Cybersecurity

Attacks, Threats, and Vulnerabilities

1.2.7 Logic Bombs

What are logic bombs and how can students defend themselves against them?

Overview

Given a scenario, the student will analyze potential indicators to determine the type of attack.

Grade Level(s)

10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

CYBER.ORG

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 1.2

- Given a scenario, analyze potential indicators to determine the type of attack.
    - Logic bombs

Logic Bombs

A ***logic bomb*** is a piece of code that waits for certain conditions to be met, known as triggers, before it executes, or explodes. Examples of triggers could be a number of transactions processed, a user event, or date in time.

Logic bombs triggered by time are known as time bombs. Time bombs continuously check the system time until a specific date is reached. At the set time, the program executes.

Often, logic bombs are installed by an insider threat. A disgruntled employee can take advantage of their privileged access to computer systems to place a logic bomb before they quit, are fired, or are laid off. The insider can set a logic bomb designed to deploy the moment the employee is removed from payroll or setup a specific logic bomb that can only be “defused” by his or her user account.

The financial services company UBS Paine Webber (now UBS Wealth Management) was the victim of a successfully deployed logic bomb in 2002. A disgruntled employee, Roger Duronio, deployed a logic bomb against UBS Paine Webber after becoming upset due to a dispute over his annual bonus. He installed a logic bomb on two thousand UBS PaineWebber systems, triggered by the date and time of 9:30a.m. on March 4, 2002. This was the day when two thousand of the company’s servers went down, which left about 17,000 brokers across the country unable to make trades. Nearly 400 branch offices were affected. Files were deleted. Backups went down within minutes of being run. The damage caused cost the company over $3.1 million to restore services. Duronio was convicted and sentenced to 8 years in federal prison and banned from working as a systems administrator, network administrator, or computer consultant. In addition, he must pay back UBS the $3.1 million – money he will likely never pay off.

Teacher Notes:

Defense

Logic bombs can be hard to identify, as they are stealthy by nature. Logic bombs, by design, are not active until triggered by a very specific set of conditions. As always, use strong anti-virus software and update it regularly. Keep your operating system up to date and be sure to patch the latest vulnerabilities. Monitor each system's scheduled tasks to ensure a script or some malicious program is not hidden away waiting to execute. Regular system backups will help restore any damages caused by an outage. Such backups were instrumental in pinning Duronio in his court case. Forensics analysts were able to pore over the tape backups to locate not only the logic bomb created but also follow server access logs back to his home computer.