From: Jun Ge [redacted]
To: Eric Gray [redacted], Ayman Khalil [redacted]
CC: Yi Wang [redacted], Ben Liaw [redacted], Craig Bradley [redacted], Andrew Yeh [redacted], Carolyn Wu [redacted], Christine Monaghan [redacted], Jason Wang [redacted], YeeWee Koh [redacted], Matt Fischer [redacted], Alastair Morse [redacted], Glenn Epis [redacted]
BCC:
Subject: Re: [ALERT:Possible Phishing] CNCERT request on malicious code of non-official XCODE
Attachments:
Sent: 09/29/2015 11:42:33 PM 0000 (GMT)

Team,

Below is the version Phil has just given his green signal. If you agree, we could delete the first sentence in the fifth paragraph.

We still need to fill in the missing data (highlighted in red below) to the best we could.

Best,

Jun

1. Apple's management has attached great importance to XcodeGhost issue.
- Internally, we have marshalled a lot of resources across all Apple to analyse the situation, check every app on the app store, remove infected apps from App Store, contact the relevant impacted developers, assist developers with checking their software and getting clean apps back on the store quickly, block any new submissions of apps with the infection.
- On Sept. 22, Phil Schiller, Apple's Senior Vice President in charge of Product Marketing, accepted Sina Technology's interview on XcodeGhost issue and answered key questions about it. Apple always recommends developers use the free, secure tools Apple provides them — including Xcode — to ensure they're creating the most secure apps for App Store customers. Apple incorporates technologies like Gatekeeper expressly to prevent non-App Store and/or unsigned versions of programs, including Xcode, from being installed. Those protections had to have been deliberately disabled by the developer for something like XcodeGhost to successfully install. Sometimes developers search for our tools, such as Xcode, on other, non-Apple sites in an effort to find faster downloads of developer tools. Apple is working to make it faster for developers in China to download Xcode betas.

2. Apple has published a XcodeGhost Q&A at its official website, explaining about the background of the issue, why it happened, how the consumers could diagnose if their devices have been infected and what they should do, and Apple's measures against the infected apps. Here is the link http://www.apple.com/cn/xcodeghost/ .

3. Apple has published a list of the top 25 most popular apps impacted at its official website. After the top 25 impacted apps, the number of impacted users drops significantly. If users have one of these apps, they should update the affected app which will fix the issue on the user's device. If the app is available on App Store, it has been updated, if it isn't available it should be updated very soon. Here is the link http://www.apple.com/cn/xcodeghost/

4. After XcodeGhost issue happened, Apple did a screening of all the apps in App Store and took off all the infected apps. We found that 4,743 apps were infected and about _____ users were affected (actual number may be less because users may not have kept those apps on their devices). Of the 4,743 apps, 1,342 apps don't have a clean version on App Store yet, with **23.7M** [to further verify] customers. We also blocked apps which were infected from being submitted.

5. Apple is working on further measures that recommend to the users to update their infected apps with clean versions and delete those without clean versions. The best way to resolve this situation is for users to automatically update their compromised apps with new apps posted by the developer. This removes the malware from users devices. That is why our focus has been on taking down compromise apps and getting developers to put back up non-compromised versions to update users' devices.

6. We believe that the malware cannot access much user data due to our system sandboxing and other built in

countermeasures, and this malware has not been used to actually gather user data at this time.

On Sep 30, 2015, at 7:33 AM, Jun Ge [redacted] wrote:

I shared the latest version with phil based on his earlier feedback. this is the point right now we have - do you think we could also delete the sentence?

5. Apple is working on further measures that recommend to the users to update their infected apps with clean versions and delete those without clean versions. The best way to resolve this situation is for users to automatically update their compromised apps with new apps posted by the developer. This removes the malware from users devices. That is why our focus has been on taking down compromise apps and getting developers to put back up non-compromised versions to update users' devices.

On Sep 30, 2015, at 7:27 AM, Eric Gray [redacted] wrote:

+ Glenn Epis

In regards to this statement:

> 5. Apple is working on further measures that recommend to the users to update their infected apps with clean versions and delete those without clean versions.

while this statement is true, we have several options, and I think it is important to get PR, GA on the same page and then we can go back to the executives with a further recommendation. Should we setup a call? Who from GA should be on that call? Bella and Jun? I'll include Tom, Christine and Carolyn from PR.

Thanks

Eric

On Sep 29, 2015, at 12:54 AM, Eric Gray [redacted] wrote:

Yes Bella,

That is correct. For the 4,743, we can provide the number of customers, but be aware that this includes very popular apps that were quickly resolved, so the number will be very large.

Ayman - do you have the number pulled already?

Thanks

Eric

On Sep 29, 2015, at 12:49 AM, Yi Wang [redacted] wrote:

Hi Eric,

Regarding the 1,342 apps, they do have been removed from App Store. Those apps have 23.7M customers. Is my understanding correct?

Can we at least provide the consumers of 4,743 apps before the deadline? MIIT experts believe this figure should be available.

As for the number of consumers who are still using infected apps, if it could not be worked out by today, I could try to ask for more time for it.

Thanks.

Bella

> On Sep 29, 2015, at 3:32 PM, Eric Gray [redacted] wrote:
>
> A few updates to consider
>
> The total infected should be 4,743 as some of the 4,955 were never put on the store (just testing phase of apps).
>
> There are 1,342 apps that were actually downloaded that have not been updated (vs. the 1,905 mentioned below). We are down to 23.7 million customers impacted (not the 30.6 million), since the three biggest apps have all been updated.
>
> Those blanks are going to be difficult to fill in, as it requires a lot of information, including apps being deleted from devices, etc.
>
> Thanks
>
> Eric
>
> > On Sep 28, 2015, at 11:44 PM, Yi Wang [redacted] wrote:
> >
> > Hi all,
> >
> > I have updated Point 4 & 5 of the response to MIIT with new input received.
> >
> > 4. After XcodeGhost issue happened, Apple did a screening of all the apps in App Store, and we found that 4,955 apps were infected and about _____ users were affected. Of the 4,944 apps, 1,905 apps don't have a clean version on App Store yet, with 30.6M customers, among which 74% (22.6M) is in China. After the measures Apple has taken, many of the affected users have updated their infected apps and by Sept. _____, there are about _____ users who still have not done the update of the infected apps they have downloaded to their devices.
> > Ayman, please help with figures for the blankets as early as possible. We need to get Phil Schiller and Eddy Cue's approval for the document by COB of Sept. 29 (Cupertino time)
> >
> > 5. Apple is working on further measures that recommend to the users to update their infected apps with clean versions and delete those without clean versions.
> > Carolyn, I have made this sentence based on the information you shared. Please confirm if it 's ok with PR.
> >
> > Attached is the updated full version. GA has started the translation.
> > <answers to MIIT on XcodeGhost_092015_ENv2.pages>
> >
> > Thanks.
> >
> > Bella
> > GA China
> >
> > > On Sep 29, 2015, at 1:21 PM, Yi Wang [redacted] wrote:
> > >
> > > Hi Ayman,
> > >
> > > Many thanks for providing the figures at such short notice. Two questions:
> > > 1. Regarding the 1,905 apps with no clean version, are they already downloaded from App Store?
> > > 2. Of the 4,955 - 1,905 = 3,050 apps with clear versions, do you have figures how many (or %) of the users have

updated to clean versions?

Regards.

Bella
GA China

> On Sep 29, 2015, at 12:58 PM, Ayman Khalil [redacted] wrote:
>
> Here are some details we are able to share right now.
>
> App Review has provided us with a list of infected apps. This list represents versions scanned in the date range 1/1/2015 - 9/24/2015.
>
> - The list is 4,955 infected apps
> - 1,905 of these apps don't have a clean version on the store
>
> Given these 1.9K apps, we are looking at 30.6M customers. The two main countries impacted:
>
> - China 22.6M (74%)
> - USA 2.7M (9%)
>
> We are currently running queries to understand how many total customers installed the 4,955 infected apps. Our estimate is to have this by EOD tomorrow.
>
> > On Sep 28, 2015, at 4:24 PM, Ben Liaw [redacted] wrote:
> >
> > + Matt for visibility
> >
> > + Ayman, Eric since they have the official numbers
> >
> > > 在 2015年9月29日，上午7:20，Jun Ge [redacted] 写道：
> > >
> > > Since we need to give the document to MIIT before the end of tomorrow, to allow us to do that, we also need to get Phil/Eddy's approval as advised and we need the translation and internal processing for coping, we are running very tight. Please all prioritize this.
> > >
> > > > On Sep 29, 2015, at 7:11 AM, Yi Wang [redacted] wrote:
> > > >
> > > > Hi Ben,
> > > >
> > > > Could you help with the numbers of users affected by the infected apps? How many were there when XcodeGhost was found, and how many by now since some users should have updated the apps? MIIT wants to see the trend, expecting a decline of the affected users.
> > > >
> > > > Thanks.
> > > >
> > > > Bella
> > > >
> > > > > On Sep 29, 2015, at 5:57 AM, Craig Bradley [redacted] wrote:
> > > > >
> > > > > Bella,

For data in Point 4 we (WWDR) can provide the number of apps affected but all other data regarding number of users needs to come from the App Store team.

//Craig

> On 29 Sep 2015, at 12:40 am, Yi Wang [redacted] wrote:
>
> Hi all,
>
> Here is a draft response GA has composed. It has 5 points.
> - The first 3 points are quotes from the Q&A and Phil's interview, covering the measures Apple has taken.
> - In point 4, I have set blank areas for figures MIIT expects us to provide. Craig and Andrew, please adjust this point as you see proper, based on the figures you get. Could you get the figures by tomorrow?
> - in point 5, in response to MIIT request for suggestion on how to inform users that have been infected but still have not made updates, GA proposes " Apple will work with some popular portals to call users to do app updates", for the team to discuss. Please suggest if you have better ideas.
>
> The deadline for us is Sept. 30. We also need some time to get the needed approvals and finalise the Chinese version. Your quick comment and response are highly appreciated.
> <answers to MIIT on XcodeGhost_092015_ENv1.pages>
>
> Many thanks.
>
> Bella
>
> > On Sep 28, 2015, at 4:27 PM, Yi Wang [redacted] wrote:
> >
> > Hi Craig,
> >
> > Thanks for coordinating for the answers. GA is composing a response on the basis of what has been published, and with your answers, we will try to get the needed approvals.
> >
> > Best,
> >
> > Bella
> >
> > > On Sep 28, 2015, at 11:49 AM, Craig Bradley [redacted] wrote:
> > >
> > > Bella/Jun,
> > >
> > > WWDR does have answers to some of these questions and we have requested the answer to the others from the App Store team in Cupertino (Ben, see separate request email to Eric and Matt from me).
> > >
> > > We will provide this currently confidential information to you with the expectation that GA will compose a response and then get approval from Phil Schiller and Eddy Cue before giving any of this to MIIT.
> > >
> > > Is this your understanding also?
> > >
> > > //Craig

On 28 Sep 2015, at 1:28 pm, Yi Wang [redacted] wrote:

Hi Craig and Andrew,

At the meeting last Friday, in order to have a clear picture of the impact of XcodeGhost, MIIT required Apple to provide a written material before National Holiday (Oct. 1) about measures we have taken and also such figures as:
a. how many apps have been infected
b. how many users have been affected, increase/decrease from beginning to present
c. how many users are still using infected apps

We are also expected to suggest how to inform users that have been infected but still have not made updates. MIIT has considered making an announcement by itself, but is concerned about the potential publicity, and this is also not what we want to see.

Fro the written material, regarding what we have done, messages in the Q&A and Phil's interview could be good enough. Regarding the figures and suggestion, could you help? We need to go back to MIIT by the noon of Sept. 30 the latest, as people will start holiday soon.

Thanks.

Bella

> On Sep 25, 2015, at 8:21 PM, Yi Wang [redacted] wrote:
>
> Hi all,
>
> Here is a summary of the meeting this afternoon at MIIT.
>
> **MIIT Host:**
> Deputy Director General LI Xuelin, Network Security Administration
> Director FU Jinguang Network Security Administration
>
> **Attending organizations:**
> China Mobile, China Unicom, China Telecom, CNCERT (National Computer Network Emergency Response Technical Team/Coordination Center of China) , Tencent, Qihu 360, Antian Technologies and Appl e (GA and DR)
>
> **MIIT clarified that the purpose of the meeting was to understand XcodeGhost's impact and reasons (initiators), efforts against it, further measures needed for both government and the companies, and how to prevent such issue from happening again.** MIIT appreciated the attending companies' efforts related to XcodeGhost in the past one or two weeks and communication with MIIT. Each company was asked to introduce about their related work and views about the XcodeGhost.
>
> GA and DR talked about Apple's measures, sticking strictly to the Q&A at our website and Phil's interview with Sina. The three Carriers, Tencent, WeChat, Qihu 360 have all screened their self-developed apps and made amendments.
>
> **CNCERT, Qihu 360 and Antian Technologies shared their research findings about XcodeGhost issue:**
> 1. Over 20million users have been infected
> 2. XcodeGhost initiator is based in Shandong China, but has rented 3 servers from Amazon's cloud service in the U.S, which are still active in getting consumer data
> 3.Though there is not yet information about the misuse of the collected consumer data, the data could be used to remote control the devices infected to open webpages, make phone calls and send messages. It could also be used to create pop-ups to seduce consumers to install certain programs. The impact is wide and long term. It is the first case in its type.
> 4. About 4000 apps of different versions have been infected.

MIIT's requirement for all attending organisations for next steps:
1. The three carriers to take measures to block the connection between XcodeGhost initiator's server and the consumers. To engage Amazon if necessary.
2. CNCERT, Antian Technologies and Qihu 360 to make further analysis about the harm of misuse of the collected consumer data, and validate the potential misuses.
3. MIIT will involve the police to identify the initiator(s).
4. CNCERT continue to monitor infected consumer data, to be compared with Apple's data
4. To support MIIT to understand the overall impact of XcodeGhost, Apple should provide a written material before National Holiday (Oct. 1) about measures taken and such figures as:
a. how many apps have been infected
b. how many users have been affected, increase/decrease from beginning to present
c. how many users are still using infected apps;

Other question to Apple:
1. XcodeGhost appeared in April, why Apple did not notice it?
2. suggestion of how to inform users that have been infected but still have not made updates **(MIIT has considered making an announcement by itself, but is concerned about the potential publicity).**

MIIT summarised that XcodeGhost issue happened because of problems at different sections of a whole chain, including Apple's verification mechanism. What all the parties should do now is to join efforts to solve the issue in a sound way.

Please comment if and how we could provide a written material as MIIT required, and involve teams as needed.

Many thanks.

Bella

> On Sep 25, 2015, at 1:00 PM, YeeWee Koh [redacted] wrote:
>
> Suggest you print out Phil's interview with Sina and our website content, and review in the car.
>
> YeeWee
> Sent from my iPhone
>
> On Sep 25, 2015, at 12:55 PM, Yi Wang [redacted] wrote:
>
> > Will do.
> >
> > Thank you all!
> >
> > Bella
> >
> > > On Sep 25, 2015, at 12:53 PM, Jun Ge [redacted] wrote:
> > >
> > > Craig and YeeWee, many thanks.
> > >
> > > Bella and Andrew, please sync up and ensure you have a strategy if any new questions that may be raised.
> > >
> > > Jun
> > >
> > > On Sep 24, 2015, at 9:49 PM, Craig Bradley [redacted] wrote:

PX-2173.7

I agree that it could make things worse and MIIT might think we are avoiding them if we don't show up. As long as there is no press and we stick to the script and not offer any more information than is already public then I am happy to OK this along with Yee Wee.

//Craig

> On 25 Sep 2015, at 2:16 pm, YeeWee Koh [redacted] wrote:
>
> I can understand this. If there are no media there, I'm ok with just Andrew and Kevin from DR to attend. There shouldn't be a need for PR.
>
> I agree with Jun that there could be a risk of aggravating this matter if we don't show up today.
>
> We just need to stick strictly to the script - which is based on Phil's interview with Sina, and what's already posted on our website.
>
> Craig? I'm happy to make this call together with you.
>
> > On Sep 25, 2015, at 12:10 PM, Jun Ge [redacted] wrote:
> >
> > I understand this meeting is not set and just for Apple to attend, where we can ask to reschedule. There are multiple parties involved. If we don't show up, would it make the matter more complicated and irritating to MIIT? They may decide to do something that are not based on what the truth is.
> >
> > Carolyn and YeeWee, could you speak with Andrew and see how to resolve this PR presence issue?
> >
> > Bella, any media will be there? Are they going to report the discussion? I assume it is a discussion without media coverage.
> >
> > We need to do the right thing here. I worry that if we don't have the right people there, this meeting will be another trigger for bad publicity.
> >
> > Jun
> >
> > On Sep 24, 2015, at 8:36 PM, Andrew Yeh [redacted] wrote:
> >
> > > Hi Bella,
> > >
> > > As discussed over the phone, we have no approval to attend this meeting without the presence of senior PR representative.
> > >
> > > Please communicate this to MII or escalate to appropriate channels.
> > >
> > > Regards,
> > > Andrew
> > >
> > > > On Sep 22, 2015, at 9:52 AM, Carolyn Wu [redacted] wrote:

We are working on this now. Stay tuned. Thanks

> On Sep 22, 2015, at 9:51 AM, Yi Wang [redacted] wrote:
>
> Hi Carolyn and all
>
> I believe we need to give a response to CNCERT, even if we could not answer all their questions. Or they will exert (or maybe already) impact on MIIT and other government authorities to create more pressure on Apple. A response from Cupertino is needed.
>
> Thanks.
>
> Bella
>
> > On Sep 22, 2015, at 5:40 AM, Craig Bradley [redacted] wrote:
> >
> > Carolyn,
> >
> > I have alerted Ron to the request as any response will need to come from Cupertino. Have you requested a response from anyone in Cupertino?
> >
> > //Craig
> >
> > Sent from my iPhone 6 Plus
> >
> > On 21 Sep 2015, at 5:23 PM, Yi Wang [redacted] wrote:
> >
> > > Carolyn,
> > >
> > > The alert refers to CNCERT's announcement at its website dated Sept. 14, at the following link.
> > >
> > > http://www.cert.org.cn/sites/main/preview_/waringdetail.htm?tid=20150914152821158428128&col_id=8_
> > >
> > > Bella
> > >
> > > > On Sep 21, 2015, at 3:01 PM, YeeWee Koh [redacted] wrote:
> > > >
> > > > + Craig
> > > >
> > > > YeeWee
> > > > Sent from my iPhone
> > > >
> > > > On Sep 21, 2015, at 2:49 PM, Carolyn Wu [redacted] wrote:
> > > >
> > > > > Adding Christine Monaghan, YeeWee and Andrew for input.
> > > > >
> > > > > Can you expand on what you mean when CNCERT has released an alert? Who receives the alert and how is it issued?
> > > > >
> > > > > Thanks,

PX-2173.9

Carolyn

On Sep 21, 2015, at 2:17 PM, Yi Wang [redacted] wrote:

Hi Carolyn and Connie,

As just talked on the phone, CNCERT (National Computer Network Emergency Response Technical Team/Coordination Center of China) has contacted GA regarding Apps with malicious code in App store. CNCERT has released an alert regarding non-official XCODE of Apple has malicious code. CNCERT claims that according to its statistics, over thousands of consumers have been infected with the malicious code for downloading apps from App Store, and the consumer information leaked as a result should be dozens of million pieces, and the private information security of the Chinese consumers have been threatened seriously.

CNCERT claims that the issue has serious impact and may face some legal challenges. CNCERT asks Apple to provide a written explanation on the following questions:

1. Why App Store, as the source spreading the malicious code, did not detect Apps with the malicious code? What is the App security auditing mechanism in Apple?
2. In reaction to the alert by CNCERT, what measures have Apple taken to get rid of the security threats?
3. What measures will Apple take to deal with malicious codes that may appear in App Store in the future?

CNCERT emphasized that Apple should give importance to the impacts of the issue. Though self claiming a non-governmental non-profit cybersecurity technical centre, CNCERT is under the guidance of MIIT (the Ministry of Industry and Information Technology) and plays important role in coordinating China's cybersecurity emergency response community.

I would like to know if the input you've got from Cupertino could answer the 3 questions? If not, could you help to involve relevant teams for the answers?

Thanks.

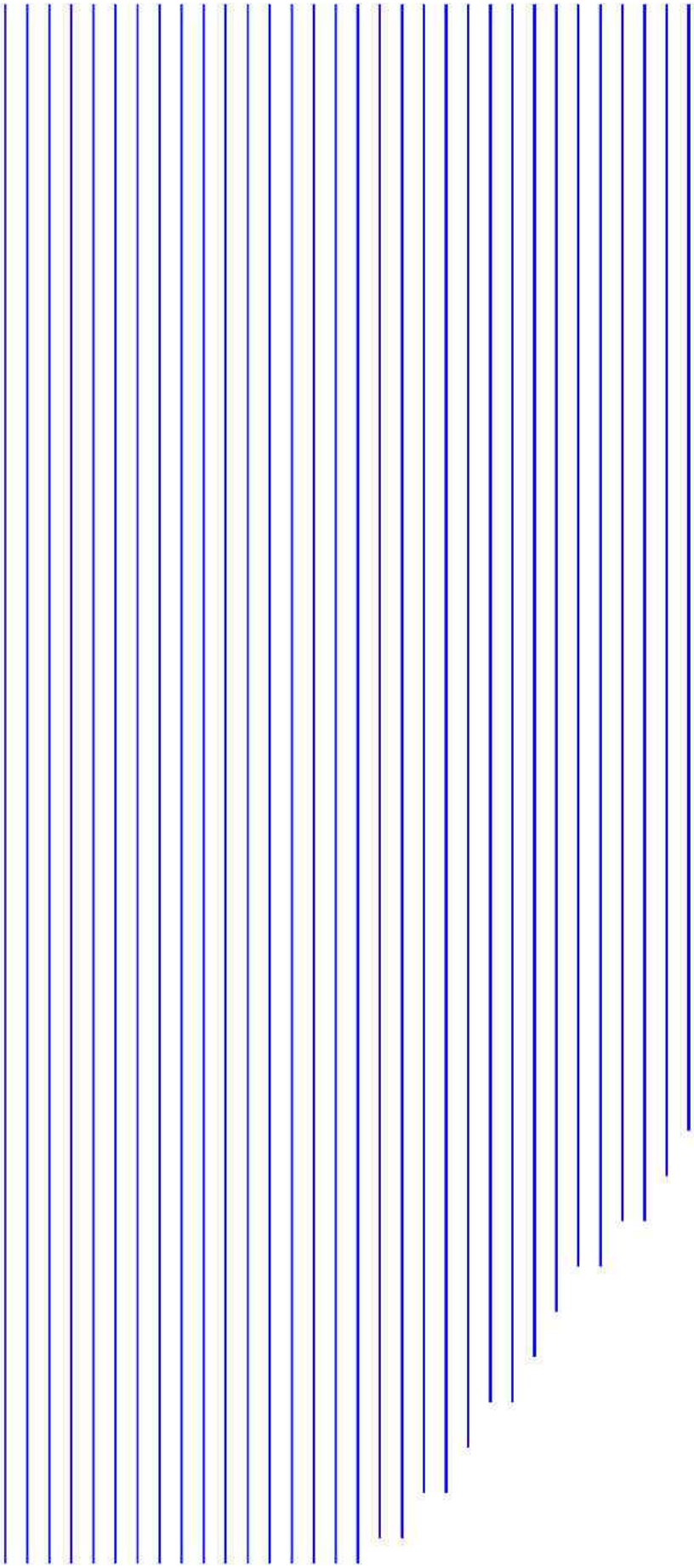
Bella
GA China

Begin forwarded message:

From: 何能强 [redacted]
To: yi_wang [redacted]
Cc: 严寒冰 [redacted] hzc [redacted]
Subject: **[CNCERT] 关于苹果APPSTORE正常上架带有恶意代码APP的情况说明**
Date: September 21, 2015 at 1:12:14 PM GMT+8

苹果，您好！

PX-2173.10



我们是国家互联网应急中心（www.cert.org.cn），隶属于工业和信息化部，负责我国的网络安全事宜。

近期，我中心发布了“关于使用非苹果官方 XCODE 存在植入恶意代码情况的预警通报”，链接如下：

http://www.cert.org.cn/sites/main/preview/waringdetail.htm?tid=20150914152821158428128&col_id=8

据我中心统计，有上千万用户因下载APP STORE 中的APP感染恶意代码，泄露的用户信息超过数千万条，严重危害了中国公民的个人信息安全。

本次事件具有严重的后果，并可能触及相关中国法律，在此 请贵司做出如下说明：

1、做为恶意代码传播的源头，苹果公司 APP STORE 为什么没有检测出带有恶意代码的APP？贵司的APP安全审核机制是什么样的？

2、对于我中心发布本次事件的预警通报后，贵司做了哪些应急措施来消除本次事件的安全威 胁？

3、对于未来可能在 APP STORE 中出现的恶意代码，贵司会有什么样的措施？

请贵司尽快提供关于以上 问题的书面回复，务必重视本次事件的影响。

****
何 能 强（HE NENGQIANG）
国家互联网应急中心（CNCERT/CC）
中国反网络病毒联盟（ANVA）
关注ANVA微博 www.weibo.com/[redacted]
****