TangleBot: New Advanced SMS Malware Targets Mobile Users Across U.S. and Canada with COVID-19 Lures

cloudmark.com/en/blog/mobile/tanglebot-new-advanced-sms-malware-targets-mobile-users-across-us-and-canada-covid-19

September 21, 2021

Blog

Malware

TangleBot: New Advanced SMS Malware Targets Mobile Users Across U.S. and Canada with COVID-19 Lures

September 23, 2021 Felipe Naves, Andrew Conway, W. Stuart Jones, and Adam McNeil

Key Takeaways

- A clever and complicated new SMS malware attack has been discovered in the United States and Canada.
- This malware, coined TangleBot, can directly obtainpersonal information, control device interaction with apps and overlay screens, and steal account information from financial activities initiated on the device.

Overview

Cloudmark threat analysts have discovered a new piece of mobile malware spreading via SMS and currently targeting Android mobile users in the United States and Canada.TangleBot uses SMS text message lures with content about COVID regulations and the third dose of COVID vaccines to trick mobile subscribers into downloading malware that compromises the security of the device and configures the system to allow for the exfiltration of confidential information to systems controlled by the attacker(s). The malware has been given the moniker TangleBot because of its many levels of obfuscation and control over a myriad of entangled device functions, including contacts, SMS and phone capabilities, call logs, internet access, and camera and microphone.

TangleBot Malware Function

Following in the footsteps of the FluBot SMS Android malware that has proven to be an ongoing threat in Europe and the UK, TangleBot attempts to trick mobile users into downloading malicious software by sending COVID-19 warning notifications (Figures 1 and 2).

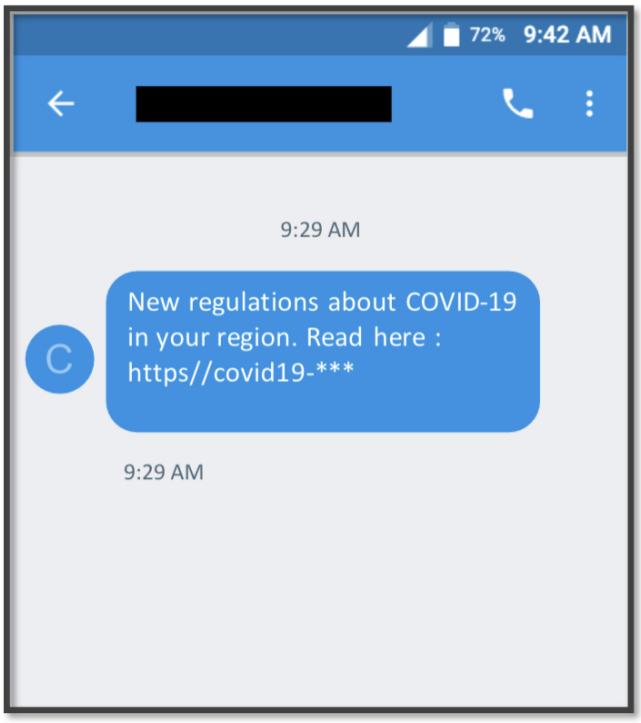

Figure 1.

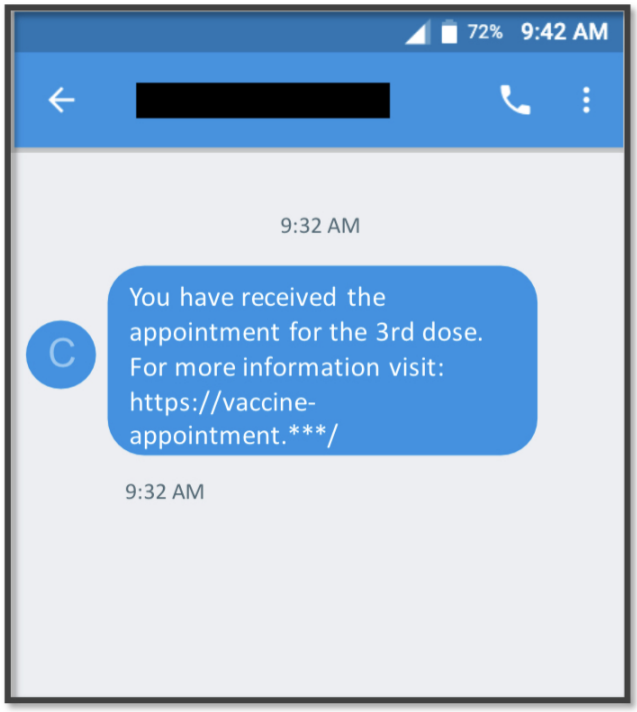

Figure 2.

Should a user fall victim and click on the link in the message, a website appears notifying the user that the Adobe Flash Player on the device is out of date and must be updated. If the user clicks on the subsequent dialog boxes, TangleBot malware is installed on the Android device.

TangleBot is then granted privileges to access and control many device functions (Figures 3 through 5), including contacts, SMS and phone capabilities, call logs, internet, camera and microphone, and GPS.

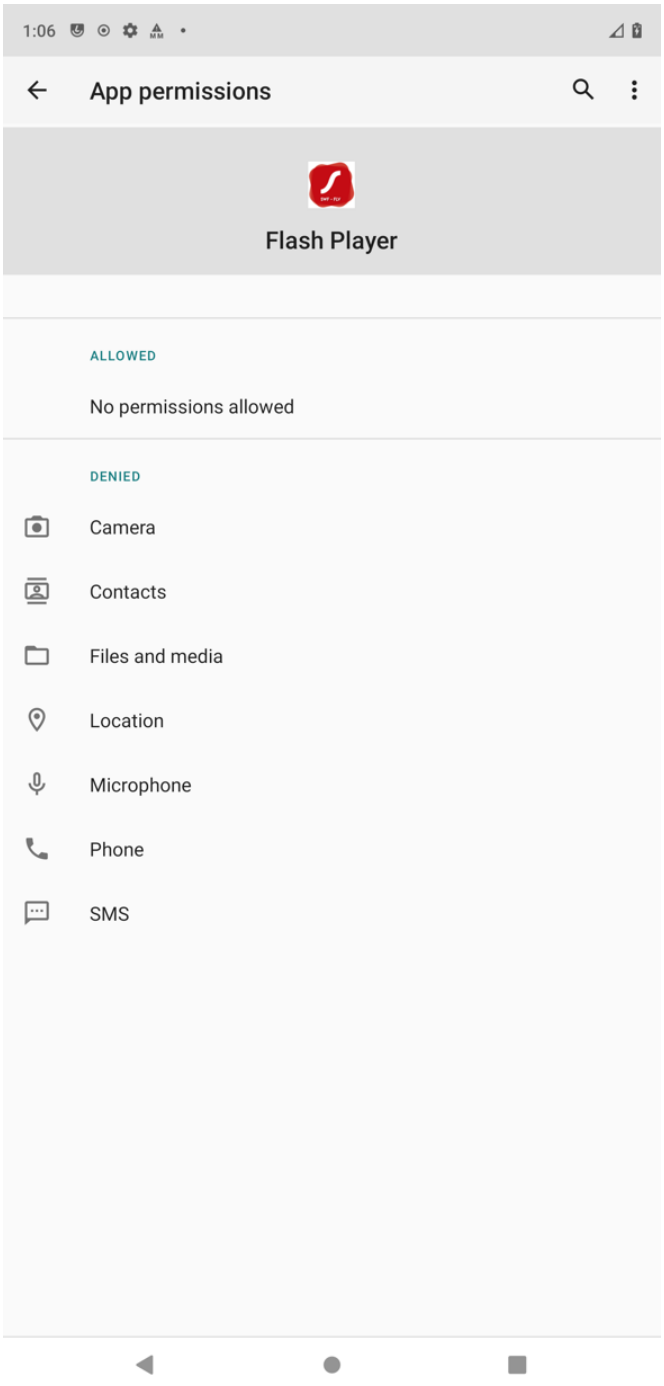

Figure 3.

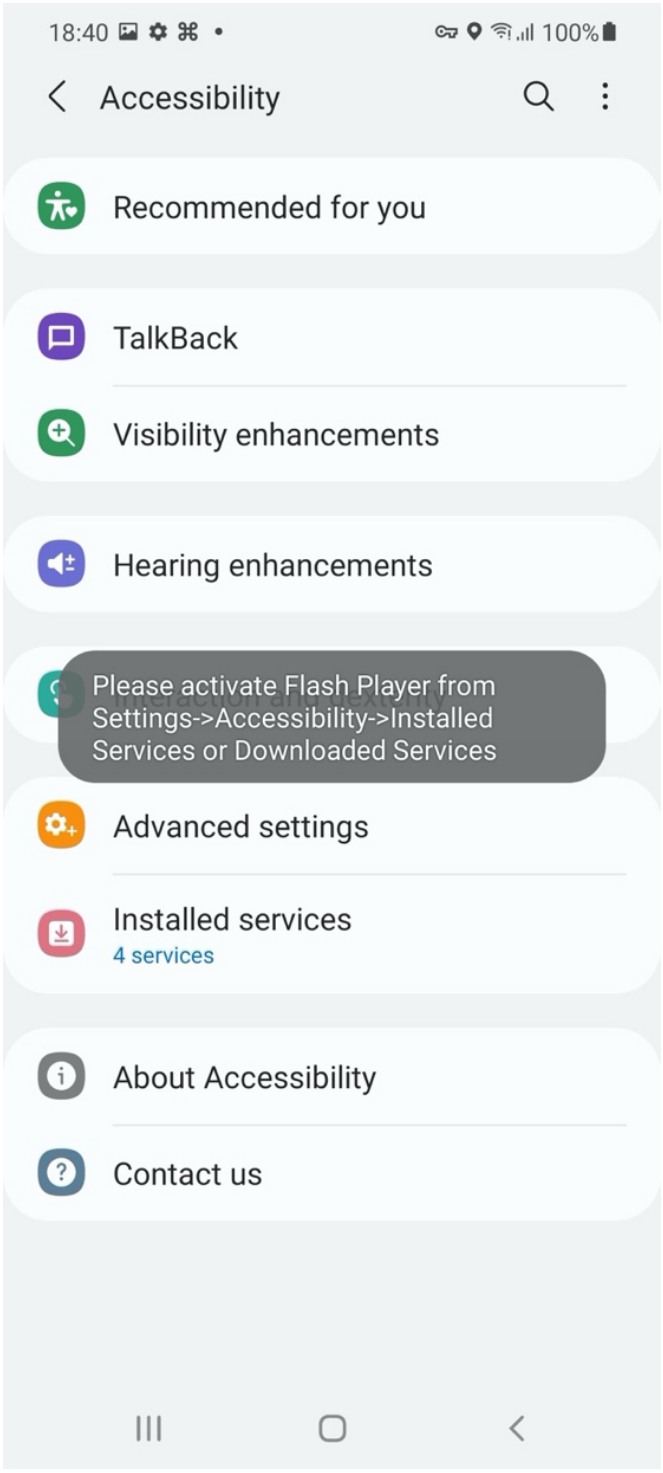
18:40
100%
Accessibility
Recommended for you
TalkBack
Visibility enhancements
Hearing enhancements
Please activate Flash Player from Settings->Accessibility->Installed Services or Downloaded Services
Advanced settings
Installed services
4 services
About Accessibility
Contact us

Figure 4.

Figure 5.

The attacker can now do the following:

- make and block phone calls
- send, obtain, and process text messages
- record the camera, screen, or microphone audio or stream them directly to the attacker
- place overlay screens on the device covering legitimate apps and screens
- implement other device observation capabilities

The ability to detect installed apps, app interactions, and inject overlay screens is extremely problematic. As we have seen with FluBot, TangleBot can overlay banking or financial apps and directly steal the victim's account credentials. Also, TangleBotcan use the victim's device to message other mobile devices spreading throughout the mobile network. The capabilities also enable the theft of considerable personal information directly from the device and through the camera and microphone, spying on the victim. Harvesting of personal information and credentials in this manner is extremely troublesome for mobile users because there is a growing market on the dark web for detailed personal and account data. Even if the user discovers the TangleBot malware installed on their device and is able to remove it, the attacker may not use the stolen information for some period of time, rendering the victim oblivious of the theft.

Mobile Users Should Be Aware

Mobile users should be alert and on the lookout for these unexpected SMS warning messages and follow these SMS best practices:

Do's

1. Be on the lookout for suspicious text messages. Criminals are increasingly using mobile messaging and SMS phishing as an attack vector.

2. Carefully consider before providing your mobile phone number to an enterprise or other commercial entity.

3. If you receive a message from any enterprise, includingsome sort of warning or package delivery notification that contains a web link, use your device's browser to access the enterprise's or service's website directly. Do not use the web link provided in the text message. Do this as well for any offer codes you receive by entering them directly into the enterprise's or service's website from your browser.

4. Report SMS phishing and spam. Use the spam reporting feature in your messaging client if it has one, or forward spam text messages to 7726, which spells "SPAM" on the phone keypad.

5. Be careful downloading and installing new software to your mobile device and read install prompts closely, looking out for information regarding rights and privileges that the app may request.

Don'ts

1. Don't respond to any unsolicited enterprise or commercial messages from a vendor or enterprise you don't recognize. Doing so will often confirm that you're a "real person."

2. Don’t install software on your mobile device outside a certified app store from the vendor or Mobile Network Operator.

For more information on our security platform for mobile messaging, please visit: https://www.cloudmark.com/en/s/products/cloudmark-security-platform-for-mobile.