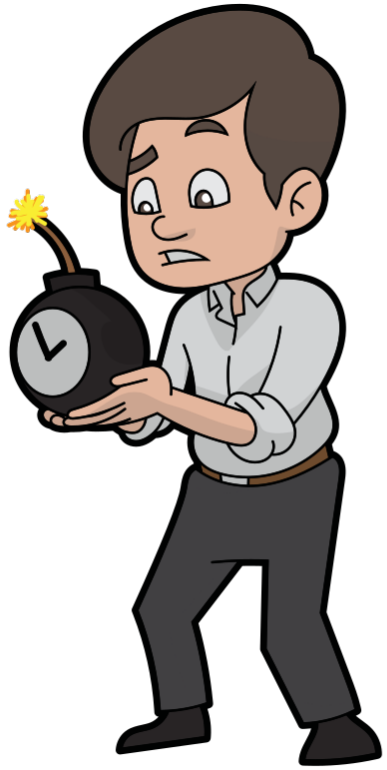
CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Logic Bombs

- A piece of code that waits for a particular set of conditions to be met, referred to as triggers
- Triggers could be
  - Number of transactions
  - Certain system events
  - User interaction
  - Date/time (Referred to as a Time Bomb in this case)
- Once triggered, the program executes
- Often these are installed by an insider threat, such as a disgruntled employee and are setup before leaving and triggered by their removal in the system.



Roger’s Logic Bomb



- In 2002, Roger Duronio successfully deployed a logic bomb against his now former employer, UBS Wealth Management, over a disagreement in his annual bonus leading to two thousand servers crashing and nearly 400 offices being hit.
- An estimated $3.1 million in damages was done and Roger got a new 9x9 home for 8 years as he served his time for computer fraud

Defending Against a Logic Bomb

- Due to their nature, logic bombs are incredibly difficult to identify and are not even active until the triggers have been met.
- Using strong anti-virus software, keeping systems updated, and monitoring system tasks can assist with catching a malicious script or program hidden away.
- Regular backups are crucial for restoring anything lost and in the case of Roger, helped by providing the logs of him accessing the system and setting up the logic bomb.

Rootkits

- Gives the user “root” access
  - root = admin account on Linux/UNIX
  - kit = the necessary software components that implement the tool
- Alters system files
  - Done to hide evidence of its existence
  - Firmware rootkits rewrite part of the BIOS to start before the OS
  - Bootkits replace a system’s bootloader for the same purpose
  - Kernel rootkits replace some of the OS kernel to start at the same time as the OS
  - Driver rootkits pretend to be a trusted driver the OS communicates with – drive shimming

A Rootkit for Everyone

- NTRootkits
  - One of the first rootkits to target the Windows Operating System
- Machiavelli
  - The first rootkit to target Mac OS X, found in 2009
- Stuxnet
  - First known rootkit for industrial control systems (ICS)

More on Stuxnet

- One of the most famous rootkits, found in 2010
- Contains three parts:
  - A worm that executes all routines related to the main payload of the attack
  - A link file that automatically executes propagated copies of the worm
  - A rootkit component responsible for hiding all malicious files and processes to prevent detection.
- Targets supervisory control and data acquisition (SCADA) systems
- Is believed responsible for damage to Iran's nuclear program

Defense Against Rootkits

- Keep your system current with:
  - The latest patches (software updates) against known vulnerabilities
  - Application updates
  - Security software updates
- If available, enable Secure Boot
  - Detects tampering with bootloaders, key operating files, and unauthorized changes in firmware by validating digital signatures.