**MALWARE INFECTION METHODS ANALYSIS**

Santhosh Reddy Miriyala

Masters of Science in Cyber Security

Cybersecurity foundation

Dr.Dadmehr Rahbari

09-02-2023

**MALWARE INFECTION METHODS ANALYSIS**

**ABSTRACT**

The research investigates three primary approaches that malware developers take when attempting to infect computer systems. Phishing, drive-by downloads, and social engineering were the techniques that were used. The use of a survey in addition to questionnaires was part of the mixed technique that was applied in this study. According to the findings, phishing accounts for an even larger percentage (80%) of the systems that cybercriminals try to break into. Drive-by downloads and social engineering accounted for the remaining twenty percent of the attack vectors. Because of this, it became necessary to put the appropriate safeguards in place, such as educating the users, setting harder passwords, and putting up firewall protectors, in order to slow the rate at which attacks were being carried out.

**OBJECTIVES:**

### **1. Phishing**

**Attack Vector:** Phishing attacks primarily leverage electronic communication channels such as email, social media platforms, and instant messaging. Attackers often masquerade as legitimate entities to deceive users into taking actions that compromise their security.

**Entry Points**: Users are typically targeted through phishing emails containing malicious links or attachments, which, when interacted with, trigger malware downloads or unauthorized access.

**Effectiveness:** Phishing campaigns rely on exploiting human psychology and user trust, yielding a moderate level of success.

**User Vulnerability:** Users vulnerable to phishing are often unaware of common tactics and may overlook red flags due to a lack of cybersecurity awareness.

**Consequences:** Successful phishing attacks can result in unauthorized access to accounts, financial losses, data breaches, and identity theft.

**Mitigation:** Effective mitigation strategies (Mansfield-Devine, 2012) include user education campaigns, email content filtering, and the implementation of multi-factor authentication to bolster security.

### **2. Drive-By Downloads**

**Attack Vector**: Drive-by download attacks target vulnerabilities in web browsers and compromised websites. Malicious code is automatically downloaded and executed when users visit compromised sites, often without their knowledge.

**Entry Points:** Users are exposed to drive-by downloads while visiting compromised websites, clicking on malicious ads, or interacting with content containing hidden exploits.

**Effectiveness:** Drive-by downloads leverage security weaknesses, making them highly effective for the rapid dissemination of malware across a large number of systems.

**User Vulnerability:** Users with outdated software, unpatched systems, and lacking security measures are particularly susceptible to drive-by download infections.

**Consequences:** Drive-by downloads lead to the stealthy installation of malware, unauthorized data access, system instability, and potential loss of control over compromised devices.

**Mitigation:** Consistently updating software and operating systems, employing browser security plugins, and using ad-blockers can significantly reduce the risk of drive-by download infections.

### **3. Social Engineering**

**Attack Vector**: Social engineering manipulates human behavior and emotions to trick individuals into divulging confidential information or performing actions detrimental to their security.

**Entry Points:** Attackers exploit trust, urgency, and familiarity, employing tactics such as impersonation, pretexting, or baiting to deceive individuals.

**Effectiveness:** Social engineering's effectiveness varies based on an attacker's ability to understand human psychology, exploit emotions, and create a false sense of urgency.

**User Vulnerability:** Users susceptible to social engineering often exhibit a lack of skepticism, making them prone to emotional manipulation and divulging sensitive information.

**Consequences:** Successful social engineering attacks can lead to unauthorized access to secure systems, the compromise of confidential data, and unauthorized transactions.

**Mitigation:** Implementing robust verification protocols, promoting critical thinking and skepticism, and enforcing access controls can mitigate the risk of social engineering attacks.

**INTRODUCTION**

The development in technology usage has given rise to different forms of malware attacks on devices. There are different infection methods that are used by the attackers so that they manage to reach out to the intended parties. This study will focus on three major infection methods: phishing, drive-in downloads and social engineering. The study will unveil the attack vectors, user vulnerability, consequences and the most effective ways of preventing them

**LITERATURE REVIEW:**

Infection with malware has become a greater hazard to the operation of most digital devices, particularly those that hold essential data. Qamar et al. (2019) clarify that the target is primarily on those devices that have personal information that can be utilized to the profit of the attackers. The phrase "can be used for the benefits of the attackers" is key here. According to Rudd et al. (2016), there are already people and organizations that have been compromised by the attacks. They obtain this by either downloading files that are infected or enabling unauthorized emails to login on their computers. Both of these methods result in the same outcome. (Rakotondravony et al., 2017) reports that as a direct consequence of this, not only a significant amount of information but also significant sums of money are thrown away. Malware attacks typically target demographics that are not very knowledgeable about the usage of technical equipment and also individuals that have passwords that are not very secure (Kara & Aydos, 2022).

**METHODOLOGY:**

In order to learn more about the subject of the study, the researchers decided to conduct the investigation using a quantitative technique throughout the whole thing. The primary focus was on various reports coming from companies and individuals who have been affected by the malware attacks. These reports came from all around the world. As a result of this, a survey was conducted on the information that had been documented in various situations, including the means by which infection had taken place and the results that had been obtained. There was also the quantitative method, which centered on the use of questionnaires that were distributed to various people in order to elicit more information regarding the manner in which they were involved in the attacks. A comprehensive study on the various ways that malware can infect a system was produced by compiling all of this material. The benefit of using a mixed technique is an increase in the overall amount of data that was obtained, which is a significant advantage. Because of this, arriving at the most appropriate conclusion regarding the matter was a simple task.

**RESULTS:**

Phishing was identified as the method of attack utilized by 80% of the parties whose systems were breached during the incident. They were sent emails that appeared to be trusted credentials, and when those emails were opened, the attackers obtained access to the data store in the systems that were being targeted. In addition, there were messages that needed an immediate reaction from the users. They did not raise any red flags at any time, and as a result, they were able to successfully get access to the system. According to the results of the survey, 20% of the systems were infected as a direct result of the downloading of malicious software.

**CONCLUSION:**

There is an urgent need to put in place the appropriate risk mitigation measures, particularly in light of the impacts that have been recognized as a result of malware assaults. The installation of more secure passwords in addition to the use of a firewall can be helpful in bringing down the total number of users who have access to the system at any given time. In addition, it is essential to educate users on the existence of the attacks so that they do not become victims of the fraudulent e-mails and messages that prepare the way for the attacks. These fraudulent e-mails and messages are what pave the way for the attacks.

**REFERENCES:**

Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for windows-based ransomware attacks. *Expert Systems with Applications*, *190*, 116198.

Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems*, *97*, 887-909.

Rakotondravony, N., Taubmann, B., Mandarawi, W., Weishaupl, E., Xu, P., Kolosnjaji, B., ... & Reiser, H. P. (2017). Classifying malware attacks in IaaS cloud environments. *Journal of Cloud Computing*, *6*, 1-12.

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks-a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013.

Rudd, E. M., Rozsa, A., Günther, M., & Boult, T. E. (2016). A survey of stealth malware attacks, mitigation measures, and steps toward autonomous open world solutions. *IEEE Communications Surveys & Tutorials*, *19*(2), 1145-1172.