cellebrite
delivering mobile expertise

Malware Solution

Keep Ahead of the Growing Mobile Malware Threat by Identifying and Removing Infections.

CELLEBRITE'S MALWARE SOLUTION IDENTIFIES MALICIOUS SOFTWARE AND DANGEROUS APPS IN 1 OF 10 DIAGNOSTIC SESSIONS

Introduction

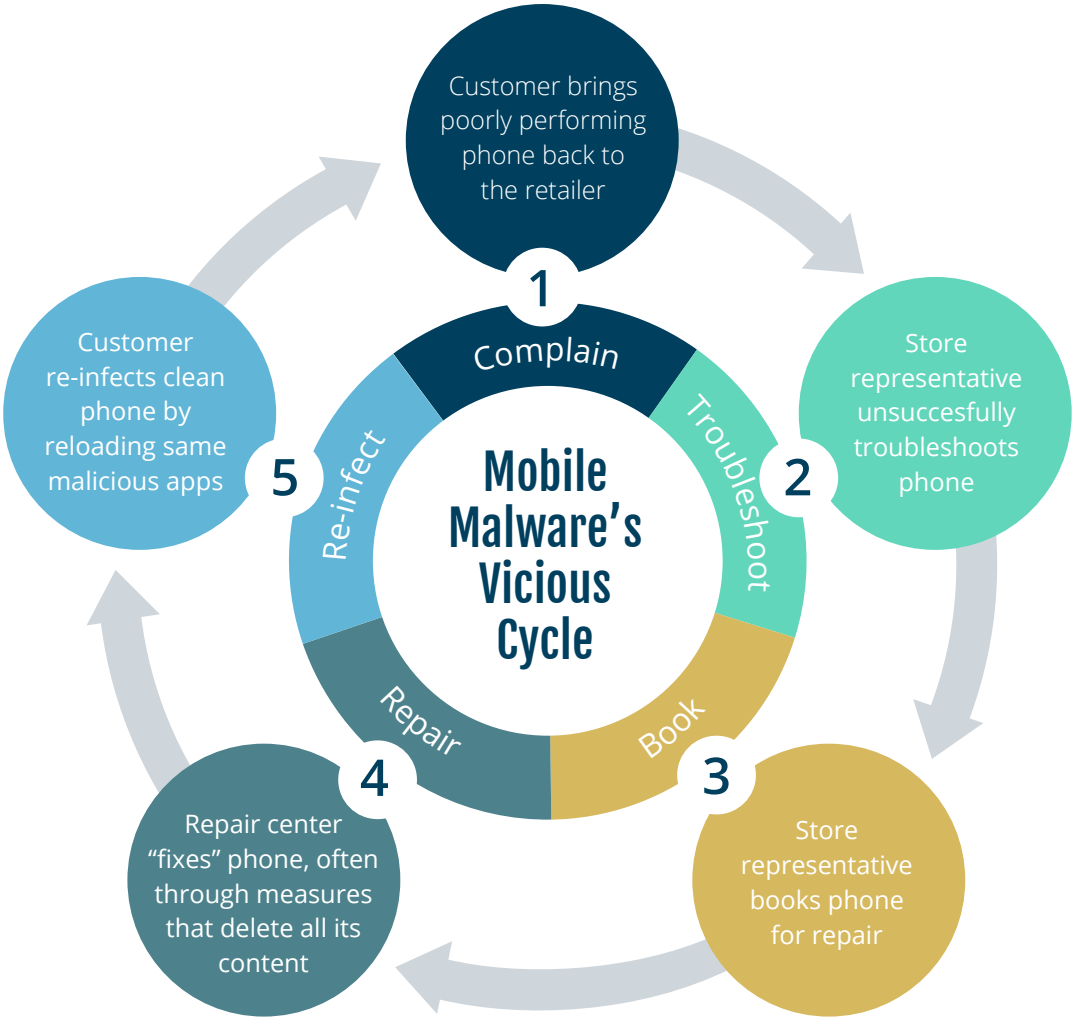
Mobile malware continues to soar to new heights according to research by Webroot, a global leader in cloud-based security. Recent intelligence performed by the Webroot team, showed that 20% of all Android apps contained malware, and 79% of the top 50 free iOS and Android apps are associated with malware activities or privacy issues[1]. Reaching alarming new levels of sophistication, malware shows no signs of slowing down. A recent industry study measured a 600% increase in mobile malware over twelve months with the chance of being a mobile malware victim becoming 10x more likely.[2]

Mobile malware presents a very real threat to both mobile subscribers and mobile retailers. In today's constantly connected mobile environment, smart phones are no longer just phones, they have become a life-line to users and carry more personal data than ever before. Once downloaded, malware can compromise the phone's security and access personal information – causing sudden bill spikes and reduced phone performance. Users, unfamiliar with malware-related issues, point the finger at mobile operators, retailers and even OEMs. The result is a negative impact on reputation and revenue.

Repercussions for mobile retailers, include higher repair costs and warranty claims, lost revenue from waived charges and reduced customer satisfaction. Yet, even more worrying, is the fact that mobile operators could potentially face threats from their own customers who unknowingly have malware on their devices which could ultimately compromise network stability.

Android is in the unfortunate lead with over 95% of malware targets. However, new threats are now emerging on iOS devices as well – even those that have not been jail-broken.

The more complex the malware, the harder it is to detect. Additional complexities include apps that are not actually infected, but are using ad servers that are known to be harmful. Recent iOS threats and continually evolving sophistication, suggests that the work of malware designers is by no means complete, in fact they are intent on expanding and improving their malware efforts.



1. Information source: Appthority
2. Information source: MaaS360

Malware's Far Reaching Effect

Customers

Not all customers are aware of the dangerous apps, websites, and text messages that are associated with mobile malware. Suspicions are normally raised when the user experiences events such as decreased battery life, a spike in phone charges and reduced phone performance.

Malicious adware for example, once downloaded, constantly displays ads, which reduces the phone's battery performance. A spike in phone charges is often caused by malicious apps constantly sending text messages to premium-rated numbers. Malware also causes problems with the phone's performance as it tries to perform many actions simultaneously, such as read, write and send data.

Retailers

Retailers, repair centers and OEMs are all at risk. If malware is not dealt with effectively, it can initiate a vicious cycle.

1. Phones are booked in to unnecessary repairs with costly warranty claims
2. Store reps are tied up trying to solve issues when they could be selling
3. Simple fixes, such as master reset or flashing, only solve the problem temporarily
4. Customers return with the same issue after unknowingly downloading the same apps that contain malware - and the cycle begins again

Mobile operators and retailers who are not able to break the malware cycle run the risk of losing their customers' trust – and future business. Failure to identify malware as the source of a problem can lead to multiple failed repair attempts that add cost and increase customer frustration. With no alternate explanation for their phones' problems, customers lay blame at the feet of those who made the device, those who sold the device, and those incapable of fixing it properly.

Operators

Once downloaded, certain malware apps take control of the device and begin sending continuous text messages or accessing premium services – both actions can result in additional fees. Consumers often refuse to pay for these unauthorized charges, and, in an effort to appease these customers, operators end up waiving the fees and end up paying the price.

In a Nutshell...

Mobile retailers have little control over the continued growth and sophistication of malware apps. Sending mobile devices time after time for repair is both costly and ineffective.

Cellebrite's diagnostics technology is the first step in protecting mobile users and retailers. In-store, on-the-spot malware identification, provides retailers with the tools to identify, remove, and prevent re-infection of mobile malware. Cellebrite Diagnostics provides intuitive, wizard-like workflows, automation, and on-screen contextual help, puts novice users on par with expert technicians.

- Reduces repair, labor, and unauthorized charge expenses
- Provides a superior level of customer experience that promotes loyalty
- Breaks the cycle of infection, cleansing, and re-infection
- Easy to integrate, easy to use
- Real-time connections to Webroot's threat database of over 9 million applications
- Continuously updates versions to ensure threats are eliminated from all subsequent versions
- Identifies and flags apps that may not have malware in the code, but are associated with a known threat
- Examines the application source code and analyzes the behavior of the app during execution
- Clean apps will be flagged, if they are collecting content from a malicious website
- Single-click activation for automated correction of issues affecting battery drainage
- Patent-pending technology

Malware can also compromise the integrity and performance of an operators' network. A widespread infection over a large number of customers can have an adverse effect on network performance if the intent of the malware is to deny services or other issues that involve network usage.

Mitigating the Threat with Cellebrite Diagnostics

To effectively deal with the threat mobile malware poses to their customers and their business, mobile operators and retailers must be able to do three things well:

Cellebrite Diagnostics

Identify

Remove

Educate

Identify... the most recent mobile malware on every Android and Apple device.

Real-time connections to Webroot's App Reputation Database enables Cellebrite Diagnostics to recognize not only apps that are known malware, but other apps whose behavior, permission requests, or use of questionable ad servers raise considerable suspicions about their safety.

Remove... malware-infected software – and only the infected software.

Across the board deletion of all apps "just to be safe" accomplishes little more than frustrating customers and reducing the value they get from their phones. Cellebrite Diagnostics employs a targeted approach with recommendations for removal based on each apps individual threat assessment. With approval from the device owner, one, some, or all removal recommendations can be accomplished with a tap or click.

Educate... consumers on how to avoid reinfection.
Identifying and removing malware solves problems on the spot, but informing the device owner of the specific apps that are considered dangerous prevents them from re-installing the problem unknowingly. This knowledge sharing increases the value delivered by the mobile operator or retailer and generates more first-touch resolutions, eliminating future complaints and repair bookings for the same issue.

These three steps are the most effective way to eliminate mobile malware threats, maintain customer satisfaction, and prevent revenue loss and network damage.

Cellebrite has partnered with Webroot, a global leader in cloud-based security intelligence, to bring to market a powerful comprehensive malware detection and removal solution. Real-time integration with Webroot's App Reputation service marks Cellebrite's Diagnostics as the first and only multi-channel mobile diagnostics solution to offer malware detection and removal.

About Cellebrite

Cellebrite is a world leader in providing Operators, Retailers and Aftermarket Service (AMS) Providers, with advanced mobile lifecycle solutions to enhance the customer experience, improve satisfaction, reduce cost, and generate revenue. With delivery channels in-store, on-device, and over the web, mobile retailers can take advantage of Cellebrite's full suite of mobile lifecycle solutions: diagnostics, phone-to-phone content transfer, backup, restore and wipe, automated phone buyback, and application and content delivery. In addition, Cellebrite offers retailers monitoring, statistics and analysis of all activities. Cellebrite's global leadership is demonstrated through its deployment of over 150,000 units at more than 200 mobile operators and retailers globally, representing well over 100,000 stores and handling hundreds of millions of transactions per year.

Founded in 1999, Cellebrite is a subsidiary of the Sun Corporation, a publicly traded Japanese company (6736/JQ).

www.cellebrite.com

For more information contact sales

cellebrite
delivering mobile expertise