**Security Incident Research (Mobile)**

The Brazilian criminal underground is well known for creating cyber-attacks on their local bank customers. However, in November 2020, the ​*Ghimob* ​banking trojan marked a more widespread and sophisticated attack that hit not only Brazil, but Paraguay, Peru, Portugal, Germany, Angola, and Mozambique.

This trojan infected mobile devices, specifically targeting financial apps from banks, fintechs, exchanges, and cryptocurrencies.

So, what is the​*Ghimob* t​rojan?

Kaspersky Lab, a leader in security software and the ones who discovered ​*Ghimob,* defines the trojan as “a full-fledged ‘spy’ in your pocket: once the device is infected, the threat actor can access the infected device remotely, completing fraudulent transactions with the victim’s smartphone.

1. **The link below, from Kaspersky Lab’s official blog, SecureList, discusses the *Ghimob​* trojan in detail.**

**SecureList Article: Ghimob https://securelist.com/ghimob-tetrade-threat-mobile-devices/99228/**

1. **Answer the following questions regarding the behaviour of the trojan:**

How does Ghimob bypass the security measures implemented by financial institutions?

* By making it possible for hackers to access remotely compromised machines. The victim's phone is then used to perform the fraudulent transaction, bypassing the security protocols put in place by banking institutions.

Why does the trojan abuse Accessibility Mode?

* To disable uninstallation and the ability to save information such as lock screen patterns to replay later to unlock a device while changing screen content to increase persistence.

How are victims lured into installing the malicious file?

* Using phishing emails that appear to be from creditors and include links that allow the receiver to view more details and download malware.

What happens once the infection is completed?

* The malware then sends infection notification messages to its notification servers, including information about phone models, information about the lock screen if it is enabled, and information about installed versions of the targeted apps.

1. **​What can be done to mitigate the risk of infection?**

* Avoiding suspicious links from sketchy emails and only downloading programs from approved marketplaces. Before doing something unfamiliar, give it some thought.