Milestone 2 – Part A: Malware Case Analysis

Case Project 3-1: Biological and File-Based Viruses

Amber Radune
CYBR-1100 Security Awareness
Date: 2025-09-07

Case Summary

Case Project 3-1 from Chapter 3 explores the parallels between **biological viruses** and **file-based computer viruses**. The project notes that the word “virus” originally referred to poisonous secretions in living organisms, and later evolved in the field of biology to describe tiny infectious agents that replicate inside cells. Similarly, in computing, the term virus came to describe self-replicating malicious code that attaches itself to host files and spreads across systems. Just as biological science has advanced to detect, classify, and treat viruses with vaccines, cybersecurity uses antivirus software, scanning, and removal techniques to detect and eliminate malicious file-based code (Ciampa, 2022).

Malware Classification & Infiltration Method

A **file-based virus** is classified as a type of **parasitic malware** that embeds itself into executable files, documents, or scripts. When the infected file is opened, the malicious code executes and attempts to spread to other files or systems. Standard infiltration methods include:

- **Email attachments** disguised as legitimate documents.
- **Removable drives/USBs** carrying infected executables.
- **File-sharing platforms** where users download compromised software.
- **Exploiting unpatched software** to inject malicious code into files.

This infiltration mirrors the way biological viruses spread through physical contact, contaminated surfaces, or airborne exposure. In both cases, a “host” is required to replicate and cause harm.

Impact Analysis

If a file-based virus were to infect my chosen community partner—a **local therapy office**—the impact could be significant:

- **Operational Disruption:** Infected systems may slow down, crash, or corrupt files, resulting in interruptions to scheduling, billing, and patient record management.
- **Data Integrity Threats:** Viruses may alter or destroy sensitive electronic health records (EHRs), undermining trust and compliance with HIPAA.
- **Propagation Risk:** Infected files sent via email could spread the virus to patients, insurance partners, or other medical networks, damaging the office's reputation.
- **Financial Losses:** Recovery costs, downtime, and potential fines for data mishandling could strain a small clinic with limited IT resources.

In a therapy office that relies heavily on trust and confidentiality, even a small-scale infection could erode patient confidence.

Mitigation Strategies

To protect against file-based viruses, at least three strong defenses should be implemented:

1. **Regular Antivirus and Endpoint Protection:** Ensure all devices have updated antivirus software capable of scanning and removing file-based threats.
2. **Email Filtering and Awareness Training:** Block suspicious attachments and train staff to recognize phishing attempts and unsafe downloads.
3. **Patch Management and Restricted Permissions:** Keep all software updated and restrict file execution rights to reduce the ability of viruses to spread.
4. **Data Backups:** Maintain secure, encrypted backups of patient records to ensure recovery in case of corruption or loss.

Why This Matters to My Service Learning Project

My service learning project focuses on cybersecurity awareness for a local therapy office. This case directly reinforces the importance of **staff training** and the use of **real-world examples**. Just as vaccines protect against biological viruses, awareness training acts as a “vaccine” for human error. By teaching staff how to avoid suspicious downloads, use portable devices securely, and update software regularly, the therapy office can prevent a file-based virus infection that could compromise patient trust. This case also highlights the importance of **layered defenses**—technology (antivirus and patches) paired with human awareness.

Works Cited

Ciampa, M. (2022). *Security Awareness: Applying Practical Security in Your World* (7th ed.). Cengage Learning.

Cisco Networking Academy. (n.d.). *Introduction to Cybersecurity*. Modules 2.1–2.2. Retrieved from https://www.netacad.com

Kaspersky. (2023). *What is a computer virus?* Retrieved from https://www.kaspersky.com/resource-center/threats/computer-viruses