LESSON NOTES

CYBERSECURITY

Domain 2.0 - General Security Concepts

2.4.6 - Logic Bomb & Rootkits

Lesson Overview:

Students will:

- Analyze potential indicators to determine the type of attacks including logic bombs and rootkits.

Guiding Question: What are logic bombs and rootkits and how can enterprises defend themselves against them?

Suggested Grade Levels: 10 - 12

CompTIA Security+ SYO-701 Objective:

2.4 - Given a scenario, analyze indicators of malicious activity

- Malware attacks
  - Logic bomb
  - Rootkit

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
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER
Copyright © 2024 Cyber Innovation Center
All Rights Reserved. Not for Distribution.

Logic Bomb & Rootkits

Logic Bomb

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 a 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 set up 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 9:30 a.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, 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.

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 be executed. Regular system backups will help restore any damage 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.

Rootkit

A ***rootkit*** is a type of malware that provides administrative, or root, access to a computer with a set of tools, or scripts, while also concealing its presence. ***Root*** refers to the admin account on Linux/Unix systems, and ***kit*** refers to the necessary software components that implement the tool. An attacker may use a rootkit to hide or protect other malicious software on a computer system.

Copyright © 2024 Cyber Innovation Center
All Rights Reserved. Not for Distribution.

One of the main roles of a rootkit is to hide any evidence of its existence. Rootkits alter system files and can even alter data reports from a system to avoid detection. This makes rootkits difficult to detect because they are installed in the core operating system of the computer. Rootkits have the ability to block some antivirus software because they activate before an operating system boots up. Antivirus software must use a specific scan to identify rootkits. Some rootkits can remain in place and dormant for long periods of time before they are noticed.

There are different types of rootkits that load during different phases of the startup process. First, firmware rootkits overwrite the firmware of the system's basic input/output system (BIOS) so the rootkit can start before the operating system (OS). Bootkits replace the system's bootloader (the software that starts the operating system), thereby allowing the rootkit to start before the OS. Kernel rootkits replace some of the OS kernel so that the rootkit can start at the same time when the OS loads. Last, driver rootkits pretend to be one of the trusted drivers the OS uses to communicate with PC hardware–sometimes referred to as "driver shimming" (see lesson on Driver Manipulation).

A well-known rootkit is NTRootkits, which was one of the first rootkits that targeted the Windows Operating System. Machiavelli was the first rootkit to target Mac OS X, it was found in 2009. Machiavelli creates hidden system calls and kernel threads. Stuxnet is the first known rootkit for industrial control systems (ICS).

One of the most famous applications of a rootkit is Stuxnet, found in 2010. Stuxnet has three parts: a worm that executes all routines related to the main payload of the attack, a link file that automatically executes the propagated copies of the worm, and a rootkit component responsible for hiding all malicious files and processes to prevent detection. Stuxnet targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran.

Defense

To safeguard your computer system from malware such as rootkits, ensure your system is current with the latest patches (software updates) against known vulnerabilities. Be sure to keep software up-to-date including the operating system, applications, and security software. If available, enable Secure Boot, which detects tampering with bootloaders, key operating system files, and unauthorized changes in firmware by validating digital signatures.

Copyright © 2024 Cyber Innovation Center
All Rights Reserved. Not for Distribution.