

You installed what?!



Thierry Sans

جامعة كارنيغي ميلور في قطر
Carnegie Mellon Qatar

What is a malware?

Malware = Malicious Software

“Software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems. Malware includes computer viruses, worms, trojan horses, spyware, adware, most rootkits, and other malicious programs.”

definition from Wikipedia

How to prevent malware?

✓ Anti-malware monitors programs running on your OS

- can detect well-known malicious programs (signature)
- can detect abnormal behaviors
- can run applications in sandboxes

✓ Awareness and good practices

A new generation of software a.k.a. "apps"

Cloud



Mobile



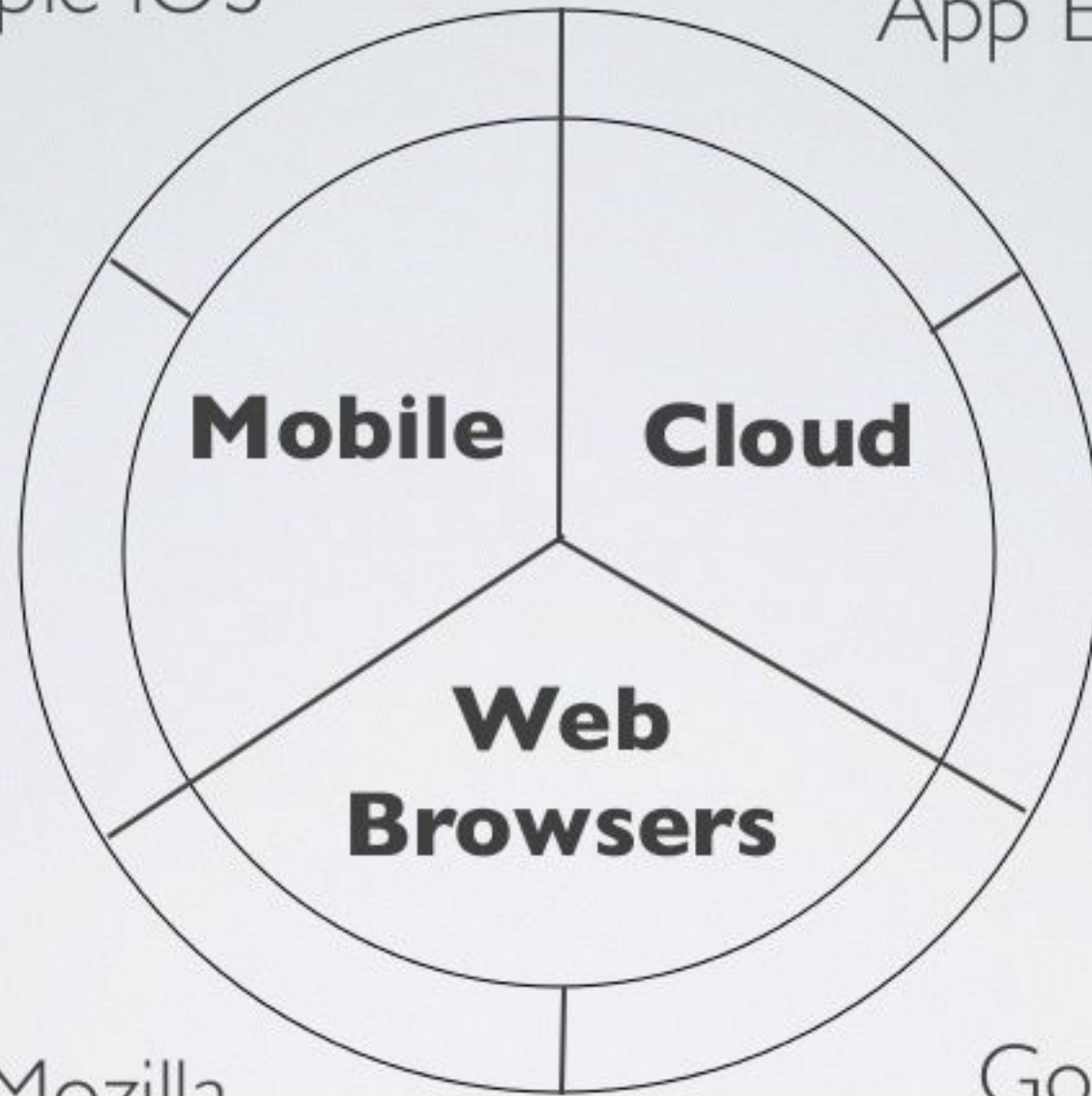
Web Browser



Apple iOS



Google
App Engine



Google
Android

Facebook



Mozilla
Firefox

Google
Chrome



Definition of an *App Ecosystem*

- apps are running on a specific platform
- apps are built based on a specific SDK
- apps are distributed through a dedicated portal



Google play



App Store



With new usages ...

... comes **new threats!**

With a new generation of software ...

... comes a **new generation of malware!**

MALWARE INC Goals



✓ 6 students = 6 hackers to develop **malware**

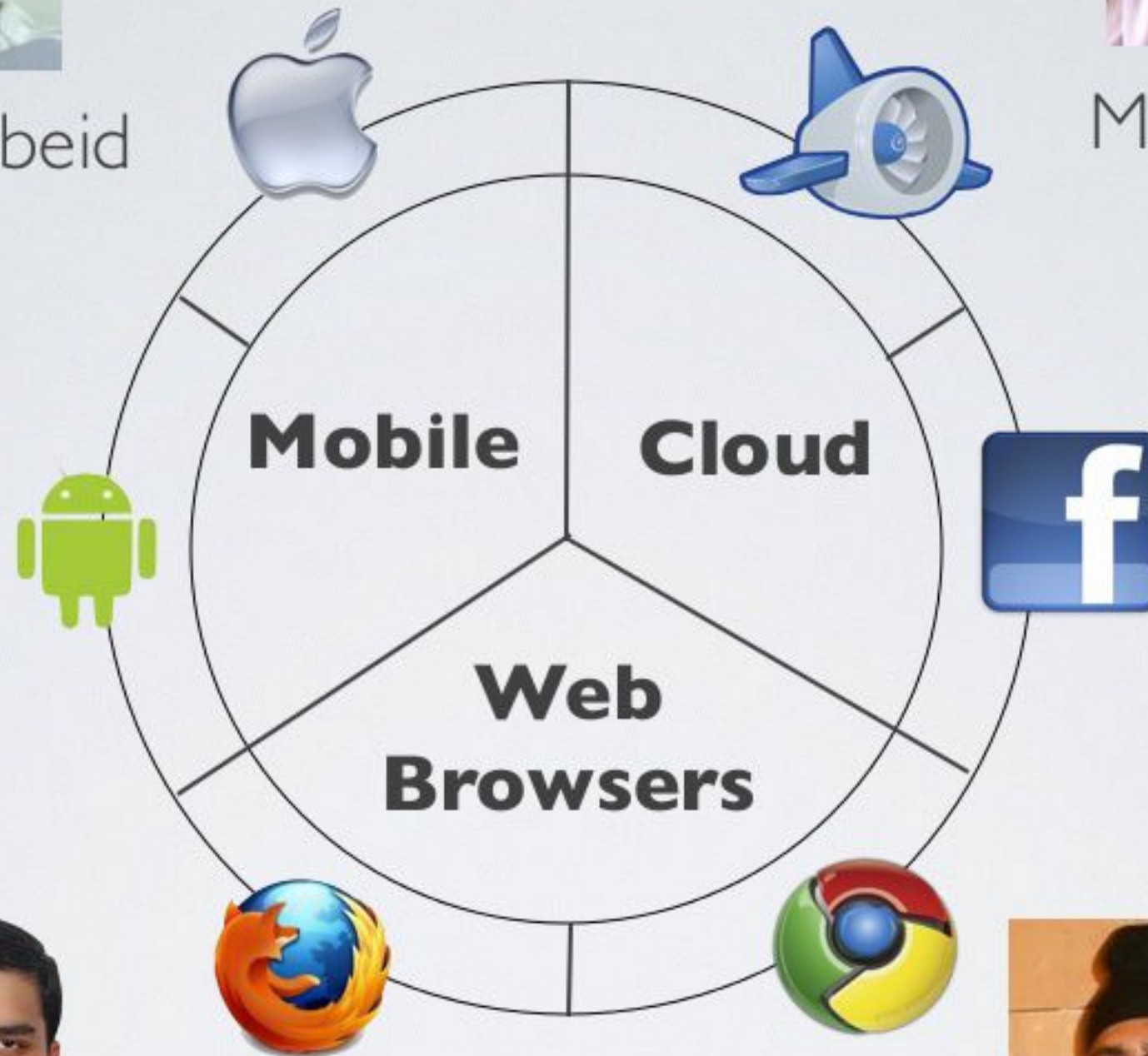
➔ become **security experts** for a specific technology



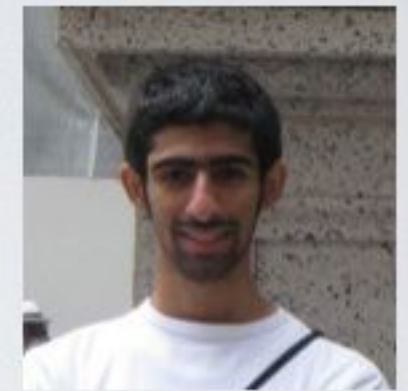
Ossama Obeid



Manoj Reddy



Rami Al-Rihawi



Talal Al-Haddad



Fahim Dalvi



Baljit Singh

Manoj Reddy



Google App Engine

What is a Google App Engine App?

- Google App Engine allows developers to build and run web applications on the Google's infrastructure
- ➔ The Google App Engine SDK gives you access to
 - General services (Search, Maps ...)
 - **User-centric services** (Gmail, Calendar, Checkout ...)

G-stats App



A cool web application that will show you some statistics about your GMAIL mailbox



Scans your mailbox for email with login and password and forward it to the hacker's website

What is the risk?

✓ Only few websites send your login and password by email

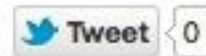
⦿ **But**

- How many different passwords do you have?
- What are the other websites that you use?
- What else can I find in your emails?

How bad is it?

Bot Herders Used Google App Engine To Spread Malware

By [Alex Williams](#) / November 9, 2009 8:24 PM / [18 Comments](#)



Google has confirmed [news today](#) that [bot herders](#) used Google App Engine to feed commands to networks of infected computers. According to [Arbor Networks](#), the bot herd was discovered over the weekend. After being notified of the attack, Google quickly shut down the infected app engine.

Also on Monday, the Koobface botnet was [attacking Google Reader](#) to send malicious links through Twitter, Facebook and other social networks.

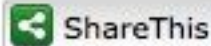
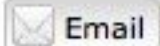
SPAMfighter

MICROSOFT
GOLD
PARTNER



SPAMfighter

SERVER Solutions



Google's AppEngine Used for Spamming Malware

According to online security company Arbor Networks, a botnet came into light during the 1st week of November 2009 that distributed spam and [malware](#) with the help of Google AppEngine.

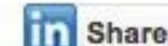
Will Google's App Engine become a malware portal?

By [Liam Tung, ZDNet.com.au](#) on April 17th, 2008

Topics



Be the first of your friends to recommend this.



application, google, oser, security, cloud

Security experts fear Google's new application hosting service App Engine will become a tool to spread malware and could ruin Web security defences.

Talal Al-Haddad



Facebook

What is a Facebook app?

- A Facebook app is a web application that can access your Facebook profile
- ✓ The authentication is done through Facebook
- ⦿ The web application is **not hosted on Facebook** but on the developer's server
- ➔ After authentication, the application can download user's data and do something useful ... or malicious

Best Buddy App



A cool application that will tell you who your best friends are on Facebook



1. Asks you to re-enter your Facebook password and send it to the hacker's website
2. Makes a copy of your profile on the hacker's website
3. Recommend the application to your friends by posting a message on their wall

How bad is it?

Malware silently hijacks Facebook account and adds apps

Posted on 14.04.2011

BOOKMARK



Several months ago, when the operators of the Sality P2P botnet pushed out malware that not only collected usernames and passwords and sends them to the C&C servers but also dumped Facebook, Blogger and MySpace login credentials into an encrypted file on the infected computer, Symantec researchers speculated about the purpose these files would serve.

Their best guess was that these credentials will be of use to some yet unrevealed piece of malware, and the theory has proven to be correct over the weekend, when Sality - a virus whose primary reason of being is to download and execute other malware - downloaded a new piece of malware that fished out that file and the credentials in it.

Home > Mobile News > Facebook News > Facebook Malware Exposes Passwords, Erodes Trust

Facebook Malware Exposes Passwords, Erodes Trust



PCWorld » Security

Recommend: Like 462 56 +1 7

Facebook Malware Scam Takes Hold

By Cameron Scott, IDG News Feb 4, 2012 12:44 am

A "worrying number" of Facebook users are sharing a link to a [malware-laden](#) fake CNN news page reporting the U.S. has attacked Iran and Saudi Arabia, [security firm Sophos said Friday](#).

If users who follow the link then click to play what purports to be video coverage of the attack, they are prompted to update their Adobe Flash player with a pop-up window that looks very much like the real thing. Those who accept the prompt unwittingly install malware on their computers.



BY JANET MARAGIOGLIO | FR

Malicious software stole thousands of Facebook usernames and passwords, calling into question the social network's trustworthiness as it becomes a frequent target for malware attacks.

Like 13

Tweet 19

Fahim Dalvi



Mozilla Firefox

What is a Firefox Extension?

- A Firefox app is an additional piece of code that provides new functionalities to Firefox or enhance the existing ones
- ➔ The Firefox SDK gives you access to
 - The user interface and the functionalities of Firefox
 - The web contents in the tabs
 - **The Operating System**

Live Edit App



A cool application that allows you to customize or translate any webpage that you are visiting



Silently downloads and executes a key-logger program that records any keystroke made on your computer and send them to the hacker's website

Another key logger ... but an undetectable one!

- Key loggers are easily detectable

- ➔ Key loggers open a network socket to send data

- ✓ *Live Edit* malware does not open any network socket

- ➔ It sends data through Firefox which is a legitimate app (tested with Symantec Anti-malware)

How bad is it?

Home > News > Security > Spyware Threats

August 29th, 2009, 09:56 GMT · By [Lucian Constantin](#)

Click Fraud Malware Hides as Firefox Extension

SHARE:  +1 0  Like 3  Send  Tweet

Adjust text size:  



Security researchers warn of a new piece of malware that functions as an extension for the Mozilla Firefox browser. The rogue add-on intercepts Google search queries and injects advertisements into the results.

The new attack has been [reported](#) by analysts from antivirus vendor Trend Micro and seems to be motivated by illegal monetary gain through an advertising scheme. The threat combines techniques previously employed by different families of malware.


For a start, it comes under the form of a Firefox extension, which is rather uncommon. A similar computer trojan running as a Firefox extension, which was used to monitor user sessions and capture online banking credentials for over 100 financial institutions, was [discovered](#) back in December 2008.

Mar

Malicious Firefox Extensions

2

5:01 am (UTC-7) | by [Joey Costoya](#) (Senior Threat Researcher)

 Share

 Like 1

 Tweet 0

 +1 0

This is a long time coming – Firefox extensions that have malicious intent. Because Firefox extensions are executable code, the coder can do anything he wants, as long as he can code it.

Firefox Extension Malware Raises Security Questions

Mozilla's diligent cleanup rather than catching malicious add-ons before they reach the public has rankled some in the security community.

By [Thomas Claburn](#)  [InformationWeek](#)

May 26, 2009 02:54 PM

Mozilla's commitment to secure software products is coming into question after a recent malware product software incident.

Earlier this month, the lack of security oversight in the Mozilla Firefox add-on community became apparent when Adblock Plus developer Wladimir Palant criticized Giorgio Maone, creator of the JavaScript-blocking extension NoScript, for altering NoScript to interfere with Adblock Plus.



Baljit Singh



Google Chrome

What is a Google Chrome Extension?

- A Chrome app is an additional piece of code that will provide new functionalities to Chrome or enhance the existing ones
- ➔ The Google Chrome SDK gives you access to
 - The user interface and the functionalities of Chrome
 - **The web content in the tabs**

Easy Screenshot App



A cool application that enables you to take a screenshot of your browser tab easily



Automatically takes screenshots when visiting specific login pages that use a virtual keyboard and send these images to the hacker's website

What is the risk?



Electronic Bank
Online and Mobile Solutions

New User?

Login ID

Password

Remember Me

[Forgot Password?](#) [Delete This User](#)

Why the virtual keyboard?



[Cb Home](#) | [How to Stay Alert](#) | [Look for Lock Icon](#)



Copyright © Commercial Bank of Qatar (Q.S.C). 2010 All rights reserved.



Welcome to eazyinternet - QNB's online e-banking service. N
conve



QNB eazyinternet

User Name Password

[Password](#) or [User Name](#)

Personal Pict



Experience our new Internet Banking
Secured Efficient
Fast and Simple

Security Tips

- Never reveal your password OR any security information to anyone.
- Doha Bank will never request for password, security information or financial information via e-mail as Doha Bank takes the privacy and confidentiality of our customer's information seriously.
- Should you receive any suspicious communication, like email requesting for account information, please alert us immediately at +974 44456000 and delete such emails immediately.

Welcome to DBank Online services from Doha Ba

User Name

Customer Number

Password

[Forgot Password?](#)

Note : Click on the Keyboard Image to Open & Close Virtual Keyboard



Why Virtual Keyboard?

How bad is it?



Trojan as Fake Google Chrome Extension

19 April 2010

As more and more people are using **Google Chrome** and its functionalities to browse the net and to organize information, cybercriminals have set their minds on exploiting this environment to spread malware and steal users' information.

Filed Under:

ALERTS

The story is simple: Google Chrome users receive an unsolicited e-mail which announces that a new extension of their favorite browser has been developed to facilitate their access to documents from e-mails.

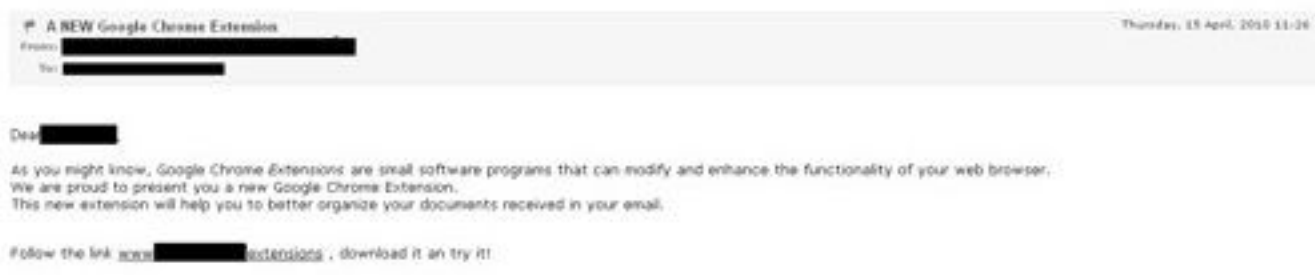


Fig. 1 The spam message used to popularize the malicious link

An apparently unsuspecting link is provided, and the recipients are advised to follow it in order to download the new extension. Once they click the link, they are redirected to a look-alike of the Google Chrome Extensions page, which, instead of the promised extension, provides them with a fake application that infects their systems with malware.

Malware Masquerading as Google Chrome Extension



By **Larry Seltzer**

April 19, 2010 06:02pm EST

2 Comments



Email



Print



BitDefender's Malware City [blog](#) is warning users about what it considers to be the first case of malware spreading via a fake Google Chrome extension.

Rami Al-Rihawi



Google Android
(work in progress)

What is an Android app?

- An Android app is a third-party application installed on your Android device
- ➔ The Android SDK gives you access to device functionalities and its data
 - text messages
 - emails
 - location
 - calendar
 - contacts
 - notes
- ➔ Apps are **not reviewed by Google** before being published on Google Play

Easy Phone Calls App



A cool application that automatically creates shortcut buttons to call people with who you were in touch recently



Can be remotely controlled to make your phone call the hacker

How bad is it?

Home > Security > Malware and Vulnerabilities

News

Massive Android malware op may have infected 5 million users

Many of the 13 'Android.Counterclank'-infected apps remain on the Android Market

By Gregg Keizer

January 27, 2012 04:02 PM ET

30 Comments

Like

652

+1

51

Computerworld - The largest-ever Android malware campaign may have duped as many as 5 million users into downloading infected apps from Google's Android Market, Symantec said today.

Dubbed "Android.Counterclank" by Symantec, the malware was packaged in 13 different apps from three different publishers, with titles ranging from "Sexy Girls Puzzle" to "Counter Strike Ground Force." Many of the infected apps were still available on the Android Market as of 3 p.m. ET Friday.

Home / News & Blogs / Zero Day

Remote-controlled Android malware stealing banking credentials

By Ryan Naraine | March 15, 2012, 9:54am PDT

Summary: The malicious Android application targets specific well-known financial entities posing as a Token Generator application.



Security researchers at McAfee have discovered a malicious Android application capable of grabbing banking passwords from a mobile device without infecting the user's computer.

The latest piece of Android Malware, dubbed FakeToken, contains man-in-the-middle functionality to hijack two-factor authentication tokens and can be remotely controlled to grab the initial banking password directly from the infected mobile device.

Google takes steps to remove malware in Android Market

by Marti Trewe on February 3, 2012 · 12 Comments · in Operating System, Smartphones, Tablets

Android security In the last year, Google has taken heat for their Android Market being vulnerable to viruses and malware as their open attitude towards app developers sharply contrasts the closed door, approval-required Apple app ...

Ossama Obeid



Apple iOS
(work in progress)

What is an iOS app?

- An iOS app is a third-party application installed on your iOS device
- ➔ The iOS SDK gives you access to the device functionalities and its data

iOS is very “controlled”

- The functionalities of the iOS SDK are more restrictive than Android
 - No access to emails (except sending emails)
 - No access to text messages
- Apps are reviewed by Apple before being published on the App Store
- Apple is very reactive and modifies its SDK when a malware is discovered

How bad is it?

Researchers discover security flaw allowing iOS malware steal user data

Posted on Nov 8th, 2011 | 0 comments

iOS Bug Allows Malware to Be Sold in Apple App Store

5:00 AM - November 9, 2011 - By Ross A. Lincoln - Source : Computer World

[Like](#) 72 [Send](#) [Twitter](#) 30 [+1](#) 9 [StumbleUpon](#) 0 [Share](#) 102

According to Denver-based security consultant Charlie Miller, the Apple App store is vulnerable to infiltration by malware apps that can pose a significant risk to Apple customers. Miller, 4-time winner of the Pwn2Own hacking contest and an employee of security consulting firm Accuvant, managed to submit and gain Apple's approval to sell an app that exploited a previously unknown iOS bug.

Time stamp bug exposes photos on locked iPhone

If your iPhone clock somehow gets set to the past the photos taken since then could be viewed despite the phone being locked.



by [Elinor Mills](#) | January 3, 2012 12:13 PM PST

[Follow](#)

A newly found iOS code signing flaw could open a door in Apple's stringent security system for disguised malware to enter the App Store. According to Mac researcher and hacker Charlie Miller, once the virus sneaked into the App Store, it is capable of infecting any iOS device to steal user data as well as get control of some iOS functions.

Conclusion

About these malware

- We did not break anything
- ✓ They are “legitimate” programs that uses functionalities offered by the SDK
- We developed these malware as proof of concepts
- ⦿ We will **not** publish these malware

MALWARE INC Goals

- Have a **better understanding** of popular app ecosystems
- **Assess the risk** of exposure to a malware
- **Create new security mechanisms** against malware

Preventing cloud-based malware

- ➔ The application runs in the cloud but not on the user's device
- ⦿ Hard to review or audit the application

Preventing malware on mobiles and web browsers

- ➔ The application runs on the user's device
- ✓ Easier to audit the application
 - Anti-malware apps are emerging on some platforms

The wrong feeling of security

- ➔ These “apps” come from a legitimate source
- ⦿ People trust these “apps”

My idea for a more **secure app ecosystem**

- We need to be more **proactive** and make programs reliable from their conception
- We need **new development tools** that will allow us to audit programs and know what they do before installing or executing them
- ✓ The Qwel programming language
- ➔ YSREP project funded by the Qatar National Research Fund (QNRF)



Thank You