Spain arrests 16 for working with the Mekotio and Grandoreiro malware gangs

therecord.media/spain-arrests-16-for-distributing-the-mekotio-and-grandoreiro-banking-trojans/

July 14, 2021

Image: Guardia Civil

- The group laundered funds stolen using banking trojans made by Brazilian gangs.
- Officials said the arrests took place before the group was able to steal more than €3.5 million from hacked bank accounts.
- This is the second time authorities dismantle a group working with banking trojan operators in Spain this year.

Spanish police arrested 16 suspects last week on charges of laundering funds stolen through banking trojans such as Mekotio and Grandoreiro.

According to the Guardia Civil, the oldest law enforcement agency in Spain and one of two national police forces, 16 suspects have been arrested in Ribeira (a city in the A Coruña province), Seseña (Toledo), Villafranca de Los Barros (Badajoz), Aranda de Duero (Burgos), Parla (Madrid), Móstoles (Madrid), and the capital Madrid.

The group was arrested last week, and suspects had their houses searched and devices seized for investigation during raids part of an operation that authorities named Aguas Vivas (Living Waters).

> Desarticulada una red dedicada a cometer estafas a través de Internet.
>
> Se ha detenido a 16 personas y se han conseguido bloquear tentativas de transferencias por un importe de 3.500.000 euros, tras analizar más de 1.800 correos electrónicos.
>
> Más info: https://t.co/0ggQlE0UxB pic.twitter.com/EOAVRuyrKq
>
> — Guardia Civil 🇪🇸 (@guardiacivil) July 10, 2021

Following the raids, authorities said they found evidence that the suspects received more than €276,470 from bank accounts compromised with the help of the two banking trojans. In addition, the Guardia Civil said the suspects also had access to bank accounts storing around €3.5 million, which they had not yet moved and stolen from their respective owners.

A well-structured operation

Both the Mekotio and Grandoreiro malware strains are believed to be the work of Brazilian cybercrime groups who rent access to their tools to other gangs responsible for distributing the trojan and laundering funds.

Both trojans are developed to target Windows computers and are usually spread using spoofed emails mimicking legitimate organizations. Once they infect a victim, they stay hidden and wait until users log into e-banking accounts, silently collecting their credentials.

Officials said the two trojans used in the attacks were capable of collecting data for up to 30 different banks. Once the attackers had access to victim bank accounts, they accessed e-banking portals and sent the funds to accounts under their control.

“One characteristic in which all the victims agreed is that, once they carried out any banking operation through the web, their computers restarted several times until access was blocked, later observing that large amounts of their money had been transferred to unknown accounts,” Guardia Civil officials said in a press release last week.

“After that, the money was split by sending it to other accounts, or by withdrawing cash at ATMs, transfers by BIZUM, REVOLUT cards, etc., in order to hinder possible police investigations,” the agency added. Officials did not say if the 16 suspects distributed the malware, but said that they were heavily involved in helping launder the stolen funds.

> The organization was perfectly structured and hierarchical, in 4 levels. On the one hand, there were those who were dedicated to receiving the amounts of fraudulent transfers (Level 1), which they later transferred to other members of the organization (Level 2). On the other hand, there were those who transferred the money to other accounts located abroad (Level 3) and, finally, those who were dedicated to masking the online operations of the accounts (Level 4).
>
> *Guardia Civil*

Expansion of Brazil's banking trojan ecosystem

The arrest of the 16 suspects in Spain confirm reports from security firms like ESET and Kaspersky, both of whom warned last year that Brazilian cybercrime groups had been updating their banking trojans with support for European banks, on top of their classic Brazilian and Latin American targets.

ESET, which has been tracking the evolution of both Mekotio and Grandoreiro throughout 2020, specifically highlighted how the two banking trojans grew in sophistication and reach last year.

While Mekotio is a relatively new operation, the Grandoreiro trojan has been around since 2016 and is a well-known name in the cybersecurity industry.

In a July 2020 blog post, Kaspersky put both Mekotio (also known as Melcoz) and Grandoreiro in the Tetrade, a codename the company was using to describe the four largest banking trojan families created, developed, and spread by Brazilian crooks on a global level. The other two part of the Tetrade cartel were Guildma (Astaroth) and Javali.

"Grandoreiro and Mekotio have been expanding to Europe (especially Spain) since around the beginning of 2020, which attracted substantially more attention to these banking trojans than before, whether it was from researchers, companies or police forces," an ESET spokesperson told *The Record* earlier today.

"The arrest demonstrates that the operation these threat actors are running is not a small one. Additionally, it gives an estimate of how successful their European campaign was by revealing how much money was stolen through Mekotio and Grandoreiro," the security firm added.

Stats released by Kaspersky today confirm both of Mekotio and Grandoreiro's expansion to Europe, with Spain being the hardest hit after their native Brazil.

The Mekotio and Grandoreiro-related arrests in Spain are also the second time Spanish authorities arrested local cybercriminals working with banking trojan malware in 2021. The first arrests took place in March when they apprehended four suspects for distributing the FluBot Android banking trojan.

Article updated shortly after publication to clarify that the group was arrested mainly for money laundering activities and not malware distribution. Article also updated with ESET comments.

Tags

- arrests
- banking trojan
- Brazil
- cybercrime
- Grandoreiro
- Law enforcement
- malware
- Mekotio
- Spain

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.