TangleBot

Threat: **SMS Malware**

Author: **Jeffrey Farnan**

Date Originally Published: **September 30th, 2021**

1. SUMMARY

- TangleBot is a new smishing malware which targets Android mobile in the U.S and Canada. This malware uses SMS text messages related to COVID-19 regulation and vaccine information to lure victims, with an attempt to steal personal and financial data. Users are fooled into clicking a link which will infect their cell phones. The malware is able to gain private data but can also overlay banking of financial apps and steal the victims account credentials.

2. MALWARE FAMILY

- **Type** = SMS Malware.
- **Sub-type** = Trojan / Spyware.

- This attack is a smishing (phishing via SMS) scam involving false vaccine appointments and misinformation to trick you into surrendering your personal data.
- Cybercriminals use either one or two methods to steal data:
  - **Malware:** The smishing URL link tricks users to download malware usually by masquerading as a legitimate app, when installed tricks you into inputting personal information.
  - **Malicious Website:** The link in the smishing message might lead to a fake site that requests user’s sensitive personal information.
- This personal information is sent back to the Cybercriminals, where it is used in a future attack or sold on to other 3rd parties.

3. MALWARE CHARATERISTICS

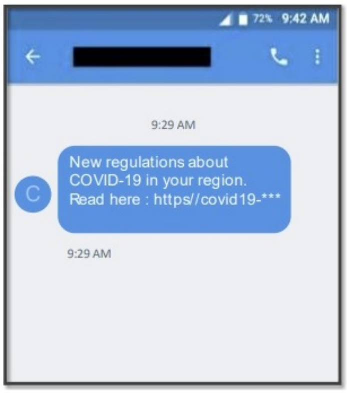
- **Suspected country of origin** = Unknown.
- **First seen date/period** = September 2021.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = September 27th, 2021.

4. MALWARE HISTORY

- This is a new threat campaign, the cybercriminals are using peoples fear over Covid-19 as an opportunity to trick users by providing false information, such as a booster shot vaccine appointments. The malware is named TangleBot because of the many layers of obfuscation and control of entangled device functions, including contacts and phone capabilities, call logs, internet access, and camera and microphone. TangleBot resembles other mobile malware such as Flu bot which is still active in England and across Europe.

5. MALWARE DESCRIPTION

- TangleBot is a clever and complicated piece of malware which sends Android users a text message providing the latest Covid-19 guidance for their area, or alerting them to their third Covid-19 vaccine appointment which has been scheduled.

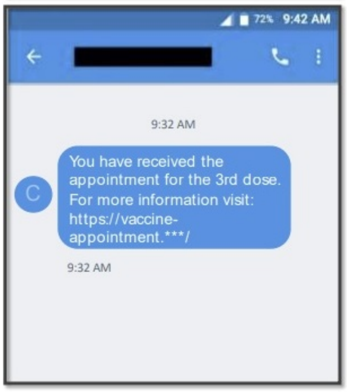


[redacted]

9:29 AM

New regulations about COVID-19 in your region. Read here : https//covid19-***

9:29 AM



[redacted]

9:32 AM

You have received the appointment for the 3rd dose. For more information visit: https://vaccine-appointment.***/

9:32 AM

- Users are advised to clink on the provided link, which will prompt them to update their phone's Adobe flash player. Once the update is applied the TangleBot malware gets installed on the Android device.
- Once infected the malware prompts you to give accessibility permissions through Settings which will enable it to access and control many device functions.
- The TangleBot malware now has access to many of the phones functions, such as SMS and phone capabilities, call logs, internet, camera and microphone and the location service. The attackers can:
    - Send and receive text messages
    - Intercept phone calls
    - Implement other device observation capabilities
    - Activate and record the microphone, camera and stream them back to the attackers
- This malware can detect installed apps, app interactions and inject overlay screens which imitate financial apps allowing them to directly steal the victim's account credentials.
- The victim's device is used to transmit the false Covid-19 alert to the victim's family and friends whose phone numbers are in their contact list.
- Even if the malware is discovered and removed the cybercriminals still has whatever personal information they took, which can be used in the future or sold on the dark web. The victims believe nothing was stolen as their personal information was not used at this time.

6. POTENTIAL CUSTOMER DEFENSE

Android users should be on the lookout for suspicious alerts or text messages, follow these SMS best practices:

- If users get a SMS message which includes a web link, they should not click on that link, but go the official website directly. This is an increasing attack method, which may look harmless but people can end up risking personal and financial information.
- Users need to particularly cautious about receiving text messages from strangers, medical institutions, insurance companies or any other entities. Check with official sites or services through other means.
- Install apps only form the official Android Play Store.
- Change your passwords. If you think you're the victim of a scam, it's advised to change you passwords immediately.
- Report SMS phishing and spams.

Research Sources:

- https://www.cbsnews.com/news/tanglebot-android-malware-covid-19/
- https://www.makeuseof.com/tanglebot-malware-covid19-target/
- https://heimdalsecurity.com/blog/us-canadian-android-mobile-users-targeted-by-tanglebot-malware/
- https://threatpost.com/tanglebot-malware-device-functions/174999/
- https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

Disclaimer: All opinions expressed in this article are the opinions solely of the author.