

Beware Android trojan posing as Clubhouse app

welivesecurity.com/2021/03/18/beware-android-trojan-posing-clubhouse-app/

March 18, 2021



The malware can grab login credentials for more than 450 apps and bypass SMS-based two-factor authentication



[Amer Owaida](#)

18 Mar 2021 - 03:47PM

The malware can grab login credentials for more than 450 apps and bypass SMS-based two-factor authentication

Cybercriminals are attempting to take advantage of the popularity of Clubhouse to deliver malware that aims to steal users' login information for a variety of online services, ESET malware researcher [Lukas Stefanko](#) has found.

Disguised as the (as yet non-existent) Android version of the invitation-only audio chat app, the malicious package is served from a website that has the look and feel of the [genuine Clubhouse website](#). The trojan – nicknamed “[BlackRock](#)” by ThreatFabric and detected by ESET products as Android/TrojanDropper.Agent.HLR – can steal victims' login data for no fewer than 458 online services.

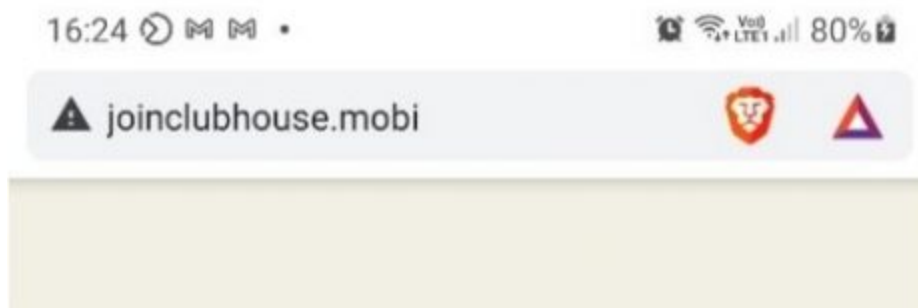
The target list includes well-known financial and shopping apps, cryptocurrency exchanges, as well as social media and messaging platforms. For starters, Twitter, WhatsApp, Facebook, Amazon, Netflix, Outlook, eBay, Coinbase, Plus500, Cash App, BBVA and Lloyds Bank are all on the list.


Malicious web claiming to offer [#Clubhouse](#) for Android spreads banking trojan Blackrock. It lures credentials from 458 apps – financial, cryptocurrency exchanges & wallets, social, IM and shopping apps. There is currently no official Clubhouse app for Android. [#ESETresearch](#) 1/2 pic.twitter.com/azlxjvlgNO

— ESET research (@ESETresearch) [March 16, 2021](#)

“The website looks like the real deal. To be frank, it is a well-executed copy of the legitimate Clubhouse website. However, once the user clicks on ‘Get it on Google Play’, the app will be automatically downloaded onto the user’s device. By contrast, legitimate websites would always redirect the user to Google Play, rather than directly download an Android Package Kit, or APK for short,” said Stefanko.

Even before tapping the button there are signs that something is amiss, such as the connection not being secure (HTTP instead of HTTPS) or that the site uses the “.mobi” top-level domain (TLD), rather than “.com” used by the legitimate app (see Figure 1). Another red flag should be that even though Clubhouse is indeed planning to [launch the Android version of its app](#) soon, the platform is at present still available only for iPhones.



 **Clubhouse**


Hey, we're still opening up but anyone can join with an invite from an existing user!

Sign up to see if you have friends on Clubhouse who can let you in. We can't wait for you to join!



16:24    •

      80% 

 joinclubhouse.com



 **Clubhouse**

Hey, we're still opening up but anyone can join with an invite from an existing user!

Sign up to see if you have friends on Clubhouse who can let you in. We can't wait for you to join!



Figure 1. Notice the difference in the URLs between the fraudulent (left) and legitimate (right) website

Once the victim is hoodwinked into downloading and installing BlackRock, the trojan tries to purloin their credentials using an overlay attack. In other words, whenever the user launches one of the targeted applications, the malware will create a data-stealing overlay of the application and request the user to log in. Instead of logging in, the user unwittingly hands over their credentials to the cybercriminals.

Using SMS-based two-factor authentication (2FA) to help prevent anyone from infiltrating your accounts wouldn't necessarily help in this case, since the malware can also intercept text messages. The malicious app also asks the victim to enable accessibility services, effectively allowing the criminals to take control of the device.

To be sure, there are other ways to spot the malicious decoy besides those shown in Figure 1. Stefanko points out that the name of the downloaded app "Install", instead of "Clubhouse" should be an instant red flag. "While this demonstrates that the malware creator was probably too lazy to disguise the downloaded app properly, it could also mean that we may discover even more sophisticated copycats in the future," he warned.



Install

Do you want to install this application? It does not require any special access.

welivesecurity

CANCEL INSTALL



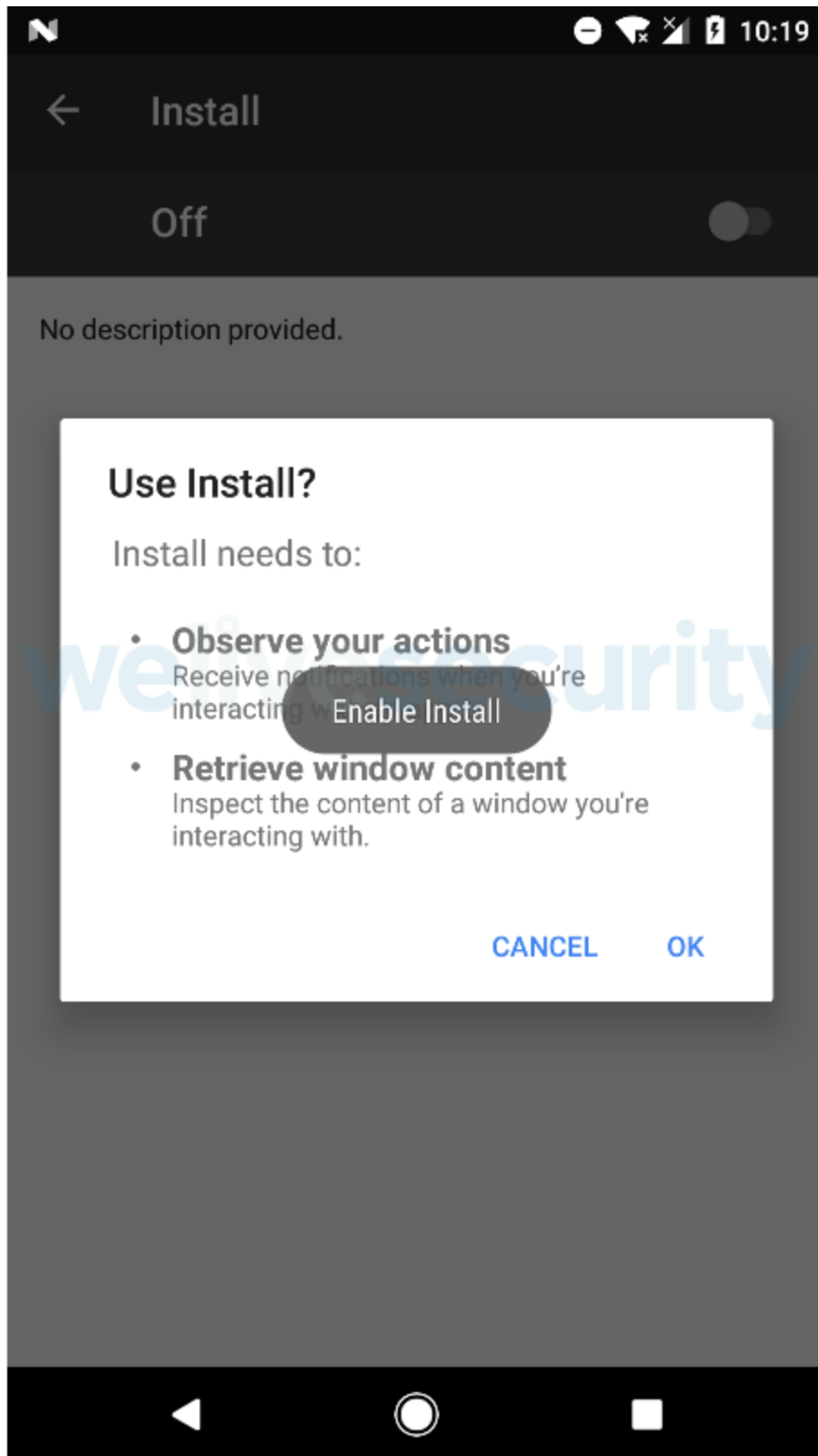


Figure 2. The installation prompt

This is perhaps also a good opportunity to brush up on mobile security best practices:

- Use only the official stores to download apps to your devices.
- Be wary of what kinds of permissions you grant to applications.
- Keep your device up to date, ideally by setting it to patch and update automatically.
- If possible, use software-based or hardware token one-time password (OTP) generators instead of SMS.
- Before downloading an app, do some research on the developer and the app's ratings and user reviews.
- Use a reputable mobile security solution.

For a more thorough take on how to protect yourself against mobile security threats, head over to [this article](#).

18 Mar 2021 - 03:47PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion
