In Q1 2014, F-Secure and Trend Micro discovered a variety of mobile malware, particularly new threat families that are focused on the Android operating system. The most interesting mobile malware technical is the recent rapid rise of Android malware, with 99% of the new threats that emerged in Q1 2014 designed to run on the Android platform. This is due to the large market share of Android devices and the relative lack of security measures in place to prevent malware installation.

**NEW FAMILIES & VARIANTS**

in Q1 2014, from sites like the Google Play Store, third-party app stores, developer tools, and other sources, F-Secure Labs found or received hundreds of thousands of mobile app samples.

**WHY ANDROID**

With 99% of the new threats that emerged in Q1 2014 designed to run on the Android platform, it's not surprising the most interesting mobile malware technical.

**BY CATEGORY**

- **Fake app scanning**
  - This was the most common mobile malware technical, with 83% of the cases involving this type of threat.
  - Fake app scanning involves apps that pretend to scan your device for malware, but instead are designed to steal your personal information.

- **Location tracking**
  - This type of malware technical involves apps that track your location and share that information with third parties.

- **Fee charging**
  - Fee charging involves apps that charge you fees for accessing certain features or services.

- **Application Privacy**
  - Application Privacy involves apps that collect and share your personal information without your consent.

- **Contact list scanning**
  - Contact list scanning involves apps that access your contact list and share that information with third parties.

- **Silently send SMS messages to premium-rate numbers or SMS-based subscription services.**
  - This type of malware technical involves apps that send SMS messages without your consent or request.

- **Malware that affects the earliest stages of the device’s bootup routine, such as bootkits or MMS apps.**

**WHAT DOES IT DO?**

- **Install charging**
  - Install charging involves apps that charge you fees for installing or updating apps.

- **Data theft**
  - Data theft involves apps that steal your personal information, such as your contacts or photos.

- **Banking trojans**
  - Banking trojans are apps that are designed to access your banking information.

- **SMS sending trojans**
  - SMS sending trojans are apps that send SMS messages to premium-rate numbers or SMS-based subscription services.

- **Malware to get on a device is still for someone to secretly manually or remotely altered firmware updates, with a new malware trojan spreading in modified firmware updates, with most infections occurring when the user is not aware.

- **MALWARE Samples**

- **Trojan:Android/Torsm.A**
  - This is a mobile banking-trojan used as a means to steal users' financial information.

- **Trojan-Spy:Android/Qdplugin**
  - This is a family of mobile spyware that can steal personal information and control the device.

- **Trojan-Spy:Android/Boqx**
  - This is a family of mobile spyware that can steal personal information and control the device.

- **DENDROID TOOLKIT**

- **Trojan-Genius/Android**
  - This is a family of mobile spyware that can steal personal information and control the device.

**WHAT YOU CAN DO**

- **Scan downloaded apps**
  - Scan downloaded apps for malware using an antimalware solution and keep your device secure.

- **Keep your connection private**
  - Keep your connection private with a Virtual Private Network (VPN) encryption.

- **See all the permissions requested by all apps**
  - See all the permissions requested by all apps on your device to ensure your data is protected.

**WHERE DOES MALWARE COME FROM?**

- **Malware samples were received from various sources, including the Google Play Store, third-party app stores, developer tools, and other sources.**

**FREEPHONE**

- **FREEPHONE**
  - FREEPHONE is a service provided by F-Secure that allows users to report suspicious apps.

**ON ANDROID**

- **Windows Trojan Hops on Android**
  - This is a type of malware that uses a Trojan horse to install additional malicious applications.

- **First CryptoMiner**
  - This is a type of malware that uses a crypto miner to steal your personal information.

- **First Bootkit**
  - This is a type of malware that uses a bootkit to install additional malicious applications.

- **Pullup exploit**
  - This is a type of malware that uses a pullup to install additional malicious applications.

**ON IPHONE & SYMBIAN**

- **Trojan-Genius/iPhone**
  - This is a type of malware that uses a Trojan horse to install additional malicious applications.

- **Trojan-Spy/Symbian**
  - This is a type of malware that uses a spyware to steal your personal information.

**TOP 10**

- **Top 10**
  - The top 10 mobile malware samples found in Q1 2014 were:

**FAREASTEN, 43%**

- **Fareasten**
  - Fareasten is a type of malware that uses a fareasten to install additional malicious applications.

**NEW FAMILIES AND VARIANTS**

- **New families and variants**
  - New families and variants from Q1 2014 include:

**WHAT YOU CAN DO**

- **Secure your log-in details with strong encryption**
  - Secure your log-in details with strong encryption to protect your personal information.

- **Use anti-theft protection**
  - Use anti-theft protection to prevent anyone else from meddling with your device's settings and installing additional malicious applications.

- **Install the latest updates**
  - Install the latest updates for your device to ensure it is protected from new threats.

- **Scan downloaded apps**
  - Scan downloaded apps for malware using an antimalware solution and keep your device secure.

- **Keep your connection private**
  - Keep your connection private with a Virtual Private Network (VPN) encryption.

- **See all the permissions requested by all apps**
  - See all the permissions requested by all apps on your device to ensure your data is protected.

**HIGHLIGHTS THE THREATS**

- **Windows Trojan Hops on Android**
  - This is a type of malware that uses a Trojan horse to install additional malicious applications.

- **First CryptoMiner**
  - This is a type of malware that uses a crypto miner to steal your personal information.

- **First Bootkit**
  - This is a type of malware that uses a bootkit to install additional malicious applications.

- **Pullup exploit**
  - This is a type of malware that uses a pullup to install additional malicious applications.

**REPORTING**

- **Reporting**
  - Reporting is an important part of the threat landscape, and it helps researchers and law enforcement to track and shut down the C&C.