A rising number of threat actors have begun developing malware designed to infect devices running Mac OS X or iOS.
OVERVIEW ................................................................. 3
Apple ecosystem security .......................................... 5
Mac OS X malware ..................................................... 10
iOS malware ............................................................ 16
Attack vectors .......................................................... 18
Mac OS X vulnerabilities .......................................... 20
iOS vulnerabilities .................................................... 24
Apple ID security ...................................................... 25
Conclusion .............................................................. 27
Protection ............................................................... 27
Appendix ................................................................... 29
Apple devices have experienced a surge in popularity in recent years. According to IDC, the company now accounts for 13.5 percent of global smartphone shipments and 7.5 percent of global PC shipments. This increase in usage has not gone unnoticed by attackers. A rising number of threat actors have begun developing malware designed to infect devices running Mac OS X or iOS.

Although the number of threats targeting Apple operating systems remains quite low when compared to the company's main competitors (Windows in the desktop space and Android in mobile), the amount uncovered has grown steadily in recent years. In tandem with this, the level of Apple-related malware infections has spiked, particularly in the past 18 months.

Security researchers have also given a greater focus on vulnerabilities in Apple software, with a number of high-profile flaws uncovered in the past year. Zero-day brokers have begun offering bounties for Apple vulnerabilities, with US$1 million paid recently for a jailbreak of iOS 9.1.

Should Apple continue to grow in popularity, it seems likely that these trends will continue. Consequently, Apple users should not be complacent about security. They need to take precautions in order to prevent their devices from being compromised.
Greater security is, in part, one of the motivations behind the design of this software ecosystem.
Apple ecosystem security

Apple maintains a stronger degree of control over the software that users may install on their devices when compared to other platforms. Greater security is, in part, one of the motivations behind the design of this software ecosystem. The company has progressively moved towards a model where hardware and operating system are closely tied, and end users by and large acquire software from the official App Store.

Although the underpinnings of both of Apple’s operating systems (iOS and Mac OS X) are based on very similar kernel and user-space frameworks, iOS features are increasingly arriving on Mac OS X as well. As these two operating systems converge, there is an increased probability that attacks targeting one Apple OS could affect the other.

The “walled garden”

Apple Mac computers are shipped with Mac OS X preinstalled, and the hardware and operating system are marketed as a single package. Since 2006, the Boot Camp feature of Mac OS X permits users to create a dual-boot system on which they can also run Windows. While other operating systems can be installed, Windows is the only alternative supported by Boot Camp. Conversely, Mac OS X cannot be installed on third-party computers.

Similarly, Apple’s mobile operating system—iOS— is only distributed on Apple devices. The platform’s main rival is Google Android, which is open source and may be used by any device developer.

Beyond the operating system, Apple has steadily increased the control it exerts over what software may be installed on its devices. This “walled garden” approach began with the introduction of iOS in the first iPhone. Initially, iOS did not permit the installation of third-party apps. However, in 2008, Apple released an iOS Software Development Kit (SDK) for third-party developers. Version 2.0 of the operating system introduced the ability to install third-party apps.

The App Store

Apple retained oversight over which third-party apps the user could install by creating its own distribution platform: the App Store. iOS users can only install apps distributed through this channel or a small number of authorized private sources (as detailed in the “Alternative iOS distribution platforms” section of this report). In order for an app to be listed on the App Store, it must first be approved by Apple.

Users can bypass this restriction by “jailbreaking” their iOS device, which essentially involves taking advantage of privilege escalation vulnerabilities to gain root access and then replacing parts of the system applications. Although jailbreaking permits the user to install a greater range of software, it is a security risk as the user could inadvertently install malware that is packaged with or disguised as legitimate software. We have seen that pirated games distributed through unofficial markets for jailbroken iPhones often contain malware.

Security breaches

One of the most serious security breaches that affected the App Store occurred in September 2015, when it was discovered that a large number of Trojanized iOS apps were being hosted on the service. The apps were developed using a malicious version of Xcode, Apple’s software developer environment for iOS and Mac OS X apps.

While the company makes Xcode freely available, developers in China experienced difficulties downloading it directly from Apple. As a result, some of the developers resorted to downloading unofficial copies hosted on local sites. Unbeknownst to the developers using it, attackers modified one such Xcode package to insert malicious code in any app that was created using the affected copy.

Dubbed XcodeGhost (detected by Symantec as OSX.Codgost on Mac OS X computers and IOS.Codgost on iOS devices), this tainted copy of Xcode configured apps to collect information on devices and upload that data to command-and-control (C&C) servers. In addition to this, the Trojanized apps are capable of receiving commands from C&C servers in order to carry out phishing attacks. A large number of apps created using XcodeGhost
managed to bypass Apple’s own security checks and were hosted on the official App Store, demonstrating that the screening process does not a guarantee a malware-free App Store. In November, a new variant of XcodeGhost was discovered in unofficial versions of Xcode 7, which enables developers to create applications for iOS 9, Apple’s latest version of iOS.

In a bid to avoid further incidents, Apple said that it will offer locally hosted downloads of Xcode to Chinese developers in the future.

In October 2015, 256 iOS apps were removed from the App Store after an advertising SDK that they used was responsible for sending back personal and device information without users’ knowledge or consent. The SDK, known as Youmi, collected the following information:

- A list of all applications installed on the iOS device
- The platform serial number of iPhones and iPads running older versions of iOS
- A list of hardware components and the serial numbers for devices running new versions of iOS
- The Apple ID email address associated with the iOS device

There is no indication that any app developer who used the Youmi SDK in their products was aware of the kit’s malicious behavior. Apple said that it would no longer accept apps developed using the Youmi SDK.

**Alternative iOS distribution platforms**

Aside from the App Store, there are a few alternative Apple-sanctioned sources for apps. The Apple Developer Enterprise program allows organizations to distribute proprietary iOS apps to internal employees. Distribution can be handled by either hosting the app on a server belonging to the organization or using a third-party mobile device management (MDM) tool.

Another alternative platform is the Volume Purchase Program for Business. This allows developers to restrict the distribution of apps to authorized buyers. Apps are privately distributed to identified customers through the Business version of the App Store.

**Attacks leveraging alternative platforms**

These alternative platforms have, on occasion, been leveraged by attackers to distribute malware to iOS devices. For example, the YiSpecter Trojan (detected by Symantec as iOS.Specter) used the Developer Enterprise framework to create malicious apps which could be installed on Apple devices. The malware was packaged and signed with legitimate enterprise certificates, allowing it to be installed directly onto a device without being listed on the App Store.

How the attackers acquired the enterprise certificates remains unknown. They may have registered themselves as developers, paying the required fee and passing the vetting process. Alternatively, they could have partnered with a registered developer or stolen the certificates from legitimate developers.

Malicious apps that have obtained legitimate enterprise certificates can be promoted in forums. They could also be linked to in social-engineering text messages or emails that are sent to potential victims. Even when using enterprise certificates to sign malware, attackers still have several hurdles to jump before they can successfully install malware on an iOS device. In older versions of iOS, the first time an end user installs an enterprise-signed app, they receive a prompt asking them if they trust the app.

Following the release of iOS 9 in 2015, this security measure has been strengthened. When the end user opens an app they've manually installed, they receive a notification that the developer of the app isn’t trusted on their device. While the user can dismiss this message, they can’t open the app until they have confirmed that they trust the developer in the Settings app.

**Mac App Store**

The relative success of the iOS App Store has prompted Apple to move in the same direction with regard to Mac OS X applications with the launch of the Mac App Store in 2011. Apple vets all apps submitted to the Mac App Store and provides a range of guidelines that developers must follow. Unlike its iOS equivalent, the Mac App
The Apple threat landscape

Store is not an exclusive distribution platform, as third-party apps from other sources can be installed on Mac OS X computers. However, Apple has progressively tightened security around third-party Mac OS X applications and has indicated that it will continue to do so in the future.

Gatekeeper

While the walled garden approach is most developed in the iOS marketplace, Apple has steadily increased the level of security around what can be installed on computers running Mac OS X. Introduced in September 2012 as an update to OS X 10.7 “Lion”, Gatekeeper is a feature that allows Mac OS X users to automatically block the opening of applications from untrusted sources.

Gatekeeper provides the user with three options. The first will only permit apps that have been downloaded from the Mac App Store to be opened. The second option, which has been the default since OS X 10.8 “Mountain Lion”, only permits the opening of apps that have either been downloaded from the Mac App Store or from developers who have received a unique Developer ID from Apple and use it to digitally sign their apps.

The third option permits the user to run applications regardless of their origin. This effectively means that Gatekeeper has been turned off. Even when this setting has been selected, Gatekeeper will still block apps that have been signed with a Developer ID but have been altered or tampered with after they were signed.

Gatekeeper does allow a user to override its settings by right clicking on the app and opening it from the context menu. The user will be presented with a warning prompt, giving the choice of opening the app or cancelling the action.

While Gatekeeper provides the user with considerable scope for bypassing its security features, administrators can lock down computers to prevent this from happening. For example, changing Gatekeeper options requires
an administrator password. Opting to override Gatekeeper on a case-by-case basis also requires administrative privileges.

It should be noted that Gatekeeper only monitors applications downloaded from the internet. Apps installed from other sources such as USB drives will not be prevented from running.

**Weaknesses in Gatekeeper**

Weaknesses have been discovered in Gatekeeper from time to time. For example, in September 2015, a vulnerability was found which could allow an attacker to secretly install malicious software on an affected computer by bundling the threat with a legitimate application.

The vulnerability was uncovered by security researcher Patrick Wardle, who found that Gatekeeper could be bypassed by including an unsigned malicious file in the same directory of a legitimate signed app.

According to Wardle, Gatekeeper only carried out checks on the parent file, which was the signed app. If the application was executed, the malicious file would also run unchecked. Wardle said that the vulnerability affects the current version—OS X El Capitan—and its predecessor, OS X Yosemite (10.10).

At the time of writing Apple is reported to be working on a short-term mitigation measure as a stop gap until a full patch is released.

**File Quarantine**

Introduced in OS X 10.5 Leopard, File Quarantine is a security measure that quarantines files that applications have downloaded from the internet. Quarantine-aware applications such as Safari, Messages, iChat, and Mail will generate a warning to the user, asking if they are sure they want to open the file.

From OS X 10.6 Snow Leopard onwards, a File Quarantine feature known as XProtect also checks downloaded files for known malware before the user opens them.

**System Integrity Protection**

The release of OS X 10.11 El Capitan in September 2015 saw the introduction of further security tightening in the form of System Integrity Protection. This bundled a number of measures designed to restrict the access of poorly designed or malicious software to system locations and processes. One of the biggest changes that System Integrity Protection introduced was the removal of unlimited access to all parts of the system given to root accounts, a legacy of Mac OS X’s origins as Unix-based operating system.

Among the changes included in System Integrity Protection are:

- **File system protections:** System locations can no longer be written to, even by root accounts. Instead, system files can only be modified by processes signed with Apple’s own code-signing identity. Processes belonging to apps now have to write to locations designated for third-party developers.
- **Runtime protections:** Third-party applications can no longer attach themselves to system processes. Now, system binaries can only be modified either by an Apple Installer or Software Update from Apple-provided packages. Runtime attachment or code injection by third-party apps is no longer possible.
- **Kernel extensions:** Kernel extensions (aka kext) must now be signed with a valid Apple Developer certificate. System Integrity Protection can be disabled. However, doing so requires the user to boot to the Mac OS X recovery partition and run a command there.
Along with malicious software, the number of new adware risks and potentially unwanted or misleading applications for Mac OS X has increased steadily in recent years.
Mac OS X malware

Contrary to some beliefs, the Mac OS X environment is not free from malware. Cybercriminals have become aware of the increasing popularity of Apple Mac computers in recent years.

Symantec telemetry has shown a significant upsurge in threat and risk detections on Mac OS X computers since midway through 2014. There are several factors influencing this rise.

Along with malicious software, the number of new adware risks and potentially unwanted or misleading applications for Mac OS X has increased steadily in recent years. A number of these new security risks have been distributed widely. For example, protection for the misleading application SearchProtect (detected by Symantec as OSX.SearchProtect) was created on June 30 2014 and has since become the Mac OS X risk most frequently detected by Symantec.

Similarly, Symantec detection for another potentially unwanted application known as Genieo was created on July 10 2014 and it has since gone on to record a high number of installations. Other prolific threats included OSX.Sudoprint (created August 4 2015) and OSX.WireLurker (created November 6 2014).

The overall trend is similar to what has been observed by other vendors. For example, a recent study by Bit9 + Carbon Black found that the number of Mac OS X malware samples it detected in 2015 was five times greater than in the previous five years combined.

Adware, and unwanted and misleading applications

While the number of infections on Mac OS X computers has increased dramatically over the past year, a significant amount of this spike has been accounted for by nuisance applications, such as adware, and potentially unwanted or misleading applications.
Although these programs have a high prevalence, they present a lower degree of risk to the end user compared to Trojans or other categories of malware, since their purpose is usually to perform less harmful activities such as modifying the default search engine on web browsers or displaying ads.

While adware, and unwanted and misleading application infections accounted for much of the surge in infections between June 2014 and March 2015, recent months have seen a significant uptick in infections involving other forms of malware.

New threats

Although still small in terms of overall malware numbers, the number of new Mac OS X threats discovered annually is trending upwards. The increase in threats targeting Mac users may, in part, be driven by the growing popularity of Apple platforms. For example, Mac OS X’s market share now stands at 8 percent, almost double what it was seven years ago. Continuing growth for Apple will mean that a greater proportion of attackers will stop regarding the company’s desktop OS as a niche market and begin targeting it more often.

A growing number of cybercriminals, corporate espionage groups and state-sponsored intelligence operations have begun targeting Apple users with malware designed to run on Mac OS X. As far back as 2011, specialist Mac OS X malware creation toolkits were beginning to be developed, such as the Weyland-Yutani BOT toolkit, believed to be the first to target the platform.
Ransomware has presented a significant threat in recent years but attackers have, to date, largely focused on Windows users. Macs have on occasion been targeted with ransomware in the form of browser-based threats. There have been instances of malicious websites targeting Safari for Mac users, with JavaScript causing the browser to display persistent pop-ups informing the user that the FBI had “locked” Safari as it was used to view illegal content.

In November 2015, a proof-of-concept (PoC) threat known as Mabouia (detected by Symantec as OSX.Ransomcrypt) was developed by Brazilian cybersecurity researcher Rafael Salema Marques to highlight the fact that Macs may not be immune to the threat of ransomware.

Marques shared a sample of the ransomware with Symantec and Apple. Symantec’s analysis has confirmed that the PoC is functional. While the threat could be used to create working Mac OS X crypto ransomware if it fell into the wrong hands, Marques said he has no intention of publicly releasing the malware, though his experiment may ultimately inspire others.

Figure 5. While malcode threats are less prevalent, their infections can be more damaging.
Butterfly: Corporate espionage attacks

A growing number of high-level attack groups have begun to broaden their capabilities by developing or acquiring malware designed to run on Apple platforms. For example, Butterfly, a corporate espionage group *uncovered by Symantec in 2015*, has a suite of custom malware tools capable of attacking both Windows and Apple computers.

The group has used different pieces of malware, all of which appear to be internally developed. Its primary tools are two back door Trojans, OSX.Pintsized is capable of opening a back door on Mac OS X computers. Its Windows counterpart is Backdoor.Jiripbot.

OSX.Pintsized is a modified version of OpenSSH that runs on Mac OS X, and contains additional code to read two new arguments and an embedded RSA key. The two additional arguments are “-z” and “-p”, which are used to pass a C&C server address and port respectively. The back door has also been observed using a very basic Perl script that opens a reverse shell.

The group is not affiliated to any nation state and appears to be financially motivated. It has attacked major corporations operating in the internet, IT software, pharmaceutical, and commodities sectors. Twitter, Facebook, Apple, and Microsoft are among the companies which have publicly acknowledged that they were targeted by the group. The campaign against Apple involved the compromise of a number of employees’ Mac OS X computers. Apple said that the exploit was delivered through a “site aimed at iPhone developers.”

WireLurker

One of the most significant recent threats targeting Apple users was WireLurker (detected by Symantec as OSX.Wirelurker).

*Discovered in November 2014*, the malware was used to Trojanize several hundred Mac OS X applications on the Maiyadi App Store, a third-party Mac app store in China. These Trojanized applications could then infect any iOS device that connects to the computer through a USB cable. The iOS device does not need to be jailbroken to be infected.

Once installed on an iOS device, WireLurker is capable of stealing information, such as contacts and messages, and uploading the data to a C&C server.

It is believed that some 467 Mac OS X applications on the Maiyadi App Store were compromised with WireLurker and these applications were downloaded more than 300,000 times. Since its discovery, Symantec has blocked over 2,000 WireLurker instances. A similar tactic was also used by the Hacking Team in order to infect its targets.

SearchProtect

SearchProtect (detected by Symantec as OSX.SearchProtect and OSX.Searchprotect!gen1) is the Mac OS X risk most frequently detected by Symantec over the past three years. SearchProtect is classed as a misleading application, since it carries out actions that the user may not have requested. In this case the app modified web browsers’ default search engine.

This misleading app must be manually installed by the end user and is usually bundled with third-party installers or download managers.
Sudoprint

Sudoprint (detected by Symantec as OSX.Sudoprint) is a Trojan horse that exploits the Apple Mac OS X DYLD_PRINT_TO_FILE Local Privilege Escalation Vulnerability (CVE-2015-3760) and may perform malicious activities on the compromised computer.

The DYLD_PRINT_TO_FILE vulnerability was disclosed in July 2014 by German security researcher Stefan Esser. The vulnerability occurred in the Mac OS X dynamic linker, DYLD. New features in DYLD were introduced in OS X 10.10, one of which was DYLD_PRINT_TO_FILE. This feature did not contain the usual safeguards for dynamic linker variables and, as a result, it afforded an easy means for the escalation of privileges.

The vulnerability attracted the attention of attackers, leading to the discovery of the Sudoprint Trojan in early August. The malware exploited the vulnerability to ensure that the attacker was not asked for a password for privileged operations on the targeted computer, enabling them to perform malicious activities without detection. This example highlights the fact that not all threats targeting Mac OS X rely on manually installing the malware or tricking the user into revealing their password.

Apple patched the vulnerability with the release OS X 10.10.5 on August 13, 2015. This update appears to have quelled activity around the Sudoprint malware, with no infections logged by Symantec since September 2015.

Genieo

Genieo (detected by Symantec as Genieo and OSX.Genieolgen1) is classed as a potentially unwanted application, since it may be bundled with other app installers, and carries out actions that the user may not have requested. In this case the application installs a browser extension that changes the browser’s default search engine. Genieo makes a user’s search query appear to be carried out using Google Search but the results will be from genieo.com.

Symantec and Norton products have blocked the application since July 2014. Genieo behaves similarly to the aforementioned SearchProtect and has also accounted for a significant number of Mac OS X infections.

RSPlug

RSPlug (detected by Symantec as OSX.RSPlug.A) is one of the most widely detected Mac OS X Trojans. The malware alters the domain name system (DNS) settings on a compromised computer which can be used to redirect the user to a malicious DNS server.

Legitimate DNS servers will translate internet address names to the IP addresses associated with them. A malicious DNS server can reroute traffic to destinations of the attackers’ choosing, such as fake websites designed to steal credentials or websites capable of installing malware on the victim’s computer.

RSPlug is one of the earlier examples of how attackers create Mac OS X variants of Windows threats. In this instance, RSPlug is a variant of the Windows Flush Trojan (detected by Symantec as Trojan.Flush.A). Flush was circulating for several years before its Mac OS X variant appeared.
The number of iOS threats discovered to date remains quite small, although it is beginning to increase...
iOS malware

The number of iOS threats discovered to date remains quite small, although it is beginning to increase, with seven new threats discovered in 2015 so far. This is up from the previous high of three in 2014.

Attackers targeting the mobile operating system need to find a way to install malware on a device, which can represent a significant hurdle. Many threats are installed when the target connects their device to a compromised desktop computer. Jailbroken devices present more opportunities for attacks, as many threats are designed to take advantage of jailbroken phones.

Figure 6. Number of new iOS threats that Symantec documented by year

Figure 7. Jailbroken devices present more opportunities for compromise and are at greater risk of attack.
KeyRaider

- Affects Jailbroken: Yes
- Affects Non-Jailbroken: No

One of the most potent iOS threats to emerge during 2015 was KeyRaider (detected by Symantec as iOS.Keyraider), a Trojan that was used to steal an estimated 225,000 Apple IDs and passwords.

The malware highlights the risk posed by jailbreaking an iOS device, as the threat was designed to target jailbroken devices. KeyRaider is distributed inside repackaged apps (i.e. free copies of commercial games and apps) on app marketplaces for jailbroken phones. Once running on an infected device, the Trojan intercepts iTunes traffic and steals the user’s login credentials, device GUID, Apple push notification service certificates and private keys, and iTunes purchase receipts. This information is then sent to a remote server.

Xagent

- Affects Jailbroken: Yes
- Affects Non-Jailbroken: No

Advanced persistent threat (APT) groups have begun to broaden their scope and have shown an interest in Apple platforms in recent years. An example of this is an attack group called Operation Pawn Storm (also known as APT28, Sednit, Fancy Bear, or Tsar Team). The group is believed to have ready access to zero-day vulnerabilities and may be responsible for an iOS threat called Xagent (detected by Symantec as iOS.Xagent).

Xagent is a Trojan that opens a back door and steals information from the compromised device. It has a broad range of capabilities. An attacker can command it to record audio, take screenshots, upload and download files, and list files and running processes on the device. It can also harvest information such as SMS messages, contacts, photos, geolocation data, a list of installed applications, and network status. It can then send the gathered data to a remote location.

The Trojan is used in a highly targeted manner and is believed to be installed on iOS devices through compromised desktop computers. The device may be infected when plugged into an infected computer. The exact method used to install Xagent is unknown, but it is only capable of infecting jailbroken devices.

Oneclickfraud

- Affects Jailbroken: Yes
- Affects Non-Jailbroken: Yes

The Oneclickfraud Trojan (detected by Symantec as iOS.Oneclickfraud) is another example of how threat actors have begun to target multiple platforms by developing variants of malware for several operating systems. Oneclickfraud was discovered by Symantec in May 2015 and targets iOS devices, attempting to trick users into paying for a subscription service.

The malware is distributed through malicious adult video websites. Victims may be directed to one of these sites either by clicking on a link in a spam email or stumbling across it while conducting an internet search. If the visitor clicks on a “play” button next to a video, they are presented with a pop-up window asking them to install an app. If they do this, their device becomes infected with the Oneclickfraud Trojan.

The malware is capable of infecting jailbroken and non-jailbroken devices. Symantec believes that the attackers abuse the Apple Developer Enterprise Program to enable their app to be installed on the device. During installation, the device notifies the user that the app comes from an untrusted developer and asks them if they wish to trust the app. The app can only run if marked trusted.

When launched, the app displays a membership page for an adult video site. The app then claims that the user has signed up for a subscription to the site and must now pay for this.

The iOS variant of this malware behaves in exactly the same was as its Android equivalent (detected by Symantec as Android.Oneclickfraud), which first appeared three years previously.
Passrobber

- Affects Jailbroken: Yes
- Affects Non-Jailbroken: No

Another example of the risk posed by jailbreaking iOS devices is Passrobber (detected by Symantec as iOS.
Passrobber), an information-stealing Trojan horse that was discovered in 2014.

The malware runs on jailbroken iOS devices that have installed Cydia Substrate (formerly known as Mobile
Substrate), an app that enables customization and modification of software on jailbroken devices.

The Passrobber Trojan is capable of intercepting outgoing SSL communications. It checks for Apple IDs and
passwords, and can send these stolen credentials to a C&C sever.

Attack vectors

Apple devices can be infected with malware through a range of different vectors. However, since Apple desktop
and mobile operating systems have a minority market share, the risk of attack is not as high as is it with more
common operating systems such as Windows or Android.

Spam email campaigns are one of the most common attack vectors. However, generally speaking, attackers
behind these campaigns aim to maximize infection numbers and consequently focus on distributing Windows-
based malware.

Apple malware is less likely to be indiscriminately spread in this fashion and instead may be distributed through
e-mails in limited, targeted attacks against an individual or organization.

Exploit kits

Exploit kits are another attack vector used for wide-ranging campaigns. None of the major exploit kits currently
in use (such as Angler, Rig, Nuclear, or Magnitude) are known to include exploits specifically targeting Apple
operating systems.

However, the major kits do exploit vulnerabilities in a number of cross-platform software packages such as Flash
or Java. In theory, this means that Mac OS X users are vulnerable to exploit kits too. However, there doesn’t
appear to be any current major exploit kit campaigns serving Mac OS X malware as a payload. By and large,
attackers again appear to be focused on maximizing infection numbers by serving Windows-based malware.

Nevertheless there some examples of smaller-scale exploit kit attacks targeting Mac OS X users. For example,
in 2012 F-Secure discovered an exploit kit hosted on a compromised Columbian transport website that checked
if the visitor was running Windows, Mac OS X, or Linux. If the kit successfully exploited a vulnerability on any of
these platforms, then it dropped a different payload tailored for each operating system.
In most years, the number of new Mac OS X vulnerabilities has been lower than the number of Windows vulnerabilities found.
The amount of new Mac OS X vulnerabilities emerging has remained relatively steady in recent years, at a rate of between 39 and 70 per year. In most years, the number of new Mac OS X vulnerabilities has been lower than the number of Windows vulnerabilities found. The greater numbers of Windows vulnerabilities may be reflective of the larger market share that the Microsoft operating system enjoys, prompting a greater level of scrutiny from attackers and security researchers.

A number of new Mac OS X vulnerabilities have drawn considerable public attention in 2015, mainly because of the threat that a successful exploit could pose to users.

**Multiple cross-app resource access (XARA) vulnerabilities**

Four separate vulnerabilities in Apple products were disclosed in June 2015 by a team of researchers based in the University of Indiana. The researchers discovered that the flaws allowed a malicious app to bypass security controls and steal sensitive data from other apps.

Apps installed through Apple’s Mac App Store and iOS App Store are normally confined to a sandbox. These apps are granted limited privileges and if they need to access any additional resources outside of their own container, then they need to get the user’s permission first. However, the following four vulnerabilities allowed unauthorized access to be granted, which the research team referred to as cross-app resource access (XARA) attacks.

- **Password stealing vulnerability:** Apple operating systems have a secure password storage feature known as Keychain which lets the user save and retrieve passwords for various apps and online services. One of the four vulnerabilities allowed a malicious app to create a preemptive keychain entry for another app. If the targeted...
app was not present on the computer and the user subsequently installs the app, its credentials were stored on the keychain entry created by the malicious app. If the targeted app was already installed, a malicious app could have deleted its existing keychain entry and created a new one, which the user would have re-entered their credentials to the next time they accessed the targeted app.

- **Container cracking:** A second vulnerability allowed a malicious app to gain access to the secure container belonging to another app and steal data from it. Each app container is given a unique identity known as a Bundle ID (BID). The Mac App Store doesn't allow submitted apps to use a BID that's already been used by another app. However, a problem occurred with sub-targets, which are apps that work embedded in another app such as extensions, frameworks, or helper programs. The Mac App Store did not verify if a sub-target's BID was identical to those belonging to other apps or their sub-targets. An attacker could have used a malicious app with sub-targets that included BIDs belonging to other apps or their sub-targets. This could have allowed the malicious app to gain full access to another app’s container.

- **Inter-process communication (IPC) interception vulnerability:** A further vulnerability lay in the fact that cross-app IPC channels on Mac OS X and others deployed across platforms such as WebSocket contain flaws which exposed critical information. For example, WebSocket is used to establish a connection between a server and a client. A malicious app could have claimed the port used by a legitimate application and intercepted data intended for it, such as passwords or other sensitive information.

- **Scheme hijacking vulnerability:** The fourth vulnerability related to the URL scheme that apps use to pass data to another app. For example, URLs beginning with “mailto” direct data to the Mail app. The vulnerability allowed a malicious app to hijack a scheme, which meant data sent to the target app would have been received by the malware instead. This could have facilitated the theft of access tokens and other information.

All apps distributed on the official Mac App Store and iOS App Stores are vetted by Apple and only the ones verified as safe are accepted. However, the researchers created a proof-of-concept malicious app which passed the vetting process and was briefly available on the Mac App Store before it was removed.

The vulnerabilities were reported to Apple in October 2014 and the company said it would require six months to roll out fixes. Apple subsequently released a server-side patch for the Mac App Store which blocked malicious apps exploiting any of the XARA vulnerabilities. The company said that additional fixes were in progress.

**Privilege escalation vulnerabilities**

Two privilege escalation vulnerabilities were discovered by Italian researcher Luca Todesco in August 2015. The findings attracted some publicity after the researcher posted a PoC exploit to GitHub. Todesco said that he reported the issue to Apple a few hours before making it public.

The exploit took advantage of two different vulnerabilities to create a memory corruption in the Mac OS X kernel. This in turn was exploited to bypass security features that blocked the exploit code from running, providing the attacker with root access to the computer.

The vulnerabilities affected Mac OS X version 10.9.5 (Mavericks) to 10.10.5 (Yosemite). The flaw was patched in the latest version, OS X 10.11 (El Capitan).

These vulnerabilities came to light days after Apple patched another privilege escalation vulnerability. The **DYLD_PRINT_TO_FILE vulnerability** (CVE-2015-3760) enabled a malicious file to gain root access to an affected computer, allowing it to install other unauthorized software.

**Extensible Firmware Interface (EFI) vulnerability**

In addition to vulnerabilities in Mac OS X itself, a number of security flaws affecting the firmware of Mac computers, known as the Extensible Firmware Interface (EFI), were also discovered in 2015.

One of the most notable of these vulnerabilities was the **Apple Mac OS X EFI Firmware Security Vulnerability** (CVE-2015-3692) which was disclosed by security researcher Pedro Villaca in May 2015. He discovered that a flawed energy conservation implementation on a wide range of Mac computers left flash memory protections...
unlocked after they woke up from sleep mode. This meant that an attacker could have reflashed the computer’s BIOS to install EFI rootkit malware.

If left unpatched, the CVE-2015-3692 vulnerability could have been remotely exploited by an attacker if used in conjunction with another exploit that provides root access. Once an attacker had this access, the only condition required for a successful exploit was that the computer entered sleep mode.

Apple released the Mac EFI Security Update 2015-001, which simultaneously patched CVE-2015-3692 and the “Rowhammer” memory corruption vulnerability (CVE-2015-3693), which affected some types of DRAM used on Mac computers.

Thunderstrike vulnerabilities

A number of other vulnerabilities that hit the headlines in recent times also affected firmware on a range of Mac OS X computers. In December 2014, researcher Trammell Hudson demonstrated that malware could be installed on the EFI boot ROM of Apple computers using the Thunderbolt port.

Hudson created a bootkit as a PoC, calling it “Thunderstrike”. The bootkit could be installed on vulnerable Macs within minutes by anyone with physical access to the computer. Furthermore, the malware could spread by copying itself to any Thunderbolt devices connected to the infected computer.

Apple patched the vulnerability (CVE-2014-4498) with the release of OS X Yosemite 10.10.2 and Security Update 2015-001.

Following on from this issue, another related vulnerability was uncovered in August 2015 when Hudson and fellow researcher Xeno Kovah developed another PoC worm capable of infecting the firmware of MacBooks. Dubbed “Thunderstrike 2”, this worm was far more dangerous than the original Thunderstrike since it could be installed remotely. The worm spread itself by infecting the option ROM on attached Thunderbolt peripherals, which may then be connected to other vulnerable computers.

Apple partially patched the vulnerability in June as part of the Mac EFI Security Update 2015-001.

Root Pipe vulnerability

Another major flaw to emerge in 2015 was the Root Pipe vulnerability (CVE-2015-1130). The issue was discovered by security researcher Emil Kvarnhammar, who found that the admin framework in Mac OS X contained a back door API to root privileges. A successful exploit could allow an attacker to gain administrative privileges without properly authenticating.

The flaw was patched with the release of OS X 10.10.3.
The number of new vulnerabilities found in iOS in recent years has been lower than in its desktop equivalent.
iOS vulnerabilities

The number of new vulnerabilities found in iOS in recent years has been lower than in its desktop equivalent. However, the amount of vulnerabilities being found annually has trended upwards over the past four years. Between 2011 and 2014, the amount of vulnerabilities affecting iOS has exceeded those that were documented for its main competitor, Google’s Android. That trend has reversed in 2015 as so far, new Android vulnerabilities have outstripped iOS.

While a number of Mac OS X vulnerabilities have attracted public attention over the past year, no flaw affecting iOS alone has caused high levels of alarm. Generally speaking, the most serious vulnerabilities impacting iOS tend to be cross-platform issues, occurring in technologies used in both iOS and Mac OS X. For example, one of the aforementioned four XARA vulnerabilities affected Apple’s mobile and desktop operating systems.

Nevertheless, iOS has begun to attract more attention from vulnerability researchers since a market for zero-day bugs affecting the platform has begun to develop. For example, one month after it offered a US$1 million bounty for a jailbreak of iOS 9.1, zero-day broker Zerodium confirmed that it was paying out to a team of researchers who uncovered a browser-based, untethered exploit.

Aside from the fact that the exploit can be triggered by visiting a specially crafted website, Zerodium didn’t reveal much about the flaw. Zerodium has described its customers as “major corporations in defense, technology, and finance” as well as “government organizations in need of specific and tailored cybersecurity capabilities.”

Figure 9. iOS and Android vulnerabilities discovered by year

The number of new vulnerabilities found in iOS in recent years has been lower than in its desktop equivalent. However, the amount of vulnerabilities being found annually has trended upwards over the past four years. Between 2011 and 2014, the amount of vulnerabilities affecting iOS has exceeded those that were documented for its main competitor, Google’s Android. That trend has reversed in 2015 as so far, new Android vulnerabilities have outstripped iOS.

While a number of Mac OS X vulnerabilities have attracted public attention over the past year, no flaw affecting iOS alone has caused high levels of alarm. Generally speaking, the most serious vulnerabilities impacting iOS tend to be cross-platform issues, occurring in technologies used in both iOS and Mac OS X. For example, one of the aforementioned four XARA vulnerabilities affected Apple’s mobile and desktop operating systems.

Nevertheless, iOS has begun to attract more attention from vulnerability researchers since a market for zero-day bugs affecting the platform has begun to develop. For example, one month after it offered a US$1 million bounty for a jailbreak of iOS 9.1, zero-day broker Zerodium confirmed that it was paying out to a team of researchers who uncovered a browser-based, untethered exploit.

Aside from the fact that the exploit can be triggered by visiting a specially crafted website, Zerodium didn’t reveal much about the flaw. Zerodium has described its customers as “major corporations in defense, technology, and finance” as well as “government organizations in need of specific and tailored cybersecurity capabilities.”
AirDrop vulnerability

Another recent cross-platform vulnerability to gain public attention occurred in AirDrop, an Apple wireless file transfer protocol. The flaw could have allowed an attacker to install malware on vulnerable iOS and Mac OS X devices simply by sending them a file. The vulnerability was deemed critical, as the target did not have to accept the file sent by the attacker for the exploit to trigger.

The vulnerability was discovered by Australian researcher Mark Dowd, who found that attackers were able to send a malicious file to any AirDrop-enabled device within range. Once the malicious file had been received, it could have then installed malicious software on the targeted device by taking advantage of a vulnerability in security checks, making the device act as if it had already marked the malware’s certificate as trusted. In Dowd’s PoC attack, he replaced an iPhone’s Phone app with another, non-functioning app.

Because the attack involved a signed app that was marked as trusted, the malicious software was granted extensive permissions, such as the ability to read contacts, use the camera, or capture location information.

Following discovery of the vulnerability, Apple incorporated additional security measures into the latest versions of Mac OS X and iOS, adding a sandbox to the AirDrop application and limiting the access it has to other parts of the operating system.

Apple ID security

The Apple ID is a credential used to sign into a broad range of Apple services, including the iTunes Store, the App Store, iCloud, and iWork. Given that the credential helps provide access to such a range of services, it is not surprising that it has attracted the attention of attackers, resulting in campaigns involving the theft of Apple IDs. A stolen Apple ID and password can be used to purchase music, movies, or software, with the owner’s payment card charged for the purchases. They can also be used to access personal information, such as files and photos backed up in iCloud.

The most high-profile Apple ID incident occurred during August 2014, when hundreds of private photos belonging to celebrities were released on the internet. The attackers were believed to have accessed the public figures’ Apple credentials, stealing any photos that the victims may have backed up on iCloud.

Following speculation that iCloud may have been compromised, Apple has said that it has found no evidence of a breach in any of its systems including iCloud or Find my iPhone. The company concluded that the leak was the result of phishing, “a very targeted attack on user names, passwords and security questions, a practice that has become all too common on the internet”.

Following the leak, Apple moved to allay privacy concerns. In a statement published on the Apple website, chief executive Tim Cook said that security and privacy were fundamental to the design of Apple products and services.

“Two-step verification, which we encourage all our customers to use, in addition to protecting your Apple ID account information, now also protects all of the data you store and keep up to date with iCloud,” Cook said.

Apple also moved to counter brute-force attacks against iCloud accounts after a proof-of-concept attack tool called iDict was released on GitHub. The tool’s author said it could bypass account lockout restrictions and secondary authentication on any Apple account. Apple immediately enforced rate limiting for login attempts such as those generated using iDict.
The success of Apple devices has generated increased interest among attackers.
Conclusion

- The success of Apple devices has generated increased interest among attackers, as a growing number of malicious actors are developing threats for Apple platforms.
- Symantec telemetry has shown a significant upsurge in malware infections on Mac OS X computers since midway through 2014.
- While the number of Symantec detections on Mac OS X computers has increased dramatically over the past year, a significant amount of this spike is attributed to nuisance applications, such as adware, and potentially unwanted or misleading applications.
- Although still small in terms of overall numbers, the amount of new Mac OS X malware discovered annually has been trending upwards over the past five years.
- The amount of iOS malware discovered to date remains quite small. Jailbroken devices present more opportunities for compromise, as many threats are designed to take advantage of jailbroken phones.

Protection

Both Symantec and Norton offerings provide a robust set of protection technologies for computers running Apple OS X. These include:

- **Network-based protection technologies.** Scanning network traffic entering and leaving a computer running OS X, these technologies (a firewall and an enterprise-grade Intrusion Prevention System [IPS]), are able to reconstruct application layer protocols on the fly to support looking for signs of malicious activity contained within and block as appropriate. This provides the ability to generically block attempts at exploiting known vulnerabilities.
- **File-based protection technologies.** The traditional file-based antivirus (AV) engines use a set of detection technologies to scan files looking for malicious content contained within. Included are real time scanning capabilities to monitor all file creation and modification activities to detect the first signs of malicious activity. These technologies provide a robust defense against all known OS X malware.

Details on Symantec protection offerings, including Symantec Endpoint Protection for OS X can be found here:

https://www.symantec.com/endpoint-protection

Details on Norton protection offerings, including Norton Security, can be found here:

www.norton.com/products
## Mac OS X threats

<table>
<thead>
<tr>
<th>Malware</th>
<th>Type</th>
<th>Discovery date</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSX.Leap.A</td>
<td>Worm</td>
<td>February 16, 2006</td>
</tr>
<tr>
<td>OSX.Inqtana.A</td>
<td>Worm</td>
<td>February 17, 2006</td>
</tr>
<tr>
<td>OSX.Inqtana.B</td>
<td>Worm</td>
<td>February 22, 2006</td>
</tr>
<tr>
<td>OSX.Exploit.MetaData</td>
<td>Trojan</td>
<td>May 31, 2006</td>
</tr>
<tr>
<td>OSX.Exploit.Launchd</td>
<td>Trojan</td>
<td>June 30, 2006</td>
</tr>
<tr>
<td>OSX.Macarena</td>
<td>Virus</td>
<td>November 2, 2006</td>
</tr>
<tr>
<td>OSX.RSPlug.A</td>
<td>Trojan</td>
<td>October 31, 2007</td>
</tr>
<tr>
<td>OSX.SaprilC.C</td>
<td>Trojan</td>
<td>June 23, 2008</td>
</tr>
<tr>
<td>OSX.Lamzev.A</td>
<td>Trojan</td>
<td>November 13, 2008</td>
</tr>
<tr>
<td>OSX.Iservice</td>
<td>Trojan</td>
<td>January 22, 2009</td>
</tr>
<tr>
<td>OSX.Iservice.B</td>
<td>Trojan</td>
<td>January 27, 2009</td>
</tr>
<tr>
<td>OSX.Tored@mm</td>
<td>Worm</td>
<td>May 5, 2009</td>
</tr>
<tr>
<td>Spyware.AoboKeyLogger</td>
<td>Spyware</td>
<td>October 27, 2009</td>
</tr>
<tr>
<td>OSX.Loosemaque</td>
<td>Trojan</td>
<td>November 3, 2009</td>
</tr>
<tr>
<td>OSX.HellRTS</td>
<td>Trojan</td>
<td>April 19, 2010</td>
</tr>
<tr>
<td>OSX.Keylogger</td>
<td>Spyware</td>
<td>April 19, 2010</td>
</tr>
<tr>
<td>OSX.Remoteaccess</td>
<td>Remote Access Trojan</td>
<td>April 19, 2010</td>
</tr>
<tr>
<td>OSX.Musminim</td>
<td>Trojan</td>
<td>February 27, 2011</td>
</tr>
<tr>
<td>MacProtector</td>
<td>Misleading Application</td>
<td>September 5, 2011</td>
</tr>
<tr>
<td>OSX.Imuler</td>
<td>Trojan</td>
<td>September 25, 2011</td>
</tr>
<tr>
<td>OSX.Revir</td>
<td>Trojan</td>
<td>September 25, 2011</td>
</tr>
<tr>
<td>OSX.Flashback</td>
<td>Trojan</td>
<td>September 30, 2011</td>
</tr>
<tr>
<td>OSX.Tsunami</td>
<td>Trojan</td>
<td>October 26, 2011</td>
</tr>
<tr>
<td>OSX.Coinbitminer</td>
<td>Trojan</td>
<td>November 1, 2011</td>
</tr>
<tr>
<td>OSX.Imauler</td>
<td>Trojan</td>
<td>March 21, 2012</td>
</tr>
<tr>
<td>OSX.Macontrol</td>
<td>Trojan</td>
<td>March 30, 2012</td>
</tr>
<tr>
<td>OSX.Flashback.K</td>
<td>Trojan</td>
<td>April 9, 2012</td>
</tr>
<tr>
<td>OSX.Sabpab</td>
<td>Trojan</td>
<td>April 13, 2012</td>
</tr>
<tr>
<td>OSX.Olyx.B</td>
<td>Trojan</td>
<td>April 18, 2012</td>
</tr>
<tr>
<td>OSX.Flashback.L</td>
<td>Trojan</td>
<td>April 24, 2012</td>
</tr>
<tr>
<td>MacDefender</td>
<td>Misleading Application</td>
<td>July 2, 2012</td>
</tr>
<tr>
<td>OSX.Crisis</td>
<td>Trojan</td>
<td>July 25, 2012</td>
</tr>
<tr>
<td>OSX.Dockster</td>
<td>Trojan</td>
<td>December 9, 2012</td>
</tr>
<tr>
<td>OSX.Getshell</td>
<td>Trojan</td>
<td>February 2, 2013</td>
</tr>
<tr>
<td>OSX.Netweird</td>
<td>Trojan</td>
<td>February 2, 2013</td>
</tr>
<tr>
<td>OSX.SMSSend</td>
<td>Trojan</td>
<td>February 2, 2013</td>
</tr>
<tr>
<td>OSX.FakeCodec</td>
<td>Adware</td>
<td>February 3, 2013</td>
</tr>
<tr>
<td>OSX.Dockster.A</td>
<td>Trojan</td>
<td>February 14, 2013</td>
</tr>
<tr>
<td>OSX.Pintsized</td>
<td>Trojan</td>
<td>February 20, 2013</td>
</tr>
<tr>
<td>OSX.Okaz</td>
<td>Adware</td>
<td>April 18, 2013</td>
</tr>
<tr>
<td>Malware Name</td>
<td>Type</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------</td>
<td>---------------</td>
</tr>
<tr>
<td>OSX.Kitmos</td>
<td>Trojan</td>
<td>May 16, 2013</td>
</tr>
<tr>
<td>OSX.Hackback</td>
<td>Trojan</td>
<td>May 18, 2013</td>
</tr>
<tr>
<td>OSX.Janicab</td>
<td>Trojan</td>
<td>July 15, 2013</td>
</tr>
<tr>
<td>OSX.Olyx.C</td>
<td>Trojan</td>
<td>September 12, 2013</td>
</tr>
<tr>
<td>OSX.Seadoor</td>
<td>Trojan</td>
<td>September 18, 2013</td>
</tr>
<tr>
<td>OSX.Hormesu</td>
<td>Trojan</td>
<td>September 30, 2013</td>
</tr>
<tr>
<td>OSX.Aniulisi</td>
<td>Trojan</td>
<td>January 31, 2014</td>
</tr>
<tr>
<td>OSX.Apptite.A</td>
<td>Trojan</td>
<td>February 17, 2014</td>
</tr>
<tr>
<td>OSX.Stealbit.A</td>
<td>Trojan</td>
<td>February 26, 2014</td>
</tr>
<tr>
<td>OSX.Stealbit.B</td>
<td>Trojan</td>
<td>April 18, 2014</td>
</tr>
<tr>
<td>OSX.SearchProtect</td>
<td>Misleading App</td>
<td>June 30, 2014</td>
</tr>
<tr>
<td>OSX.Freezer</td>
<td>Trojan</td>
<td>August 27, 2014</td>
</tr>
<tr>
<td>OSX.Laoshu</td>
<td>Trojan</td>
<td>August 27, 2014</td>
</tr>
<tr>
<td>OSX.Slordu</td>
<td>Trojan</td>
<td>September 5, 2014</td>
</tr>
<tr>
<td>OSX.Luaddit</td>
<td>Trojan</td>
<td>October 3, 2014</td>
</tr>
<tr>
<td>Genieo</td>
<td>Potentially Unwanted App</td>
<td>October 7, 2014</td>
</tr>
<tr>
<td>OSX.Ventir</td>
<td>Trojan</td>
<td>October 19, 2014</td>
</tr>
<tr>
<td>OSX.Wirelurker</td>
<td>Trojan</td>
<td>November 6, 2014</td>
</tr>
<tr>
<td>OSX.Trojan.Gen</td>
<td>Trojan</td>
<td>November 26, 2014</td>
</tr>
<tr>
<td>OSX.Adware.Gen</td>
<td>Adware</td>
<td>December 31, 2014</td>
</tr>
<tr>
<td>OSX.PUA.Gen</td>
<td>Potentially Unwanted App</td>
<td>December 31, 2014</td>
</tr>
<tr>
<td>OSX.Mailcol</td>
<td>Trojan</td>
<td>January 5, 2015</td>
</tr>
<tr>
<td>OSX.Mailcol.2</td>
<td>Trojan</td>
<td>February 12, 2015</td>
</tr>
<tr>
<td>OSX.Genieo.gen1</td>
<td>Potentially Unwanted App</td>
<td>May 18, 2015</td>
</tr>
<tr>
<td>OSX.MACDefender.gen1</td>
<td>Potentially Unwanted App</td>
<td>June 3, 2015</td>
</tr>
<tr>
<td>OSX.Searchprotect.gen1</td>
<td>Potentially Unwanted App</td>
<td>June 3, 2015</td>
</tr>
<tr>
<td>OSX.Backloader</td>
<td>Spyware Trojan</td>
<td>July 3, 2015</td>
</tr>
<tr>
<td>OSX.Dropper</td>
<td>Trojan</td>
<td>July 3, 2015</td>
</tr>
<tr>
<td>OSX.Sudoprint</td>
<td>Trojan</td>
<td>August 4, 2015</td>
</tr>
<tr>
<td>OSX.Codghost</td>
<td>Trojan</td>
<td>September 18, 2015</td>
</tr>
<tr>
<td>OSX.CnetDownloader</td>
<td>Potentially Unwanted App</td>
<td>October 21, 2015</td>
</tr>
<tr>
<td>OSX.Ransomcrypt</td>
<td>Trojan</td>
<td>November 9, 2015</td>
</tr>
</tbody>
</table>
### iOS threats

**Table 2. Threats and security risks targeting iOS devices from 2009 to 2015**

<table>
<thead>
<tr>
<th>Malware</th>
<th>Type</th>
<th>Targets jailbroken devices only?</th>
<th>Discovery date</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS.Ikee</td>
<td>Worm</td>
<td>Yes</td>
<td>November 10, 2009</td>
</tr>
<tr>
<td>IOS.Ikee.B</td>
<td>Worm</td>
<td>Yes</td>
<td>November 22, 2009</td>
</tr>
<tr>
<td>IOS.Finfish</td>
<td>Trojan</td>
<td>Unknown</td>
<td>August 30, 2012</td>
</tr>
<tr>
<td>IOS.Passrobin</td>
<td>Trojan</td>
<td>Yes</td>
<td>April 22, 2014</td>
</tr>
<tr>
<td>IOS.Fitikser</td>
<td>Trojan</td>
<td>Yes</td>
<td>October 2, 2014</td>
</tr>
<tr>
<td>IOS.Lastacloud</td>
<td>Trojan</td>
<td>Yes</td>
<td>December 12, 2014</td>
</tr>
<tr>
<td>IOS.Xagent</td>
<td>Trojan</td>
<td>Yes</td>
<td>February 5, 2015</td>
</tr>
<tr>
<td>IOS.Oneclickfraud</td>
<td>Trojan</td>
<td>No</td>
<td>May 31, 2015</td>
</tr>
<tr>
<td>IOS.Keyraider</td>
<td>Trojan</td>
<td>Yes</td>
<td>August 31, 2015</td>
</tr>
<tr>
<td>IOS.Specter</td>
<td>Trojan</td>
<td>No</td>
<td>October 5, 2015</td>
</tr>
<tr>
<td>IOS.Muda</td>
<td>Adware</td>
<td>Yes</td>
<td>October 9, 2015</td>
</tr>
<tr>
<td>IOS.Crisis</td>
<td>Trojan</td>
<td>Yes</td>
<td>October 18, 2015</td>
</tr>
<tr>
<td>IOS.Codgost</td>
<td>Trojan</td>
<td>No</td>
<td>November 4, 2015</td>
</tr>
</tbody>
</table>