# Police disrupt Grandoreiro banking malware operation, make arrests

bleepingcomputer.com/news/security/police-disrupt-grandoreiro-banking-malware-operation-make-arrests/

Bill Toulas

By
Bill Toulas

- January 30, 2024
- 10:46 AM
- 0

The Federal Police of Brazil and cybersecurity researchers have disrupted the Grandoreiro banking malware operation, which has been targeting Spanish-speaking countries with financial fraud since 2017.

The operation was supported by ESET, Interpol, the National Police in Spain, and Caixa Bank, all providing critical data leading to identifying and arresting individuals controlling the malware's infrastructure.

Brazil's federal police announced five arrests and thirteen search and seizure actions in Sao Paulo, Santa Catarina, Para, Goias, and Mato Grosso.

"This Tuesday, January 30, the Federal Police launched Operation Grandoreiro to investigate the activities of a criminal group responsible for electronic banking fraud, using banking malware with victims outside Brazil," the Brazilian police said in a machine-translated press release.

"The criminal structure is suspected of moving at least 3.6 million euros through fraud since 2019."

According to Caixa Bank's records, the malware operators are linked to fraud that has caused roughly $120,000,000 in losses.

## The Grandoreiro malware

Grandoreiro is a Windows banking trojan first documented by ESET in 2020, which has been one of the primary threats to Spanish speakers since the beginning of its operation in 2017.

The malware actively monitors the foreground window, looking for web browser processes related to banking activities, and if there's a match, it initiates communication with its command and control (C2) servers.

Attackers must manually interact with the malware to conduct financial theft, like loading the right web injections, indicating a targeted and hands-on approach.

The malware can serve victims fake pop-up windows that phish for credentials, simulate mouse and keyboard input to help in remote navigation, send live feed of the victim's screen, block local viewing to hinder detection and intervention, and log keystrokes.

Grandoreiro developers released frequent updates to add new features and enhance the malware's capabilities, which indicates its operators' continued use of the project.

In August 2022, a Zscaler report presented a Grandoreiro campaign targeting high-value company employees in Spain and Mexico.

## Tracking ops and victims

ESET could trace Grandoreiro's servers despite the malware's use of a Domain Generation Algorithm (DGA) through a combination of tracking and analysis techniques.

The researchers analyzed the DGA mechanism, which generates a new domain every day, and found that it uses the current date and hardcoded configuration, allowing them to predict future domains.

"ESET has extracted a total of 105 different dga_ids from the Grandoreiro samples known to us," explains ESET.

"79 of these configurations at least once generated a domain that resolved to an active C&C server IP address during the course of our tracking."

The cybersecurity firm observed patterns where domains generated by different DGA configurations resolved to the same IP addresses, indicating multiple victims connected to the same C2 server.

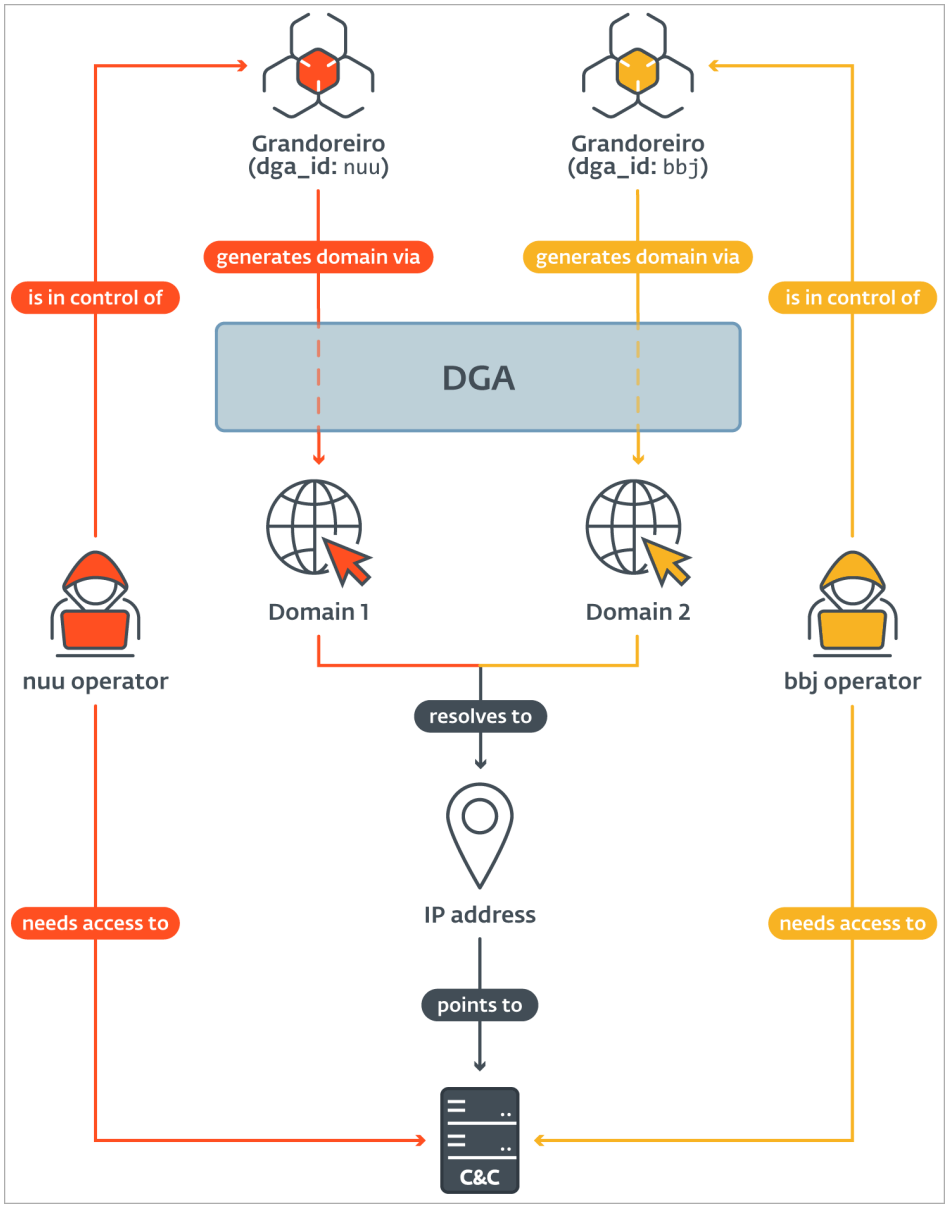
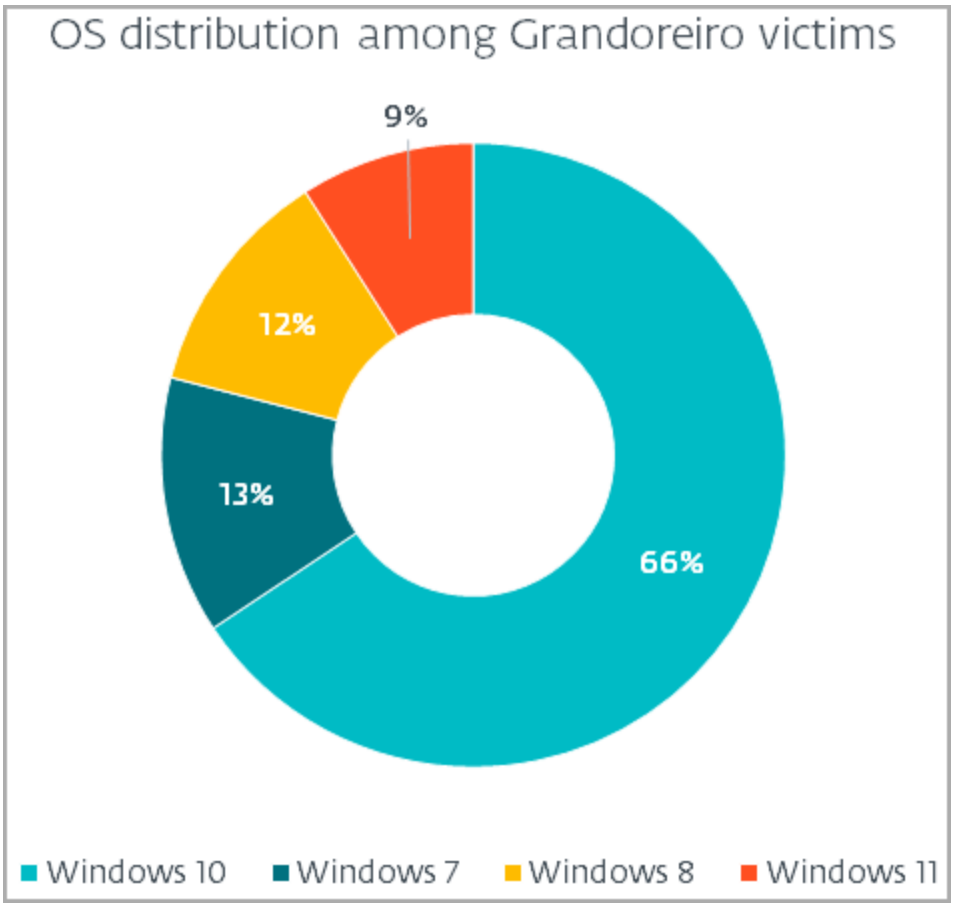



**Diagram showing the overlap**

*Source: ESET*

Using this lead, Grandoreiro's infrastructure was clustered, and ESET could gain insights into the operation's victimology and volume.

Most of the victims are in Spain, Mexico, and Brazil, while the most impacted operating system is Windows 10, followed by 7, 8, and 11.




**Grandoreiro victims by Windows version**

*Source: ESET*

ESET reports seeing 551 unique connections to Grandoreiro's infrastructure daily, with 114 being "new daily victims."

If we extrapolate this to the duration of a year, Grandoreiro potentially infected over 41,000 new computers.

At this time, it is unclear if the arrested individuals held a leading role in the operation or if there's a risk of Grandoreiro returning in the future using new infrastructure.

Still, the latest disruption has brought the malware operations to a complete halt for now.

## Related Articles:

Hacker arrested for selling bank accounts of US, Canadian users

FBI seizes Warzone RAT infrastructure, arrests malware vendor

Hackers abuse Google Cloud Run in massive banking trojan campaign

Anatsa Android malware downloaded 150,000 times via Google Play

New ‘Gold Pickaxe’ Android, iOS malware steals your face for fraud