**Malicious Apps in The App Store and How They Are Effecting Our Security**

Nuriddin Mirodilov

George Mason University

IT 104- Introduction to Computing

Eugene Lord, Ph.D., PMP

2/18/2024

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://catalog.gmu.edu/policies/honor-code-system/ and as stated, I as a student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of 2 text, any material copied directly from a web page, and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on https://universitypolicy.gmu.edu/policies/responsible-use-of-computing/ website."

**Introduction**

The proliferation of malicious apps in app stores poses a significant threat to user privacy and security, raising concerns about the integrity of digital ecosystems. As highlighted by Messmer (2011), "More malware apps sneak into Google Market: 25 malicious apps are yanked from Google Market, security firm says." This underscores the growing prevalence of malicious apps disguised as legitimate applications, which can compromise the personal data and device security of unsuspecting users.

**Current Use**

Currently, app store scanning systems implemented by companies like Google and Apple serve as the first line of defense against malicious apps. However, as highlighted by Wolf (2023), "Android/Xamalicious trojans are apps related to health, games, horoscope, and productivity,” warns McAfee." This quote underscores the deceptive tactics employed by malicious apps to evade detection by automated scanning systems, posing a significant challenge to user security. Despite efforts to remove malicious apps from official app stores, they may still proliferate through third-party marketplaces, exposing users to potential data breaches and security risks.

**Legal Aspects**

From a legal standpoint, the distribution of malicious apps raises questions about liability and accountability for app developers and platform operators. As noted by ProQuest (2022), "YOU can't order at the bar, sit down and we'll bring the drinks over,' said the landlady of a Cornish pub I visited during the height of the Covid crisis.

I was told to use my mobile to scan a barcode stuck to the table. This would allow me to read the menu online. But first I had to add something called a QR reader to my smartphone. I did this in a rush, got my drinks, and haven't thought about it since. Until now that is. Earlier this month, a fraud expert told me a rogue QR reader had been found lurking in the Google Play store, where mobile apps are made available." This highlights the ease with which users can inadvertently download malicious apps, often without understanding the potential risks involved. While app store operators have implemented policies and procedures to mitigate the spread of malicious apps, the dynamic nature of cybersecurity threats necessitates ongoing legal and regulatory efforts to address emerging challenges and protect user rights.

**Security aspects**

The presence of malicious apps poses significant security risks to both individual users and organizations. According to Akram (2023), "The Xamalicious apps are disguised as health, games, horoscope, and productivity apps but actually contain a backdoor designed to trick users into granting accessibility privileges." This quote underscores the deceptive tactics employed by malicious apps to gain unauthorized access to sensitive user data and device features. Once installed, malicious apps can exploit vulnerabilities in the operating system to steal personal information, track user activities, and facilitate unauthorized access to corporate networks. As such, addressing the security implications of malicious apps requires a multi-faceted approach that combines technological solutions, user education, and regulatory measures to mitigate risks and safeguard digital assets.

**Ethical Concerns**

The proliferation of malicious apps in app stores raises significant ethical concerns regarding user trust, autonomy, and the responsible handling of personal data. As emphasized by Wolf (2023), "The presence of malicious apps underscores the importance of understanding the risks associated with app usage." This highlights the ethical imperative to prioritize user security and privacy, emphasizing the importance of ethical considerations in app development and distribution. In addition to the ethical considerations surrounding user trust and autonomy, the proliferation of malicious apps also raises broader ethical questions about the societal impact of cybercrime and digital exploitation. Addressing these ethical concerns requires collaborative efforts from stakeholders across the technology industry, government, academia, and civil society to promote ethical app development practices, enhance cybersecurity awareness, and advocate for stronger regulatory safeguards.

**Bibliography (Reference in APA style and annotation\*):**

(1) ProQuest | Better Research, Better Learning, better insights. The malicious apps that become spies inside your phone: We happily download apps for everything from games to fitness. But now fraud experts warn that some may have installed spyware that could cost you thousands. (2022, May 18). https://www.proquest.com/pqrl/docview/2665469360/8360759559C7435EPQ/3?accountid=14541&sourcetype=Newspapers

This article discusses the growing threat of malicious apps that infiltrate mobile devices, posing as harmless utilities or games while actually spying on users and stealing sensitive information, such as banking credentials. The author recounts a personal experience with QR code scanning in a pub, highlighting how easily users can unknowingly download malicious software. The article warns about recent discoveries of infected apps on Google Play, emphasizing that although these apps have been removed, users remain unaware of the risks to their data. It explains the tactics of fraudsters, who create seemingly legitimate apps before infecting them with malware to gain unauthorized access to personal information. The article also discusses efforts by banks and cybersecurity firms to combat fraud, including the development of advanced detection technologies to identify suspicious activities and protect customers from financial losses. It concludes with recommendations for users to exercise caution when downloading apps and to rely on established apps with a significant user base for enhanced security.

(2) Messmer, E. (2011, May 31). ProQuest | Better Research, Better Learning, better insights. More malware apps sneak into Google Market: 25 malicious apps are yanked from Google Market, security firm says. https://www.proquest.com/pqrl/docview/870318442/8360759559C7435EPQ/2?accountid=14541&sourcetype=Trade%20Journals

Lookout Mobile Security reported that approximately 25 malicious apps, collectively termed "Droid Dream Light," were identified and removed from the Google Market by Google. These apps, disguised as legitimate applications, managed to infect an estimated 30,000 to 120,000 users before their true nature was discovered. Some of the infected applications mentioned include "Magic Photo Studio," "Mango Studio," "E.T. Tean," and "BeeGoo." Notably, the malicious components of these apps do not require manual launch to initiate their harmful activities. This incident follows a previous attack known as "DroidDream" in March, during which over 50 malicious apps were found on the Google Market, leading to increased concerns among Google Android users and the security community. Google has expressed its commitment to preventing such incidents in the future.

(3) Bennett, Coleman & Company Limited. (2023, July 10). ProQuest | Better Research, Better Learning, better insights. PERMISSION OVERLOAD: HOW APPS RISK PRIVACY [Times City]: “More Than 425 Malicious Apps Removed From App Stores.” https://www.proquest.com/pqrl/docview/2834828368/citation/8360759559C7435EPQ/1?accountid=14541&sourcetype=Newspapers

This article from The Times of India highlights the risks associated with downloading and using certain mobile apps, particularly those that request excessive permissions and pose threats to user privacy and security. Forensic experts from the Cybercell of Gujarat CID discussed the dangers of malicious apps during a cyber awareness session called 'Hacked', co-organized by TOI and the Cybercell.

The CID sleuths revealed that over the past year, they have removed 425 such malicious apps from app stores. These apps typically request multiple permissions from users, with many of them classified as "dangerous" by mobile platforms' permission systems. For instance, they may request permission to access external storage, camera, and SMS messages, potentially compromising sensitive data without users' knowledge.

The article also highlights the use of cleartext network traffic by these apps, which exposes users to various security threats such as eavesdropping and identity theft. Residents who attended the session expressed concerns about cybercriminal tactics and emphasized the importance of practicing good cyber hygiene to prevent such crimes.

4) Wolf, A. (2023, February 7). *What Are Malicious Apps?* Arctic Wolf. https://arcticwolf.com/resources/glossary/malicious-apps/#:~:text=Malicious%20apps%20are%20a%20method

This text provides an overview of malicious apps, their characteristics, and tips for users to avoid them. It defines malicious apps as tools used by cybercriminals to deceive users into downloading malware, potentially leading to the theft of personal information or control over the user's device. The text warns that while malicious apps are commonly found in third-party app stores, they can also infiltrate official stores like Apple's App Store and Google Play.

To avoid downloading malicious apps, users are advised to be cautious of apps with names, images, or descriptions resembling popular or legitimate ones. Additionally, they should be wary of fake reviews meant to boost the credibility of malicious apps. The text highlights that some malicious apps may remain dormant until triggered, and updating them could activate harmful features.

Signs indicating the presence of a malicious app include persistent pop-up ads, unauthorized app installations, rapid battery drain, and device slowdowns. To combat malicious apps, users are encouraged to check app developers and reviews, restrict unnecessary permissions, uninstall unused apps, and download apps only from reputable developers. Additionally, users should be vigilant for mentions of scams or malicious activities in app reviews by other users.

5)Akram, Z. (2023, April 25). Delete These 19 Malicious Android Apps Now! Gizchina.com. <https://www.gizchina.com/2023/04/25/delete-these-19-malicious-android-apps-now/>

his article warns users about 19 malicious Android apps that have been identified as threats by an anti-malware company, urging immediate deletion to prevent potential data theft or ransom demands. It emphasizes that Android devices are more susceptible to hacking compared to iOS devices and that cybercriminals often exploit this vulnerability through malicious apps containing adware, spyware, and trojans.

The text explains that these malicious apps can infiltrate users' devices by downloading legitimate apps from the Google Play Store, injecting malicious code, and then re-uploading them under new names. Common types of Android app malware mentioned include Autolycos, Joker spyware, and Harly Trojan, each with specific malicious functionalities such as collecting contact lists, SMS messages, or registering devices for premium services without consent.

6) Doffman, Z. (n.d.). Serious New Google Android Warning—Delete These 13 “Malicious” Apps Now. Forbes. Retrieved February 11, 2024, from https://www.forbes.com/sites/zakdoffman/2023/12/28/new-google-android-and-chrome-warning-for-malicious-threats-hiding-on-phones/?sh=70009c804614

This article serves as a warning to Android users about 13 malicious apps, collectively referred to as "Xamalicious," recently discovered on the Google Play Store. The author emphasizes the importance of users taking responsibility for their device security and not solely relying on Google and Apple for protection.

The Xamalicious apps are disguised as health, games, horoscope, and productivity apps but actually contain a backdoor designed to trick users into granting accessibility privileges. These privileges allow the apps to take control of device features, potentially compromising user security. Although Google has removed these apps from its store, they may still be available for download from third-party marketplaces.

The article highlights another recent accessibility warning regarding the "Chameleon" trojan, which similarly exploits accessibility requests to compromise devices' biometric security and steal financial information.

Users are urged to delete the Xamalicious apps listed in the article immediately, as banning an app from the Play Store does not automatically remove it from users' devices. The author stresses the importance of being cautious about granting accessibility privileges to any app, especially those from third-party sources, and advises users to regularly review and revoke app permissions in their device settings to maintain security.