Applications designed to steal Facebook login information: a case study

Akshata Lolayekar

CY5010 Foundations of Information Assurance

November 10, 2022

Abstract

Facebook is known to have privacy concerns and be involved in legal battles for over a decade. They had their first privacy issue in December of 2007 when a third-party service used Facebook data to track users' purchase activity, without getting permission from the user. Since then, Facebook has had over 19 incidents of interest. Meta recently released a list of malicious applications that may have compromised login credentials of up to 1 million users. This data was based up on security research spanning one year, and the applications were shortly removed from the app stores. Meta also released resources outlining attack vectors and prevention techniques.

Keywords: 2022 Meta Data Breach, Login Information Theft, Account Compromise

Introduction

On October 7th 2022, David Agranovich, Director of Threat Disruption along with Ryan Victory, Malware Discovery and Detection Engineer released a statement warning roughy 1 million Facebook users that their login credentials may have been compromised through third-party applications. Facebook's parent company Meta stated that security researchers had found more than 400 malicious Android as well as iOS mobile applications that were designed in a way that they were able to connect users' Facebook accounts to the applications. These applications stole user login credentials resulting in account compromise. On notification from Meta, Apple's app store and Google's play store removed the applications and the users were notified of the potential account compromise. Over the next few weeks, Meta security researched studied the attack vectors and reported on different ways that users can follow to recover and prevent account takeovers. This paper studies the case in detail, outlining exactly how the malicious applications were able to steal Facebook login information and potentially use it. The case study also details the detection, exploitation, response and impact caused.

Attack Development

Mobile application statistics for the year 2022 state that out of 6.3 billion mobile phone users, 21% millennials open an application 50+ times a day. Gaming and lifestyle applications specifically have become highly popular today. Attackers use this vector to create and design applications that steal user login information which is then used to login and access personal information. In this case, a total of 402 malicious applications were found: 355 Android and 47 iOS apps. These applications were disguised as photo editors, games, VPN services, business apps, and other utilities. The applications hijacked the credentials along with any two-factor authentication codes and stored them on private servers. There was no clear source determined and the motive of the attack was to steal user data.

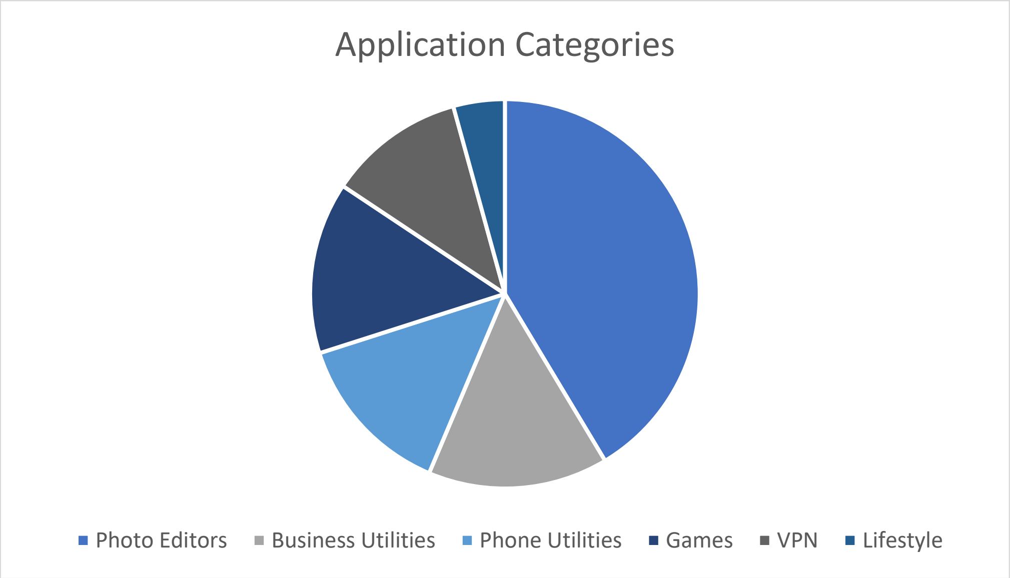


Figure 1.1 Application Categories

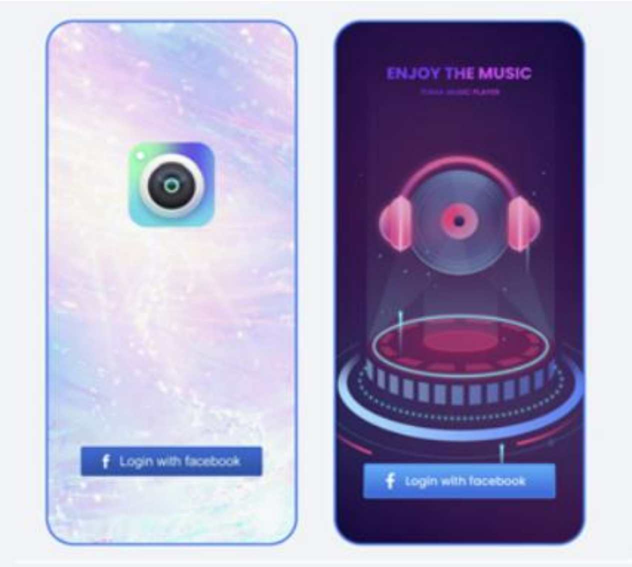
The malicious applications were found over the year 2022 and were taken down in the month of October. This event results in two speculations; has user data including login information and personal data been exploited over the period of the entire year or more?

Secondly, how is breached PII being recovered or compensated for? Meta advised users to change passwords and delete any third-party applications that may look suspicious. The statement indicates that there may be more malicious applications yet to be discovered.

Attack Techniques:

1. Masquerade: The applications gained user trust by imitating commonly used applications in utility and lifestyle categories.
2. Phishing: The applications asked the users to login using their Facebook credentials to avail some kind of points or benefits, phishing users into logging in to bypass certain limits.
3. Social Engineering: Fake reviews were posted to offset negative reviews and change rating.
4. Malware: Under the normally functioning application, attackers embed malware that collect social media credentials.

Figure 1.2 Login Prompt



According to Malwarebytes lab, malware is stored as, for example, Android/Trojan.Spy.Facestealer and arrives as an app disguised as a useful utility. Meta said that these applications were reported to industry peers, security researchers and policymakers to enable further research and update security policies. Exact detection methods are not shared publicly, however application package names/iOS application IDs along with threat indicators are shared on the official blog post.

MITRE Attack Technique Mapping

1. [Reconnaissance] Phishing for Information: Spear phishing Service- Phishing by imitating to be legitimate utility applications offering services using Facebook login.
2. [Reconnaissance] Gather Victim Identity Information: Credentials- Collecting credentials inputted into the application.
3. [Resource Development] Compromise Accounts: Social Media Accounts- Facebook account takeover and misuse.
4. [Resource Development] Develop Capabilities: Malware- Developing applications with inbuilt malware designed to steal credentials.
5. [Defense Evasion] Masquerading: Masquerade Task or Service- Imitating popular photoshop or VPN applications
6. [Exfiltration] Automated Exfiltration- Transferring collected user information to private server for misuse.
7. [Impact] Account Access Removal- Password resetting to prevent legitimate users from accessing their account.

Response, recovery actions and impact

Security researchers from Meta had been working on finding and compiling a single list of malicious applications from around one year. As soon as the list was released, Meta notified and requested Apple and Google to remove the applications from the respective app stores. Apple & Google have released statements and confirmed the removal of the applications. David Agranovich, Meta's director of threat disruption, told reporters that it's impossible for his team to determine the exact number of Facebook users who fell for this scam since the attack happened on their personal devices.

Meta sent out notifications to all the potential victims of the attack and asked them to reset credentials, set log-in alerts and activate two-factor authentication. They further asked users to be delete any suspicious applications and avoid downloading any third-party applications. Meta asked users to pay attention to the following 3 questions to determine if an application is legitimate or not:

1. Is the app unusable if you don't provide your Facebook information?
2. Is the app reputable?
3. Does the app provide the functionality it says it will, either before or after logging in?

The exact impact of the attack is unknown and difficult to calculate. However, the rough figure of 1 million users displays that this case is a critical find and may have played a silent part in PII leak. The company is yet to comment on the approximate amount of loss caused by the malicious applications.

Assessment & Conclusion

Based on the available data and impact information, we can assess that the case was being researched up on since a long time. This indicates that the amount of loss caused was exponentially increasing as time passed. Secondly, we can also assert that there was a considerable loss of Personally Identifiable Information along with loss of credentials. The company did not comment on PII loss, however, it is safe to assume that the attackers would at some point used the login credentials to access and use PII for various reasons. This data might have been used to advertise the malicious application, message the user’s connections or even defame the person of interest for monetary gain. In this position, I would plan and roll out smaller lists of malicious applications that are to be banned, as soon as possible, to reduce attack surface area.

The second point in question is: is this a targeted attack by an individual party or is it a common attack geographically spread across with multiple attack sources? While it is difficult to believe that this attack was not launched by a single party, there is serious lack of motive. On further investigation, Meta’s spokesperson confirmed that there were unable to find a single attack source.

The third point of discussion is the period of time that the attack is being carried out for. While Meta may not reveal the exact timeline for business impact purposes, I believe it is a very important question that may help determine the risk factor and the efficiency of the billion-dollar company. Meta is known to cover privacy issues such as the one being discussed here, and in doing this it may end up hurting the exact thing that it is trying to protect: its reputation. Meta should reveal technical details as it would help support open ended research on such applications which would in turn support and expedite forensic processes.

The final point of discussion is if there are any more applications that may be still stealing and using user data. Meta commented on how they were unsure of the exact impact and stated that there may be more of such malicious applications. Meta has also clearly outlined a few steps to follow, to clear any such applications and to avoid being a victim of such attacks in the future. I would, in this case, prioritise updating and reviewing security policies to make sure they're up to date. From Meta's point of view, it would be a good suggestion to review risk management policies to ensure meta is not liable for third-party breaches.

Bibliography

1. Malwarebytes Labs. *Warning: "FaceStealer" iOS and Android apps steal your Facebook login.* https://www.malwarebytes.com/blog/news/2022/10/warning-facestealer-ios-and-android-apps-steal-your-facebook-login
2. David Agranovich, Ryan Victory. *Protecting People From Malicious Account Compromise Apps.* https://about.fb.com/news/2022/10/protecting-people-from-malicious-account-compromise-apps/
3. MITRE ATT&CK. https://attack.mitre.org/
4. Ravie Lakshmanan. *Facebook Detects 400 Android and iOS Apps Stealing Users Log-in Credentials.* https://thehackernews.com/2022/10/facebook-detects-400-android-and-ios.html