PRODAFT

Threat Intelligence Insights

ERMAC 2.0

The Android Banking Trojan That Steals Financial Data

Last week, the PRODAFT Threat Intelligence (PTI) team observed *increasing activity* of an Android *banking Trojan* called ERMVK or ERMAC 2.0. The banking Trojan ERMVK steals mobile and app users' banking and crypto credentials. We have identified that the Trojan has *affected over 1500 victims* up until now.

A banking Trojan is a malicious software disguised as a legitimate one. They are created to steal sensitive information from users, such as financial information, credit card information, and login credentials.

Attack Highlights

Threat Type:
Banking Trojan

Motivation:
Financial

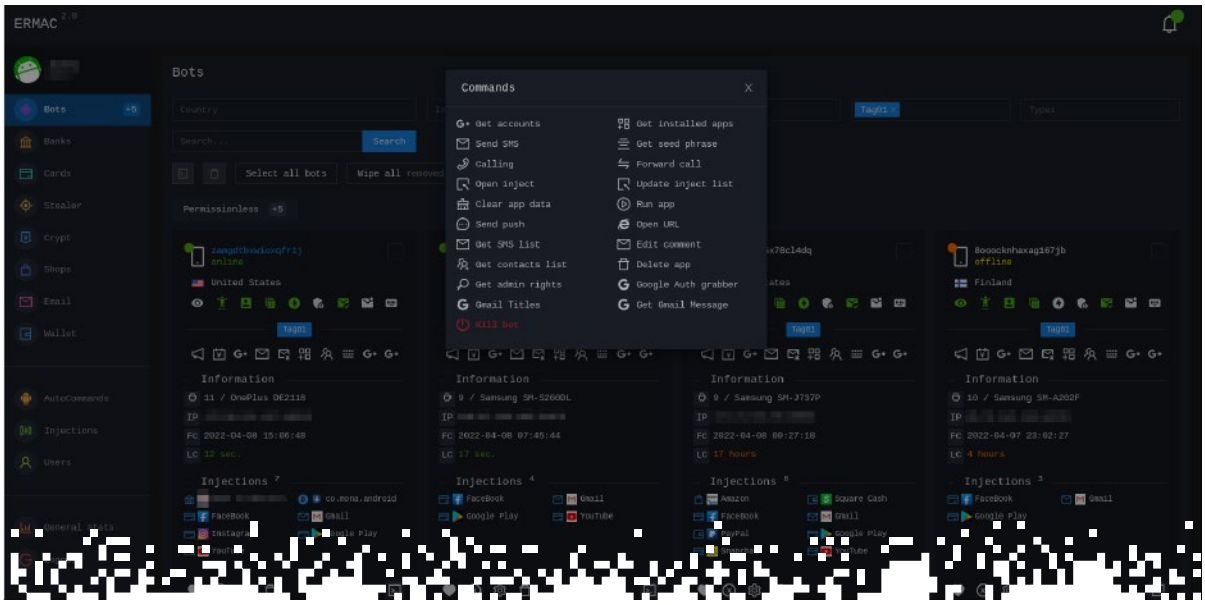
Most Targeted Countries:
US, ES, PT, IT

Total Victims:

1500+

The Strategy

A JSON file containing all the targeted apps is injected into the panel. Once the list is injected, the attacker distributes the Trojan via a fake Chrome update pop-up. As soon as users react and download the malware, they get affected. The attack becomes successful, and the malware can access critical information.



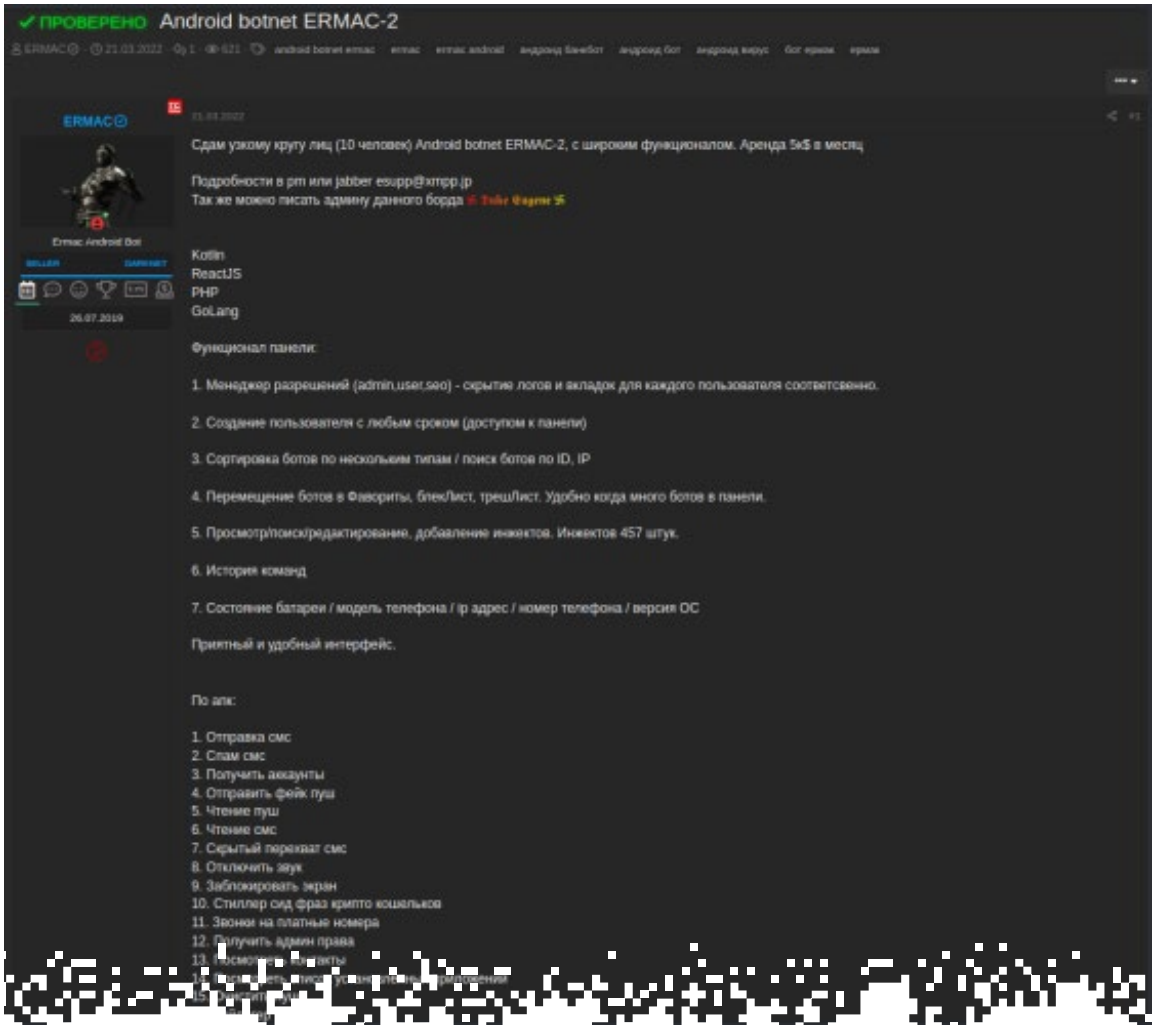
Management Interface of the ERMAC 2.0

The banking Trojan was advertised on two underground forums using the Russian language. When it was first released in 2020, the cost of the malware was **$3'000 per month.**

Recently, additional features have been added to the Trojan, setting the price of the malware at **$5'000 per month.**

The Attacker

The threat actor who sells the malware goes under the alias ERMVK and is first seen in 2020. The PTI team uncovered the server location and provider of the threat actor, both of which are located in Russia.



2nd Advertisment Topic (21 March 2022)

The Findings

The Android banking Trojan has affected more than 1500 victims so far, and the motivation behind the attacks is financial gain. The devices that the ERMVK infected include:

The most targeted countries are the USA, Portugal, Italy, and Spain. Other target countries include France, Great Britain, Romania, Finland, and Turkey.

When the PTI team investigated the ERMVK, it found that this Trojan was based on the code of the well-known malware Cerberus. Cerberus is an Android banking malware that appeared in 2019 and is actively distributed as malware-as-a-service across several underground forums.

How to Prevent Trojans

Banking Trojans can compromise your systems and reputation, so it is essential to take a proactive approach and educate your employees about cyber security threats and countermeasures.

Our threat intelligence platform responds directly and effectively to complex cyber threats. PRODAFT's cyber security experts will monitor the activity on your network and identify any suspicious activity and security incidents.