From: Dan Martinez [redacted]
To: Trystan Kosmynka [redacted]
CC: Ali Menbari [redacted] Stoney Gamble [redacted] Sam Muther Bavaro [redacted]
BCC:
Subject: Re: New iPhone Threat: These 17 Malicious Apps May Be On Your Device—Delete Them Now
Attachments:
Sent: 10/24/2019 08:46:30 PM 0000 (GMT)

Hi Trystan,

This app was removed sale on 10/22/19 (not sure how long it took for the app to come down from the Store). No one has approved it since, or immediately leading up to the removal. The last approval was on 7/31/19. It appears the note's history in MG is not in chronological order.

However, this incident appears to be an issue with our TDP process and developer vetting. We had this developer and rejected their app for consolidation back on 9/21/17. After going back and forth, the developer eventually complied. Since then the app has been rejected numerous times for various reasons; 2.1.0, 3.1.2, and 5.1.1.

@Sam, given the developer's history we can use multiple rejections over an app's history as a signal to further investigate a developer's account? What do you think?

> On Oct 24, 2019, at 11:32 AM, Trystan Kosmynka <[redacted]> wrote:
>
> Dan, can we look at this please.
>
> Weird one, looks like we took it down, it came back to review, two folks ignored the notes (not hard to do that) and approved the app. The app was arc hidden, not hidden refusal, so it did not come back to the ARC team. The second person to review an update after the ARC even marked the issues as resolved (not sure how either of them verified it without going back to TI)
>
> We are making critical errors, it's a game of telephone where the instructions are left in a note for the next person to action.
>
> magellan://open?fgid=272136171 (EMI Calculator & Loan Planner)
>
> +Sam for MG3 considerations

Begin forwarded message:

From: Ali Menbari <[redacted]
Subject: Re: New iPhone Threat: These 17 Malicious Apps May Be On Your Device—Delete Them Now
Date: October 24, 2019 at 10:55:47 AM PDT
To: Trystan Kosmynka <[redacted]
Cc: Stoney Gamble <[redacted]

Investigating.

Best,
Ali

On Oct 24, 2019, at 10:46 AM, Trystan Kosmynka <[redacted] wrote:

I thought all these apps were removed? Also, I see some of the many that were hidden are in review, we should not be returning these to store without escalation.

https://mozart.itunes.apple.com/search/details/fgid/276956057

Begin forwarded message:

From: Bill Havlicek <[redacted]
Subject: New iPhone Threat: These 17 Malicious Apps May Be On Your Device—Delete Them Now
Date: October 24, 2019 at 8:28:24 AM PDT
To: AR-PR-Response <[redacted] ARC Team <[redacted]

https://www.forbes.com/

New iPhone Threat: These 17 Malicious Apps May Be On Your Device—Delete Them Now

Zak Doffman

<960x0 jpeg>

Getty

Apple iPhone users are being warned to check their devices against a list of malicious apps disclosed in a new report. The exposure of such dangers on Google's Play Store has become a theme this year, with apps laced with adware, subscription fraud and worse exposed and removed. Now Apple is taking its turn in the spotlight. A new report from the research team at Wandera has identified 17 apps from one developer that load a malicious clicker trojan module on an iOS device. This will come as a shock to Apple users who assume downloads from the App Store are safe from such dangers.

The trojan focuses on ad fraud, but it also encrypts and sends data from the infected device to an external command and control server, raising the risk profile. Wandera told me that an even more worrying element of the trojan, one not included in the write-up, is a set of devious techniques to evade detection. The malware triggered only when loaded with an active SIM and left running for two days. We have seen this before on Android—an attempt to hide from security researchers in lab conditions. This isn't what Apple users have come to expect from the locked down world of iOS.

"We were amazed with this one," Wandera VP Michael Covington tells me ahead of the report's release. "We've seen a couple of issues creep into the Apple App Store over the last few months—and it always seems to be the network element." In his view, Apple misses the runtime element of an app's behaviour when scanned before approval. "They don't have a deep threat research

expertise," he explains, "but to find malicious network traffic, you have to watch live apps and see how they perform."

At the time of writing, the apps are all still available to install in various countries. And, just as with Google Android, the fact that these 17 apps have escaped Apple's lockdown means there will be more—likely many, many more. "This just scratches the surface of what's in the app store," Covington says, "it throws the door wide open."

Wandera discovered the malicious apps when its monitoring platform detected network traffic back to the external C&C server. "That forced us to work backwards," Covington tells me, "we found one of those apps, and from there we found the developer and then the other indicators of compromise that led to the other apps."

<960x0 png>

WANDERA

Each of the apps contain the "malicious" clicker trojan module. "Malicious," Covington explains, because the module can do more than just generate fraudulent ads. "It could potentially steal information, or open a backdoor," he says. "Any time I see an app opening a connection to the outside, I think we may have more than just bad ads, we have some malicious functionality that's being introduced."

All of the apps will "carry out ad fraud-related tasks in the background," the report explains, "such as continuously opening web pages or clicking links without any user interaction." The module generated revenue for the operators "on a pay-per-click basis by inflating website traffic." The evasive behaviour, which is not in the report, points to a level of sophistication beyond simple ad fraud. To design malware specifically to outwit a security research lab is a level beyond.

Covington also wants users warned that the outside connection means a high risk of data compromise—at least to some extent. The malware sends device and location information, some user data as well potentially. The apps are not games. "One managed contacts, another travel information, another had access to accelerometer and location—even without special permissions for the camera or microphone, the apps likely accessed contacts and location, with privacy implications."

The fact there's an external link involved carries more insidious threats. "Certain information about the device and the user is used to determine what ads to deliver," Covington says. "But we have seen C&C servers deliver other types of commands—to change configurations or trigger phishing attacks, to deliver legitimate-looking login pages to steal credentials. Or to deliver malicious payloads to bulk ups apps or install others. Once you open a connection to the outside, bad things can happen."

What the Wandera team has seen is performance degradation, battery drain, heavy bandwidth use—one ad runs a video stream for more than five minutes, others contain large images. The same C&C server was disclosed by Dr. Web as part of an Android malware campaign. Dr. Web reported that the server could target ads, load websites, alter the configuration of devices, fraudulently subscribe users to premium content. The encryption between the malware and the C&C server has not been cracked.

The developer is AppAspect Technologies, based in India, an operator with apps for both iOS and Android. Wandera examined the Android apps—none contained the clicker trojan module, but they used to, they were pulled from the store, the module removed, the apps republished. Perhaps the heat being turned up on the Play Store forced a retreat? Perhaps the operator turned its focus to iOS where there is less expectation of such compromises? Covington thinks this is a real possibility.

Wandera is in discussions with Apple, sharing its findings. But in the meantime the apps remains available for install. The good news is that deleting the apps appears to solve the problem, no remnants are left behind. "There is no access to special frameworks that might have left something behind," Covington explains.

For Apple, in light of other security challenges in recent months, including a targeted WhatsApp hack, the Chinese malware attack on the Uighurs, new jailbreak options, this casts more doubt over the integrity of the platform. The bulletproof reputation Apple has built over the years has been knocked in recent months. And the issue now is that every cybersecurity research house will be turning its attention to the App Store to find other apps hiding similar dark secrets.

–

Here is the list of infected apps:

1. RTO Vehicle Information
2. EMI Calculator & Loan Planner
3. File Manager - Documents
4. Smart GPS Speedometer
5. CrickOne - Live Cricket Scores
6. Daily Fitness - Yoga Poses
7. FM Radio PRO - Internet Radio
8. My Train Info - IRCTC & PNR (not listed under developer profile)
9. Around Me Place Finder
10. Easy Contacts Backup Manager
11. Ramadan Times 2019 Pro
12. Restaurant Finder - Find Food
13. BMI Calculator PRO - BMR Calc
14. Dual Accounts Pro
15. Video Editor - Mute Video
16. Islamic World PRO - Qibla
17. Smart Video Compressor

Bill Havlicek | [redacted] [redacted]

Version 6.2

Approved (Kenji Baba)
7/31/19, 5:36:06 PM PDT

Kin Cho Tsui (Apple) 10/22/19, 6:20:29 PM PDT

This app has a previously unresolved issue which has been communicated to the developer. Please verify if the following issue is resolved in the newly submitted version and process the app accordingly. It is not necessary to reassign the app to the ARC team.

2.3.1 & 3.2.2 - App contains a hidden functionality that artificially increases ad click-throughs
4.3 - Spamming across accounts with similar apps (please refer to the ARC elevate ticket for more details)
Please escalate the resubmission to TI for further investigation.

New Binary Submission **Build 6.2.1**

Version 6.1

Approved (Kota Kato)
7/10/19, 6:11:23 PM PDT

Version 6.2

Approved (Kenji Baba)
7/31/19, 5:36:06 PM PDT

Kin Cho Tsui (Apple) 10/22/19, 6:20:29 PM PDT

This app has a previously unresolved issue which has been communicated to the developer. Please verify if the following issue is resolved in the newly submitted version and process the app accordingly. It is not necessary to reassign the app to the ARC team.

2.3.1 & 3.2.2 - App contains a hidden functionality that artificially increases ad click-throughs
4.3 - Spamming across accounts with similar apps (please refer to the ARC elevate ticket for more details)
Please escalate the resubmission to TI for further investigation.

New Binary Submission Build 6.2.1

Version 6.1

Approved (Kota Kato)
7/10/19, 6:11:23 PM PDT