Grandoreiro malware now targeting banks in Spain

By Dani Abramov, Limor Kessem

Published: 2020-04-13 · Archived: 2026-04-06 02:08:10 UTC

Author

Dani Abramov

Threat Researcher

IBM

Limor Kessem

X-Force Cyber Crisis Management Global Lead

IBM

During the past few months, IBM X-Force researchers have noticed a familiar malware threat that typically affects bank customers in Brazil has spread to attack banks in Spain. The rise in campaigns prompted us to look into it further.

Grandoreiro, a remote-overlay banking Trojan, has migrated to Spain without significant modification, proving that attackers who know the malware from its Brazilian origins are either collaborating with attackers in Spain or have themselves spread the attacks to the region. Remote-overlay Trojans are easy to find and purchase in underground and dark web markets.

A recent campaign delivered Grandoreiro using COVID-19-themed videos to trick users into running a concealed executable, infecting their devices with a remote-access tool (RAT) designed to empty their bank accounts.

The remote-overlay malware trend is highly prolific across Latin America. While it began trending in Brazil circa 2014, this simple malware attack continues to gain popularity among local cybercriminals and is considered the top financial malware threat in the region.

There is a large variety of remote-overlay malware codes active in the wild, each featuring similar code with a modified deployment process and infection mechanism.

Users become infected via malspam, phishing pages or malicious attachments. Once installed on a target device, the malware goes into action upon access to a hardcoded list of entities, mostly local banks.

Once the user enters the targeted website, the attacker is notified and can take over the device remotely. As the victim accesses their online banking account, the attacker can display full-screen overlay images (hence the name “remote overlay”) designed to appear like they are part of the bank’s website. These pages can either block the

victim's access to the site, allowing the attacker to move money after initial authentication, or include additional data fields that the user is prompted to fill out.

In the background, the attacker initiates a fraudulent money transfer from the compromised account and leverages the victim's presence in real time to obtain any required information to complete it.

The latest tech news, backed by expert insights

Stay up to date on the most important—and intriguing—industry trends on AI, automation, data and beyond with the Think Newsletter, delivered twice weekly. See the IBM Privacy Statement.

X-Force researchers who analyzed recent Grandoreiro attacks note the following observations:

- The malware is typically spread via malspam campaigns containing a URL that directs recipients to an infection zone.
- The first stage of infection is a loader component. Our team located a number of loaders used by Grandoreiro attackers masked as invoice files with a .msi extension and placed into an easily accessible GitHub repository.
- The second stage of the infection fetches the Grandoreiro payload via a hardcoded URL within the loader's code.
- Grandoreiro is executed and infects the device.

The Grandoreiro executable is initially a standalone dropper without additional modules. After its execution, it writes a run key based on the location where it was executed.

Figure 1: Grandoreiro run key

Some sample images from Grandoreiro attacks show that it informs victims they need to install a supposed security application.

Grandoreiro's bot communication with its command-and-control (C&C) server is encrypted and transmitted over SSL protocol. As an operational security feature on the attacker's side, the infected device's set date has to match with a recent campaign date in order to successfully connect to the C&C server. This is verified by an algorithm that would otherwise direct the communication to localhost as shown in the image below.

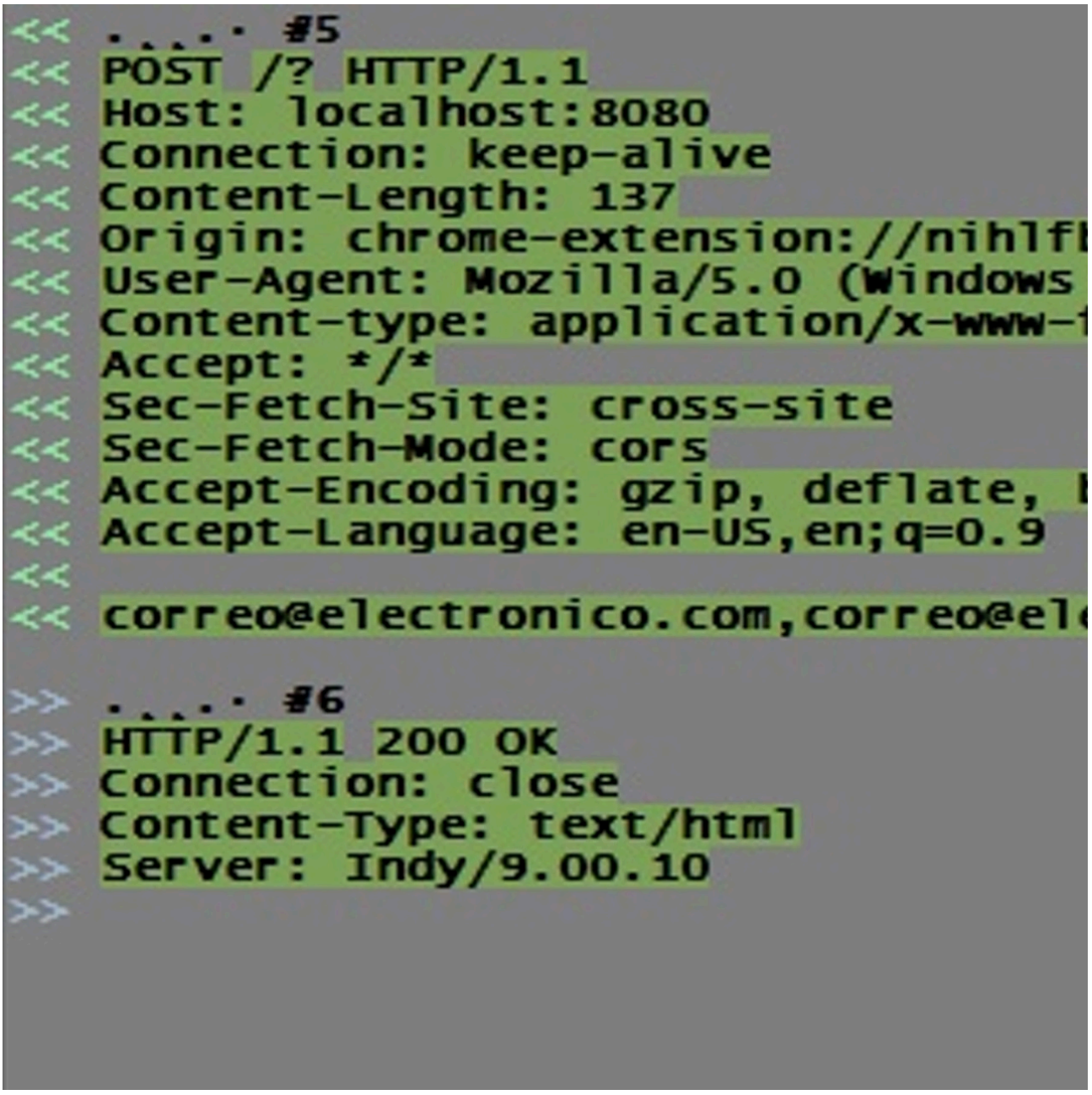

Figure 2: Grandoreiro bot communication pattern via HTTP POST request

Once there is a match with the communication algorithm, communication packages will be sent and receive info through *sites.google.com/view/*. This is only part of the URL, and it is hardcoded into the malicious code. To

complete the URL path, information on the infected device needs to match with the attacker's communication algorithm, which generates the second part of the path. For example:

hxxps://sites.google[.]com/view/brezasq12xwuy

Once the connection is established, the malware will likely use it to send notifications to the attacker when a victim accesses a banking site. Machine information, clipboard data and remote-access capabilities are also facilitated via the C&C.

After execution, the sample runs for about six minutes, at which point the machine will abruptly reboot. A few minutes after the boot, the malware writes a compressed archive file named *ext.zip* from which it will extract additional files, placing them into a directory under *C:/%user%/*extension folder*/*.

The extracted files are modified versions of an existing, legitimate Google Chrome browser extension called Edit This Cookie.

In the next step, the dropper writes a new chrome .lnk or Windows OS shortcut file extension file or replaces the original if one already exists.

The new Chrome browser shortcut contains a "—load-extension" parameter to load the new extension upon starting the browser.

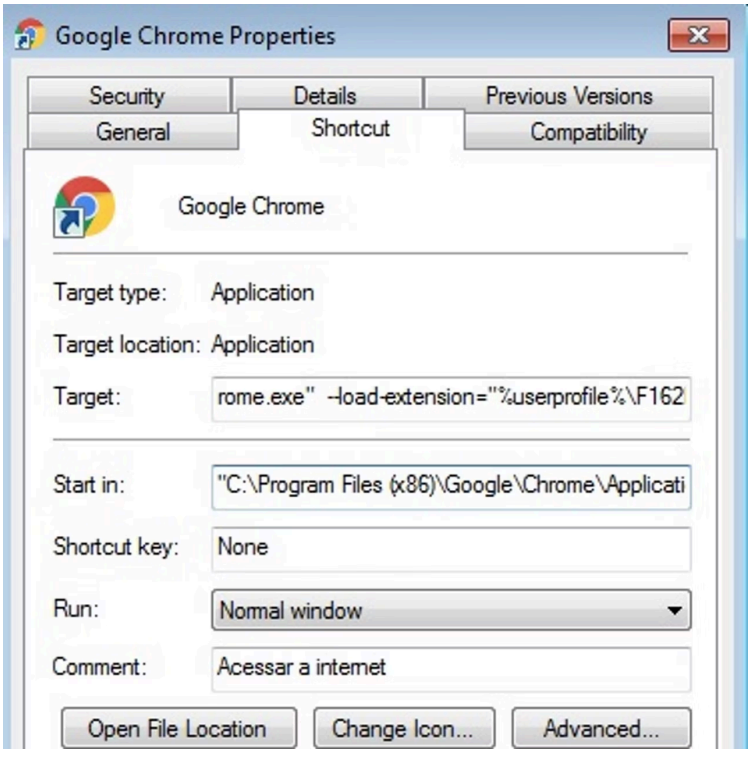

Figure 3: Fake browser extension created by Grandoreiro

Here is an example of a target path from our analysis:

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" –load-extension="%userprofile%\F162FD4091BD6D9759E60C3"

If Chrome was already open before the infection started unfolding, the malware will force closure of all *chrome.exe* threads to kill the process. This will also force the victim to re-open the browser using the newly written .lnk file, which is now loaded with Grandoreiro's malicious extension. This extension will load on every browser startup using this specific .lnk file.

Note that the browser itself is not hooked. Executing the browser from any other Chrome shortcut link will start and run it normally without the malicious extension, canceling out the malware's ability to control what the victim does.

Since this malicious extension is trying to pass for a legitimate Chrome plugin, Grandoreiro's developer named it "Google Plugin" version 1.5.0. Visually, it adds a square button to the browser window instead of the "cookie" button on the original plugin.

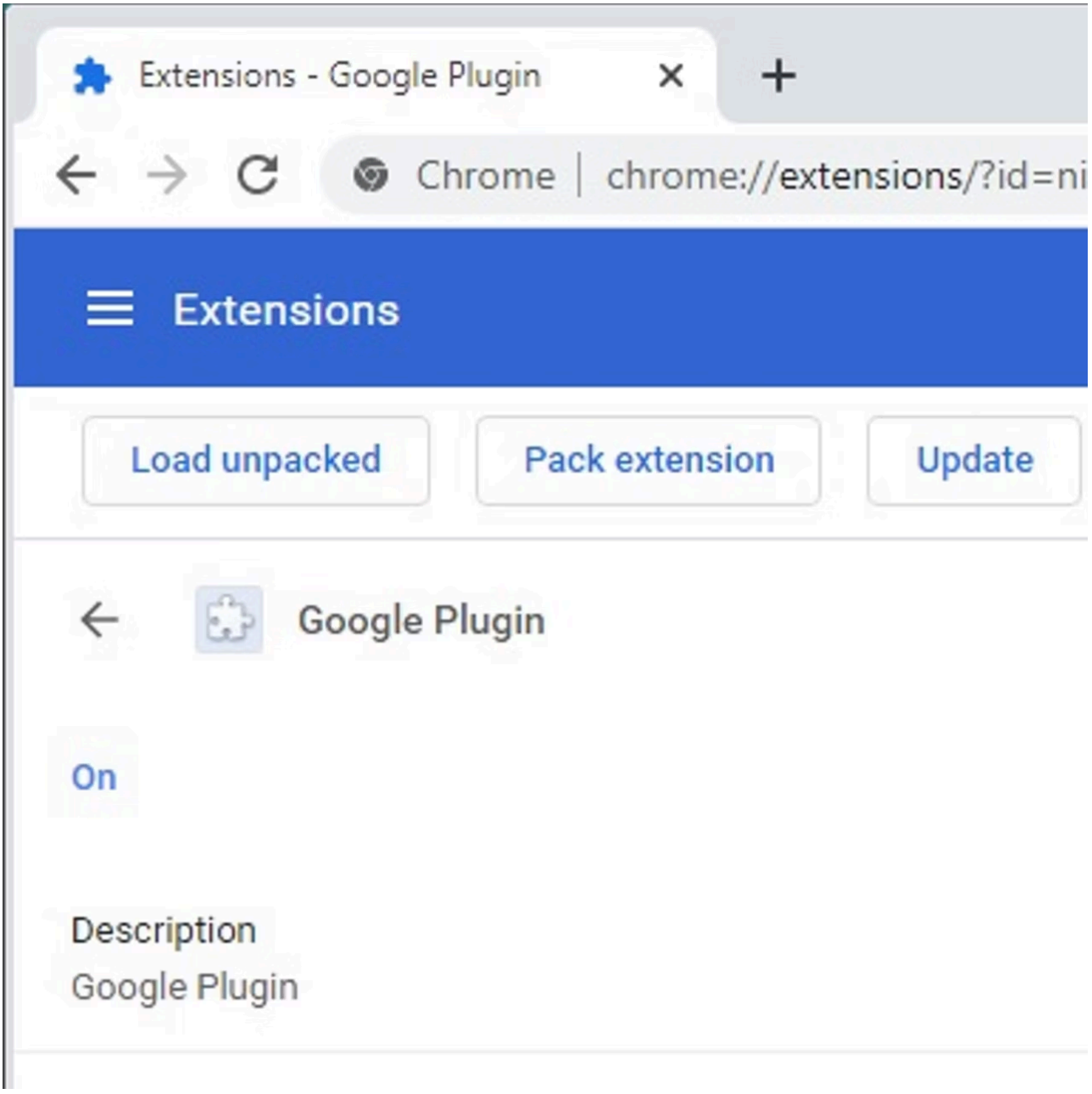

Figure 4: Fake browser extension created by Grandoreiro — fake button

This extension will also ask the user for various permissions:

- Reading your browsing history
- Displaying notifications
- Modifying data you copy and paste

Actual in-code permissions:

- “tabs”
- “activeTab”
- “webNavigation”
- “all_urls”
- “cookies”
- “contextMenus”
- “unlimitedStorage”
- “notifications”
- “storage”
- “clipboardWrite”
- “browser”
- “webRequest”
- “webRequestBlocking”
- “<all_urls>”

After the extension is deployed and installed, the dropper writes three additional files under *%appdata%/local/*/*:

- EXT.dat
- RB.dat
- EML.dat

The malware runs a watchdog on the *EXT.dat* file and will re-write it after any removal attempt.

Using the modified extension, the attacker can collect user information from cookies. Some of the collected information includes the following fields:

- “url”
- “tabid”
- “PASSANDO PARAMETRO”
- “cookie”
- “name”
- “domain”
- “value”
- “expired”
- “FormData”
- “WEBMAIL”
- “LoginForm[password]”

- “CHECKBOX_TROCA_SENHA”
- “ccnumber”

We suspect that the malware uses this extension to grab the victim’s cookies and use them from another device to ride the victim’s active session. With this method, the attacker won’t need to continue controlling the victim’s machine.

Note that some of the strings in the collected data remain written in Portuguese. Another tidbit that connects Grandoreiro variants to Brazil is the “default_locale” setting within the malicious browser extension code that is set to “pt_BR” (likely meaning Portuguese_Brazil).

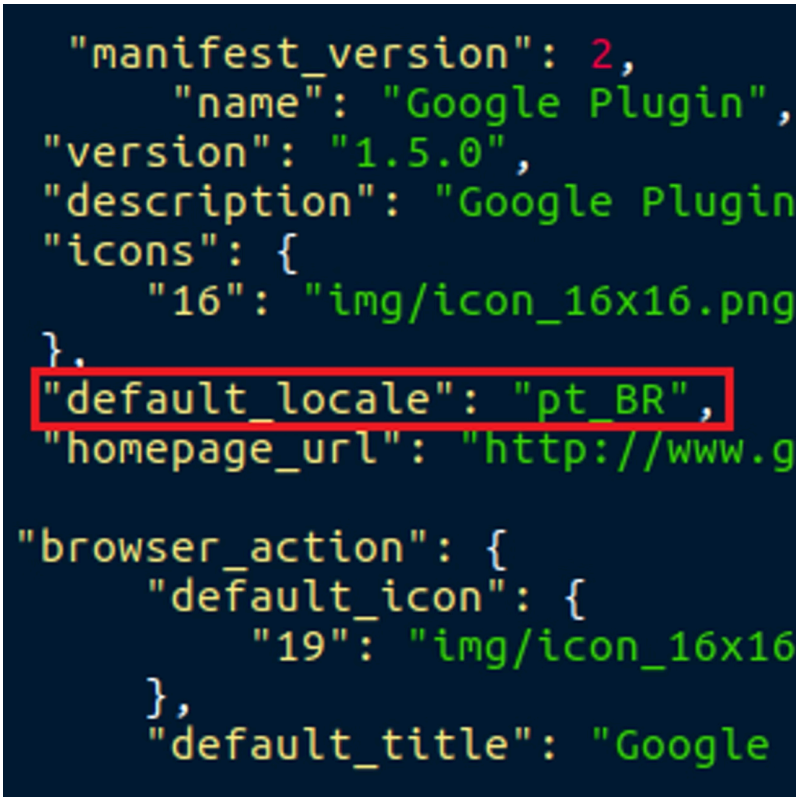

Figure 5: Grandoreiro — Brazilian origins

Once active on the infected device, Grandoreiro waits in the background for the victim to take an action that will trigger it, such as browsing to a targeted bank’s website. That’s when the attack would invoke the remote-access feature of the malware and engage with the victim in real time by launching malicious images on their screen to trick them into keeping the session alive and providing information that can help the attacker.

The images are premade to look like the targeted bank’s interface, and the attacker can launch them in real time.

After discovering Grandoreiro attacks in Spain, our team looked into the code for modifications. We established that the source codes are 80–90 percent identical. It stands to reason that the attackers deploying Grandoreiro in Spain have some tie to those operating it in Brazil.

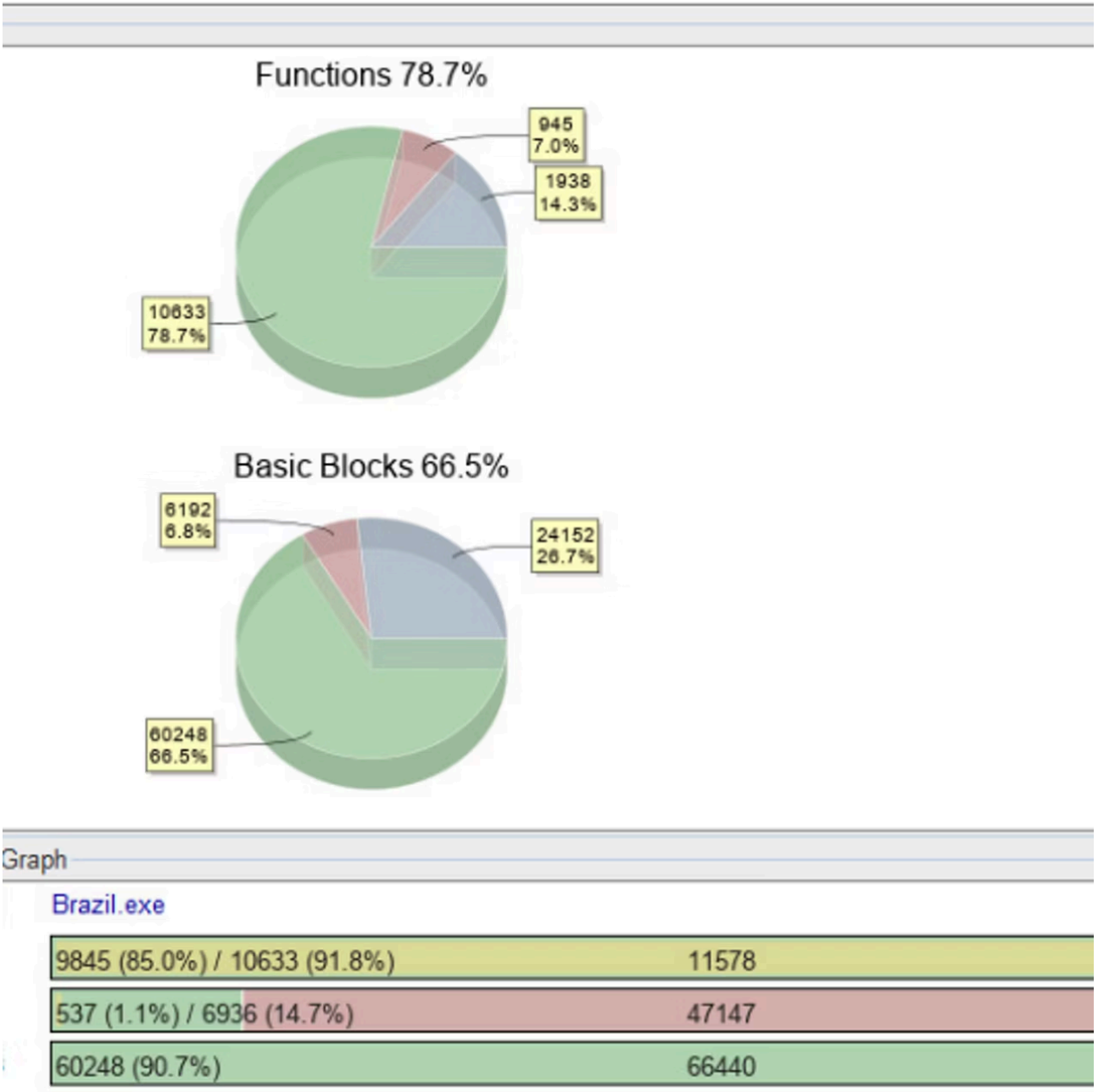

Figure 6: Grandoreiro versions in Spain and Brazil are 80–90 percent similar

Banking Trojans are a popular tool among various attackers around the globe who use them to rob the bank accounts of unsuspecting victims by infecting the devices they bank from.

In the global arena, sophisticated, modular banking Trojans like TrickBot and IcedID, operated by organized cybercrime gangs, are what we usually find being used against large banks in various countries. But that stands in stark contrast to what we continue to see in the LATAM region and wherever else the language barrier can enable the same cybercriminals to operate, namely Spanish/Portuguese-speaking countries outside of LATAM.

Notoriously simplistic malware codes reign supreme in these regions, allowing almost any level of attacker to access and use them against consumers and businesses alike. While relatively simple, its power lies in the attacker’s ability to take over devices and trick the victim in real time within the context of their normal online banking activities.

IBM X-Force research continues to monitor these threats and keep our readers up to date on how they evolve. To read more from our teams, check out our Security Intelligence blogs, and join us on X-Force Exchange for timely indicators of compromise (IoCs) and threat intel on emerging attacks.
