ERMAC 2.0: Perfecting the Art of Account Takeover

By Intel 471

Published: 2026-04-01 · Archived: 2026-04-05 14:03:02 UTC

Android device security has improved dramatically in recent years, motivated by market and competitive forces. In part, Android security development teams have accomplished this by focusing on the tools used by malware developers and mitigating their effectiveness. Malware developers, in response, have had to get creative to achieve their nefarious tasks.

One example is ERMAC, an Android banking trojan that surfaced in August 2021. Based on the Cerberus banking trojan, ERMAC abuses a built-in feature in the Android Accessibility Suite intended for users with disabilities. The feature enables actors to accomplish tasks on Android devices that they otherwise could not do. Specifically, ERMAC uses the Accessibility Suite to determine when certain apps are launched and then overwrites the screen display to steal the user’s credentials. Users are usually infected with ERMAC through fake browser update sites.

Overlay Attacks

Commonly known as an "Overlay" or "Web Injection" attack, ERMAC targets over 400 banking, financial and ecommerce mobile applications – including Amazon, PayPal, and Microsoft - to hijack credentials. Injections are amongst the oldest and most dangerous attacks aimed at applications. In this case, HTML code is injected, resulting in overwritten apps that fool users.

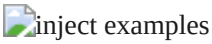

Figure 1: Examples of the phishing pages that ERMAC overlays on top of legitimate applications.

Users of those apps think they have opened a legitimate app but are presented with illegitimate content from the malware. When users enter their credentials, the ERMAC trojan captures them. From the end-user perspective, it is hard to discern whether anything is different or wrong.

Users must explicitly grant ERMAC access to the Accessibility Suite to perform the overlay attack. ERMAC typically attempts this by asking users to grant access via a pop-up. If access is granted, users unknowingly give this set of privileges to the malware.

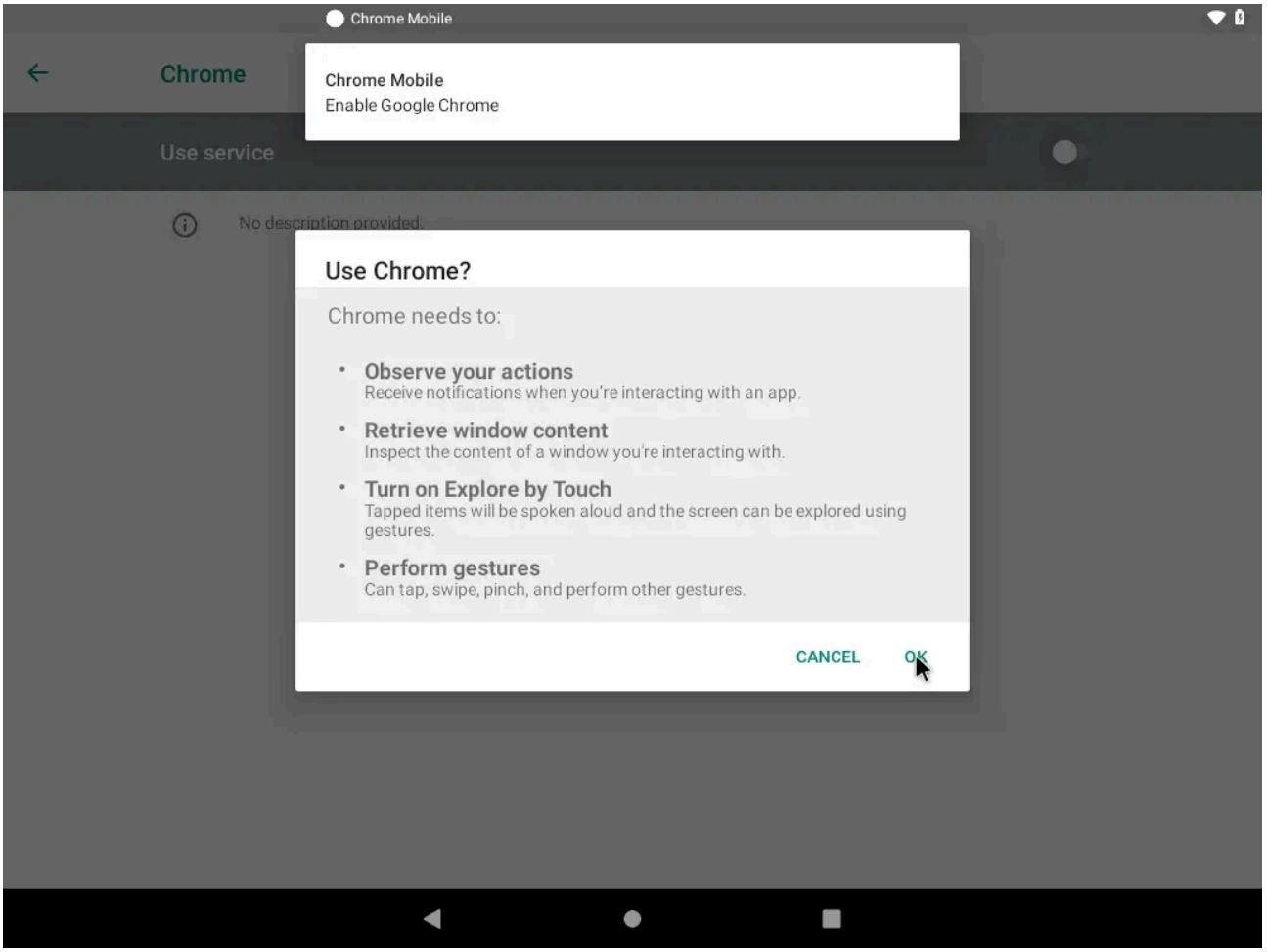

Figure 2: ERMAC generates a window, prompting the user to grant Accessibility privileges.

Once active, the malware performs actions such as knowing which apps are being launched and redrawing the screen while another app is in focus. Further, it gathers and forwards a list of all installed apps to the command-and-control server. In response, the server sends back injection content for other applications.

Subverting Multi-factor Authentication

According to Duo Labs (Cisco/Duo Security) State of the Auth report, multi-factor authentication (MFA) has gained significant adoption, with 79% of respondents using it in 2021. And most end users do feel they have strong protection against credential theft and account takeover when using MFA for their online and mobile transactions. After all, if your credentials are stolen but MFA is enabled, your data and apps are still safe, right?

Wrong! What makes ERMAC so formidable is its ability to get around authentication methods, thus circumventing MFA. An ERMAC feature known as Google Authentication Grabber essentially turns ERMAC into an account takeover tool as it steals Google Authentication tokens. ERMAC can also steal authentication tokens sent via SMS. So, even if you are doing all the right things – strong passwords and MFA – you are still subject to account takeover.

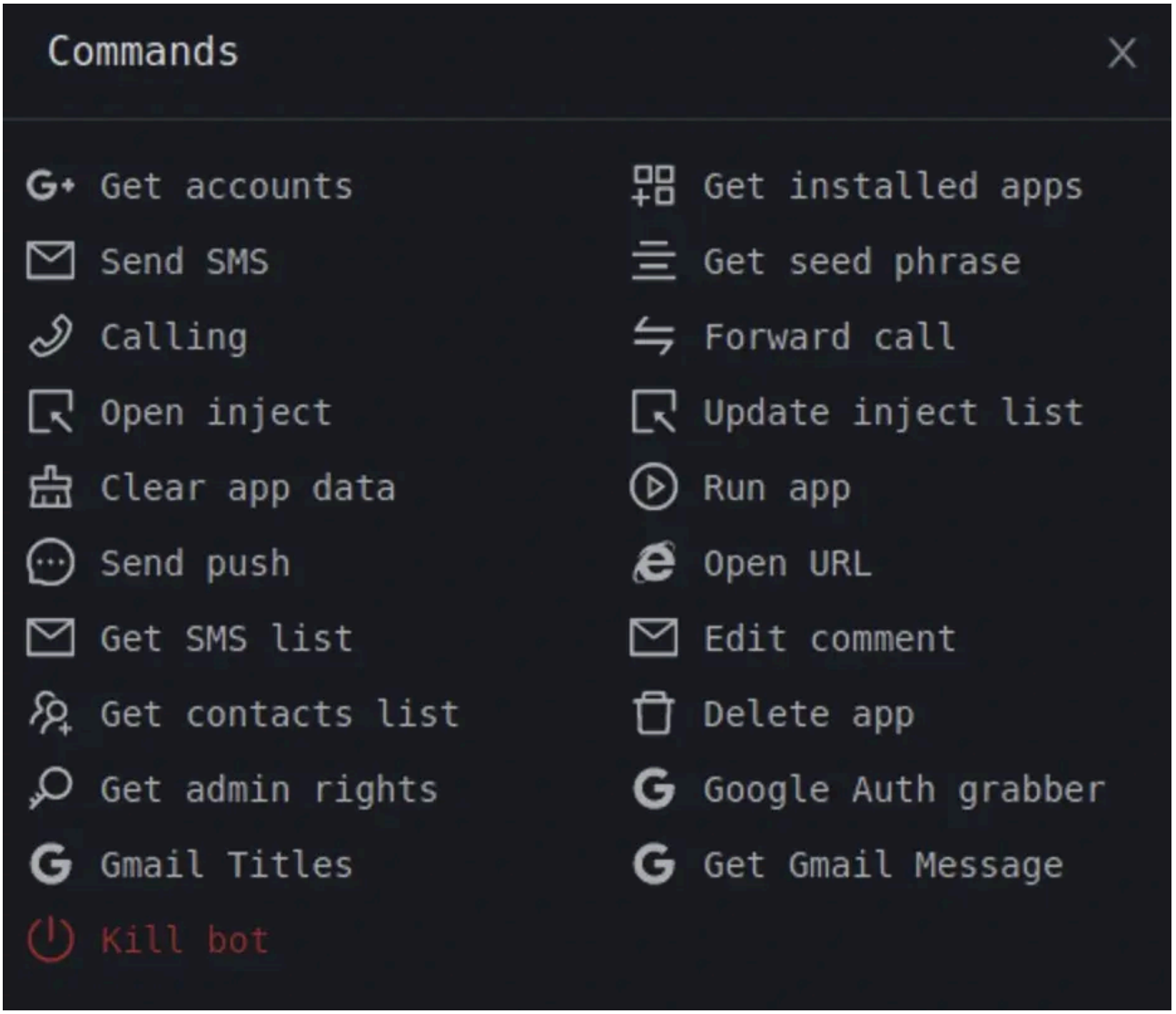

Figure 3: Screenshot of ERMAC control panel, showing commands available to the operator.

The Bigger Picture

It is easy to become complacent and categorize any malware as a one-off. But a detailed analysis reveals that a highly sophisticated e-crime ecosystem supports ERMAC, its developers and users.

As reported by researchers, the mastermind group promoting the ERMAC malware is **DukeEugene,** aka **Duke Eugene** or **Eugene**. They rent the malware, as a service (MaaS), on underground forums for $5,000 per month, facilitate client communications and provide access to the malware control panel. DukeEugene has history and expertise in this area, claiming to be the 2020 author of the BlackRock Android banking trojan. That trojan also used the MaaS model.

The online forums serving as a marketplace for selling ERMAC and other MaaS offerings are hosted by "bulletproof posting (BPH) services," which provide infrastructure and hosting services to criminal actors. These BPHs offer the basic building blocks for illicit command and control servers and services. BPH providers advertise specific services but often provide support beyond what they tout on the underground forums.

One of the world's "top tier" bulletproof hosting providers, actor **Yalishanda** is associated with ERMAC. Intel 471's research revealed that some bot configurations, designed for ERMAC to connect to command and control servers, lead to Yalishanda's bulletproof hosting infrastructure. Yalishanda has been active for years, reportedly moving between China and Russia. His methods and longevity underscore that this high level of e-crime sophistication is not going away.

ERMAC will likely continue to undergo feature enhancements just like any other app. But it is essential to realize this is not just another clever, creative piece of malware; it is malware supported by a sophisticated criminal group with expertise, longevity and infrastructure. Android users who rely on banking, financial and ecommerce apps must thus remain vigilant and aware of this persistent threat.
