HOOKBOT – a new mobile malware

cebrf.knf.gov.pl/komunikaty/artykuly-csirt-knf/362-ostrzezenia/858-hookbot-a-new-mobile-malware

Surveys show that more than 90% of the population now owns a mobile phone, with smartphones running the Android operating system being the most popular. Criminals know this and are eager to exploit this fact to steal sensitive user data, which can ultimately be used for financial gain. An example of this is the mobile malware known as HookBot, which was discovered in January 2023 and is the subject of this article.

It all started with the identification of an advertisement claiming to sell a new mobile malware (Figure 1). Analysis showed that the author of the post was already responsible for other well-known malware families - BlackRock and ERMAC - which were active in Polish cyberspace and caused losses to Polish bank customers. In view of the above, the KNF CSIRT team took action, acquired an application belonging to the new malware family and performed its analysis. Below is a brief description of the scope of the HookBot malware, and at the end of the article we have included a detailed technical analysis for those who wish to delve deeper into the technical aspects of its operation.

Figure 1 - An advertisement posted by the author of HookBot on the criminal forum.

The HookBot Trojan is malware designed to gain access to a user's private information, such as passwords to online banking, email accounts, cryptocurrency wallets or popular social networking sites. In the current version of the malware in question, the creators have prepared a record 772 forms impersonating legitimate applications, 24 of them come from the Polish domain. Among the prepared forms impersonating an application from the .pl domain, we identified the following brands (Figure 2)):

- Allegro
- Bank BPH
- Bank Polskiej Spółdzielczości
- Santander Bank Polska
- Ceneo
- Rossmann
- EnveloBank
- Euro Bank
- Fakturownia
- Idea Bank
- iFirm

- ING Bank Śląski
- mBank
- Millennium Bank
- Nest Bank
- Noble Bank
- Novum Bank
- Orange Polska
- PKO BP
- Raiffeisen Bank

Figure 2 - Forms impersonating applications of the .pl domain

The criminals also prepared forms for the most popular social networks (Fig. 3):

Figure 3 - Examples of fake applications impersonating popular social networks

The malware also targets applications that support cryptocurrency wallets, such as:

- Cryptopay
- MyWallet
- BitPay

A full list of forms used can be found in the technical analysis report. HookBot is distributed by fake applications that masquerade as legitimate, often popular software. For example, the HookBot in question first presents itself as a Google Chrome browser (Figure 4).

Figure 4 - HookBot malware masquerading as the Google Chrome application.

Once the device is infected, the malware can access system functions to track and capture sensitive information. Through reverse engineering, CSIRT KNF analysts have identified a number of functions that the malware can perform. One of these is what is known as privilege escalation, a process by which the malware gains privileges that are not granted by default. HookBot uses so-called Accessibility Services (Figure 5) for privilege escalation. These are features designed for people with dissabilities to make the device easier to use.

Figure 5 - From the left: Attempted access to the Accessibility feature by malware. Privileges gained through privilege escalation.

What is new compared to other malware families, even previous families from the same developer, is the support for WhatsApp application. The malware can read, write and send messages in this messenger. The process of monetising the infection takes place when the victim of an infected device launches an application that is on the malware's target list. The

malware uses the system's WebView component to display a fake login page for the service the user has launched (this is known as the overlay mechanism) (Figure 6). For example, if a banking application is on the criminals' target list and the user who has infected his device decides to open banking application, a fake login window will be displayed on top of the original application. If the user does not realise that this is not the real banking application and enters their credentials, it will be sent to a server controlled by the malware. If the user has a SMS-based two-factor authentication mechanism, the received SMS codes can be read and also sent to the attackers.

Figure 6 - Examples of fake overlays using bank logos

The HookBot Trojan poses a serious threat to data security and user privacy. To protect yourself from infection, the CSIRT KNF advises you to:

- download applications from the official Google Play store,
- check the permissions required by the application before installing it (this information is available in the Google Play store),
- check which applications have been granted accessibility services and disable those that are not necessary,
- update the software on your device regularly.

Below is a report on the technical analysis of the malware's operation. The content includes information on the details of how each component works, as well as full list of forms used to impersonate legitimate applications. We encourage you to read it!

Click here to download the full report:

HOOKBOT_CSIRT_KNF_ENG.pdf

- Hookbot
- Malware
- Android
- Hook
- mobilemalware
- malicioussoftware