Grandoreiro: How engorged can an EXE get?

welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get

ESET Research April 28, 2020

In this installment of our series, we introduce Grandoreiro, a Latin American banking trojan targeting Brazil, Mexico, Spain and Peru. As such, it shows unusual effort by its authors to evade detection and emulation, and progress towards a modular architecture.

We have seen Grandoreiro being distributed solely through spam. The authors usually utilize a fake Java or Flash update, but recently, perhaps unsurprisingly, we have observed their spam abusing the fear around COVID-19 as well.

We have named this malware family based on its most notable characteristic – its binaries being bloated to at least a few hundred megabytes. Its development is quite rapid and feature changes and additions are happening very often. In this blogpost, we will focus on the most noteworthy.

Characteristics

Grandoreiro is another Delphi-written Latin American banking trojan we have identified during our research. Grandoreiro has been active at least since 2017 targeting Brazil and Peru, expanding to Mexico and Spain in 2019 (see Figure 1 for a current detection heat map). The fact that it attacks its victims by displaying fake pop-up windows that try to persuade victims to divulge sensitive information should come as no surprise to anyone who has read the previous pieces in the series.

.

Figure 1. Heat map showing ESET's detections of Grandoreiro.

Grandoreiro, as with any other Latin American banking trojan, employs backdoor functionality, being capable of:

- manipulating windows
- updating itself
- capturing keystrokes
- simulating mouse and keyboard actions
- navigating the victim's browser to a chosen URL
- logging the victim out or restarting the machine
- blocking access to chosen websites

Persistence is ensured by creating a .LNK file in the Windows startup directory. Of importance is the fact that Grandoreiro uses the same algorithm for decrypting its internal strings as Casbaneiro. We believe this is due to information sharing between authors of banking trojans in Latin America.

Grandoreiro collects the following information about its victims:

- computer name
- username
- operating system version and bitness
- whether Diebold Warsaw GAS Tecnologia (an application, popular in Brazil, to protect access to online banking) is installed
- list of installed security products

In some versions, it also steals credentials stored in the Google Chrome web browser and data stored in Microsoft Outlook.

The authors of Grandoreiro seem to be developing the banking trojan very rapidly, as we observe at least several new versions each month. We also suspect they are developing at least two variants simultaneously.

The authors seem to focus mainly on two areas. The first is hiding the actual C&C address using the Domain Generation Algorithm (DGA) described in next section. The second is making the banking trojan modular. This is an interesting approach as the authors first introduced separate Delphi forms for each bank targeted (which is quite common), but lately even created separate DLLs for each targeted bank. We have not seen this approach in any other Latin American banking trojan we have analyzed.

DGA

Grandoreiro's DGA uses two strings (*prefix* and *suffix*) hardcoded in the binary and the local date as inputs. Those values are processed by a simple algorithm yielding a result in the form https://sites.google[.]com/view/%DATA%, where %DATA% is the generated string (we provide pseudocode in Figure 2). The C&C domain and port are used as the site

title, as you can see in Figure 3. Note that based on the DGA, a different website is required for each day. We have observed some variants also using a custom base64 alphabet.

```
1  def dga(prefix, suffix):
2  ts = get_current_time()
3  mid_data = "%02d/%02d/%04d" % (ts.day, ts.month, ts.year)
4  mid_data = b64encode(mid_data)
5  mid_data = mid_data.replace("==", "")
6  return "https://sites.google.com/view/" + prefix + mid_data + suffix
```

Figure 2. Pseudocode of Grandoreiro's DGA

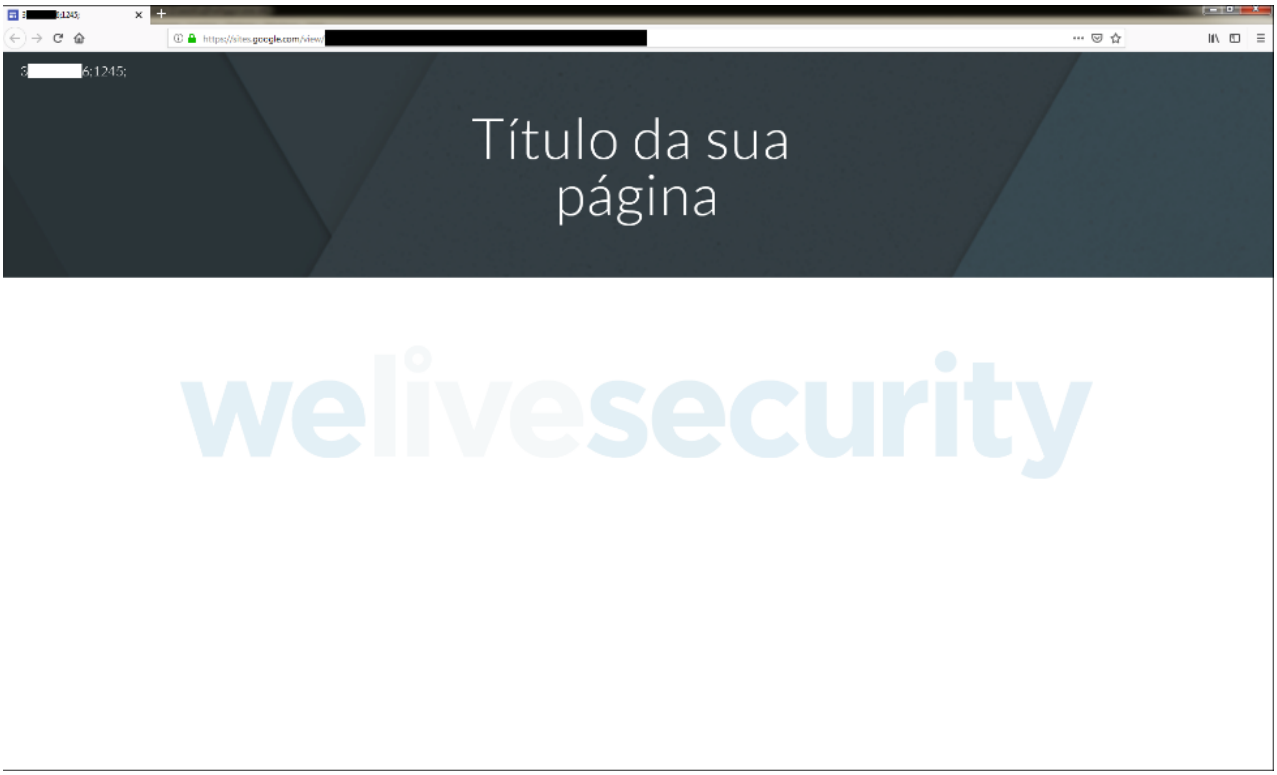

Figure 3. Example of a Google site set up by authors of Grandoreiro (translation: "Title of your page")

Configuration data

In older versions of Grandoreiro, there was a small .ini file distributed alongside the banking trojan that served as a primitive configuration file, containing only a version identifier and an index into a table in the binary that decided which C&C server should be used.

Lately, the configuration mechanism has been changed and is now stored in the Windows Registry at HKCU\Software\ under keys with names like %USERNAME% and ToolTech-RM. Those names, as well as the names of values they contain, change frequently, but the information contained consists of:

- an identifier unique for each victim (generated via CoCreateGuid API)
- executable name and path
- geolocation of the victim (retrieved via http://ipinfo.io/json)
- strings necessary for creating and deleting the startup .LNK file
- notes specific to the victim device (the C&C operator supplies these, if any, via a backdoor command)
- flags to indicate an action has already been performed, such as
    - stealing Google Chrome stored credentials
    - stealing Outlook data

C&C communication

Grandoreiro implements communication with its C&C server using the RealThinClient SDK. This component uses a protocol that operates over HTTP. After connecting to the server, Grandoreiro performs a handshake and then periodically checks for commands every few seconds. If the trojan misses a check, the server drops the connection.

As we described in our Botconf presentation in December 2019, and as reported recently by SonicWall, there is a very interesting thing about the first "command" received from the C&C server. It is always a list of all currently connected victims, including all the collected information about their machines, as you can see in Figure 4. Note that not all the victims are identified by a string with the same format. Due to Grandoreiro's rapid development, this string changes quite often, but victims compromised with different variants still connect to the same C&C server.

Figure 4. C&C server responding to initial Grandoreiro connection with a list of currently connected victims.

Distribution

Spam seems to be the sole distribution method for Grandoreiro. The spam emails appear to contain a link pointing to a website offering fake Flash or Java updates (see Figure 5). Notice the red arrow in lower left corner tailored for the Google Chrome web browser, but displayed in other browsers too. We have seen Grandoreiro abusing the fear around COVID-19 as well (see Figure 6), as we already announced on our @ESETresearch Twitter account.

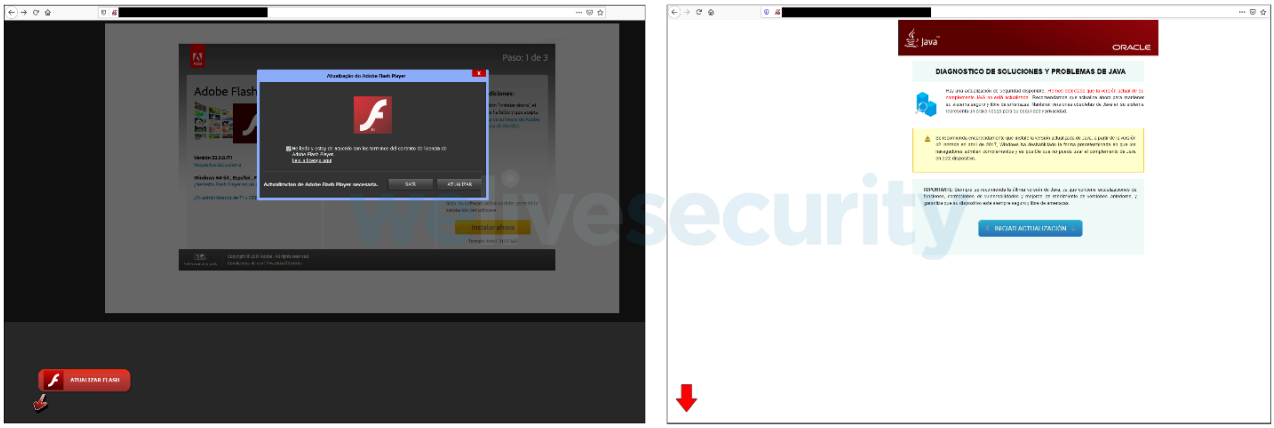

Figure 5. Fake Flash (left) and Java (right) update websites (the left checkbox states that the user agrees with terms and conditions; the text on the right urges the user to install the latest version of Java to avoid issues with security and vulnerabilities)

Figure 6. Fake COVID-19 website. Clicking the video leads to the ZIP archive being downloaded (translation: "Construction of 2 hospitals in 7 days: accelerated video shows construction of hospital in China in 7 days")

Unlike the majority of Latin American banking trojans, Grandoreiro utilizes quite small distribution chains. For different campaigns, it may choose a different type of downloader, as we illustrate in Figure 7. These downloaders are often stored on well-known public online sharing services such as GitHub, Dropbox, Pastebin, 4shared and 4Sync.

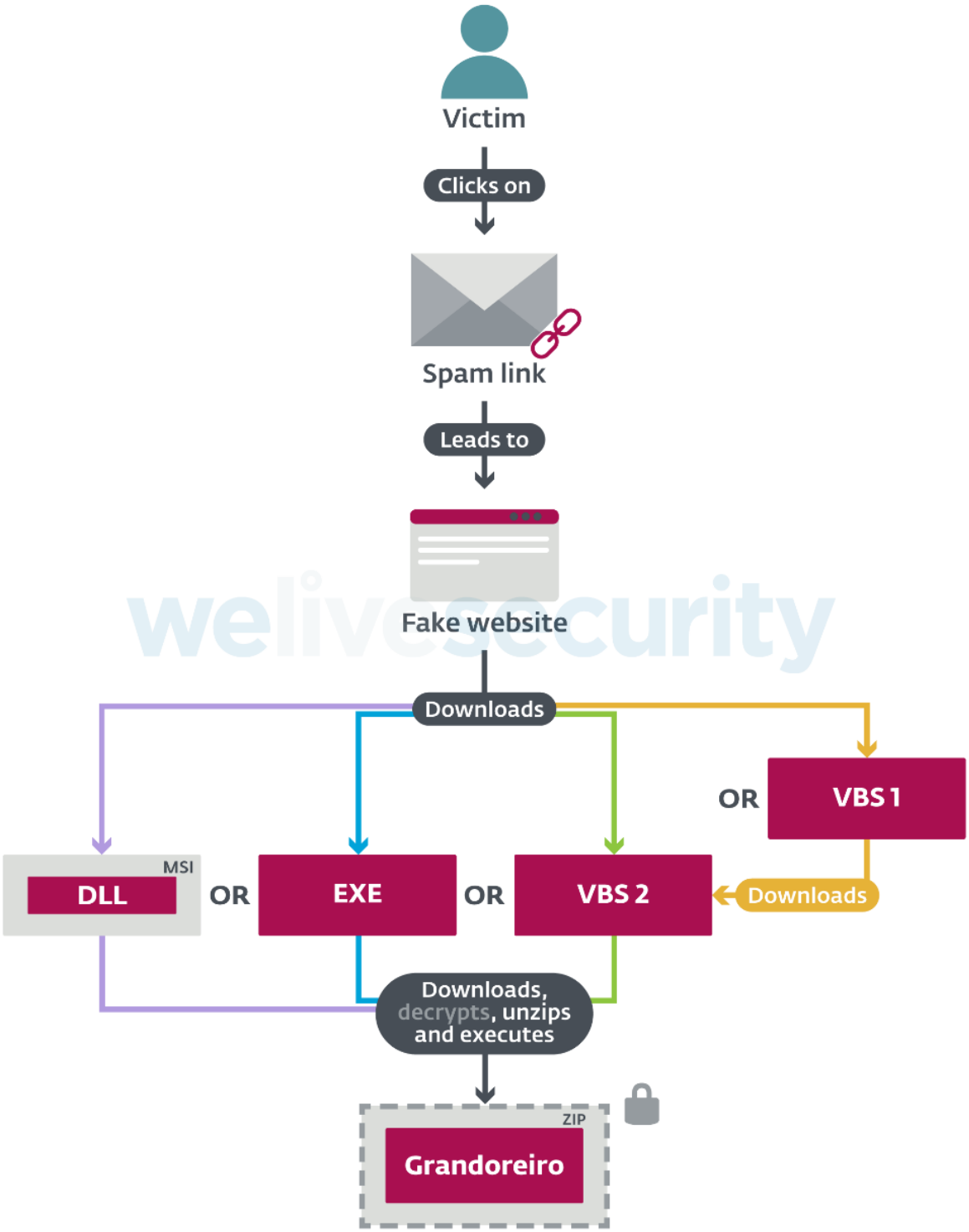

Figure 7. Possible ways that Grandoreiro distribution chains may appear (different colors show different paths the chain may take). The final ZIP archive may be encrypted and in some cases also protected by a password.

The final payload is a ZIP archive that is usually encrypted by the algorithm shown in Figure 8 and, in a significant number of cases, we saw it being password-protected as well.

```
1 def decrypt_archive(data_enc, key):
2 data_dec = list()
3 for (i, c) in enumerate(data_enc):
4 d = c ^ (~(key >> (i % 32))) & 0xFF
5 data_dec.append(d)
6 return data_dec
```

Figure 8. Pseudocode of the archive decryption algorithm used by Grandoreiro

Distributing the final payload in a ZIP archive is very common among these banking trojans, but in the case of Grandoreiro, it holds extra importance, as you will see in the next section.

Binary padding

The vast majority of Grandoreiro samples utilize a very interesting application of the binary padding technique. This technique is all about making the binaries large and we have seen it being used even by more sophisticated malware. We have also observed some other Latin American banking trojans employing it occasionally, but only in the simplest form of appending a large amount of junk at the end of the binary.

Grandoreiro chooses a different approach – a simple, yet very effective one. The resources section of the PE file is augmented by (usually 3) *grande* BMP images, making each binary at least 300 MB in size. Notice in Figure 9 that the size of the whole EXE is 425 MB, yet the size of the code is only 4 MB and the size of the .rsrc section 419 MB (98.5% of the total size). After examining the contents of the .rsrc section, we see three images with sizes of 112 MB, 112 MB and 105 MB respectively (taking up 78.5% of the section size). We provide examples of such images in Figure 10.

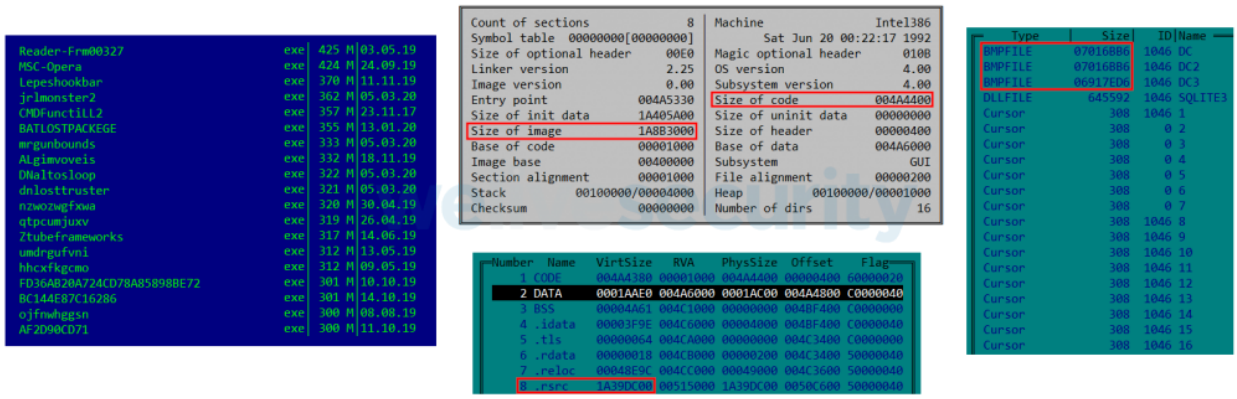

Figure 9. Details of a Grandoreiro binary. Several Grandoreiro binaries are shown in the image on the left. The rest show details of one such binary.

Figure 10. BMP images used by Grandoreiro for binary padding. Their artistic "style" suggests the malware's authors create them manually.

Because of the structure of those BMP files, compressing the binary into a ZIP archive yields a file of only a few MB, making it much easier to distribute the payload. The BMP files seem to change frequently, most likely to avoid detection. The images shown in Figure 10 come from three different builds of Grandoreiro. The visible similarities lead us to believe the authors update the images manually.

Let us look at the possible outcomes of this technique because, even though it is very simple, it is surprisingly effective. The upload file size limit on VirusTotal was changed to 550 MB during 2019, but used to be 256 MB, so a victim was unable to scan the file using that platform. Working with such a huge file is harder in general, making any automated or manual analyses much slower. At the same time, it is very hard to get rid of these large images while keeping a valid PE file, and by discarding the whole .rsrc section, interesting information such as the fake pop–up windows is lost.

Self-protection & anti-emulation

For a Latin American banking trojan, Grandoreiro utilizes a surprisingly large number of tricks to evade detection and emulation. In this section, we talk about the most notable ones that appeared in several recent versions we have analyzed.

Diebold Warsaw GAS Tecnologia and Trusteer are known banking access protection software popular in Latin America. Every banking trojan described so far in our series has implemented some sort of check for these programs. Grandoreiro is no exception, by

- hooking the LdrLoadDll and LoadLibrary(Ex) APIs to prevent loading DLLs belonging to those products
- checking if any of those modules are already loaded
- trying to kill their running processes (based on process names)
- blocking Diebold Warsaw on the firewall level
- trying to break Trusteer by changing its file system path (see Figure 11)
- changing ACLs on main Trusteer binary by running this command twice:
  - cacls %PROGRAM_DATA%; Trusteer\Rapport\store\exts\RapportCerberus\baseline\RapportGH.dll" /T /E /C /P *user:perm*
  - with *user:perm* set to Todos:N and then Everyone:N

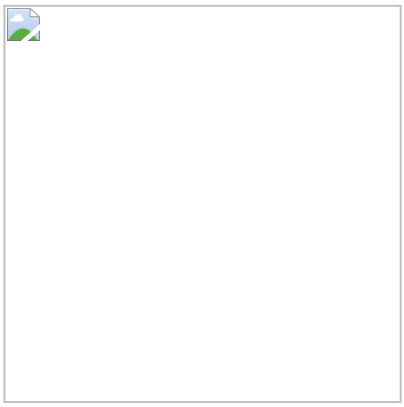

Figure 11. Simple BAT script used by Grandoreiro to change Trusteer file path in hopes of making it unable to execute

Besides that, it also monitors hooks on important functions. If such a function starts with 0xE9 (assembly opcode for the jmp instruction), the trojan reloads the function from the corresponding library. Based on window and process names, it also checks for tools like RegMon, RegShot, Wireshark and Process Explorer. It tries to avoid being debugged by calling the IsDebuggerPresent API and setting up a hook via SetWindowsHookEx that returns ERROR_ACCESS_DENIED on the WH_DEBUG event.

Grandoreiro also employs a technique for privilege escalation described in more detail here. The method relies on registering a binary as the default handler for .MSC files and then running such a file. By doing so, the binary will be executed with elevated privileges. This technique no longer works on patched systems due to a fix released in 2017.

Finally, Grandoreiro detects two virtual environments – VMWare via its special I/O port and Virtual PC via the vpcext instruction. Both methods are described in detail here (techniques 1 and 2).

Spam tool

During our investigation, we discovered a tool used for Grandoreiro's spam campaigns. It is not a tool that automatically registers large numbers of email accounts, as in the case of Amavaldo and Casbaneiro; it is actually used to create and send the spam messages. It does so by utilizing the EASendMail SDK.

Besides its main purpose, the tool sets up persistence using the Windows Registry Run key and disables UAC. The most probable scenario is that the attackers distribute this tool to some victims via Grandoreiro.

A small backdoor component is included and used to receive configuration files. Those files dictate what the emails will look like, what they will point to or where to send them. We provide a complete list of the configuration files and their purpose in Table 1.

Table 1. List of configuration files used by Grandoreiro's spam tool

File-name	Purpose	Description
ID.txt	None	Seems not to be used for the spam emails
html.txt	Email body template	Template for the email body (including placeholders - those are replaced by values from other config files)
assun-to.txt	Subject template (assunto = subject)	Template for subject (similar to html.txt for email body)
nomes.txt	List of fake names	Replaces [NOME] placeholder in the templates
link.txt	List of malicious URLs	The email will link to one of these
lista.txt	List of recipients	The email will be sent to all of these
login.txt	List of usernames	Information required to log into the email account that will be used to send the emails
senha.txt	List of passwords	
smtp.txt	SMTP server address	

As you can see, the tool is not fully automated, but relies completely on the configuration data. This shows a lower level of sophistication. Its implementation shows similarities with the Grandoreiro banking trojan, which is why we believe it was written by the same authors.

Conclusion

In this installment of our series, we have focused on Grandoreiro, a Latin American banking trojan known to target Brazil, Mexico, Spain and Peru. We have mentioned aspects that are typical for that type of banking trojan, such as being written in Delphi, containing backdoor functionality, targeting Latin America and using fake pop-up windows to attack its victims.

A novel feature of Grandoreiro is its great effort to evade detection. That includes many techniques to detect or even disable banking protection software. It also utilizes a very specific application of the binary padding technique we have not seen before that makes it hard to get rid of the padding while keeping a valid file.

Spam appears to be the exclusive distribution method for Grandoreiro. The emails contain a link that points victims to fake websites set up by the operators. While they usually use simple mechanisms such as fake Flash or Java updates, we have seen them exploiting the current fear of COVID-19 as well.

Grandoreiro shows similarities with other banking trojans previously described in this series, mainly Casbaneiro, with which it shares the string decryption algorithm.

For any inquiries, contact us at threatintel@eset.com. Indicators of Compromise can also be found in our GitHub repository.

Indicators of Compromise (IoCs)

Hashes

Grandoreiro banking trojan

SHA-1	Description	ESET Detection name
40FBC932BD45FEB3D2409B3A4C7029D-DDE881389	Older version of Grandoreiro (2017)	Win32/Spy.-Grandoreiro.A
7905D-B9BBE2CB29519A5371B175551C6612255EF	Grandoreiro	Win32/Spy.-Grandoreiro.AE
BD88A809B05168D6EFDBA4D-C149653B0E1E1E448	Grandoreiro	Win32/Spy.-Grandoreiro.AJ

Grandoreiro Win32 downloaders

SHA-1	Description	ESET detection name

SHA-1	Description	ESET detection name
7C2ED8B4AA65BEFC-C229A36CE50539E9D6A70EE3	Grandoreiro downloader	Win32/TrojanDownloader.Banload.YJR
27A434D2E-F4D1D021F283BCB93C6C7E50ACB8EA6	Grandoreiro downloader	Win32/TrojanDownloader.Banload.YLZ
28D58402393B6BCA73F-F0EAC319226233181EDC9	Grandoreiro downloader	Win32/TrojanDownloader.Banload.YJB
42892DF64F00F4C091E1C02F74C2B-B8BAD131FC5	Grandoreiro downloader	Win32/TrojanDownloader.Banload.YMI

Grandoreiro spam tool

SHA-1	Description	ESET detection name
BCED5D138ACEADA1E-F11BFD22C2D6359CDA183DB	Grandoreiro spam tool	Win32/Spy.Grandoreiro.AD

Windows Registry

- HKCU\Software\%USER_NAME%
- HKCU\Software\ToolTech-RM

User-Agent

h55u4u4u5uii5

Filenames

%INSTALL_DIR%\ *
- MDL_YEL_01.dll
- MDL_BLU_BR_02.dll
- MDL_SIC_BR_03.dll
- MDL_SANT_BR_04.dll
- MDL_ITA_BR_05.dll
- MDL_BRADA_BR_06.dll
- MDL_SICCB_BR_07.dll
- MDL_SAFRA_BR_08.dll
- MDL_ORIGI_BR_09.dll
- MDL_NORDES_BR_10.dll
- MDL_BANEST_BR_11.dll
- MDL_BANEZE_BR_12.dll
- MDL_AMAZON_BR_13.dll
- MDL_UNICRE_BR_14.dll
- MDL_BRB_BR_15.dll
- MDL_WUPDATE_BR_001.dll

* %INSTALL_DIR% is the path where Grandoreiro is installed

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Initial Access	T1192	Spearphishing Link	Grandoreiro distribution chains start with an email link pointing to a fake website.
Execution	T1106	Execution through API	Grandoreiro is executed either by WinExec or WScript.Shell.Exec API.
Persistence	T1060	Registry Run Keys / Startup Folder	Grandoreiro ensures persistence by creating a .LNK file in the startup folder.
Privilege Escalation	T1088	Bypass User Account Control	Grandoreiro bypasses UAC by registering as the default handler for .MSC files.
Defense Evasion	T1009	Binary Padding	Grandoreiro inserts large BMP files into its .rsrc section to make the binaries much larger.
	T1089	Disabling Security Tools	Grandoreiro tries to disable Diebold Warsaw and Trusteer banking protection software.
	T1140	Deobfuscate/Decode Files or Information	Grandoreiro is distributed in a ZIP archive that usually needs to be decrypted.

Tactic	ID	Name	Description
	T1222	File and Directory Permissions Modification	Grandoreiro changes the ACL for Trusteer to disable it.
	T1036	Masquerading	Downloaders that distribute Grandoreiro masquerade as fake update installation files.
	T1112	Modify Registry	Grandoreiro stores its configuration in the Windows Registry.
	T1064	Scripting	Grandoreiro implements some of its distribution chain stages in VBScript.
	T1497	Virtualization/Sandbox Evasion	Grandoreiro detects VMWare and Virtual PC.
Credential Access	T1503	Credentials from Web Browsers	Grandoreiro steals credentials from the Google Chrome browser.
	T1081	Credentials in Files	Grandoreiro parses Outlook .pst files to extract email addresses.
Discovery	T1010	Application Window Discovery	Grandoreiro discovers various security tools based on window names.
	T1083	File and Directory Discovery	Grandoreiro discovers protection software based on file system paths.
	T1057	Process Discovery	Grandoreiro discovers security tools based on process names.
	T1063	Security Software Discovery	Grandoreiro detects the presence of banking protection products.
	T1082	System Information Discovery	Grandoreiro collects information about the victim's machine, such as %USERNAME%, %COMPUTERNAME%, and product names.
Collection	T1056	Input Capture	Grandoreiro is capable of capturing keystrokes.
Command and Control	T1483	Domain Generation Algorithms	Grandoreiro generates its C&C address using a DGA.
	T1071	Standard Application Layer Protocol	Grandoreiro's network protocol is implemented by RealThinClient, which is built over HTTP.

Tactic	ID	Name	Description
Exfil-tration	T1041	Exfiltration Over Command and Control Channel	Grandoreiro sends the data it retrieves to its C&C server.

Further reading

The other parts of the series

From Carnaval to Cinco de Mayo – The journey of Amavaldo

Casbaneiro: Dangerous cooking with a secret ingredient

Mispadu: Advertisement for a discounted Unhappy Meal

Guildma: The Devil drives electric

ESET Research 28 Apr 2020 - 11:30AM