Malware for iOS

This is a list of known malware (including spyware, adware, trojans, viruses, worms, and similar tools) that have targeted iOS, including jailbroken iOS. The dates are approximate dates when people discovered, publicized, or started discussing the tool.

The goal of this list is to aid better understanding of the risks of using iOS and jailbroken iOS - it's helpful to have as much accurate information as you can. If you're concerned about avoiding malware on your jailbroken device, check out this guide to making informed guesses about whether packages are reasonable to install (https://www.reddit.com/r/jailbreak/wiki/howtoresearch).

Some context:

- Some of these tools targeted old iOS versions and do not work on current iOS versions.
- Some of these are harmful and some are merely annoying.
- Many of these require the device to be jailbroken, and some work on non-jailbroken devices (including via misuse of enterprise and developer certificates).
- Cydia is an open platform - it includes a specific set of default repositories, and it also allows users to type in any third-party repository that they want to use (much like a web browser that allows you to visit any website). Anyone can run a third-party repository and distribute any software they choose to distribute.
- Some of these tools are built to target specific people instead of the general public.
- Especially for malware that targets a specific person and requires the device to be jailbroken (such as commercial spyware tools used by governments and people spying on family members (http://www.forbes.com/sites/sarahjeong/2014/10/28/surveillance-begins-at-home/)), it's important to consider that *the vulnerabilities in iOS that allow it to be exploited with a jailbreak* are part of what allows that malware to exist - the process may include finding a way to secretly jailbreak the target's device if it's not jailbroken already.

For an earlier list of known malware, see "iOS Malware Does Exist" (https://blog.fortinet.com/2014/06/09/ios-malware-does-exist) (June 2014).

Related research: "On the Feasibility of Large-Scale Infections of iOS Devices" (https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/wang_tielei) (August 2014).

Contents

Youmi Ad SDK (October 2015)
AceDeceiver (March 2016)
Safari JavaScript pop-up scareware (March 2017)
mainrepo RAT

Tools used by governments (and similar) to target individuals

FinSpy Mobile (August 2012)
DROPOUTJEEP (December 2013)
Hacking Team tools (June 2014 and July 2015)
Inception (December 2014)
XAgent (February 2015)
Pegasus (August 2016)
Cellebrite (February 2017)
CIA "Vault 7" materials (March 2017)

Tools developed as part of research

iSAM (June 2011)
Instastock (November 2011)
Mactans (July 2013)
Jekyll (August 2013)
XARA attacks (June 2015)
NeonEggShell (August 2015)

Tools for sale to the public to target individuals

1mole
Copy9
Copy10
FlexiSPY
iKeyGuard Key Logger
iKeyMonitor keylogger
InnovaSPY
Mobile Spy
MobiStealth
mSpy
OwnSpy
Spy App
SpyKey
StealthGenie
Trapsms

Tools found in the wild that target the public

iKee and Duh (November 2009)

The Ikee-virus (also called Eeki) is a worm transmitted between jailbroken devices that have OpenSSH installed and haven't changed the default root password. It changes the lockscreen background to a photo of Rick Astley.

Two weeks later, the similar Duh worm (https://nakedsecurity.sophos.com/2009/11/23/lightning-strikes-iphone-malware-malicious/) spread, which was "much more serious than the original Ikee worm because it is not limited to infecting iPhone users in Australia, and communicates with an internet Control & Command centre, downloading new instructions - effectively turning your iPhone into part of a botnet."

"Find and Call" (July 2012)

Find and Call was an app on the App Store that automatically uploaded users' contact lists to the company's server, then spammed those contacts with a link to the app ("from" that user). This undisclosed, unwanted behavior makes the software fit the definition of a trojan. Articles: Kaspersky SecureList (https://securelist.com/blog/incidents/33544/find-and-call-leak-and-spam-57/), Ars Technica (http://arstechnica.com/apple/2012/07/find-and-call-app-becomes-first-trojan-to-appear-on-ios-app-store/), Sophos NakedSecurity (https://nakedsecurity.sophos.com/2012/07/06/find-call-ios-android-malware/). It is also called FindCall.

Packages by Nobitazzz (August 2012 and September 2013)

A tweak developer who went by various names (Felix, FelixCat, isoftjsc, Martin Pham, Nitram88, Nobitazzz, Nobita.ZZZ, Sara_Nobita, sara_nobita_zzz, tuyentq2009, vietSARA) included adware in his tweaks. These were many free packages along with some paid packages sold via the Cydia Store, mostly distributed by default repositories (until the problem was discovered). The adware ran ads in the background of iOS, displaying off-screen so that the user wouldn't notice them, with the revenue from those ads going to this tweak developer. This was first reported in August 2012 on the ModMyi forum (http://modmyi.com/forums/cydia-support/810633-new-adware-malware-found-cydia.html) and analyzed in September 2013 (http://ryanhileman.info/posts/webgl) (discussion on Reddit (https://www.reddit.com/r/jailbreak/comments/1n5702/anatomy_of_a_jailbreak_trojan/)).

Packages by this developer included: Animated ICS LockScreen & HomeScreen, BetterChrome, Chrome Download Enabler, ChromeMe, Enable Copy text in Facebook app, Enable WebGL, Facebook Photo Library integration, FacebookThis, Handwriting recognition, Insta9gag, InstaFacebook for NotificationCenter, Instagram Image saver, InstaSocial for Notification Center, InstaTwitter for NotificationCenter, iOS 6 Photos Menu, Make Gmail as default, Notification Lunar Calendar, Olympic 2012 Medal for Notification Center, PhotoFilters, Sara, Sara Dictation Keyboard, VoiceTweet.

AdThief/Spad (March and August 2014)

AdThief (also called Spad) is malware targeting jailbroken iOS devices, which "tweaks a developer ID that's intended to tell ad developers when their ads are either viewed or clicked and in turn, generate revenue. In the malware's case, infected devices funnel those small payments away from the developers to the hacker", as explained by Kaspersky Threatpost (https://threatpost.com/adthief-ios-malware-affecting-75k-jailbroken-devices/107907). Security researchers estimated it had infected 75,000 devices.

Unflod (April 2014)

Unflod is a malicious piece of software targeting jailbroken iOS devices, which attempts to capture the user's Apple ID and password by using MobileSubstrate to hook into the SSLWrite function of Security.framework and then listening to data passed to it. Once the Apple ID and password are captured, it is sent to a Chinese IP address. It was inadvertently discovered by a Reddit user on April 17th, 2014. Also called "Unflod Baby Panda" and "SSLCreds".

AppBuyer (September 2014)

AppBuyer, as discussed in this article by Palo Alto Networks (http://researchcenter.paloaltonetworks.com/2014/09/appbuyer-new-ios-malware-steals-apple-id-password-buy-apps/), is malware that "will connect to C&C server, download and execute malicious executable files, hook network APIs to steal user's Apple ID and password and upload to the attacker's

server, and simulate Apple's proprietary protocols to buy apps from the official App Store by victim's identity." It targets jailbroken devices.

WireLurker and Masque Attack (November 2014)

As discussed at Misuse of enterprise and developer certificates: according to Palo Alto Networks (http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/), WireLurker is "a family of malware targeting both Mac OS and iOS systems for the past six months...It is the first in-the-wild malware to install third-party applications on non-jailbroken iOS devices through enterprise provisioning."

Masque Attacks are a related technique, also discussed by Palo Alto Networks (https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html): "an iOS app installed using enterprise/ad-hoc provisioning could replace another genuine app installed through the App Store, as long as both apps used the same bundle identifier."

Xsser mRAT (December 2014)

Xsser mRAT is a piece of malware that targets jailbroken devices. As described by Akamai (https://blogs.akamai.com/2014/12/ios-and-android-os-targeted-by-man-in-the-middle-attacks.html): "The app is installed via a rogue repository on Cydia, the most popular third-party application store for jailbroken iPhones. Once the malicious bundle has been installed and executed, it gains persistence - preventing the user from deleting it. The mRAT then makes server-side checks and proceeds to steal data from the user's device and executes remote commands as directed by its command-and-control (C2) server."

Lock Saver Free (July 2015)

Lock Saver Free is a free tweak, originally distributed on a default repository (removed from the repository after discovery of the problem), that installs an extra tweak that hooks into ad banners to insert its own ad identifier, presumably in order to give ad revenue to the author of the tweak instead of to the author of the website/app where the ad was found. Discussion on Reddit (https://www.reddit.com/r/jailbreak/comments/3eis8g/news_lock_saver_free_contains_a_trojan_that/).

KeyRaider (August 2015)

KeyRaider, as discussed in this article by Palo Alto Networks (http://researchcenter.paloaltonetworks.com/2015/08/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/), is a piece of malware for jailbroken devices that "steals Apple account usernames, passwords and device GUID by intercepting iTunes traffic on the device." These security researchers said it has over 225,000 stolen accounts in its database.

XcodeGhost (September 2015)

XcodeGhost is a form of malware that was found in some unofficial redistributions of Xcode targeted at Chinese developers (who often download redistributed copies because official Apple download speeds are slow in China). XcodeGhost infects apps compiled with those versions of Xcode, which included at least 39 apps published in the iOS App Store. Palo Alto Networks published a series of posts about it: original post explaining it (http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/), a list of additional infected apps on the App Store (http://researchcenter.paloaltonetworks.com/2015/09/malware-xcodeghost-inf

ects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/), more about its capabilities (http://researchcenter.paloaltonetworks.com/2015/09/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/). It adds code that can upload device and app information to a central server, create fake iCloud password signin prompts, and read and write from the copy-and-paste clipboard.

YiSpecter (October 2015)

YiSpecter, also discussed by Palo Alto Networks (http://researchcenter.paloaltonetworks.com/2015/10/yispecter-first-ios-malware-attacks-non-jailbroken-ios-devices-by-abusing-private-apis/), is malware that uses private APIs to perform malicious actions on both non-jailbroken and jailbroken iOS. It gets installed in the form of apps signed with enterprise certificates. Palo Alto Networks says "On infected iOS devices, YiSpecter can download, install and launch arbitrary iOS apps, replace existing apps with those it downloads, hijack other apps' execution to display advertisements, change Safari's default search engine, bookmarks and opened pages, and upload device information to the C2 server."

Muda (October 2015)

Muda (also called AdLord), discussed by Claud Xiao (https://twitter.com/claud_xiao/status/653606471876263936), is a form of adware for jailbroken devices. It has been in the wild at least since October 2013. He writes "It spreads via third party Cydia sources in China, and only affects jailbroken iOS devices. Its main behaviors include to display advertisements over other apps or in notification bar, and to ask user downloading iOS apps it promoted. "

Youmi Ad SDK (October 2015)

This advertising SDK, mostly used by Chinese App Store developers, was discovered by SourceDNA (https://sourcedna.com/blog/20151018/ios-apps-using-private-apis.html) to be abusing private APIs in order to collect more personal information than is allowed by Apple security and privacy guidelines, including the list of apps installed on a device, serial numbers of a device and internal components, and user's Apple ID email address. Youmi exploited a weakness in App Store review process and evaded detection by obfuscating private API calls using simple string manipulation. 256 apps with estimated 1 million downloads were found to be affected, including the official Chinese McDonald's app.

AceDeceiver (March 2016)

AceDeceiver, reported by Claud Xiao of Palo Alto Networks (https://researchcenter.paloaltonetworks.com/2016/03/acedeceiver-first-ios-trojan-exploiting-apple-drm-design-flaws-to-infect-any-ios-device/), is malware for non-jailbroken iOS devices. It gets on non-jailbroken devices through a desktop application that exploits design flaws in Apple's DRM mechanism to install a malicious iOS app from the App Store. It can install the malicious app even after the app is removed from the App Store, and it doesn't require misusing an enterprise certificate.

Safari JavaScript pop-up scareware (March 2017)

Lookout reported (https://blog.lookout.com/blog/2017/03/27/mobile-safari-scareware/) that scammers had "abused the handling of pop-up dialogs in Mobile Safari in such a way that it would lock out a victim from using the browser. The attack would block use of the Safari browser on iOS until the victim pays the attacker money in the form of an iTunes Gift Card. During the lockout, the attackers displayed threatening messaging in an attempt to scare and coerce victims into paying. However, a knowledgeable user could restore functionality of Mobile Safari by clearing the browser's cache via the the iOS Settings — the attack doesn't actually encrypt any data and hold it ransom."

iOS 10.3 changed the handling of JavaScript pop-ups to prevent this problem, making pop-ups "per-tab rather than taking over the entire app".

mainrepo RAT

Certain packages on the jailbreak API repository named "mainrepo" contain a remote access trojan. info: https://twitter.com/esetresearch/status/1374889630399619080. This malware is still being used and distributed in the wild at time of writing (4-30-2021).

Tools used by governments (and similar) to target individuals

FinSpy Mobile (August 2012)

FinFisher is a suite of commercial surveillance tools sold to governments, which have been used to target activists and other people. The suite includes spyware tools for many mobile operating systems, including iOS (https://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/).

DROPOUTJEEP (December 2013)

In December 2013, a conference presentation included information about a NSA tool called DROPOUTJEEP: "a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device. SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted." (http://www.forbes.com/sites/erikkain/2013/12/30/the-nsa-reportedly-has-total-access-to-your-iphone/) The information was from an internal NSA software catalog from 2008. The presenter speculated that Apple had helped build this tool, and Apple said it "has never worked with the NSA to create a backdoor in any of our products" (http://techcrunch.com/2013/12/31/apple-says-it-has-never-worked-with-nsa-to-create-iphone-backdoors-is-unaware-of-alleged-dropoutjeep-snooping-program/).

Hacking Team tools (June 2014 and July 2015)

Hacking Team is a company that "sells offensive intrusion and surveillance capabilities to governments and law enforcement agencies", including iOS spyware tools. The iOS spyware tools appear designed for targeting/attacking specific people, not for broad surveillance of the public. Their main tool (Remote Control System) requires a jailbroken device, and they were researching options for non-jailbroken devices.

Inception (December 2014)

Inception is an "attack framework" from an unknown source that targets individuals to steal information, using phishing emails and other techniques along with malware for iOS and other mobile operating systems, described in this post by security researchers who identified it (https://www.bluecoat.com/security-blog/2014-12-09/blue-coat-exposes-%E2%80%9C-inception-framework%E2%80%9D-very-sophisticated-layered-malware). According to the whitepaper from those security researchers (http://images.machspeed.bluecoat.com/Web/BlueCoat/%7B7f2dda62-f240-48dc-b05e-5cc620747b73%7D_bcs_wp_The_Inception_Framework_Cloud-Hosted_APT_EN_1d.pdf), a target may receive a phishing email

with a link that says it's a WhatsApp update, and if clicked on jailbroken iOS, it triggers "the download of a Debian installer package, WhatsAppUpdate.deb, also 1.2Mb in size. This application impersonates a Cydia installer, and can only be installed on a jailbroken phone" (page 23). It's unclear what they mean by "impersonates a Cydia installer", but a .deb file is the standard format for software packages installable via Cydia. The iOS malware collects the device's ICCID, address book, phone number, MAC address, and other information.

Another group of security researchers also identified this attack framework and called it Cloud Atlas (http://www.cso.com.au/article/562325/sophisticated-malware-targets-execs-pcs-android-blackberry-ios-devices/).

More articles: Apple Insider (http://appleinsider.com/articles/14/12/11/massive-sophisticated-inception---cloud-atlas-malware-infects-windows-and-android-but-cant-exploit-apples-ios-without-jailbreak), Forbes (http://www.forbes.com/sites/thomasbrewster/2014/12/10/iphone-android-attacks-on-diplomats/). There is a sample download available via this blog (http://contagiominidump.blogspot.de/2014/12/cloud-atlas-inception-ios.html).

XAgent (February 2015)

XAgent is a surveillance tool targeting specific people (such as people in governments, the military, and journalists) that can affect both non-jailbroken and jailbroken devices, as described in this article by Trend Micro (http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/). Also covered by PCWorld (http://www.pcworld.com/article/2880152/new-spyware-targets-ios-devices-steals-pictures-and-data.html).

Pegasus (August 2016)

Pegasus is a spyware product for iOS built by NSO Group, sold to governments, which has been used for attacks against political dissidents. It uses a chain of exploits nicknamed Trident to silently jailbreak the target device, and then it installs malware. Lookout Security described it in a post (https://blog.lookout.com/blog/2016/08/25/trident-pegasus/) and a technical analysis (https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf). Citizen Lab wrote a post about its use (https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/).

In June 2017, the New York Times reported (https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html?_r=0) that the Mexican government used Pegasus to target human rights lawyers, journalists and anti-corruption activists.

Cellebrite (February 2017)

As reported by Motherboard in February 2017 (https://motherboard.vice.com/en_us/article/hacker-dumps-ios-cracking-tools-allegedly-stolen-from-cellebrite), Cellebrite is "an Israeli firm which specializes in extracting data from mobile phones for law enforcement agencies". According to leaked information, "much of the iOS-related code is very similar to that used in the jailbreaking scene", such as limera1n and QuickPwn, with additions: "some of the code in the dump was designed to brute force PIN numbers". The leaked files are available online (https://www.reddit.com/r/jailbreak/comments/5rtffh/newsfirm_that_helped_fbi_break_into_san/ddan91v/).

CIA "Vault 7" materials (March 2017)

On March 7, 2017, WikiLeaks released a collection of CIA documents called Vault 7 (https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html), dated from 2013 to 2016, that include information about CIA hacking tools for iOS devices. The materials include documentation for CIA iOS exploitation research (https://wikileaks.org/ciav7p1/cm

s/space_2359301.html) and a list of iOS exploits they have (https://wikileaks.org/ciav7p1/cms/page_13205587.html).

Tools developed as part of research

iSAM (June 2011)

iSAM is a malware tool developed by security researchers (http://link.springer.com/chapter/10.1007%2F978-3-642-21424-0_2) as a proof of concept. It affects both jailbroken and not-yet-jailbroken devices: it scans for jailbroken devices that have SSH running and the default root password, and it also includes a malicious version of the Star exploit (JailbreakMe 2.0) so it can jailbreak a device that isn't jailbroken yet.

Instastock (November 2011)

Charlie Miller, a security researcher, submitted an app to the App Store called Instastock (http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/) to demonstrate "a flaw in Apple's restrictions on code signing on iOS devices". The app was initially accepted and then pulled from the store.

Mactans (July 2013)

At the Black Hat 2013 conference, security researchers presented a tool called Mactans, a small device that looks like a charger but can insert malware if you plug an iOS device into it (http://www.zdnet.com/article/researchers-reveal-how-to-hack-an-iphone-in-60-seconds/). The iOS device does not have to be jailbroken.

Jekyll (August 2013)

At the USENIX Security Symposium in 2013, security researchers described a method for getting a malicious app approved for the App Store, "created with remotely-exploitable vulnerabilities built in, masked by legitimate features to evade detection during the App Store approval process, but ready to be triggered once the app was installed on an iOS device." (http://www.theguardian.com/technology/appsblog/2013/aug/19/ios-malware-apple-iphone-ipad-jekyll) They successfully got an app approved for the App Store with this method (which "was only active for a few minutes following its launch in March, and during that time it wasn't installed by anyone not involved in the experiment" (http://arstechnica.com/security/2013/08/seemingly-benign-jekyll-app-passes-apple-review-then-becomes-evil/)).

XARA attacks (June 2015)

Security researchers found methods for "cross-app resource access" (XARA) attacks on OS X and iOS, and they submitted malicious proof-of-concept apps to the Mac and iOS App Store. Apple approved the apps, and the researchers immediately removed them from the stores. These XARA attacks were ways of bypassing the sandboxes that are supposed to prevent an app from accessing files that don't belong to that app, described by the security researchers in a paper (https://drive.google.com/file/d/0BxxXk1d3yyuZOFlsdkNMSGswSGs/view). Ars Technica article (http://arstechnica.com/security/2015/06/serious-os-x-and-ios-flaws-let-hackers-steal-keychain-1password-contents/).

NeonEggShell (August 2015)

NeonEggShell (http://neoneggplants.com/projects/neoneggshell/) is a command shell creation tool for iOS and OS X. The author says "This project is a proof of concept way to demon strate how easy it is to take over a whole device with a piece of code no bigger than a twitter post." The project includes tools for making payloads for jailbroken iOS, with features such as keylogging and location tracking. By default, the tool includes a "prompt that asks for permission before allowing any connection to the remote server."

Tools for sale to the public to target individuals

1mole

1mole (http://www.bosspy.com/user/iphoneos.aspx) is a spying tool available to the public via their own repository, authored by Bosspy. It describes itself on its website (http://www.bosspy.com/user/default.aspx) as "For Parents" ("Have your children going home after school? Consult their GPS position to be sure."), "For individuals" ("You think about your lost or stolen mobile phone."), and "For Employers" ("Install the software on your business phones and locate them in real time"). Its feature list includes "Track GPS locations" and "Capture the lock sreen passcode" for free, and "Record text messages", "Log Calls details", "Website monitoring", and "Keylogger" as paid services.

Copy9

Copy9 (http://cydia.saurik.com/package/com.goldenspy.copy9/) is a spying tool available to the public via the ModMyi repository (a default repository), authored by Copy9. It describes itself as "will be installed on target iDevice to find out a thief, cheating spouses, monitor chidren/employees or simply backup data from your devices to our cloud server. This is the best spyware on the world in spying field." Copy9 website (http://copy9.com/).

Copy10

Copy10 (http://cydia.saurik.com/package/com.copy10.copy10/) is a similar but separate spying tool available to the public via the ModMyi repository (a default repository), authored by IntelMobi/goldenspy. Their description includes "Are you having trust issues in your relationship? Sign that your kid's personality has changed and their behaviors, does your teenager hang out with friends you're concerned about? What if you believe one of your employees is a spy or is stealing company's technology, intellectual property or trade secrets?" IntelMobi website (https://www.intelmobi.com/).

FlexiSPY

FlexiSPY (http://www.flexispy.com/en/iphone-tracker-spy-on-iphone.htm) is a spying tool available to the public presumably via their own repository (this isn't specified on their website, but it's specified that you need the device to be jailbroken), authored by Flexispy, Ltd. Their website says "If you have a committed relationship with your partner or are responsible for a child or employee YOU HAVE A RIGHT TO KNOW To protect your relationship, spy on their iPhone."

iKeyGuard Key Logger

iKeyGuard Key Logger (http://cydia.saurik.com/package/com.ikeyguard.ikg/) is a keylogging tool available to the public via the BigBoss repository (a default repository), authored by iKeyGuard. Its description includes "Warning: Logging other people without their permission might be illegal in your country! Make sure you abide by your local law."

iKeyMonitor keylogger

iKeyMonitor keylogger (http://cydia.saurik.com/package/com.aw.mobile.ikm/) is a keylogging tool available to the public via the BigBoss repository (a default repository), authored by Awosoft Technology. Its website (http://ikeymonitor.com/) includes "How to monitor your children's cell phone to discover the truth and protect them from potential dangers? Now with iKeyMonitor you can uncover the truth by secretly monitoring mobile phones and tablets such as iPhone/iPad/iPod and Android device."

InnovaSPY

InnovaSPY (http://cydia.saurik.com/package/com.innovaspy.innovaspy/) is a spying tool available to the public via the ModMyi repository (a default repository), authored by Innovaspy. Its description says "Perfect iPhone spy app" and lists reasons to use it as "Protect your child from cyber predators" and "Find out THE TRUE from cheating spouse?" Related package: InnovaMonitor (http://cydia.saurik.com/package/com.innovaspy.innovamonitor/), a monitoring app for use with the spy tool. InnovaSPY website (http://innovaspy.com/).

Mobile Spy

Mobile Spy (http://www.mobile-spy.com/iphone-v7.html) is a spying tool available to the public via their own repository, authored by Retina-X Studios. Their website (http://www.mobile-spy.com/) says "View your Child or Employee's Smartphone and Tablet Usage. Monitor text messages, GPS locations, call details, photos and social media activity. View the screen and location LIVE!"

MobiStealth

MobiStealth (http://www.mobistealth.com/iphone-spy) is a spying tool available to the public for both jailbroken iOS (http://www.mobistealth.com/iphone-spy) (presumably installed via their own repository) and non-jailbroken iOS (http://www.mobistealth.com/ios-non-jailbreak) ("All that you require is the Apple ID and password of the iPhone or iPad that you want to monitor to get remote access to"). Their website includes "Are your employees misusing company owned phones? Are your kids getting more possessed and do not want to share anything with you? Stop wondering and thinking all day long, Mobistealth iPhone spy app is exactly what you need."

mSpy

mSpy (http://cydia.saurik.com/package/com.mtechnology.mspy.trial/) is a spying tool available to the public via the BigBoss repository (a default repository), authored by Mtechnology. Its description of itself: "mSpy is the best tracking and spy application that allows users to keep a check on the cell phone activities of their kids other family members or employees in order to avoid any unwanted behavior or for safety purposes."

The mSpy website indicates that they also have a version for non-jailbroken devices (http://www.mspy.com/compatibility.html).

In May 2015, mSpy had a customer data breach (http://krebsonsecurity.com/2015/05/mspy-denies-breach-even-as-customers-confirm-it/).

OwnSpy

OwnSpy (http://cydia.saurik.com/package/com.ownspy.daemon/) is a spying tool available to the public via the ModMyi repository (a default repository), authored by Antonio Calatrava. It describes itself as "Spy your own iPhone or iPad", with call recording, location tracking, and other features. It has a warning that says "Installing OwnSpy on a device that does not belong to you is a criminal offense and may be prosecuted. Mobile Innovations will help authorities if required." OwnSpy website (http://en.ownspy.com/P000001-install-on-ios).

Spy App

Spy App (http://cydia.saurik.com/package/com.spyapp.daemon/) is a spying tool available to the public via the ModMyi repository (a default repository), authored by dmarinov. Its description includes "Remotely spy SMS, Emails, Call Logs, GPS Location, Key presses (Keylogger)" and other features. It says it is "absolutely invisible and undetectable."

SpyKey

SpyKey (http://cydia.saurik.com/package/com.kobisnir.spykey/) is a keylogging tool available to the public via the BigBoss repository (a default repository), authored by Kobi Snir. Its description includes "a simple app that let you monitor your PC Keyboard activity in real time, Simply connect your iphone to your compute using your Wifi or 3G connection and start monitoring." The SpyKey website (http://www.ioslinks.com/spykey/) includes "Great use for parental control purposes, protect your kids from chating with strangers!", "Discover usernames & passwords", and "Spy unfaithfull husband or wife."

StealthGenie

StealthGenie was a spying tool available to the public via their own repository (http://blog.flexispy.com/remove-stealthgenie-iphone-android/). It also supported other mobile operating systems. In November 2014, the person who advertised and sold this product was charged with a federal crime and fined $500,000 (http://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine). The charge was "sale of an interception device and advertisement of a known interception device", a wiretapping crime. A Forbes article (http://www.forbes.com/sites/kashmirhill/2014/09/30/stealthgenie-ugly-marketing-of-spyware/) says "according to the FBI, Akbar and his team developed an internal business plan that revealed that — duh — the primary target audience for the app was people who thought their partners were cheating." The Forbes article points out #Mobile Spy, #mSpy, #FlexiSPY, and #MobiStealth as similar products.

Trapsms

Trapsms was an early spying tool available to the public, described in this post by a security researcher in July 2009 (http://blog.fortinet.com/post/detecting-spyware-for-iphones). She says: "The spyware installs on any jailbroken iPhone. In Cydia (an iPhone front-end to help installing third-party applications), you first add the URL of the spyware's repository and then install the two spyware packages."
