Lab 3 Report – Malware Case Study

Student Name: \_\_\_James Jordon \_\_\_  
Date: 2025-09-03  
Course: CYBR-1100 Security Awareness  
Week 3 Assignment

**Case Project 3-3: Infamous Logic Bombs**

Search the Internet for examples of logic bombs. Select three logic bombs and write a report about them. Who was responsible? When did the bombs go off? What was the damage? What was the penalty for the person responsible? Did the organization make any changes after the attack? Is there any way to prevent logic bombs? Write a one-page paper about what you have learned.

# Malware Type

Instructions:

Identify and define the malware discussed in your selected Chapter 3 Case/Hands-On Project.

Response:

\_\_\_I have chosen logic bombs, a piece of malicious code placed into a legitimate program that, when certain conditions are met, create a chain reaction that launches a malicious payload aimed at the hardware, operating system, or network. The main issue with logic bombs is that they remain dormant until activated by certain conditions, contain malicious payload that can cripple or destroy a system, and are built to discharge the malicious payload system-wide when certain parameters are in place (Fruhlinger, 2024). \_\_\_

# Infection Method & Symptoms

Instructions:

Explain how the malware spreads and what symptoms appear on an infected system.

Response:

\_\_\_\_\_\_ According to Fruhlinger (2024), logic bombs can become some of the trickiest malware to locate and terminate as insiders typically can imbed the code into the system compared to a virus or worm that infects the system externally. This means that even stronger malware checkers can miss these malicious codes. Rumor has it, the original logic bomb was, during the Cold War, an actual bomb. According to Rconnon12 (2014), the Soviets were having problems automating a natural gas pipeline deep in Siberia. They had infiltrated an American lab and stolen the software capable of running the pumps, valves, and fans for the system. Little did the Soviets know there was a logic bomb embedded in the software built to reset the parameters of the system, pushing the pressures way above specs. This resulted in one of the largest non-nuclear blasts no one had ever heard of. Or it may have been due to incompetence of one engineer who noticed a leak and pushed the PSI of the system past its capabilities. The first logic bomb documented was the 1982 Pennsylvania software engineer that created a logic bomb to go off in the even of his termination at the insurance company he worked for. According to SAGE AI, he was terminated, logic bomb detonated, shutting down their systems. The most famous example of which in popular culture is the /whiterabbit code Dennis Nedry placed inside Jurassic Park system, crippling it as he committed corporate espionage and stole the dinosaur embryos. The White Rabbit code is considered an example of a user-activated logic bomb. Even GitHub has a logic bomb built into their system that displays a Merry Christmas message every December 25th, showing a time-activated logic bomb.

# Evidence

Instructions:

Insert notes, screenshots, or log excerpts collected during the guided lab.

Response:

**SAGE AI (ChatGPT) Notes on Logic Bombs:**  
A screenshot of a computer

AI-generated content may be incorrect.

**A strong list of famous logic bomb examples, crippling many systems (Fruhlinger, 2024).:**

A screenshot of a computer error

AI-generated content may be incorrect.

A white and black page with black text

AI-generated content may be incorrect.

# Defenses & Mitigations

Instructions:

List at least three concrete defenses or countermeasures.

Response:

\_According to SAGE AI, the best strategies for a logic bomb due to their unstable nature, is prevention, detection, and response. For prevention, you must make sure to let only people that require access to the system in. This reduces the ability for an inside to be where they are not supposed to and upload the code with no one knowing. Second, with the use of endpoint detection & response (EDR) as well as intrusion detection systems (IDS/IPS) to constantly scan your systems for irregularities and monitor them. I would also recommend scanning executables and source code on a regular cycle to check for anomalies. Last, to minimize damage, always make sure to have backups for your systems in case of catastrophic failure as well as testing the backups on a regular basis. SAGE also states that having an incident protocol report and response plan as well as utilizing recovery drills to practice when these scenarios occur will help mitigate the destruction caused by the code.

# NetAcad Linkage

Instructions:

Explain how this connects to NetAcad Modules 2.1–2.2 (Analyzing a Cyber Attack, Methods of Infiltration).

Response:

\_Logic bombs as malware are directly connected to the NetAcad Module as it is imbedded within the software similar to how a backdoor on a legitimate piece of software would have for programming during alpha and beta testing. The key difference would be the logic bomb’s code is malicious and is there to create disruptions if certain criteria are met while backdoors just allow access from another network into the program’s system. As stated, viruses and worms are infected files acting from outside the system looking to gain access and replicate in their respective ways while logic bombs are maliciously placed there by insider programmers looking to damage systems they created or maintained.

# References

Instructions:

Add References here.

Response:

Fruhlinger, J. (2024, July 5). *Logic bombs explained: Definition, examples, prevention*. CSO Online. https://www.csoonline.com/article/510947/logic-bomb.html

rconnon12. (2014, November 24). *The original Logic Bomb*. Cyber Warfare and Terrorism. https://rconnon12.wordpress.com/2014/10/26/third/

\*AI Use Note (if used): I used Sage (ChatGPT) to study and check the authenticity of my sources as well as create concise summaries of my sources and used said screenshots.