Apple XcodeGhost Malware: List of iOS Apps You Should Delete Immediately

By Ryan De Souza (https://www.hackread.com/author/ryan-de-souza/) on September 23, 2015 (https://www.hackread.com/apple-xcodeghost-malware-ios-apps/)
Email (mailto:ryan@hackread.com) *@hackread (http://twitter.com/hackread)*

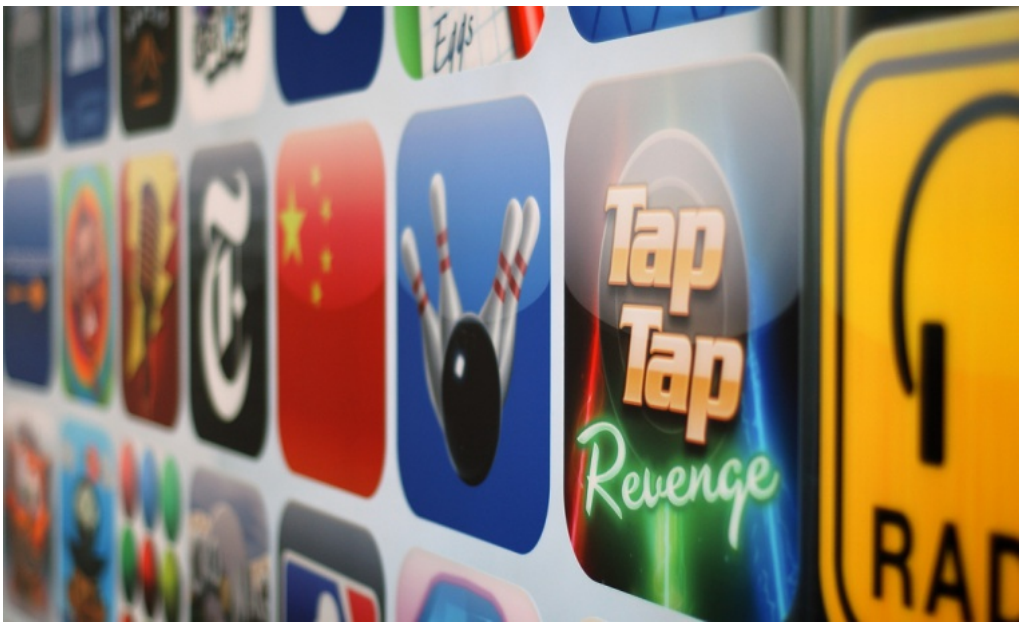


Image Source: Flickr

Apple's App Store in China has apparently been penetrated by Hackers which experts say has placed the devices of hundreds of millions of people at risk.

The **malware (https://www.hackread.com/tag/Malware/)** named XcodeGhost, believed to be a malicious and modified version of **Apple** (https://www.hackread.com/tag/Apple/)'s very own development software, is said to have compromised a significant number of applications.

Apple Inc. said on Sunday that it was in the process of cleaning up its **iOS App Store (https://www.hackread.com/tag/iOS/)** to remove the malicious iPhone and iPad programs which have been identified as having the XcodeGhost malware embedded into them. It is believed that the number of Apps infected runs into the hundreds making this the first large-scale attack on the software platform.

The security company, **Palo Alto Networks (https://www.paloaltonetworks.com/)**, which is investigating the breach said in a blog post:

> ***"BASED ON THIS NEW INFORMATION, WE BELIEVE XCODEGHOST IS A VERY HARMFUL AND DANGEROUS MALWARE THAT HAS BYPASSED APPLE'S CODE REVIEW AND MADE UNPRECEDENTED ATTACKS ON THE IOS ECOSYSTEM."***

They also warned:

> ***"THE TECHNIQUES USED IN THIS ATTACK COULD BE ADOPTED BY CRIMINAL AND ESPIONAGE FOCUSED GROUPS TO GAIN ACCESS TO IOS DEVICES."***

Apple has yet to reveal exactly how many Apps have been compromised by this malware and when asked directly, they declined to answer. A Chinese security firm Qinhoo360 Technology Co did, however, announce in its blog that it had uncovered up to 344 apps which have thus far been compromised.

How Big a Deal Is It?

According to Palo Alto Networks Director of Threat Intelligence Ryan Olson, it is a "pretty big deal" because it proves that Apple's App Store can be compromised on a large scale by virtue of developers being hacked and having their machines infected. He also believes that other attackers will, in all probability, attempt to copy this approach which has proved to be very hard to defend against. It is his view that "developers are now a huge target".

Although the Chinese App Store was the target and almost all the Apps affected are used in **China (https://www.hackread.com/tag/China/)**, it is not the case for all of them. The apps affected include Tencent Holdings Ltd's, We Chat, Didi Kuaidi which is a car-hailing app and CamCard which is a business card scanner available for use outside of China.

Targeting Developers

Alibaba, the giant e-commerce firm, had initially flagged up the malware when it was discovered by its researchers. They found that hackers had uploaded a number of altered versions of Xcode which is a tool used to build iOS Apps onto a cloud storage service in China.

The hackers then posted links to the software on forums which are common with Chinese developers. **Palo Alto networks stated (http://researchcenter.paloaltonetworks.com/2015/09/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/#)**:

"In China – and in other places around the world – sometimes network speeds are very slow when downloading large files from Apple's servers,"

"As the standard Xcode installer is nearly three gigabytes, some Chinese developers choose to download the package from other sources."

The posting of the links to the altered version of the Xcode on developer forums shows that Developers were indeed the principle target of the hackers.

What About The Gatekeeper?

Apple's security tool, Gatekeeper, which is specifically designed to warn users of any unauthorised programs and stop them running appears to have been disabled by the developers – this allowed them to continue to create iOS apps using the XcodeGhost malware.

What Does this Mean For Users?

All iOS Apps infected with the XcodeGhost malware will collect information about the unsuspecting users device, encrypt and upload that data to command and control servers which are run by the hackers. This is done through HTTP Protocol. According to Palo Alto Networks, the information collected are:

1. Network type
2. Device names and type
3. Infected Apps name
4. Current time
5. Devices UUID
6. System's language and country
7. The apps Bundle identifier

It will then receive the following commands according to Palo alto Networks:

1. Phish user credentials
2. Read and write data to clipboard
3. Hijack specific URLs allowing for vulnerability exploitation.

What Is Being Done?

Apple has issued a statement regarding their plan of action to date:

"We've removed the apps from the App Store that we know have been created with this counterfeit software. We are working with the developers to make sure they're using the proper version of Xcode to rebuild their apps."

To protect oneself from the XcodeGhost malware, users need to immediately uninstall any infected Apps from the list which can be **found here (http://forums.macrumors.com/threads/what-you-need-to-know-about-ios-malware-xcodeghost.1918784/#post-21896151)**. Alternatively they can update to the latest version which has had the malware removed. Other things which all users should do immediately change your iCloud password as well as any passwords which have been inputted on your device.

If you are a developer, you should install the official version of Xcode 7 & or Xcode 7.1 beta – you can do this **from here (https://developer.apple.com/xcode/download/)** and always avoid downloading the software from unofficial sources.

Despite the discovery of the malware in Apples App store being unprecedented and embarrassing to say the least and despite the exposure potentially encouraging other hackers to copy; it is believed that this breach will not shake consumer confidence and experts such as Wee Teck Loo, who is head of consumer electronics at market research firm Euromonitor International, do not forecast any major losses for Apple whether that be revenue or sales.

List of apps that should be deleted immediately:

- WeChat
- Didi Chuxing
- Angry Birds 2
- NetEase
- Micro Channel
- IFlyTek input
- Railway 12306
- The Kitchen
- Card Safe
- CITIC Bank move card space
- China Unicom Mobile Office
- High German map
- Jane book
- Eyes Wide

- Lifesmart
- Mara Mara
- Medicine to force
- Himalayan
- Pocket billing
- Flush
- Quick asked the doctor
- Lazy weekend
- Microblogging camera
- Watercress reading
- CamScanner
- CamCard
- SegmentFault
- Stocks open class
- Hot stock market
- Three new board
- The driver drops
- OPlayer
- Mercury
- WinZip
- Musical.ly
- PDFReader
- Perfect365
- PDFReader Free
- WhiteTile
- IHexin
- WinZip Standard
- MoreLikers2
- CamScanner Lite
- MobileTicket
- iVMS-4500
- OPlayer Lite
- QYER
- golfsense
- Ting
- Golfsensehd
- Wallpapers10000
- CSMBP-AppStore
- MSL108
- TinyDeal.com
- snapgrab copy
- iOBD2
- PocketScanner
- CuteCUT
- AmHexinForPad
- SuperJewelsQuest2
- air2
- InstaFollower
- CamScanner Pro
- baba
- WeLoop
- DataMonitor
- MSL070
- nice dev
- immtdchs

- OPlayer
- FlappyCircle
- BiaoQingBao
- SaveSnap
- Guitar Master
- jin
- WinZip Sector
- Quick Save

If there are other infected apps we will let you know. Stay tuned..

SOURCE

PALO ALTO NETWORKS ("HTTP://RESEARCHCENTER.PALOALTONETWORKS.COM/2015/09/MALWARE-XCODEGHOST-INFECTS-39-IOS-APPS-INCLUDING-WECHAT-AFFECTING-HUNDREDS-OF-MILLIONS-OF-USERS/#")

[redacted] APPLE (HTTPS://WWW.HACKREAD.COM/TAG/APPLE/) CHINA (HTTPS://WWW.HACKREAD.COM/TAG/CHINA/)
CYBER CRIME (HTTPS://WWW.HACKREAD.COM/TAG/CYBER-CRIME-2/) HACKING (HTTPS://WWW.HACKREAD.COM/TAG/HACKING/)
INFOSEC (HTTPS://WWW.HACKREAD.COM/TAG/INFOSEC/) IOS (HTTPS://WWW.HACKREAD.COM/TAG/IOS/) IPAD (HTTPS://WWW.HACKREAD.COM/TAG/IPAD/)
IPHONE (HTTPS://WWW.HACKREAD.COM/TAG/IPHONE/) MALWARE (HTTPS://WWW.HACKREAD.COM/TAG/MALWARE/) SECURITY (HTTPS://WWW.HACKREAD.COM/TAG/SECURITY/)
XCODEGHOST (HTTPS://WWW.HACKREAD.COM/TAG/XCODEGHOST/)


(https://www.hackread.com/author/ryan-de-souza/)

RYAN DE SOUZA

Ryan is a London-based member of the HackRead Editorial team. A graduate of Maths and physics with a passion for geopolitics and human rights. Ryan places integrity at the pinnacle of successful journalism and believes this is somewhat lacking in traditional media. Ryan is an educator who balances his time between family, social activism and humanitarian causes and his vice is Football and cars.

(https://twitter.com/https://twitter.com/Ryan_HackRead)
(https://www.facebook.com/profile.php?id=100010248247812)

MORE FROM HACK READ

Your IOS 9 Lockscreen Can Be Bypassed In 30 Seconds (Https://Www.Hackread.Com/Ios9-Lockscreen-Bypass-Security-Flaw/)

Facebook Following NSA Footsteps To Spy On Users: Belgium's Privacy Advocate (Https://Www.Hackread.Com/Facebook-Nsa-Spying-Privacy-Belgium/)

US Navy Developing Cyber Protection System To Protect Ships From Cyberattacks (Https://Www.Hackread.Com/Us-Navy-Cyber-Attack-Protection-System/)

US Air Force EC-130H Aircraft With Hacking Kit Can Hack Enemy Networks (Https://Www.Hackread.Com/Us-Air-Force-Ec-130h-Aircraft-Hacking-Enemy/)

Anonymous Hacks Embarcadero News Group Websites Against Harmful Content (Https://Www.Hackread.Com/Anonymous-Hacks-Embarcadero-News-Group-Websites/)

ADD YOUR COMMENTS:

JOIN OUR FREE NEWSLETTER

RECENT POSTS

(https://www.hackread.com/ios9-lockscreen-bypass-security-flaw/)
YOUR IOS 9 LOCKSCREEN CAN BE BYPASSED IN 30 SECONDS (HTTPS://WWW.HACKREAD.COM/IOS9-LOCKSCREEN-BYPASS-SECURITY-FLAW/)

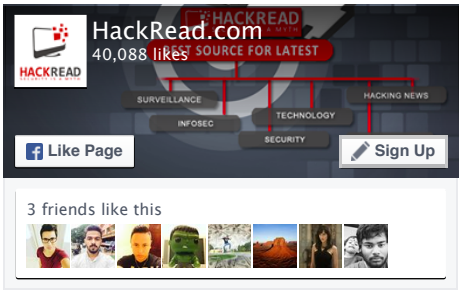
(https://www.hackread.com/facebook-nsa-spying-privacy-belgium/)
FACEBOOK FOLLOWING NSA FOOTSTEPS TO SPY ON USERS: BELGIUM'S PRIVACY ADVOCATE (HTTPS://WWW.HACKREAD.COM/FACEBOOK-NSA-SPYING-PRIVACY-BELGIUM/)

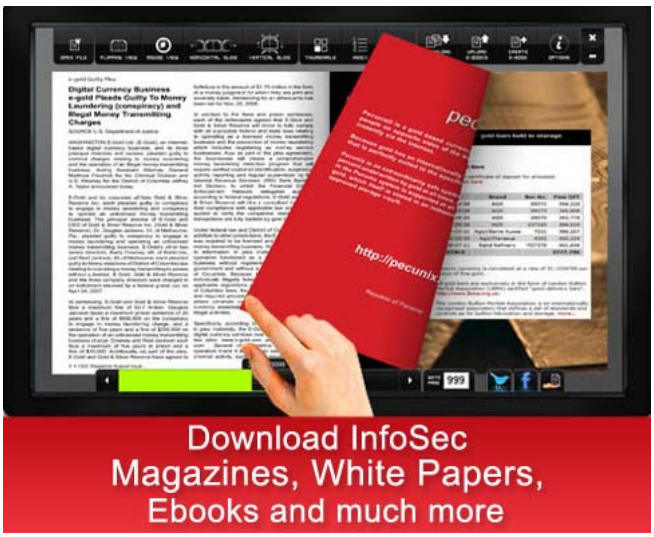
(https://www.hackread.com/us-navy-cyber-attack-protection-system/)
US NAVY DEVELOPING CYBER PROTECTION SYSTEM TO PROTECT SHIPS FROM CYBERATTACKS (HTTPS://WWW.HACKREAD.COM/US-NAVY-CYBER-ATTACK-PROTECTION-SYSTEM/)

(https://www.hackread.com/nude-selfies-phone-teen/)
HAVING NUDE SELFIES ON PHONE MAY SEND YOU TO PRISON IN THE U.S. (HTTPS://WWW.HACKREAD.COM/NUDE-SELFIES-PHONE-TEEN/)

(https://www.hackread.com/us-air-force-ec-130h-aircraft-hacking-enemy/)
US AIR FORCE EC-130H AIRCRAFT WITH HACKING KIT CAN HACK ENEMY NETWORKS (HTTPS://WWW.HACKREAD.COM/US-AIR-FORCE-EC-130H-AIRCRAFT-HACKING-ENEMY/)

LIKE US ON FACEBOOK





(http://goo.gl/s9hr1b)

(//revolution-news.com/)

HACKREAD (http://hackread.com)

is a News Platform that centers on InfoSec, Cyber Crime, Privacy, Surveillance and Hacking News with full-scale reviews on Social Media Platforms & Technology trends. Founded in 2011, HackRead is based in Dubai, UAE.

ABOUT US (HTTPS://WWW.HACKREAD.COM/ABOUT-US/)

SITEMAP (HTTPS://WWW.HACKREAD.COM/SITEMAP-HACKREAD/)

CONTACT US (HTTPS://WWW.HACKREAD.COM/CONTACT-US/)

(https://www.facebook.com/HackRead) (https://instagram.com/hackread/) (https://twitter.com/HackRead) (https://plus.google.com/+Hackread) (http://hackread.com/feed) (http://www.youtube.com/channel/UCRhpFkd8GYCfwsWqY6WQvdw/)