EINPRESSWIRE

ESET Research discovers trojanized WhatsApp and Telegram applications stealing crypto funds and with new functionalities

DUBAI, DUBAI, UNITED ARAB EMIRATES, March 23, 2023 /EINPresswire.com/ -- SET researchers have discovered dozens of copycat Telegram and WhatsApp websites targeting mainly Android and Windows users with trojanized versions of these instant messaging apps. Most of the malicious apps we identified are clippers — a type of malware that steals or modifies the contents of the clipboard. All of them are after victims' cryptocurrency funds, with several targeting cryptocurrency wallets. This was the first time ESET Research had seen Android clippers focusing specifically on instant messaging. Moreover, some of these apps use optical character recognition (OCR) to recognize text from screenshots stored on the compromised devices, which is another first for Android malware.

Based on the language used in the copycat applications, it seems that the operators behind them mainly target Chinese-speaking users. Because both Telegram and WhatsApp have been blocked in China for several years now, with Telegram being blocked since 2015 and WhatsApp since 2017, people who wish to use these services have to resort to indirect means of obtaining them.

The threat actors first set up Google Ads leading to fraudulent YouTube channels, which then redirected the viewers to copycat Telegram and WhatsApp websites. ESET Research immediately reported the fraudulent ads and related YouTube channels to Google, which promptly shuttered them all.

"The main purpose of the clippers we discovered is to intercept the victim's messaging communications and replace any sent and received cryptocurrency wallet addresses with addresses belonging to the attackers. In addition to the trojanized WhatsApp and Telegram

Android apps, we also found trojanized Windows versions of the same apps," says ESET researcher Lukáš Štefanko, who discovered the trojanized apps.

Despite serving the same general purpose, the trojanized versions of these apps contain various additional functionalities. The analyzed Android clippers constitute the first instance of Android malware using OCR to read text from screenshots and photos stored on the victim's device. OCR is deployed in order to find and steal a seed phrase, which is a mnemonic code composed of a series of words used for recovering cryptocurrency wallets. Once the malicious actors get hold of a seed phrase, they are free to steal all the cryptocurrency directly from the associated wallet.

In another instance, the malware simply switches the victim's cryptocurrency wallet address for the attacker's address in chat communication, with the addresses being either hardcoded or dynamically retrieved from the attacker's server. In yet another instance, the malware monitors Telegram communication for certain keywords related to cryptocurrencies. Once such a keyword is recognized, the malware sends the full message to the attacker's server.

ESET Research also found Windows versions of the wallet-switching clippers, as well as Telegram and WhatsApp installers for Windows bundled with remote access trojans (RATs). In a departure from the established pattern, one of the Windows-related malware bundles is not composed of clippers, but of RATs that enable full control of the victim's system. This way, the RATs are able to steal cryptocurrency wallets without intercepting the application flow.

"Install apps only from trustworthy and reliable sources, such as the Google Play store, and do not store unencrypted pictures or screenshots containing sensitive information on your device. If you believe you have a trojanized version of Telegram or WhatsApp, manually remove it from your device and download the app either from Google Play or directly from the legitimate website," advises Štefanko. "For Windows, if you suspect that your Telegram app is malicious, use a security solution to detect the threat and remove it for you. The only official version of WhatsApp for Windows is currently available in the Microsoft store."

For more technical information about the clippers built into instant messaging apps, check out the blog post "Not-so-private messaging: Trojanized WhatsApp and Telegram apps go after cryptocurrency wallets" on WeLiveSecurity. Make sure to follow ESET Research on Twitter for the latest news from ESET Research.

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

Sanjeev Kant
Vistar Communications
0559724623
email us here