kaspersky

The rise of Cerberus: Android banking malware is available for free in underground forums

The full Cerberus source code has been leaked on underground forums and is now available to cybercriminals for free. Kaspersky experts have actively tracked the Android banking malware's revival since July 2020, following the original developer's abandonment, attempted sale, and eventual release of the project. Through evolving functionality including two-factor (2FA) authentication stealing and remote access tool (RAT) features, the level of Cerberus infections has already increased, especially in Russia and Europe.

Cerberus is a sophisticated Android banking malware, originally tracked in the summer of 2019, and actively distributed on a MaaS (Malware-as-a-Service) basis across various underground forums. The recent source code leak – referred to as Cerberus v2 – opens up new, public opportunities for cybercriminals looking to threaten the banking sector through Android devices.

Despite Cerberus' Russian speaking developers earmarking a new vision for the project in April this year, auctions for the source code began in late July due to the breakup of the development team. Due to an unclear culmination of factors, the author later decided to publish the project source code for premium users on a popular Russian-speaking underground forum.

The result has been an immediate rise in mobile application infections and attempts to steal money from consumers in Russia and across Europe, as more and more cybercriminals acquire the malware for free.

Since first tracking its activity in July, the sophistication of Cerberus has been elevated to new levels of functionality, in much the same way as Anubis – another Android banking malware example which went public in late 2019 to the detriment of customers and banks themselves.

Kaspersky is in the process of investigating 'v2' further, having obtained the published archive which included the revealed source code. In-depth analysis of the infrastructure has already unearthed the malware's ability to covertly send and steal SMS codes, to open tailored overlays for various online banks, and to steal 2FA-codes including from Google Authenticator. Additional capabilities include accessing customer credit card and contact details, the ability to redirect calls or tamper with mobile

functionality via its RAT features, and to automatically grant required permissions as part of its authentication attributes.

This barely scratches the surface, however, and it's vital that consumers take precautionary actions to offset the threat.

"Cerberus is dead… long live Cerberus. Kaspersky's findings regarding Cerberus v2 are an early warning to everyone implicated by Android security and Android banking security in particular. We're already seeing an increase in attacks on users since the source code was published. It's not the first time we've seen something like this happen, but this boom of activity since the developers abandoned the project is the biggest developing story we've tracked for a while.

"We continue to investigate all found artefacts associated with the code, and will publish further in-depth analysis very soon. But, in the meantime, the best form of defence that users can adopt involves aspects of security hygiene that they should be practicing already across their mobile devices and banking security," comments Dmitry Galov, Security Researcher at Kaspersky.

Kaspersky's security advice for mobile banking users

• Only download and install applications from official app stores such as Google Play on Android devices, or in the App Store on iOS.

• Deactivate the function for installing programs from unknown sources in the settings of the smartphone.

• Never "root" devices as this gives cybercriminals unlimited possibilities to carry out attacks.

• Install system and application updates promptly to fix security gaps. Updates to the mobile operating system should never be downloaded from external resources.

• When it comes to financial or personal details, always adopt a default strategy of attentiveness and scepticism, so as to remain vigilant.

• Use a reliable security solution such as Kaspersky Security Cloud to protect against a wide range of threats.

To learn more about Cerberus, please visit our Securelist web page.

kaspersky

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 250,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.