Medusa TangleBot Malware Leveraging COVID-19 Theme to Attack U.S. Targets

Executive Summary
Medusa (AKA TangleBot) is a malware that is spreading via SMS and is currently targeting the Android mobile operating system. There are reports of this malware going back to 2019 and it appears to have reemerged in popularity. Medusa is similar to Europe’s Flu Bot malware which tricks the target into installing the malicious software received by a fake Covid-19 alert. Medusa’s wide-ranging access to mobile device functions is what sets it apart. Attackers have been leveraging COVID-19 themes to entice victims in the United States to unknowingly install Medusa onto their devices. Medusa is capable of collecting data and installing additional malware.

Report/Analysis
The Medusa malware is targeting Android users and taking advantage of the pandemic by sending COVID-19 related text messages that informs receipts of, “New regulations about COVID-19 in your region,” and another sends an alert stating, “You have received the appointment for the 3rd dose.” Each text message is sent with a malicious link as shown in Figure 1.

The attack is initiated when the victim clicks on a malicious link in a SMS text, they are directed to a website that gives a notification that the user’s Adobe Flash Player is out of date and must be updated. Clicking on the resulting dialog box results only in downloading malware onto the device. It is important to mention that while Adobe Flash Player was natively supported on Android devices, it no longer is, however as you can see in Figures 2-4. (Courtesy of Cloudmark) this is how the attack is carried out.)

![Figure 1](image1.png)

![Figure 2](image2.png)
Once the Medusa malware infects a device, it has a number of data gathering capabilities it can leverage, including accessing the victim’s internet, call logs and GPS. This is particularly concerning because it can allow the threat actor to know the victim’s location at any time. Additionally, the attacker can record the camera, screen, or microphone audio or stream them directly to the attacker. The attacker can also place overlay screens on the device covering legitimate apps and screens. In addition to this, Medusa can use the victim’s device to message other mobile devices spreading throughout the mobile network.

**Patches, Mitigations, and Workarounds**

It is recommended for mobiles user to utilize safe messaging practices and avoid clicking on any links in texts, even if they appear from a reputable source. When downloading apps, read the install prompts carefully and be aware of rights and privileges the app may request. Additionally, users should only install apps from trusted sources.

According to experts, once the malware is installed to a device it can be difficult to detect and remove. In Figure 5 below, courtesy of Hybrid Analysis, you will see that AppRisk:Generisk , which is linked to TangleBot, is hard to detect with Antivirus.

**References**

Broadcom: Protection Bulletins
[https://www.broadcom.com/support/security-center/protection-bulletin#blt5dc4cb156b238046_en-us](https://www.broadcom.com/support/security-center/protection-bulletin#blt5dc4cb156b238046_en-us)

Phone scammers use COVID-19 vaccine appointments to try tricking victims into downloading malware
New TangleBot malware is targeting Android devices in the US and Canada


We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback