SCHOLARS
STRATEGY NETWORK

IMUTA Malware Breaches Google Play Security, Spying on Millions of Users

Zia Muhammad, North Dakota State University

Google Play is the largest and most popular app distribution platform for Android devices. It provides a safe and secure environment for users by using Google Play Protect, a program that scans apps for malware and other harmful behavior before and after installation.

However, a recent study reveals a serious vulnerability in Google Play's vetting policies, which can allow malicious developers to bypass Play Protect and distribute highly intrusive malware to unsuspecting users. This vulnerability is called the Incremental Malicious Update Attack (IMUTA), and it poses a significant threat to Google Play's security and user privacy.

What is IMUTA, and How Does It Work?

IMUTA is a novel attack technique that exploits the trusted relationship between Google Play, developers, and users. The attack works as follows: First, the attacker develops a benign app that provides some useful functionality and does not request any sensitive permissions or access any user data. The attacker then submits the app to Google Play, where it passes the initial vetting process and is published on the platform. Users who download the app are not aware of any malicious intent and may even rate it positively. Next, the attacker gradually adds malicious features to the app through incremental updates, which are less scrutinized by Play Protect as compared to new apps. The updates may request additional permissions, access user data, or perform harmful actions such as spying, stealing, or deleting data. The attacker may also make it challenging for security analysts or security software to detect their malicious code by using various techniques to obscure or hide its true nature. By the time Play Protect detects the malware, it may be too late for many users who have already installed the app and its updates.

How Serious is IMUTA, and What are Its Consequences?

In the study mentioned above, the researchers demonstrate the feasibility of IMUTA by developing a proof-of-concept malware app—a tool used in cybersecurity research to highlight vulnerabilities or weaknesses in software, systems, or networks—that mimics a popular voice search application. The app initially provides a legitimate voice search functionality and does not request any permissions or access any data. However, after several updates, the app becomes a spyware that can record audio, take screenshots, access contacts, messages, call logs, location, device information, and browser history, and send them to a remote server controlled by the attacker. **The researchers tested their app against 14 major anti-malware solutions and found that none of them could detect the malware in its initial or intermediate stages.**

IMUTA is a serious threat to Google Play's security and user privacy that can undermine the trust and confidence of millions of Android users. The malware can cause various damages to users, such as:

- Violation of privacy by accessing user's personal information and online activities
- Exposure to identity theft, fraud, blackmail, or harassment by leaking user's data to third parties
- Consumption of user's battery, bandwidth, or storage resources by running in the background or sending data to remote servers
- Corruption or deletion of user's data by modifying or erasing files or settings
- Infection of other devices or networks by spreading through Bluetooth, Wi-Fi, or SMS

How Can Google Play Stop IMUTA Attacks?

The researchers who conducted the study suggest some possible countermeasures to prevent or mitigate IMUTA attacks, including:

- Improving Google Play's vetting policies to monitor app updates more closely and flag any suspicious changes in permissions, functionality, or code structure
- Developing more advanced malware detection tools that can analyze app behavior dynamically and identify any abnormal or malicious activities
- Enforcing stricter penalties for developers who violate Google Play's terms of service or distribute harmful apps
- Collaborating with other app distribution platforms or security vendors to share information and best practices on combating malware

How Can Users Protect Themselves from IMUTA Attacks?

Without either Congressional action or changes to internal policies at Google, it is essential that users be more vigilant and cautious about what apps they install and what permissions they grant, and report any suspicious or abusive apps to Google Play. Some tips for users to stay safe from IMUTA attacks are:

- Stay educated about the risks of installing apps from unknown sources or granting permissions without understanding their implications.
- Read app reviews and ratings carefully before downloading an app and check for any negative feedback or complaints from other users.
- Review and revoke app permissions at any time and uninstall any unwanted or harmful apps.
- Update device's operating system and security software regularly to fix any vulnerabilities or bugs.
- Avoid clicking on any links or attachments from unknown or untrusted sources that may lead to malicious downloads.

Although these tips are helpful for users trying to avoid IMUTA attacks, ultimately the burden should not be completely on the individual. It is crucial that Congress investigate these new attacks and work with Google to find a path forward. For instance, the establishment of the Cybersecurity Enhancement Act of 2023 is a remarkable achievement. Such bills can further be emphasized to improve the coordination and collaboration between the government and the industry, and to enhance the detection and prevention of the latest threats and novel cyberattacks.