Grandoreiro banking trojan unleashed: X-Force observing emerging global campaigns

securityintelligence.com/x-force/grandoreiro-banking-trojan-unleashed/

Since March 2024, IBM X-Force has been tracking several large-scale phishing campaigns distributing the Grandoreiro banking trojan, which is likely operated as a Malware-as-a-Service (MaaS). Analysis of the malware revealed major updates within the string decryption and domain generating algorithm (DGA), as well as the ability to use Microsoft Outlook clients on infected hosts to spread further phishing emails. The latest malware variant also specifically targets over 1500 global banks, enabling attackers to perform banking fraud in over 60 countries including regions of Central and South America, Africa, Europe, and the Indo-Pacific. Although campaigns have traditionally been limited to Latin America, Spain and Portugal, X-Force observed recent campaigns impersonating Mexico's Tax Administration Service (SAT), Mexico's Federal Electricity Commission (CFE), Mexico's Secretary of Administration and Finance, the Revenue Service of Argentina, and notably the South African Revenue Service (SARS). The reworked malware and new targeting may indicate a change in strategy since the latest law enforcement action against Grandoreiro, likely prompting the operators to start expanding the deployment of Grandoreiro in global phishing campaigns, beginning with South Africa.

Key findings

- Grandoreiro is a multi-component banking trojan likely operated as a Malware-as-a-Service (MaaS).
- It is actively deployed in phishing campaigns impersonating government entities in Mexico, Argentina and South Africa.
- The banking trojan specifically targets over 1500 global banking applications and websites in over 60 countries including regions in Central/South America, Africa, Europe, and the Indo-Pacific.
- The latest variant contains major updates including string decryption and DGA calculation, allowing at least 12 different C2 domains per day.
- Grandoreiro supports harvesting email addresses from infected hosts and using their Microsoft Outlook client to send out further phishing campaigns.

Grandoreiro operators expand campaigns

LATAM-focused campaigns

Since March 2024, X-Force has observed phishing campaigns impersonating Mexico's Tax Administration Service (SAT), Mexico's Federal Electricity Commission (CFE), the Secretary of Administration and Finance for the city of Mexico, and the Revenue Service of Argentina. The emails target users within Latin America, including top-level domains (TLDs) from Mexico, Colombia, and Chile "**.mx**", "**.co**", and "**.cl**". Any real identities have been redacted from the images for personal privacy.

The first campaign appears to be an attempt to be perceived as official and urgent and informs the target that they are receiving a final notice regarding a debit to the Federal Taxpayer Registration Fee (RFC) that has not been paid. If unpaid, consequences may include penalties, fines and a block on the user's tax identification number impacting the target's ability to conduct business and access government services legally. An additional campaign impersonates Mexico's Federal Electricity Commission (CFE) and reminds the recipient that they subscribed to CFEMail, and therefore can access their account statement in PDF and XML format by clicking one of the embedded links. A third campaign imitating the Secretary of Administration and Finance, directs the recipient to click on a PDF to read details regarding a compliance notice. A campaign imitating the Revenue Service of Argentina instructs the user to download a new tax document and take applicable actions.

In each campaign, the recipients are instructed to click on a link to view an invoice or fee, account statement, make a payment, etc. depending on the impersonated entity. If the user who clicks on the links is within a specific country (depending on the campaign, Mexico, Chile, Spain, Costa Rica, Peru, or Argentina), they are redirected to an image of a PDF icon, and a ZIP file is downloaded in the background. The ZIP files contain a large executable disguised with a PDF icon, found to have been created the day prior to, or the day of the email being sent.

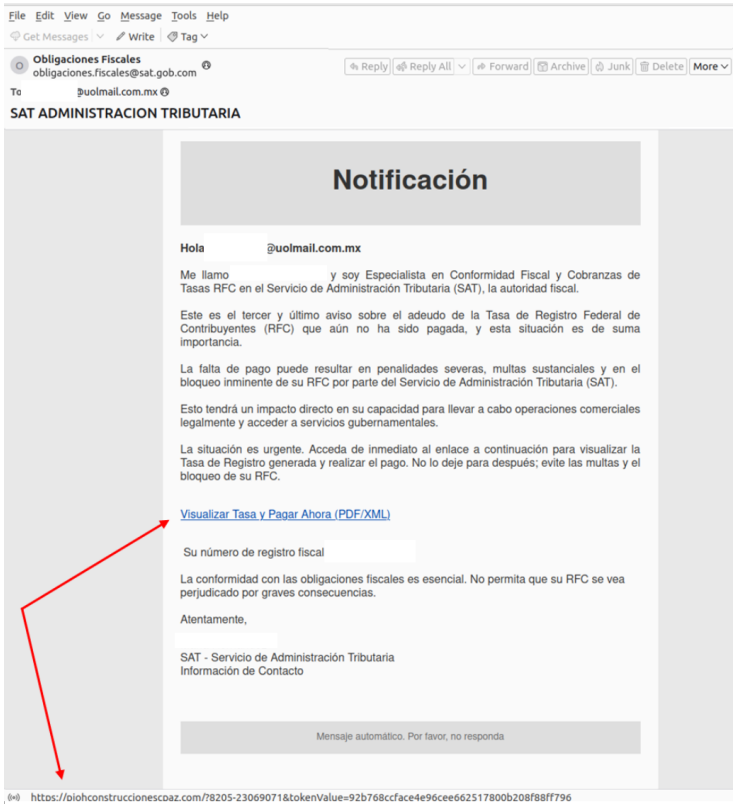


Fig 1, 2: Sample emails impersonating SAT, and CFE

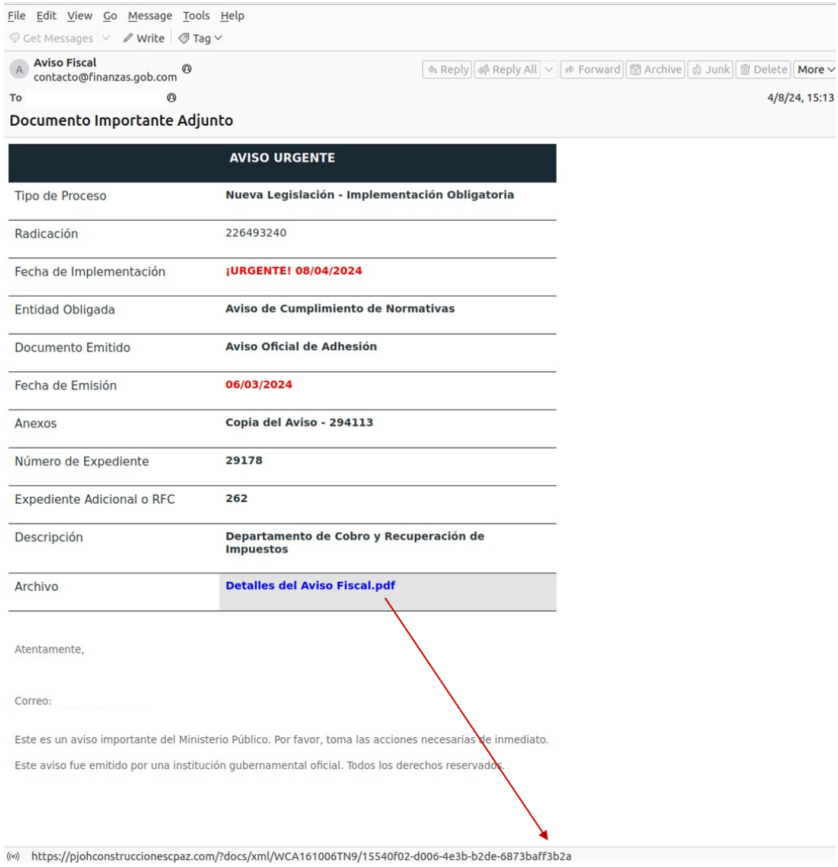
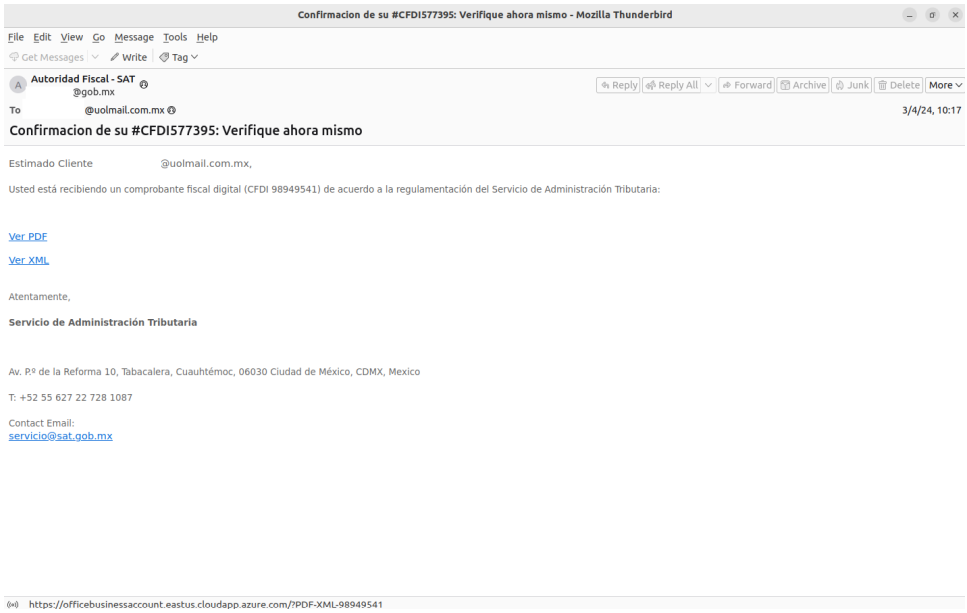


Fig 3, 4: Secretary of Admin and Finance, and AFIP

Campaign Impersonating the South African Revenue Service

Typically Grandoreiro malware is seen in campaigns that target users within Latin America; however, after recent arrests made involving Grandoreiro operators, X-Force has seen a surge in campaigns reaching areas outside of LATAM, including TLDs from Spain, Japan, the Netherlands, and Italy. X-Force observed a phishing campaign impersonating the South African Revenue Service (SARS), purporting to be from the Taxpayer Assistance Services Division. Likely executed by the same operator, X-Force also observed two campaigns impersonating the Tax Administration Service of Mexico. Emails are written in either English, or Spanish, and resemble the same format. The emails reference a Tax number and inform the recipient that they are receiving an electronic tax invoice that is in compliance with the regulations set forth by the South African Revenue Service, or in accordance with the regulations of the Tax Administration Service. The user is provided both a PDF or XML link to view the invoice which initiates a ZIP archive download containing the Grandoreiro loader executable "**SARS 35183372 eFiling 32900947.exe**" (digits vary between samples).



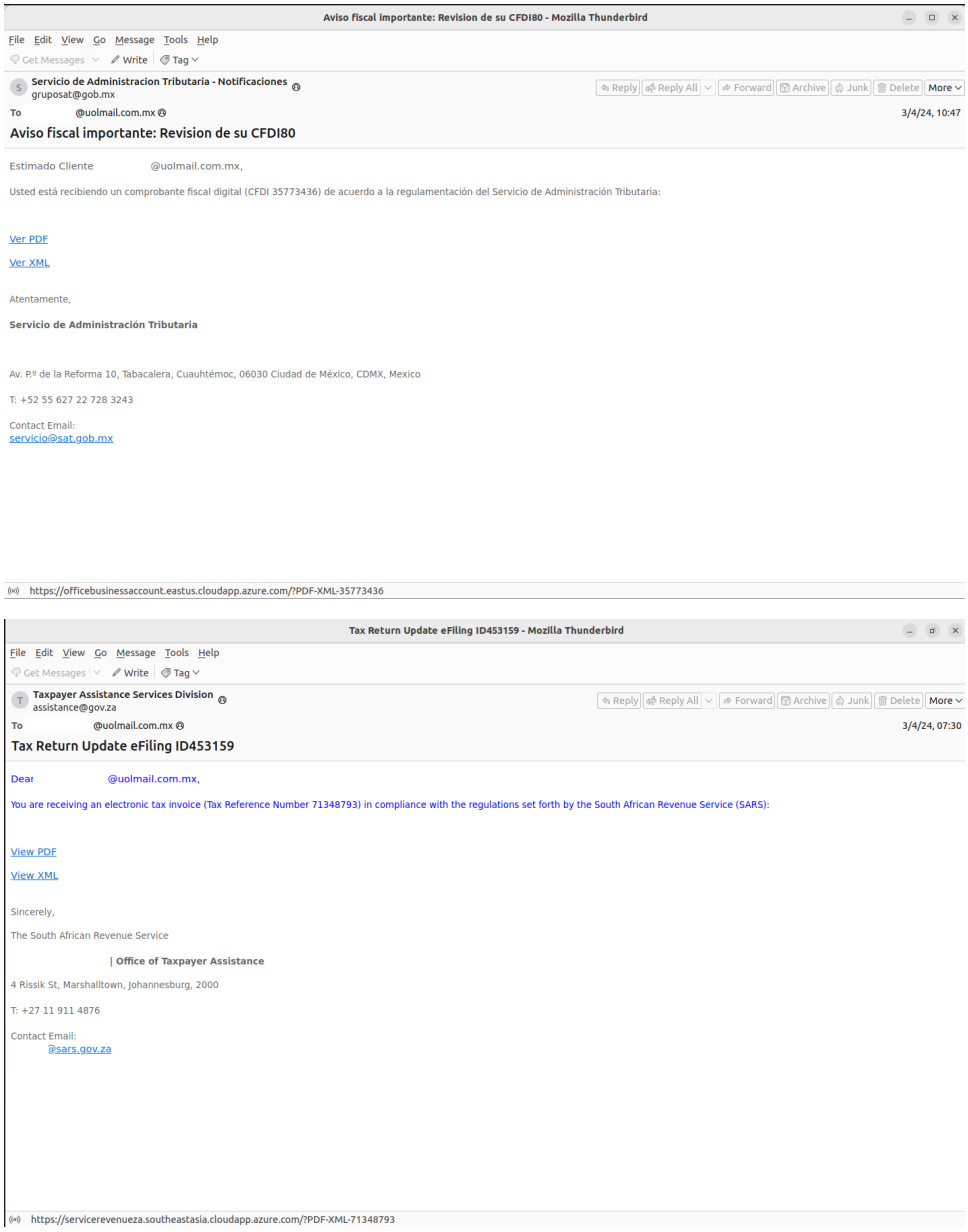


Fig 5, 6, 7: Sample emails impersonating SAT and SARS

Analysis: Grandoreiro Loader

In line with previous campaigns, Grandoreiro's infection chain begins with a custom loader. Often, the executable is bloated to a size of more than 100MB to hinder automatic anti-virus scanning. In hopes of circumventing automated execution, it displays a small CAPTCHA pop-up imitating Adobe PDF reader, which requires a click to continue with the execution.

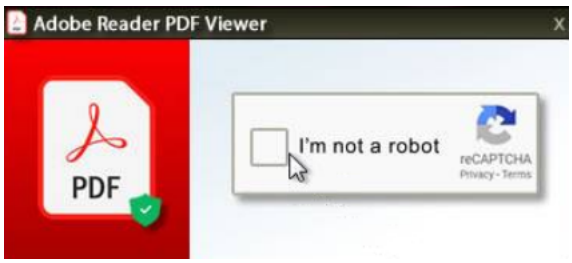


Fig 8: Grandoreiro fake Adobe PDF reader CAPTCHA

The loader has three main tasks:

1. Verify if the client is a legitimate victim (not a researcher or a sandbox)

2. Enumerate basic victim data and send it back to its C2
3. Download, decrypt and execute the Grandoreiro banking trojan

String decryption

All of these tasks require more than 120 important strings, which are encrypted using an improved algorithm.

First, Grandoreiro starts by generating a large key string, which is hardcoded and triple-Base64-encoded. The key observed in these samples begins with **"D9JL@2]790B{P_D}Z-MXR&EZLI%3W>#VQ4UF+O6XVWB16713NIO!E…".** It then takes the encrypted string and uses a custom decoding to convert it into a series of hexadecimal characters interpreted as bytes.

```
{
  case '!':
    System::__linkproc__ UStrCat(&result, dword_81F260);// G
    break;
  case '"':
    System::__linkproc__ UStrCat(&result, dword_81F230);// X
    break;
  case '#':
    System::__linkproc__ UStrCat(&result, dword_81F300);// E
    break;
  case '$':
    System::__linkproc__ UStrCat(&result, dword_81F310);// F
    break;
  case '%':
    System::__linkproc__ UStrCat(&result, dword_81F2C0);// C
    break;
  case '&':
    System::__linkproc__ UStrCat(&result, dword_81F320);// H
    break;
  case ')':
    System::__linkproc__ UStrCat(&result, dword_81F2E0);// B
    break;
  case '*':
    System::__linkproc__ UStrCat(&result, dword_81F2F0);// D
    break;
```

Fig 9: Grandoreiro custom hex encoding (note that non-hex character encoding like '"' are never used)

Grandoreiro decrypts the result via the old Grandoreiro algorithm using the key string. Below is a Python implementation of the decryption routine:

```
def decrypt(ciphertext, key):
    plain = ''
    cipher = bytes.fromhex(ciphertext)
    for i in range(1, len(cipher)):
        n = cipher[i] ^ key[(i-1) % len(key)]
        c = cipher[i-1]
        c = n - c if c < n else n + int(0xff) - c
        plain += chr(c)
    return plain
```

Lastly, it undergoes a final round of 256-bit AES CBC decryption and unpadding to retrieve the plaintext string. Both the AES key and Initiation Vector (IV) are also stored as encrypted strings and have to be decrypted using the same algorithm as above, however skipping the AES decryption. The graph below gives an overview of the full decryption process:

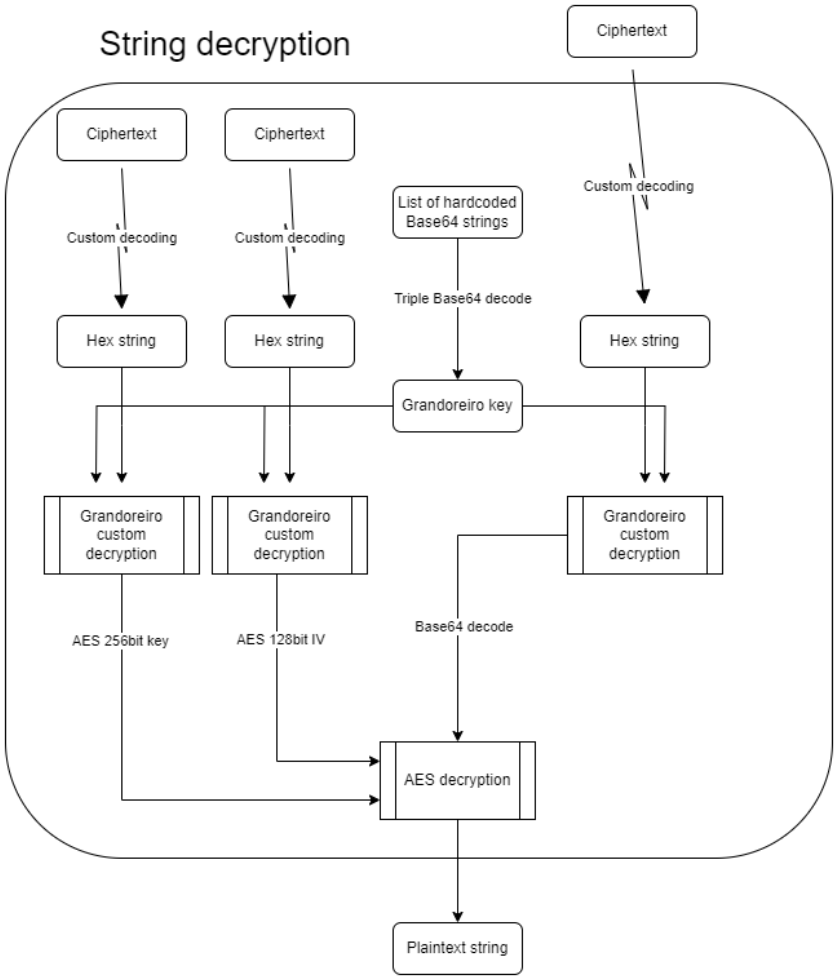


Fig 10: Grandoreiro loader string decryption

Victim verification

To verify that a victim is not part of a sandboxed environment, the Grandoreiro loader collects the following information and checks it against a list of hardcoded values (see Appendix):

1. Computer name
2. Username
3. OS version information
4. Installed Antivirus solution
5. Country of the victim's public IP (via http://ip-api.com/json)
6. List of running processes

This verification step is also used to disallow victims of specific countries. One sample did not continue execution for infections with public IPs from:

- Russia
- Czechia
- Poland
- Netherlands

The sample also prevented infections of Windows 7 machines based in the US without anti-virus.

Victim profiling

The next execution step attempts to build a basic profile of the victim to display on the C2 panel. The malware enumerates the following information on the victim machine:

- Public IP country
- Public IP region

- Public IP city
- Computer name
- Username
- OS Version information
- Installed AV solution
- Check in the registry subkey “Software\Clients\Mail” if the Outlook mail client is installed. If true, the value is set to “SIM”, which means “Yes” in Portuguese
- Check if crypto-wallets exist: Binance, Electrum, Coinomi, Bitbox, OPOLODesk, Bitcoin
- Check if special banking security software is installed: IBM Trusteer, Topaz OFD, Diebold
- Number of Desktop monitors
- Volume Serial Number
- Date of infection
- Time of infection

Grandoreiro concatenates the results using the string “*~+” and sends it as part of the encrypted payload request to the C2 server.

C2 communication and loading Grandoreiro

Grandoreiro loader’s C2 server can be decrypted via the same algorithm explained above. The resulting domain name is resolved via DNS over HTTPS through the URL **https://dns.google/resolve?name=<C2 server>** to circumvent DNS-based blocking. After receiving the C2 IP address, the malware takes the first 4 digits of the IP and runs 4 different digit-to-digit mappings over it resulting in the 4-digit port number.

It then concatenates the victim profiling string from above together with a capitalized Portuguese message “CLIENT_SOLICITA_DDS_MDL” (likely translated to “Client asks for module data”). An example string would be:

```
CLIENT_SOLICITA_DDS_MDL|SOLICITADO*~+GB*~+England*~+London*~+GHPZRGFC*~+Admin*~+7*
~+0*~+SIM*~+0*~+0*~+1*~+399BB819*~+28/04/2024*~+22:34:13*~+*~+
```

The string is encrypted and sent as the URL path via an HTTP GET request to the C2 server requesting the final Grandoreiro payload.

If successful, the C2 server replies with an HTTP 200 status code containing another encrypted message. It contains the following information:

1. Payload download URL
2. C2 server
3. Directory name
4. Payload name
5. Payload size

Example:

```
http://15[.]228.49.78:55842/AudioSnapLtRoWinTechHub.xml|15[.]228.49.78|ssdextzjsbO
KIPrinterResetter|ssdextnkhgDellPrinterHubrxudMSIAfterburner.exe|8533387
```

To download, Grandoreiro issues another HTTP GET request to the payload URL. The downloaded file is stored in the specified directory name under “**C:\ProgramData**“. Next, the file is decrypted via an RC4-based algorithm using the key “7684223510”. Finally, it is decompressed using the “ZipForge” Delphi library, and the originally downloaded file is deleted.

The archive may contain two files, a .EXE (Grandoreiro banking trojan) and a .CFG (config file).

Prior to execution, the loader performs an enumeration of the current process token’s group membership, specifically checking for the presence of the SECURITY_NT_AUTHORITY SID. If the process possesses the required privileges, the loader utilizes the *ShellExecuteW()* function with the ‘runas’ verb to execute the Grandoreiro payload with elevated privileges. Conversely, if the necessary privileges are not available, the loader resorts to executing itself via *ShellExecuteW()* without elevation.

During all stages of infection—the payload download, decryption, and execution—the Grandoreiro loader reports back status messages to its C2 server. Some examples are:

- ERRO_FALHA_DOWNLOAD (“Download failed error”)
- ERRO_EXTRACAO (“Extraction error”)
- AV_COMEU_MODULO (“AV ate module”)
- ERRO_EXECUCAO (“Execution error”)
- INFECTADO (“Infected”)

Grandoreiro Banking Trojan

The final payload is the Grandoreiro banking trojan. The latest version has undergone major updates mainly within the string decryption and DGA calculation algorithms. It has also included a vast number of global banking applications to target, support execution and enable attackers to perform banking fraud in dozens of countries. Together with a specialized Outlook spreader module and a wide range of features, it is one of the largest known banking trojans and analysis is still ongoing. The following sections present an in-depth look at Grandoreiro's most notable characteristics, highlighting its essential features and functionalities.

Persistence and configuration

Grandoreiro begins by establishing persistence via the Windows registry. It runs the following command to create a new registry Run key and launch the malware on user login:

```
cmd.exe /C powershell.exe -Command ""Set-ItemProperty -Path
HKLM:\Software\Microsoft\Windows\CurrentVersion\Run -Name RadeonSettings/Q-1,I(MVA
-Value '<path_to_grandoreiro_executable> /runas'""
```

Note that the name of the key may differ among samples, but is often related to the original filename of the downloaded payload. If Grandoreiro does not run in an elevated process, the "/runas" verb is omitted.

In addition to the .CFG file, Grandoreiro also creates a .XML file in the **C:\Public** directory. It is encrypted via the loader's string encryption routine and stores the Grandoreiro executable filename, path and date of infection.

If Grandoreiro can't find its .CFG file, it will populate a new .CFG with default values specifying which Grandoreiro functions are enabled, the victim's country and date of infection. The .CFG file is encrypted via the Grandoreiro string encryption algorithm explained further below.

Targeted applications

Grandoreiro operators significantly upgraded the list of targeted banking applications, now targeting more than 1500 banks worldwide. The latest variants start by first determining if the victim is on the list of targeted countries. Each country is also mapped to a larger region, which Grandoreiro uses to determine which string searches it should run on currently active windows. This means that, if the victim country for instance is identified as Belgium, it will search for all targeted banking applications associated with the Europe region. Grandoreiro internally maps countries to the region categories **Europe, North America, Central America, South America, Africa, Indo-Pacific and global islands**, with each region having an associated Delphi class to search for bank applications. In addition, Grandoreiro has a class searching for 266 unique strings identifying cryptocurrency wallets, which is run on every infection.

```
310   zf_get_encrypted_string8_countries(57, &v73);
311   zf_decrypt_string(0, v73, &v74);              // PL
312   LStrEqual(*v0, v74);
313   if ( v2 )
314     goto LABEL_47;
315   zf_get_encrypted_string8_countries(58, &v71);
316   zf_decrypt_string(0, v71, &v72);              // PT
317   LStrEqual(*v0, v72);
318   if ( v2 )
319     goto LABEL_47;
320   zf_get_encrypted_string8_countries(59, &v69);
321   zf_decrypt_string(0, v69, &v70);              // UK
322   LStrEqual(*v0, v70);
323   if ( v2 )
324     goto LABEL_47;
325   zf_get_encrypted_string8_countries(60, &v67);
326   zf_decrypt_string(0, v67, &v68);              // FR
327   LStrEqual(*v0, v68);
328   if ( v2
329     || (zf_get_encrypted_string8_countries(61, &v65), zf_decrypt_string(0, v65, &v66), LStrEqual(*v0, v66), v2)
330     || (zf_get_encrypted_string8_countries(62, &v63), zf_decrypt_string(0, v63, &v64), LStrEqual(*v0, v64), v2)
331     || (LStrEqual(*v0, *v1), v2) )              // ES or IE
332   {
333 LABEL_47:
334     lib_create_thread(&cls_TR_HUB008_EpsonPrinter01c0004855bo3p1a0043008);// Europe class
335     vcl_forms_tapplication_processmessage(*off_13CD780, v9, v10);
```

Fig 11: Grandoreiro launching a new thread based on the detected country region

The heatmap below highlights the number of unique banking applications associated with each country. Note that each app may be detected with multiple strings:

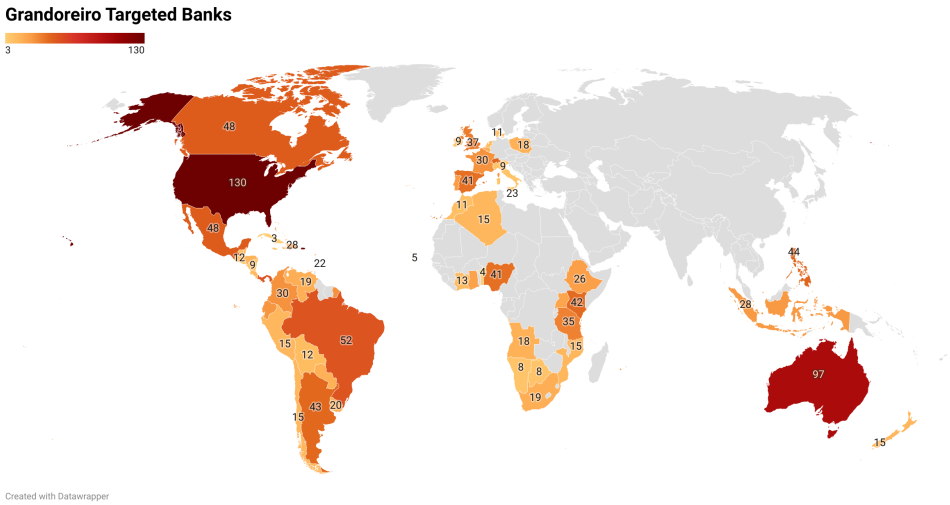


Fig 12: Grandoreiro targeted banking applications per country (created using Datawrapper and populated with information from the X-Force team's research)

DGA

Grandoreiro has traditionally relied on domain generation algorithms (DGA) to calculate its active C2 server based on the current date. The newest iteration of Grandoreiro contains a reworked algorithm and takes it one step further by introducing multiple seeds for its DGA. These seeds are used to calculate a different domain for each mode or functionality of the banking trojan, allowing separation of C2 tasks among several operators as part of their Malware-as-a-Service operation. Each Grandoreiro sample may have a main default seed in case the config file is missing, as well as a list of function-specific seeds. The sample X-Force analyzed contained 14 different seeds, leading to 14 possible C2 domains every day. To explain the algorithm, we will calculate the domains for April 17, 2024. The following chart provides a visualization of the algorithm with an explanation below:

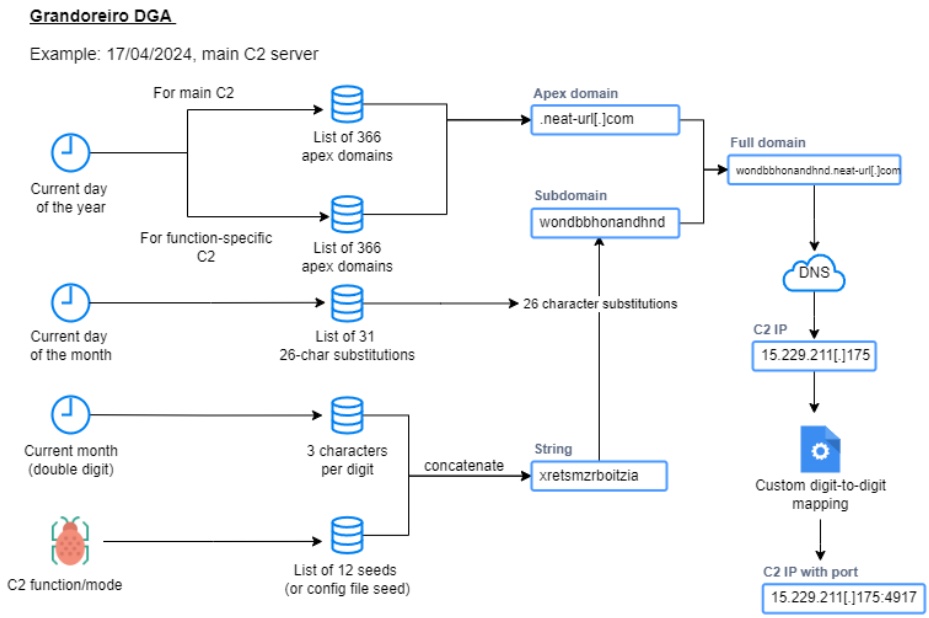


Fig 13: DGA visualization

Starting with the domain apex, Grandoreiro has one domain mapped to every day of the year. There are two of these mappings, one for the main C2 and one for all function-specific C2s. However, of the 732 apex domains, only 337 are unique. For the given day, the primary apex is **dnsfor[.]me** and the secondary is **neat-url[.]com**.

For the next part, Grandoreiro concatenates the seed "xretsmzrb" (the main seed) with the 2 digit formatted current month, replacing each digit with three hardcoded characters. The digits "0" and "4" are replaced with "oit" and "zia" respectively, resulting in the full string "xretsmzrboitzia".

Finally, for each day of the month, Grandoreiro has a custom character to character replacement mapping. For the 17th, after running all 26 character replacements iteratively, the final subdomain string is "wondbbhonandhnd".

After calculating the remaining domains for all hardcoded seeds, the list of C2 domains for April 17, 2024 becomes:

```
lndddkhnnndandhnd.dnsfor[.]me
bfnwnhonakdandhnd.dnsfor[.]me
noowbnwqnbdandhnd.dnsfor[.]me
kbnbnnfokddandhnd.dnsfor[.]me
annboobkbddandhnd.dnsfor[.]me
fdhbonbadwbandhnd.dnsfor[.]me
bnonbdnkbadandhnd.dnsfor[.]me
bkbbalbnbandhnd.dnsfor[.]me
nohbbdnowandhnd.dnsfor[.]me
bnkndhdabandhnd.dnsfor[.]me
bkdnbhdanandhnd.dnsfor[.]me
wondbbhonandhnd.neat-url[.]com
```

X-Force was able to confirm at least 4 of the domains did resolve on that day to Brazil-based IPs:

```
18.231.181[.]227
18.231.158[.]159
15.228.245[.]103
15.229.211[.]175
```

The C2 server's port is calculated from the first four digits of the IP address via a custom digit-to-digit mapping just like the Grandoreiro loader. See Appendix for a full list of all pre-calculated Grandoreiro domains. Note that Grandoreiro does change seeds frequently. A few weeks after the initial infection X-Force observed only the main seed C2 server staying active.

Research into X-Force DNS telemetry for early May shows current infections are mainly located in Latin America:

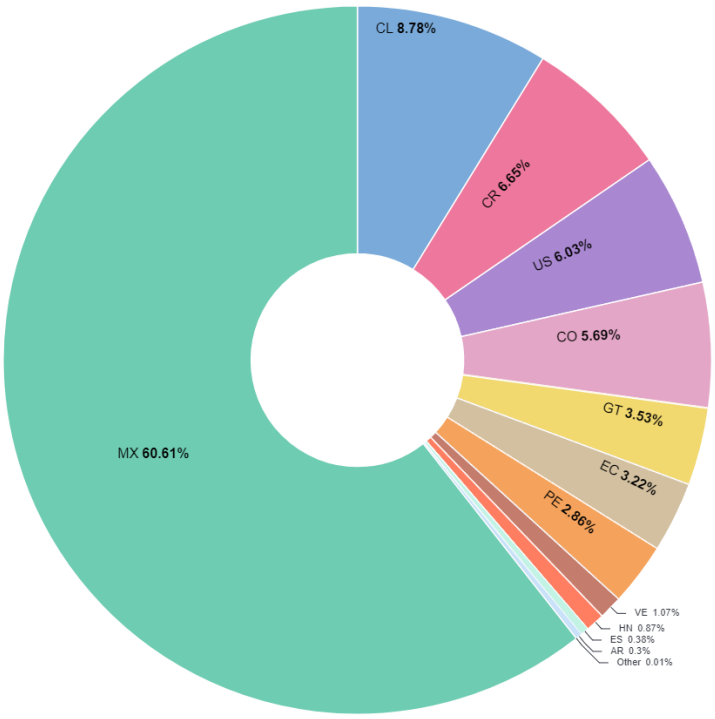


Fig 14: Infection geolocations in early May

Command and control

After attempting to resolve the calculated DGA, Grandoreiro sends one of several registration messages concatenated with enumeration data and encrypted, just like the Grandoreiro loader. The following messages may be sent based on privileges, installed AV and active C2 domains:

- CLIENT_SOLICITA_DD_FULL
- CLIENT_SOLICITA_DD_WLT_FULL
- CLIENT_SOLICITA_DD_FULL_ADMIN
- CLIENT_SOLICITA_DADOS_ARQ

Grandoreiro supports a large number of different commands, including the following:

Remote control:

- Enabling and disabling mouse input
- Sending new mouse positions or clicks, hide/show mouse
- Hide/show taskbar
- Sending new clipboards
- Simulate keyboard input (all special keys)
- Rebooting PC
- Start/stop webcam viewer
- List current windows, close/restore/maximize windows, set as foreground window, move window position
- List processes, kill processes by PID
- Start/stop keylogger
- Open browser (MS Edge, Chrome, Internet Explorer, Firefox, Opera, Brave)

Activating and deactivating modes (also possible through configuration file)

- Admin mode
- Registered mode
- Outlook sending mode (see Outlook Harvest & Spam section)
- Restart locked mode
- Always on mode
- “Good DNS exchange” mode (also internally referenced as “PK” mode). Likely to make use of a DGA seed hardcoded within the config file.
- “Caption blocking” or “thread blocking” likely to prevent users from opening new windows

File upload/download

- Receive BMP/XML file (possibly to imitate authentication windows of detected banking applications)
- Receive module update (not yet implemented)
- Execute a new .EXE file (not yet implemented)
- Enumerate host filesystem

Malware control

- Look for DLLs needed by the malware (such as MouseA.dll)
- “Cleaning” DLLs or ZIPs (downloading components again)
- Send client enumeration data
- Update country info

The malware also specifically supports opening hardcoded Banco Banorte URLs:

```
https://nixe.ixe.com.mx/NBXI/Personal/Consultas/Saldos/ResumenBEC.aspx
https://nixe.ixe.com.mx/NBXI/Personal/Consultas/Movimientos/General.aspx
https://nixe.ixe.com.mx/NBXI/Personal/Inversiones/Sociedades/VentaAcciones.aspx
https://nixe.ixe.com.mx/NBXI/Personal/Configuraciones/Catalogos/MisCuentasTerceros
.aspx
https://nixe.ixe.com.mx/NBXI/Personal/Transferencias/SPEI.aspx
```

It further allows execution of JavaScript commands in the browser to simulate HTML button clicks:

```
javascript:document.getElementById('ctl00_Contentplaceholder1_lbNuevaCuenta').click();
javascript:document.getElementById('ctl00_Contentplaceholder1_btnAceptar').click();

javascript:document.getElementById('ctl00_Contentplaceholder1_btnContinuar').click();

javascript:document.getElementById('ctl00_Contentplaceholder1_Button17').click();
```

Scroll to view full table

Due to the large number of different commands and their naming, the Grandoreiro codebase seems to contain newly added commands as well as legacy features no longer actively used. The banking trojan is likely going through frequent development cycles to add new features without much refactoring, contributing to the overall size of the codebase.

Outlook Harvest & Spam

One of Grandoreiro’s most interesting features is its capability to spread by harvesting data from Outlook and using the victim’s account to send out spam emails. There are at least 3 mechanisms implemented in Grandoreiro to harvest and exfiltrate email addresses, with each using a different DGA seed. By using the local Outlook client for spamming, Grandoreiro can spread through infected victim inboxes via email, which likely contributes to the large amount of spam volume observed from Grandoreiro.

Harvesting

For the Outlook harvesting mode, Grandoreiro switches its C2 to DGA seed 7 which is used to exfiltrate data. Logging and status messages continue to the main C2 server. For instance, before starting the harvesting process, it sends a log back containing the same victim profiling data as well as the strings “CLIENT_SOLICITA_DD_EMSOUT” (Client asks for EMSOUT data) and “COLHENDO” (harvesting).

In order to interact with the local Outlook client, Grandoreiro uses the Outlook Security Manager tool, a software used to develop Outlook add-ins. The main reason behind this is that the Outlook Object Model Guard triggers security alerts if it detects access on protected objects. Outlook Security Manager allows Grandoreiro to disable these alerts during both the harvesting and spamming behavior. Depending on system architecture, the tool requires the DLL “secman.dll” or “secman64.dll” to be registered as COM servers. It then uses MAPI to interact with Outlook.

The malware begins by locating the root mailbox folder and then recursively iterates through the email items. For each email, it checks the “SenderEmailAddress” property and runs a blocklist against it, to filter out unwanted email addresses for harvesting:

```
"noreply", "notificaciones", ".americanexpress.com", "promocion",
"atencionaclientes", "banorteporinternet@banorte.com", "banca-
empresarial@citibanamex.com", ".rsgsv.net", ".mcdlv.net", "not-reply",
".uber.com", "marketing", "Mailer-Daemon", ".mcsv.net", "linkedin.com",
"feedback", "newsletter", ".cloud.", "promociones", "Alertas@",
"estadosdecuenta@citibanamex.com", ".bmsend.com", "aforeenlinea@citibanamex.com",
"answers@", "amazon.com", "americanexpress.com", "facebookmail.com",
"atencionaclientes", "email-replies", "mail.wish.com", ".dptagent.net", "mailing",
"anti-spam", "postmaster", "customer.", "foliofiscal", "factura",
"mailcontrol.com", "getresponse", "email-alert", "no-responder", "sandbox",
"alertaid", "friendupdates", "zohoaccounts.com", "@zoom.us", "@dropbox.com",
"zaccounts.com", "smtp.info", "segurosbancomer@bbva.bancomer.com", "zohocrm.com",
"mlsend2.com", "netflix.com", "avisos@", "invoices", "sodexo.com", "dattanet.com",
"livechatinc.com", "@tickets", "@dyndns.com", "vps.ovh", "twitter.com",
"facebook", "comunicaciones@", "comunicacion@", ".ariba.com", "secureserver",
"emsend1.com", "acemsc5.com", "acemsd1.com", "antivirus", "antsspam",
"activescan", "bitdefender", "kaspersky", "mcafee", "avast", "nortonvpn",
"windowsdefender", "firewall", "Spamhaus", "Spamcop", "Exploits", "Barracuda",
"SenderScore", "abusix.zone", "black.mail", "shorthash.", "diskhash.",
"gbudb.net", "mailspike.org", "http.", ".spam.", ".spam", "junkemailfilter",
".s5h.net", "blacklist", "Blocklist", "security.", "unsubscore.com",
"nordspam.com", "fusionzero.com", "virusfree", "Bitdefender", "Adaware",
"Symantec", "tencent.", "avira.", "google@", "address-verification",
"activacion_", ".adidas.com", "@enviasms", ".alibaba.com", "AmericanExpress",
"auto-confirm", "avisos.clientes", "mandrillapp.com", "Clientes_HBMX@hsbc.com.mx",
"clientes@bbva.mx", "alwaysafreeconsultation.com", "adobesystems.com",
"HSBC_hsbc@", "HSBC_Mexico@", "community@", ".info@", "advising.service",
"hsbcnet.hsbc.com", "@costco.mx", "@whatsappweb.com", "telemarket@", "message-
service", "mejora-tu-perfil.profesional", "feedback", "instagram.com", "spammer",
"spamming"
```

Email addresses that do not contain any of the strings above are aggregated in a text file, ZIP compressed and exfiltrated.

In addition to the harvesting process above, Grandoreiro also supports adding a PST file to Outlook first via the Namespace.AddStore() function. Another supported harvesting mechanism recursively goes through the victim’s file system and scans files for email addresses. Files with the following extensions are opened and scanned:

“*.txt”, “*.csv”, “*.html”, “*.xml”, “*.dat”, “*.db”, “*.sqlite”, “*.xlsx”, “*.xls”, “*.xlsm”, “*.dbf”, “*.doc”, “*.docx”, “*.docm”

Scroll to view full table

To prevent unnecessary scanning, Grandoreiro maintains yet another blocklist of paths not to scan, excluding common system directories.

Spamming

To send out spam emails, Grandoreiro uses phishing templates which it receives from its C2 server. It then goes through the template and fills out placeholder fields such as:

- $replyto → the Reply-to value
- $link → a link to the payload
- $hora → formatted current time
- $data → formatted current date
- $email_destino → destination address
- $valor → A randomly generated float value such as “123,45.67”, likely used to create random invoice values
- $letnum_rand_branco → random string of capital letters and digits, pasted into the email HTML between white font tags “<font style=”color: white;”>”. Use unknown.
- $assunto → email subject
- $nome_saudacao → name and greeting

- $nome_empresa → company name
- $link_imagem → link to image, likely to support company logos, signatures or banners

Just before beginning to send out emails, Grandoreiro starts a thread to detect any appearing dialog boxes and click them away by sending specific TAB and SPACEBAR key presses. After sending out the emails, the malware carefully covers its tracks by deleting the sent messages from the victim's mailbox. Also, for a lot of the harvesting and spamming behavior Grandoreiro makes sure that the last input on the infected machine is at least 5min ago (or in some cases longer). The developers likely wanted to make sure victims would not notice any suspicious behavior.

During spamming, Grandoreiro reports back the following status messages:

- PRONTO ("Ready")
- EM_REPOUSO ("In rest")
- DISPARANDO ("Firing")
- ENVIO_PAUSADO ("Sending paused")
- SEM_CONTA_DISPONIVEL ("No account available")
- MAX_ERROS ("Maximum errors")

String encryption

With Grandoreiro being such an extensively large malware, it requires a huge amount of strings, which would make detection very easy if they were left unencrypted. Grandoreiro features more than 10k strings dispersed among more than a hundred feature-specific string-loading functions. The decryption mechanism differs slightly from the loader's string decryption:

It uses the same Grandoreiro key as the loader, which it decrypts via its custom encryption and the key "A". Once it has the key, it custom-decodes the encrypted string using the same encoding as the loader and then decrypts the resulting bytes via AES ECB mode using the ElAES Pascal implementation. The AES key is a scrambled version of the previously decrypted Grandoreiro key. After another round of custom decoding, the string is finally decrypted via the old Grandoreiro algorithm and the Grandoreiro key.

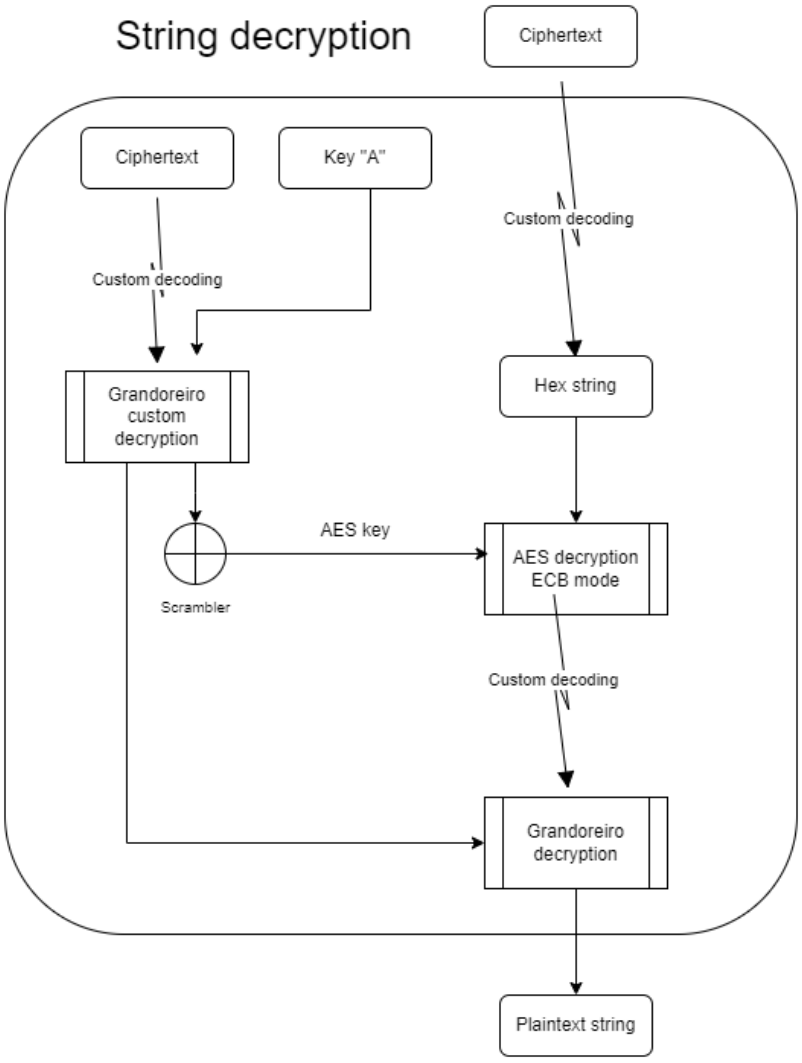


Fig 15: Grandoreiro banking trojan string decryption

Conclusion

X-Force observed several recent phishing campaigns impersonating official government entities to deliver the Grandoreiro banking trojan. Grandoreiro distributors typically target users in Latin America; however, since the latest law enforcement action against Grandoreiro operators, X-Force has observed the malware being spread outside of LATAM to include regions in Central and South America, Africa, Europe, and the Pacific. The Grandoreiro banking trojan samples that X-Force has analyzed have undergone major updates within the string decryption and DGA Calculation algorithms. These newly analyzed samples now include a vast number of at least 1500 global banking applications to target, which support execution and enable attackers to perform banking fraud in over 60 countries. The updates made to the malware, in addition to the significant increase in banking applications across several nations, indicate that the Grandoreiro distributors are seeking to conduct campaigns and deliver malware on a global scale.

We encourage organizations that may be impacted by these campaigns to review the following recommendations:

- Exercise caution with emails and PDFs prompting a file download
- Monitor network traffic for multiple consecutive requests to http://ip-api.com/json as a potential indicator of a Grandoreiro infection
- Consider blocking pre-calculated DGA domains via DNS
- Monitor registry Run keys used for persistence
    - **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run**
    - **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**
- Install and configure endpoint security software
- Update relevant network security monitoring rules
- Educate staff on the potential threats to the organization

Indicators of Compromise (IOCs)

Indicator
root@yhsp**<two digit number>**.rufnag.com
hxxps[:]//pjohconstruccionescpaz[.]com/?8205-23069071&tokenValue=92b768ccface4e96cee662517800b208f88ff796
97f3c0beef87b993be321b5af3bf748cc8e003e6e90cf5febf69dfd81e85f581
afd53240a591daf50f556ca952278cf098dbc5b6c2b16c3e46ab5a0b167afb40
f8f2c7020b2d38c806b5911acb373578cbd69612cbe7f21f172550f4b5d02fdb
10b498562aef754156e2b540754bf1ccf9a9cb62c732bf9b661746dd08c67bd1
aviso.**<four digit number>**@cfe.mx
hxxps[:]//hilcfacdigitaelpichipt[.]norwayeast[.]cloudapp.azure[.]com/?docs/pdf/15540f02-d006-4e3b-b2de-6873baff3b2a
55426bb348977496189cc6a61b711a3aadde155772a650ef17fba1f653431965
.**<four digit number>**
root@<6 alpha-numeric value>.rufnag.com
bfcd71a4095c2e81e2681aaf0239436368bc2ebddae7fdc8bb486ffc1040602c
3f920619470488b8c1fda4bb82803f72205b18b1ea31402b461a0b8fe737d6bd
84572c0de71bce332eb9fa03fd342433263ad0c4f95dd3acd86d1207fa7d23f0
hxxps[:]//pjohconstruccionescpaz[.]com?docs/xml/WCA161006TN9/15540f02-d006-4e3b-b2de-6873baff3b2a
29f19d9cd8fe38081a2fde66fb2e1eff33c4d4b5714ef5cada5cc76ec09bf2fa
hxxps[:]//onwfacttasunslahf[.]norwayeast[.]cloudapp[.]azure[.]com?_task=mail&_action=get&_mbox=INBOX&_uid=19101&_token=rbrJMXNUOQvrlaWOOxGAyj7vcufaFN3r&_part=1.2.3&_embed=1&_mimeclass=

Indicator
2ab8c3a1a7fe14a49084fbf42bbdd04d6379e6ae2c74d801616e2b9cf8c8519c
hxxps[:]//servicerevenueza[.]southeastasia[.]cloudapp.azure[.]com/?PDF-XML-71348793
root[@]zpmbnoxf[.]crazydocuments[.]com
d005abe0a29b53c5995a10ce540cc2ffbe96e7f80bf43206d4db7921b6d6aa10
70f22917ec1fa3a764e21f16d68af80b697fb9d0eb4f9cd6537393b622906908
fb3d843d35c66f76b1b1b88260ad20096e118ef44fd94137dbe394f53c1b8a46
6772d2425b5a169aca824de3ff2aac400fa64c3edd93faaabd17d9c721d996c1

hxxps[:]//officebusinessaccount[.]eastus[.]cloudapp[.]azure[.]com/?PDF-XML-<eight digit number>
hxxps[:]//servicerevenueza[.]southeastasia[.]cloudapp[.]azure[.]com/?PDF-XML-<eight digit number>
18.231.181[.]227
18.231.158[.]159
15.229.211[.]175
15.228.245[.]103

Scroll to view full table

Topic updates

Get email updates and stay ahead of the latest threats to the security landscape, thought leadership and research.
Subscribe today

Analysis and insights from hundreds of the brightest minds in the cybersecurity industry to help you prove compliance, grow business and stop threats.