

Grandoreiro Strikes Again: Geofenced Phishing Attacks Target LATAM

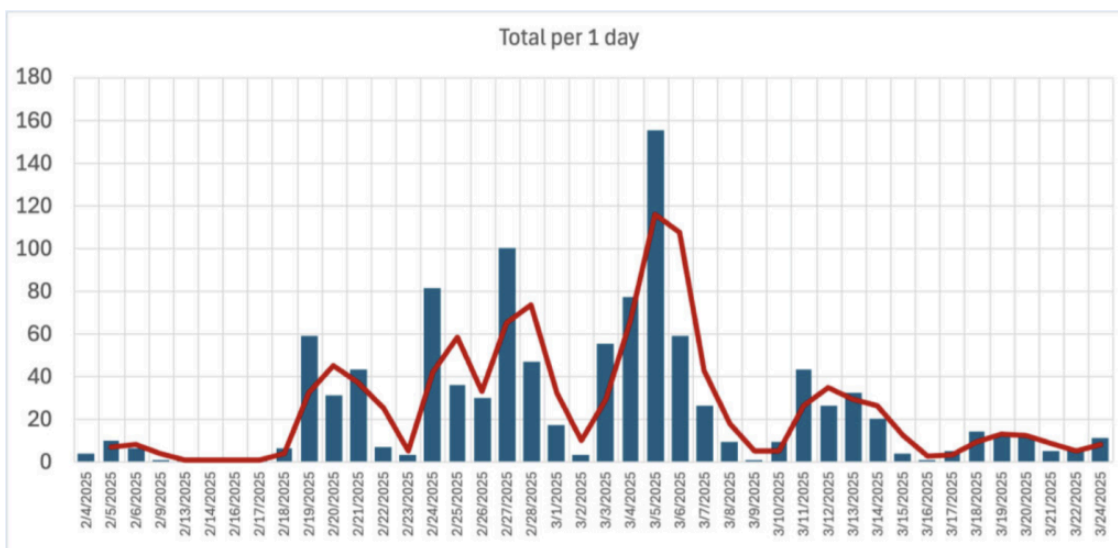
Published: 2025-04-09 · Archived: 2026-04-05 16:21:48 UTC

A new phishing campaign is targeting users across [Latin America](#), and at the center of it is Grandoreiro, a banking trojan known for stealing sensitive financial data. With geofencing and stealthy evasion tactics, this malware is proving difficult to catch with standard defenses.

Let's take a closer look at the campaign, how the attack unfolds, and what makes it so effective.

Grandoreiro Attack Overview

Between February 19 and March 14, researchers noticed a surge in phishing activity tied to Grandoreiro, and signs show the campaign is still ongoing.



A spike of Grandoreiro was detected

Grandoreiro has been around for years, constantly evolving to stay ahead of detection. It's designed to steal banking credentials, monitor user activity, and grant remote access to attackers.

One of the standout techniques in this campaign is geofencing. Before running, the malware checks the victim's IP address to determine their location. If the user isn't in a targeted Latin American country, the malware simply stops executing. This makes the campaign more focused, reduces unnecessary exposure, and helps it slip past global security monitoring.

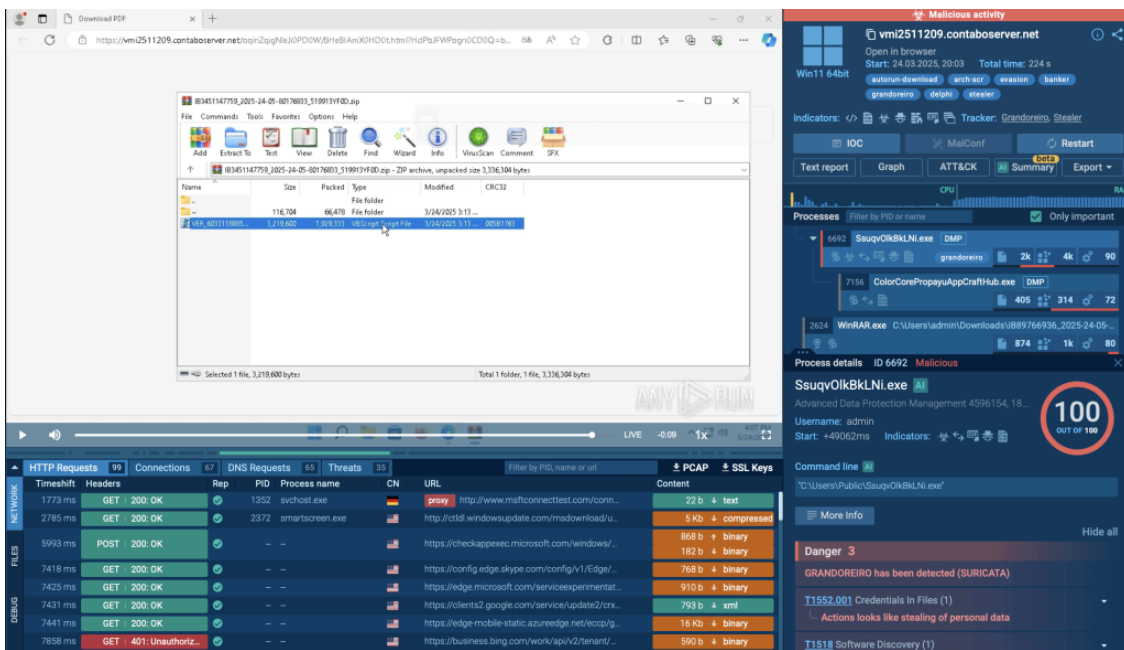
Grandoreiro Attack Chain

Grandoreiro is known for slipping past traditional security tools, making it tough to detect using automated solutions alone. However, with the help of interactive sandboxes, it's possible to observe the malware's full

behavior in real time.

Here’s a complete look at the execution chain inside a secure sandbox:

[View sandbox analysis session](#)

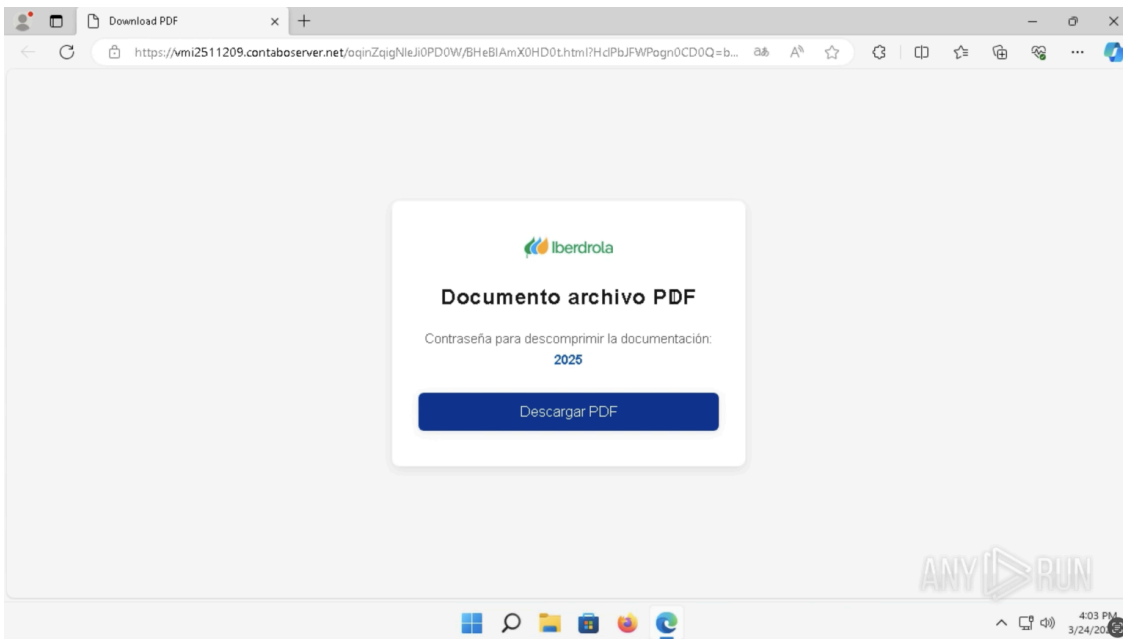


The full execution chain of Grandoreiro is displayed inside ANY.RUN sandbox

Understanding the who, when, and how behind this campaign will help security teams proactively strengthen their defenses. Real-time threat analysis platforms not only uncover these details but also make them immediately actionable.

Initial Access: Phishing Email

The infection begins with a phishing page that lures the victim into clicking a link or downloading a fake PDF document. Instead of a PDF, the file is actually a compressed archive (.ZIP or .RAR) containing the Grandoreiro loader.

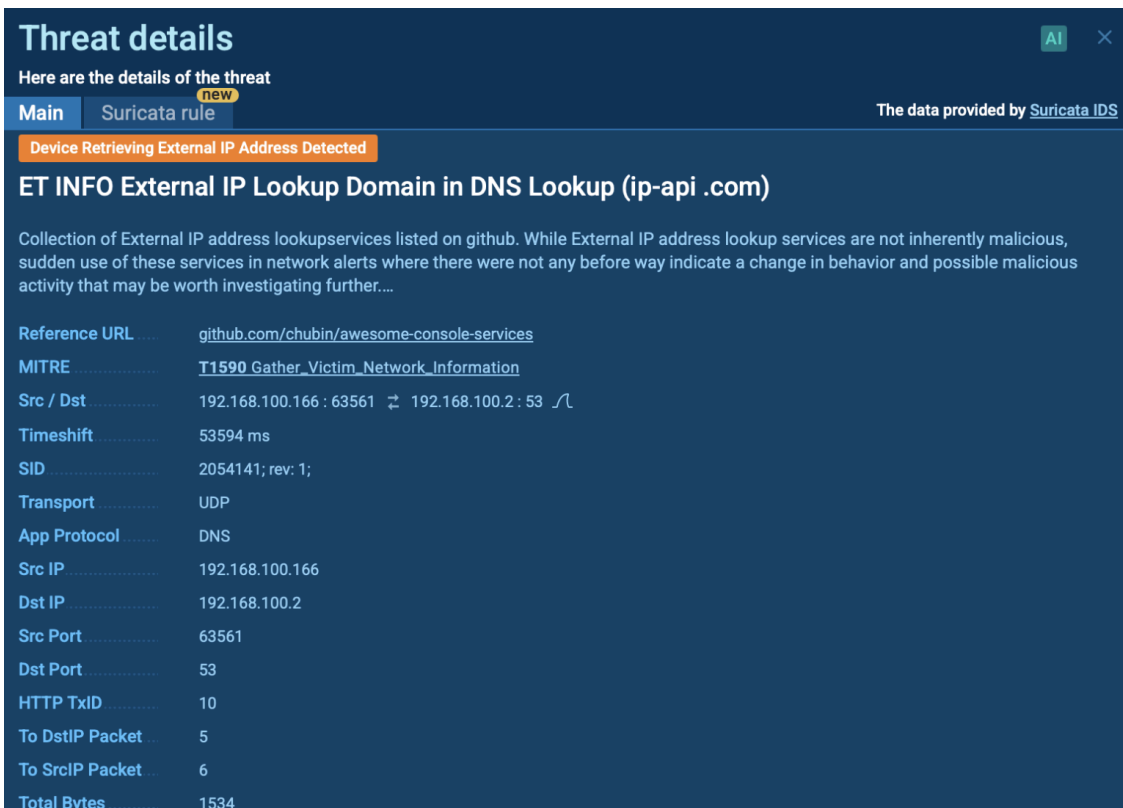


Phishing link with a fake PDF document displayed inside ANY.RUN sandbox

Execution & Geofencing

Once the file is extracted and opened, the malware sends a request to ip-apicom to determine the user's geolocation.

If the IP address falls outside the targeted LATAM countries, the malware halts execution, but if it matches a targeted region, the attack proceeds.



Suricata rule triggered inside ANY.RUN sandbox

DNS Evasion: Google DNS

Grandoreiro avoids local DNS queries by sending a request to `dns.google`. It provides the domain name of its command-and-control (C2) server, which Google resolves to an IP address.

This step helps it bypass DNS-based blocking mechanisms and improves its chances of successful communication.

Traditional solutions often miss these evasion tricks, but ANY.RUN captures them in real time, helping teams build effective detection logic that actually reflects how modern malware behaves.

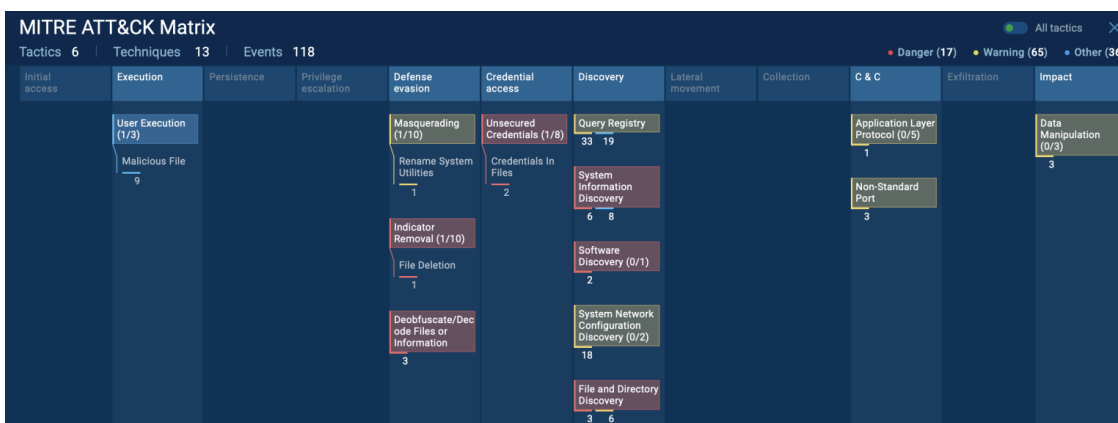
Connection to C2

After resolving the C2 domain, the malware sends a GET request to the retrieved IP address to establish a connection. This opens the door for the attacker to deliver additional payloads, steal credentials, or take remote control of the infected machine.

Grandoreiro in Action: Tactics & Techniques

Establishing a connection to the C2 server is just the beginning. Once communication is successful, Grandoreiro kicks off a series of actions designed to stay hidden, gather data, and prepare for further exploitation.

In this specific attack, ANY.RUN's sandbox reveals a wide range of techniques triggered across multiple MITRE ATT&CK categories. You can see all of them mapped in the ATT&CK tab of the analysis session:



MITRE ATT&CK tactics and techniques used by adversaries

Detection & Response Tips

Detecting Grandoreiro isn't easy; it blends in well and uses clever tricks. But here's how you can stay one step ahead:

- **Watch for phishing lures** posing as PDF downloads (often .ZIP or .RAR archives).
- **Monitor external DNS requests**, especially to `dns.google`, right after execution.
- **Flag geolocation lookups** to services like ip-apicom; it's a key part of Grandoreiro's filtering tactic.

- **Use behavior-based analysis** to catch post-execution tactics like file deletion, credential access, or system discovery.

Catch the Attack Before It Spreads

The Grandoreiro campaign shows how modern threats evolve and why visibility into behavior matters more than ever.

With ANY.RUN sandbox, security teams can interact with malware in real time, uncover hidden tactics, and respond with confidence. From phishing to post-exploitation, everything is mapped, visualized, and ready for action.

Source: <https://hackread.com/grandoreiro-strikes-geofenced-phishing-attacks-latam/>