**Malware**

Student’s Name:

Institution:

Course:

Professor:

Date:

**Malware**

**Overview**

Finance Ventures is a microfinance institution that aids low and moderate-income households, immigrants, and the vulnerable population to access loans and saving services. The company needs a cybersecurity expert because of the recurring malware attacks in the past five months. This is an interference of the computer system to allow unauthorized data access, distortion, and manipulation. The Trojans and virus malware were the main concern at the institution. They enabled the attackers to exploit and modify critical data without the authority of a legitimate user (Kara, 2019). Similarly, the virus attacks introduced programs and codes that corrupt and erase clients’ personal information. For this reason, the Finance Ventures Company hired my services and expertise to address the cybersecurity issue. This is inspired by the institution’s role and mandate to protect clients’ personal information and sensitive financial data. Malware attacks expose the institution to legal and ethical implications accompanied by hefty fines and litigation.

**Details of the Malware**

The institution has been battling malware attacks in the past five months. The first incident involved Trojan malware, where a harmful software code disguised as valid software infects the device. It enabled the attackers to access personal financial information for different clients at the Finance Ventures microfinance. As a result, the malicious software increased the risks of data deletion and manipulation. It also causes data stealing and disrupts the institution's performance (Ghillani & Gillani, 2022). The second incidence involved virus malware entailing malicious software that causes file duplication and deletion without the help of a legitimate user. This program undergoes self-replication to corrupt websites, storage devices, and downloads (Kara, 2019). In some circumstances, individuals may fail to recover corrupted files and data. This is a critical issue at the institution that requires immediate interventions to protect clients' financial records.

**The Exploited Vulnerabilities and its Attack Vector**

The institution displays multiple vulnerabilities that act as the access point to malware attacks. These loopholes enable cybercriminals to run malicious codes and software in the computer system. The Finance Ventures organization identifies its various cyber-security weaknesses in its computer hardware, software, network, and personnel. The hardware susceptibility concerns poor encryption and dust. This impacts the effective functioning of the computer system during data entry and transmission. Secondly, software vulnerabilities entail design flaws, input validation errors, and privilege-confusion bugs (Ghillani & Gillani, 2022). The institution records evidence of damages in the operating system (OS) that hinder efficiency during transactions and access to clients’ financial information. It also permits unauthorized modification and manipulation of personal data. It also demonstrates evidence of hidden backdoor programs, which is a critical weakness in its operating system.

Furthermore, the Finance Ventures Company has network vulnerabilities that expose its computer system to unauthorized external access. It constitutes an insecure network architecture that is susceptible to hacking and illegal entry (Wazid et al., 2019). Similarly, it reveals evidence of insecure communication lines and lacks authentication to guarantee data security. The typical examples of network weaknesses at the institution entail poorly-configured firewalls and insecure Wi-Fi access points. Lastly, personnel vulnerabilities are critical aspects that increase the risk of Malware attacks at the Finance Ventures Company. This entails the human element that exposes clients’ personal information to unauthorized persons. For instance, most employees displayed limited awareness and understanding of data security issues. Similarly, some fail to comply with the security training requirements and regulations. Furthermore, personnel vulnerabilities entail poor password management that results in unauthorized access to personal information by external parties.

**Two Risks of this Malware**

The Trojans and virus malware pose two critical risks at the institution. First, they result in file deletion and manipulation by unauthorized persons or corrupted software. The Trojans form a replica of valid software that infects the computer system. Besides, the virus duplicates files and data to corrupt websites and storage devices (Wazid et al., 2019). This type of malware enables illegal access to personal information within the network. As a result, clients' data is at risk of modification and loss if the computer and other devices contract malware. Secondly, malware attacks in the institution expose the computer system to severe damage. The viruses introduce malicious software and files that affect the effective functioning of the operating system (OS). Similarly, they hinder communication and coordination of activities between different departments at the institution. This increases the risk of losing their savings and financial information from the Finance Ventures Company.

**Step-by-Step Instruction to Resolve the Malware Attacks**

The management must adopt the appropriate strategies to resolve recurring malware attacks. First, the team must isolate the affected parts to mitigate the spread of malware to other regions. Secondly, the management must identify the type of malware strain affecting the computer system (Densham, 2015). This is essential for adopting an effective plan to address the issue. Thirdly, the team must report the malware attacks to relevant stakeholders for assistance. This ensures the institution coordinates the counterattack measures. Fourthly, the management must assess and identify alternatives and diverse options that offer desired solutions to the malware attacks. This requires them to settle for the best intervention. Fifthly, the management should restore and refresh its computer system after adopting the best alternative. This is an integral element of disaster recovery and continuity plans. Lastly, the team must plan for intervention to address the malware attacks.

References

Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security*, *2015*(1), 5–8. <https://doi.org/10.1016/s1353-4858(15)70007-3>

Ghillani, D., & Gillani, D. H. (2022). *A perspective study on Malware detection and protection, A review*. <https://doi.org/10.22541/au.166308976.63086986/v1>

Kara, I. (2019). A basic malware analysis method. *Computer Fraud & Security*, *2019*(6), 11–19. <https://doi.org/10.1016/s1361-3723(19)30064-8>

Wazid, M., Das, A., Rodrigues, J., Shetty, S., Park, Y., & Kumar Das, A. (2019). *IoMT Malware Detection Approaches: Analysis and Research IoMT Malware Detection Approaches: Analysis and Research Challenges Challenges Part of the Databases and Information Systems Commons, Digital Communications and Networking Commons, Electrical and Electronics Commons, and the Theory and Algorithms Commons SPECIAL SECTION ON DEEP LEARNING ALGORITHMS FOR INTERNET OF MEDICAL THINGS IoMT Malware Detection Approaches: Analysis and Research Challenges*. *7*. <https://doi.org/10.1109/ACCESS.2019.2960412>