Tactical Intelligence Bulletin // UnityGhost: the ghost adventure continues

CTO-TIB-20150925-01A September 2015 threatintelligence@uk.pwc.com
Tags: iOS, mobile app, Apple, Xcode, XcodeGhost, UnityGhost

Executive Summary

Apple iOS has long been purported to be the safest mobile operating system due to the closed access to the underlying source code, the restrictive design of the API and the rigorous review of mobile apps submitted for the App store. However, recent reports have emerged from China that some rogue versions of the Xcode development toolset have been found which inject malicious code (named XcodeGhost) into any apps compiled using the rogue toolset.

Although much have been reported on Xcode since, not much have been said about other mobile app development platforms. This report presents a high level overview of XcodeGhost as well as some of our findings on this threat including additional domains, cloned websites and an online persona we believe to be associated with this threat. We have also uncovered indications that Unity apps have also been compromised in a similar fashion – which is referred to as UnityGhost.

Background: XcodeGhost

First reported by a Weibo user[1] on 17th September 2015 (see Figure 1 below), malicious versions of the Xcode[2] development framework were recently found. The frameworks were modified so that the malicious version of the code framework (dubbed 'XcodeGhost[3]' by researchers at Alibaba) is injected into any iOS apps[4] compiled using these corrupted frameworks.

Figure 1: Report emerged on Weibo about the rogue versions of Xcode.

[1] http://www.weibo.com/1650375593/CAV5fqdo3?from=page_1005051650375593_profile&wvr=6&mod=weibotime&type=comment
[2] https://developer.apple.com/xcode/
[3] http://jaq.alibaba.com/blog.htm?id=82
[4] The name of some of the affected apps can be found in the Appendix.

Since then, several other security teams have undertaken analysis of the malicious additions to the framework. These are summarised in the next section.

When you see it

XcodeGhost has been discovered to have the following malicious functionalities[5]:

1. Collect information about victim machine;
2. Generate fake prompt windows to phish user credentials;
3. Hijack opening specific URL schemes; and,
4. Access to clipboard data.

Once the malicious app executes, device information such as current time, device UUID, device name and type, system language and country and network type are collected and sent to designated C2 servers.

Furthermore, infected apps can receive instructions from the C2 servers to generate fake windows prompt to phish for user credentials. The commands are sent in JSON format which contain the following information:

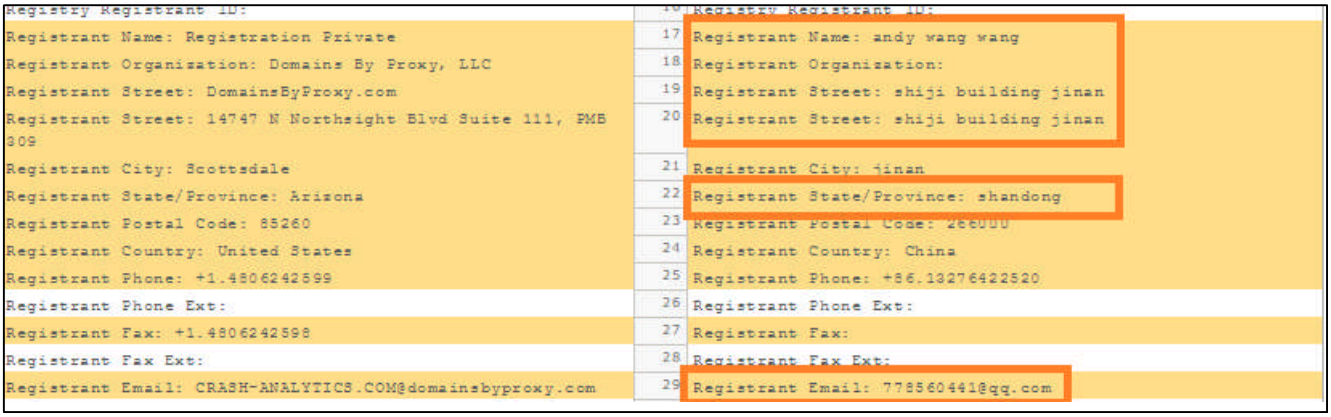
- alertHeader;
- alertBody;
- appID;
- cancelTitle; and,
- confirmTitle.

The following are the three command and control (C2) domain names associated with XcodeGhost[6]:

Command and Control (C2) Servers	
Domain	`http://init.crash-analytics[.]com`
Domain	`http://init.icloud-diagnostics[.]com`
Domain	`http://init.icloud-analysis[.]com`

Through research on domain registration information, we find that the WHOIS privacy-protection of two of the C2 domains have been removed since the discovery that they were used in conjunction with the malicious activity. Although it is unclear whether this was a mistake or deliberate action by the threat actor or domain registrar, the removal of the privacy protect reveals that the domain was registered using a QQ email address, `778560441@qq.com`.

[5] http://researchcenter.paloaltonetworks.com/2015/09/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/
[6] http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/



Registrant Name: Registration Private	17	Registrant Name: andy wang wang
Registrant Organization: Domains By Proxy, LLC	18	Registrant Organization:
Registrant Street: DomainsByProxy.com	19	Registrant Street: shiji building jinan
Registrant Street: 14747 N Northsight Blvd Suite 111, PMB 309	20	Registrant Street: shiji building jinan
Registrant City: Scottsdale	21	Registrant City: jinan
Registrant State/Province: Arizona	22	Registrant State/Province: shandong
Registrant Postal Code: 85260	23	Registrant Postal Code: 266000
Registrant Country: United States	24	Registrant Country: China
Registrant Phone: +1.4806242599	25	Registrant Phone: +86.13276422520
Registrant Phone Ext:	26	Registrant Phone Ext:
Registrant Fax: +1.4806242598	27	Registrant Fax:
Registrant Fax Ext:	28	Registrant Fax Ext:
Registrant Email: CRASH-ANALYTICS.COM@domainsbyproxy.com	29	Registrant Email: 778560441@qq.com

Figure 2: Removal of privacy protection for `crash-analytics[.]com`.

A reverse WHOIS lookup using the email address `778560441@qq.com` returned seven more domain names[7], which also share the iOS development theme:

Domain	Registration date
iostool.com	2015-04-07
ioscode.org	2015-04-07
iossdk.org	2015-04-07
sdkdev.net	2015-04-07
sdkdev.org	2015-04-07
allsdk.org	2015-04-07
allsdk.com.cn	2015-08-17

None of the sites in question are still online, however cached search results for the domains `allsdk.org` and `iossdk.org` indicate that the domains were used to host websites containing cloned content from legitimate websites. Broadly, the sites were used for sharing iOS, Unity 3D as well as Cocos2d-x development source code and tools (see images below). Although it is unclear whether the shared code and tools were malicious, the use of cloned content in the websites to share similar code, where the download links are not from the official source may suggest that they were used in separate attempts to distribute malicious code.

[7] A full list of domains associated with the email address 778560441@qq.com is provided in the Appendix.

Figure 3: Screenshots of cloned websites `allsdk[.]org` and `iossdk[.]org`.

UnityGhost

Since the websites show that this threat actor was interested in not just iOS development but also Unity and Cocos2d-x, there is evidence which suggest that other app development frameworks may also have been targeted which could be a bigger problem than Xcode as the Unity platform can be used to create apps for not just iOS but also Android, Windows and Wii.

This is supported by a claim made by a user on Weibo, which states that some Unity apps have also been compromised[8] and the C2 domain `init.icloud-diagnostics[.]com` is also observed in conjunction with these applications:

Figure 4: Reports of similar tampering with Unity builders.

[8] http://www.weibo.com/1627825392/CBGopinKh?type=comment

Following the claim, the Baidu Security Team[9] examined some Unity platforms and they found that some Unity platforms were indeed modified in a similar way to XcodeGhost in that malicious code has been added to the framework to infect the generated apps.

More specifically, the attacker made modifications to the `libiPhone-lib-il2cpp.a` archive and added a file called `libiPhone-lib-il2cpp.a-arch-masterx.x.o`. To make sure that the additional file is loaded, the project manifest `project.pbxproj` has also been modified and which can be used to verify if the Unity platform being used has been tampered with.

Below is an image[10] which highlights the extra line '`-ObjC`' which is added in the malicious versions of Unity.

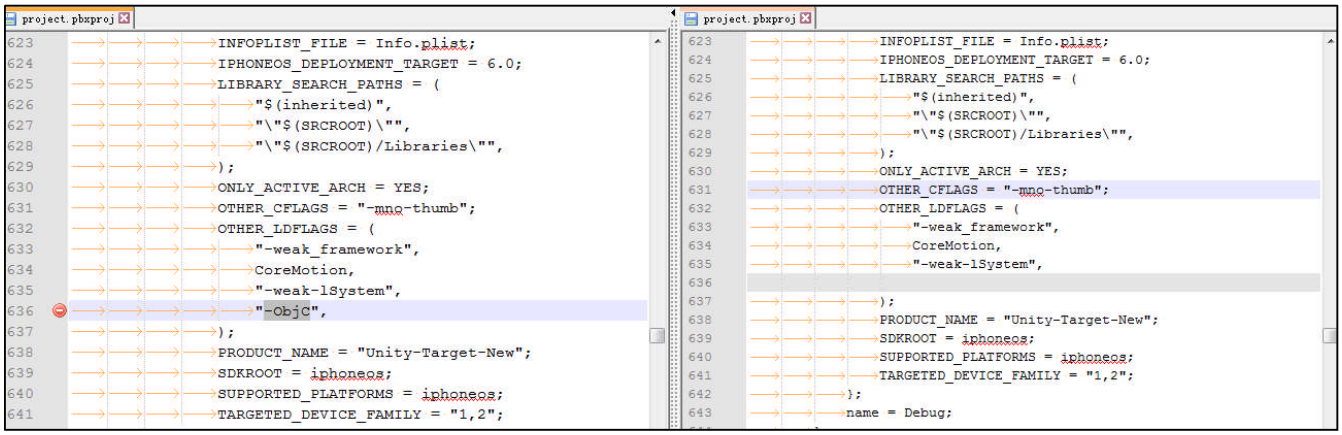


Figure 5: The tampered project manifest has an extra line "`-ObjC`".

The affected archive file `libiPhone-lib-il2cpp.a` can be found in the following paths:

Mac OS	`/Unity/Unity.app/Contents/PlaybackEngines/iossupport/Trampoline/Libraries/ libiPhone-lib-il2cpp.a`
Windows	`Unity/Editor/Data/PlaybackEngines/iossupport/Trampoline/Libraries/libiPhone-lib-il2cpp.a`

Attribution

The email address used to register the domains is a QQ email address. The numeric prefix of a QQ address is referred to as a 'QQ number' which often has other associations, such as social media accounts, that can be easily identified.

Our research on the QQ number shows that the QQ account previously had an alias called "济大周文洋" which can be translated to "Jinan University[11] Zhou Wen Yang". The QQ account was also previously connected to a QQ

[9] http://xteam.baidu.com/?p=351
[10] Source: http://xteam.baidu.com/?p=351
[11] www.ujn.edu.cn

Group 62768619 called "山东省挑战杯竞赛", a group designated for "Shandong District Challenge Cup Competition". The University of Jinan is located in Shandong, so it is likely the owner of the account has a geographical nexus to Shandong province.

Below image depicts this relationship:

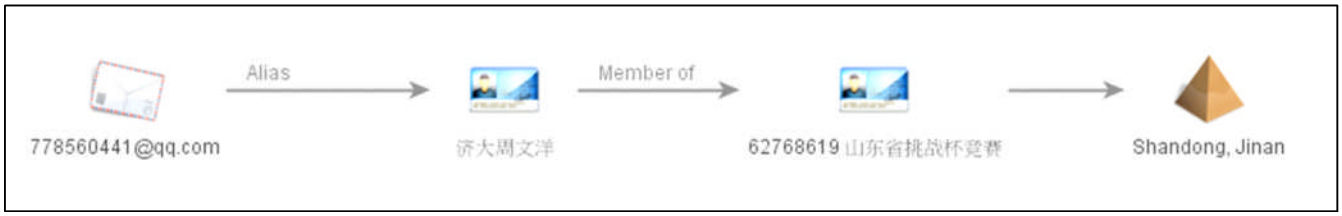


Figure 6: Tying the domain registrant to a geolocation via past QQ group membership.

Based on the reference to Jinan University and the association with a QQ group designated for Shandong district, we believe with medium confidence that this threat actor is likely to be male, have lived in Jinan in the past and very likely to have attended Jinan University.

Below is the current[12] profile of the QQ account which states that the individual is male, 22 years of age and current location is Chengdu, Sichuan. However, as this information can be easily falsified, we are unable to draw any conclusions based on this information, especially as the owner may have had additional cause to edit the profile following the recent exposure of the association between his QQ number and the domains used in the XCodeGhost framework.

The only evidence we can take from this profile is the fact that the account was registered eight years ago in 2007.

Figure 7: The current profile of the QQ account 778560441.

[12] At the time of writing – 25/09/2015.

Conclusion

The findings presented in this report show that the initial details posted relating to the XcodeGhost campaign can easily be expanded upon, as there are more than 15 domain names associated with the threat actor. Our research on these domain names show that several of these were cloned websites which are likely to have been setup to distribute code and tools relating to iOS, Unity and Cocos2d-x app development.

Based on these findings, we have also identified reports emerging on Weibo which suggest that Unity apps have also been compromised in a similar fashion. Finally, research based on the WHOIS details associated with two of the C2 domains allowed us to identify an individual behind the campaign, whose real name may be Zhou Wen Yang and who may have attended Jinan University.

Recommendations

For users of any of the affected apps (see Appendix), we recommend removing the apps from all mobile devices and changing credentials of any email and social media accounts associated with the apps.

Further Information

We specialise in providing the services required to help clients resist, detect and respond to advanced cyber-attacks. This includes crisis events such as data breaches, economic espionage and targeted intrusions, including those commonly referred to as APTs. If you would like more information on any of the threats discussed in this alert please feel free to get in touch, by e-mailing threatintelligence@uk.pwc.com.

Appendix

Associated domain names

Domain	Registration date
crash-analytics.com	2015-08-26
icloud-diagnostics.com	2015-05-07
icloud-analysis.com	2015-02-25
iostool.com	2015-04-07
ioscode.org	2015-04-07
iossdk.org	2015-04-07
sdkdev.net	2015-04-07
sdkdev.org	2015-04-07
allsdk.org	2015-04-07
allsdk.com.cn	2015-08-17
bang2shou.com	2014-10-07
qdczvv.com	2015-08-03
tiao2shou.com	2014-10-07
libocast.com	2015-07-15
kytr.pub	2015-06-27
gu2shou.com	2014-10-07
91meiche.com	2014-10-27
daimaku.net	2015-04-07
madou360.com	2014-09-29
592qiche.com	2014-09-28

Affected mobile apps

Mobile apps reported to have been affected by XcodeGhost include[13]:

WeChat
iVMS-4500
OPlayer Lite
QYER
golfsense
同花顺
installer
下厨房
golfsensehd
Wallpapers10000
CSMBP-AppStore
礼包助手
MSL108
ChinaUnicom3.x
TinyDeal.com
snapgrab copy
iOBD2
PocketScanner
CuteCUT
AmHexinForPad
SuperJewelsQuest2
air2
InstaFollower
CamScanner Pro
baba
WeLoop
DataMonitor
爱推
MSL070
nice dev
immtdchs
OPlayer
FlappyCircle
高德地图
BiaoQingBao
SaveSnap
Guitar Master
jin
WinZip Sector
Quick Save
CamCard

[13] Note that the 'compromised status' of these apps has not been verified by PwC.

Tactical Intelligence Bulletin UnityGhost: the ghost adventure continues

CTO-TIB-20150925-01A September 2015 threatintelligence@uk.pwc.com

Tags: iOS, mobile app, Apple, Xcode, XcodeGhost, UnityGhost