ESET takes part in global operation to disrupt the Grandoreiro banking trojan

welivesecurity.com/en/eset-research/eset-takes-part-global-operation-disrupt-grandoreiro-banking-trojan/

ESET RESEARCH

ESET provided technical analysis, statistical information, known C&C servers and was able to get a glimpse of the victimology

ESET Research

30 Jan 2024 , 18 min. read

ESET has collaborated with the Federal Police of Brazil in an attempt to disrupt the Grandoreiro botnet. ESET contributed to the project by providing technical analysis, statistical information, and known command and control (C&C) server domain names and IP addresses. Due to a design flaw in Grandoreiro's network protocol, ESET researchers were also able to get a glimpse into the victimology.

ESET automated systems have processed tens of thousands of Grandoreiro samples. The domain generation algorithm (DGA) the malware has used since around October 2020 produces one main domain, and optionally several failsafe domains, per day. The DGA is the only way Grandoreiro knows how to report to a C&C server. Besides the current date, the DGA accepts static configuration as well – we have observed 105 such configurations as of this writing.

Grandoreiro's operators have abused cloud providers such as Azure and AWS to host their network infrastructure. ESET researchers provided data crucial to identifying the accounts responsible for setting up these servers. Further investigation performed by the Federal Police of Brazil led to the identification and arrest of the individuals in control of these servers. In this blogpost, we look at how we obtained the data to assist law enforcement to execute this disruption operation.

Background

Grandoreiro is one of many Latin American banking trojans. It has been active since at least 2017 and ESET researchers have been closely tracking it ever since. Grandoreiro targets Brazil and Mexico, and since 2019 Spain as well (see Figure 1). While Spain was the most targeted country between 2020 and 2022, in 2023 we observed a clear switch of focus towards Mexico and Argentina, the latter being new to Grandoreiro.

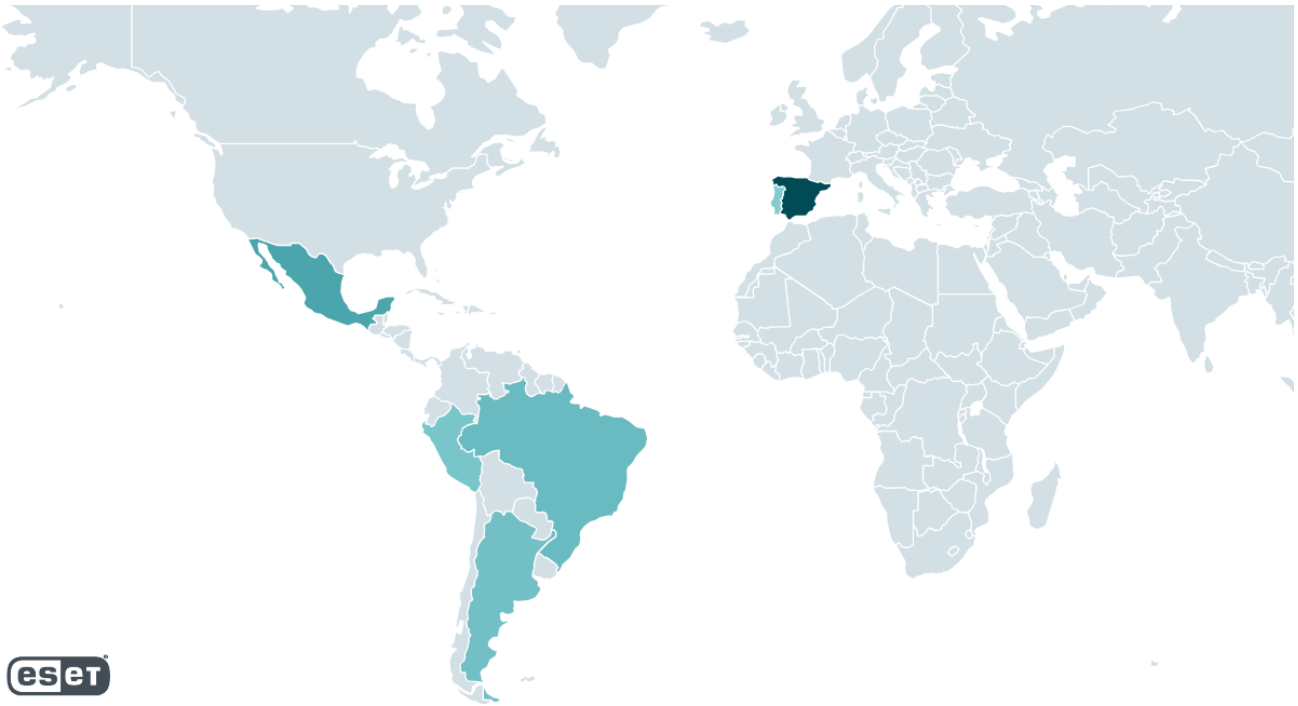


Figure 1. Grandoreiro detection rate (data since January 2020)

Functionality-wise, Grandoreiro hasn't changed very much since our last blogpost in 2020. We offer a brief overview of the malware in this section and dive into the few changes, mainly new DGA logic, later.

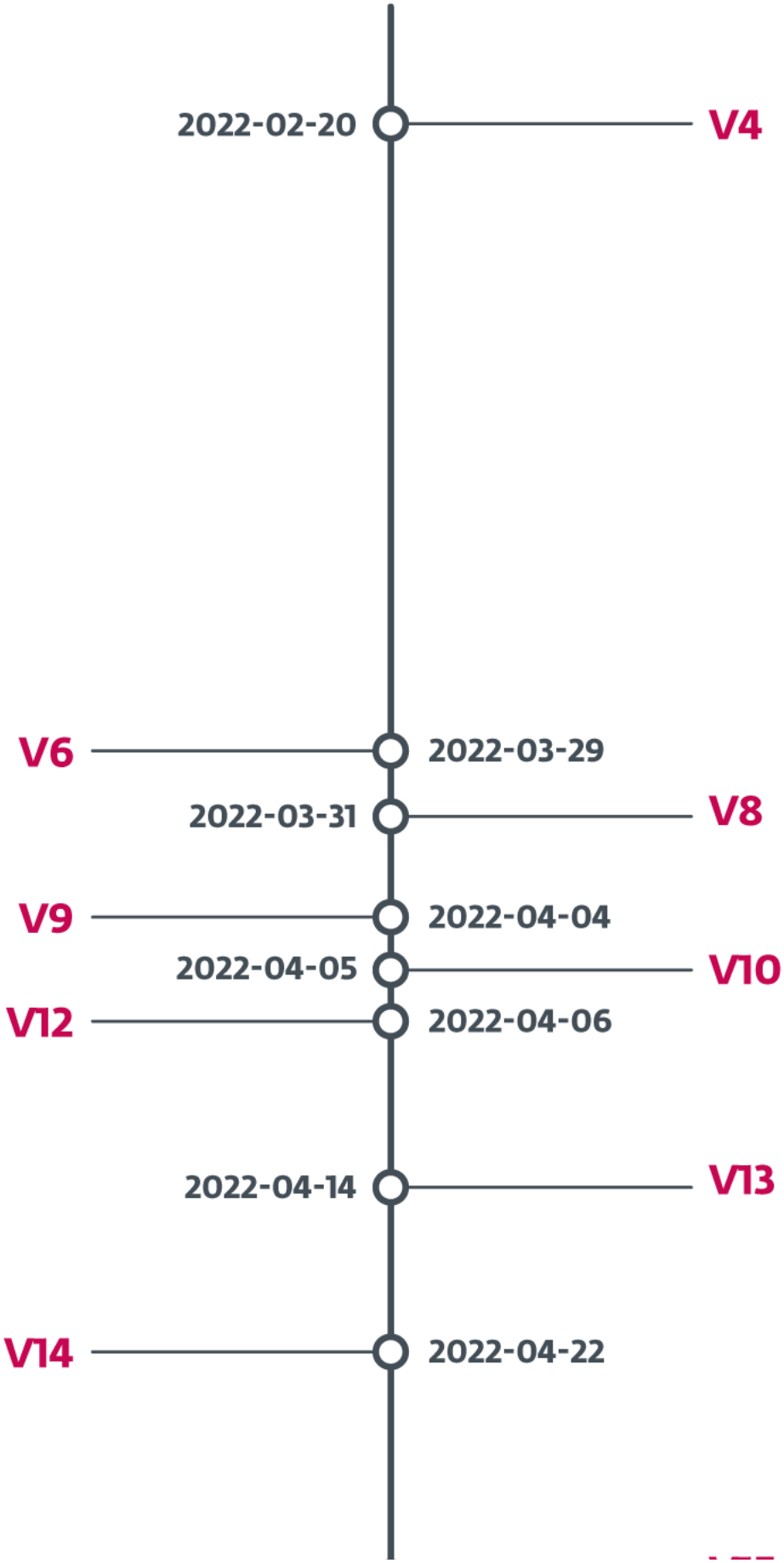
When a Latin American banking trojan successfully compromises a machine, it usually issues an HTTP GET request to a remote server, sending some basic information about the compromised machine. While older Grandoreiro builds implemented this feature, over time, the developers decided to drop it.

Grandoreiro periodically monitors the foreground window to find one that belongs to a web browser process. When such a window is found and its name matches any string from a hardcoded list of bank-related strings, then and only then the malware initiates communication with its C&C server, sending requests at least once a second until terminated.

The operator has to interact manually with the compromised machine in order to steal a victim's money. The malware allows:

- blocking the screen of the victim,
- logging keystrokes,
- simulating mouse and keyboard activity,
- sharing the victim's screen, and
- displaying fake pop-up windows.

Grandoreiro undergoes rapid and constant development. Occasionally, we even saw several new builds a week, making it difficult to keep track. To demonstrate, in February 2022, Grandoreiro's operators added a version identifier to the binaries. In Figure 2 we show how quickly the version identifier changed. On average, it was a new version every four days between February 2022 and June 2022. In the month-long gap between May 24th, 2022 and June 22nd, 2022 we continued to see new samples with progressing PE compilation times, but they lacked the version identifier. On June 27th, 2022 the version identifier changed to V37 and we haven't seen it change since then, leaving us to conclude that this feature was dropped.


2022-02-20
V4
V6
2022-03-29
2022-03-31
V8
V9
2022-04-04
2022-04-05
V10
V12
2022-04-06
2022-04-14
V13
V14
2022-04-22

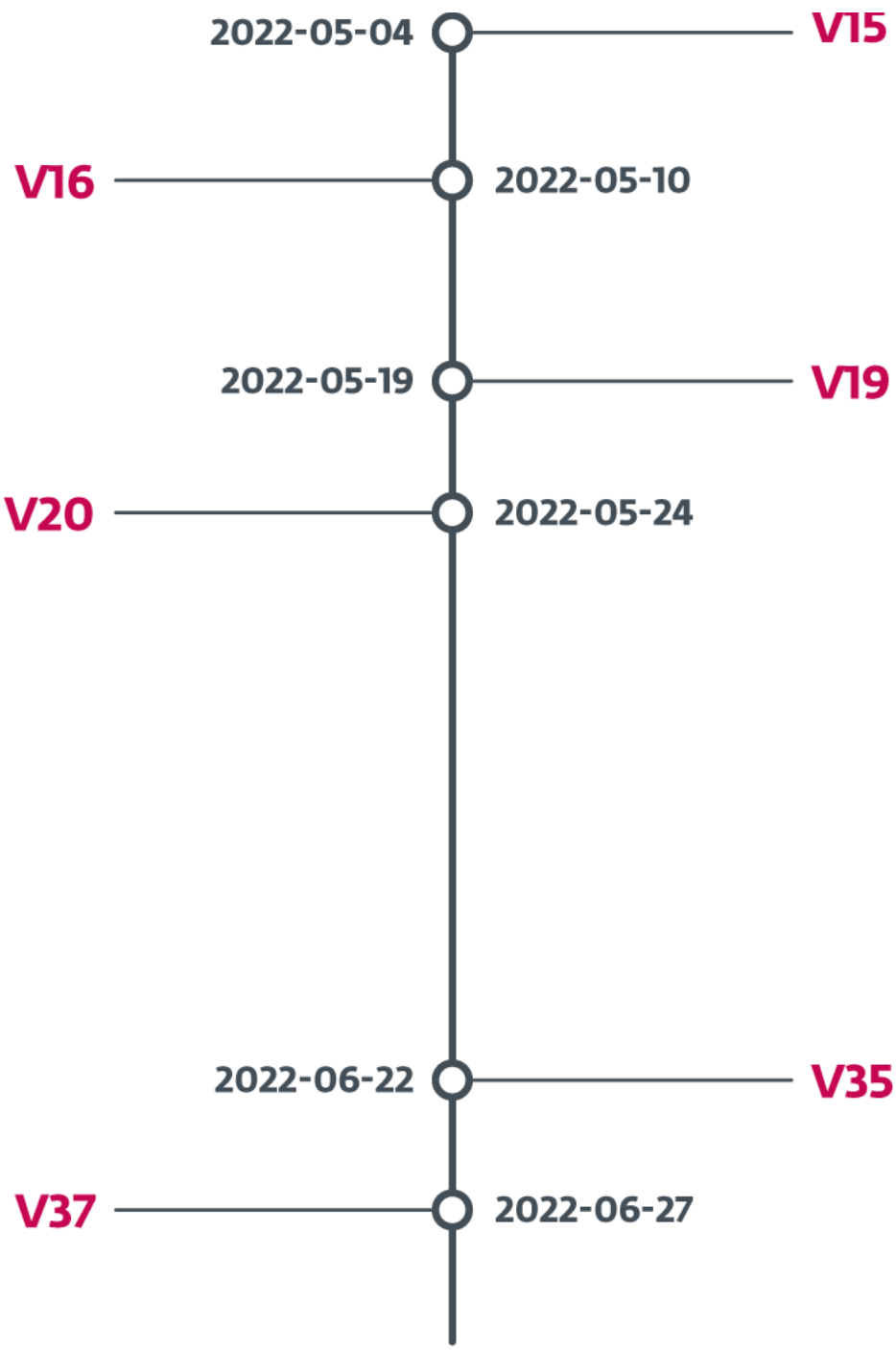


Figure 2. Grandoreiro version history between February and June 2022

Latin American banking trojans share a lot of commonalities. Grandoreiro is similar to other Latin American banking trojans mainly by the obvious core functionality and in bundling its downloaders within MSI installers. In the past, we have observed a few cases where its downloaders were shared with Mekotio and Vadokrist, though not in the last two years. The Grandoreiro banking trojan's main distinction from the other families had been its unique binary padding mechanism that massively engorges the final executable (described in our blogpost in 2020). Over time, Grandoreiro's operators added this anti-analysis technique to its downloaders as well. To our surprise, in Q3 2023, this feature was completely dropped from the banking trojan and downloader binaries and we haven't observed it since.

Since February 2022, we have been tracking a second variant of Grandoreiro that differs significantly from the main one. We saw it, in small campaigns, in March, May, and June 2022. Based on the vast majority of its C&C server domains not resolving, its core features changing quite often, and its network protocol not functioning properly, we strongly believe it is a work in progress; hence we will focus on the main variant in this blogpost.

Grandoreiro long-term tracking

ESET systems designed for automated, long-term tracking of selected malware families have been monitoring Grandoreiro since the end of 2017, extracting version information, C&C servers, targets and, since the end of 2020, DGA configurations.

DGA tracking

The DGA configuration is hardcoded in the Grandoreiro binary. Each configuration can be referred to by a string we call dga_id. Using different configurations for the DGA yields different domains. We dive deeper into the DGA mechanism later in the text.

ESET has extracted a total of 105 different dga_ids from the Grandoreiro samples known to us. 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 generated domains are registered via No-IP's Dynamic DNS service (DDNS). Grandoreiro's operators abuse the service to frequently change their domains to correspond with the DGA and to change IP addresses at will. The vast majority of the IP addresses these domains resolve to are provided by cloud providers, mainly AWS and Azure. Table 1 illustrates some statistics about IP addresses used for Grandoreiro C&C servers.

Table 1. Statistical information about Grandoreiro C&C IP addresses since we started our tracking

Information	Average	Minimum	Maximum
Number of new C&C IP addresses per day	3	1	34
Number of active C&C IP addresses per day	13	1	27
Lifespan of C&C IP address (in days)	5	1	425

Very soon after we began to track the generated domains and their associated IP addresses, we started to notice that many domains generated by DGAs with different configurations resolve to the same IP address (as illustrated in Figure 3). This means that on a given day, victims compromised by Grandoreiro samples with different dga_id all connected to the same C&C server. This phenomenon was no coincidence – we observed it almost on a daily basis during our tracking.

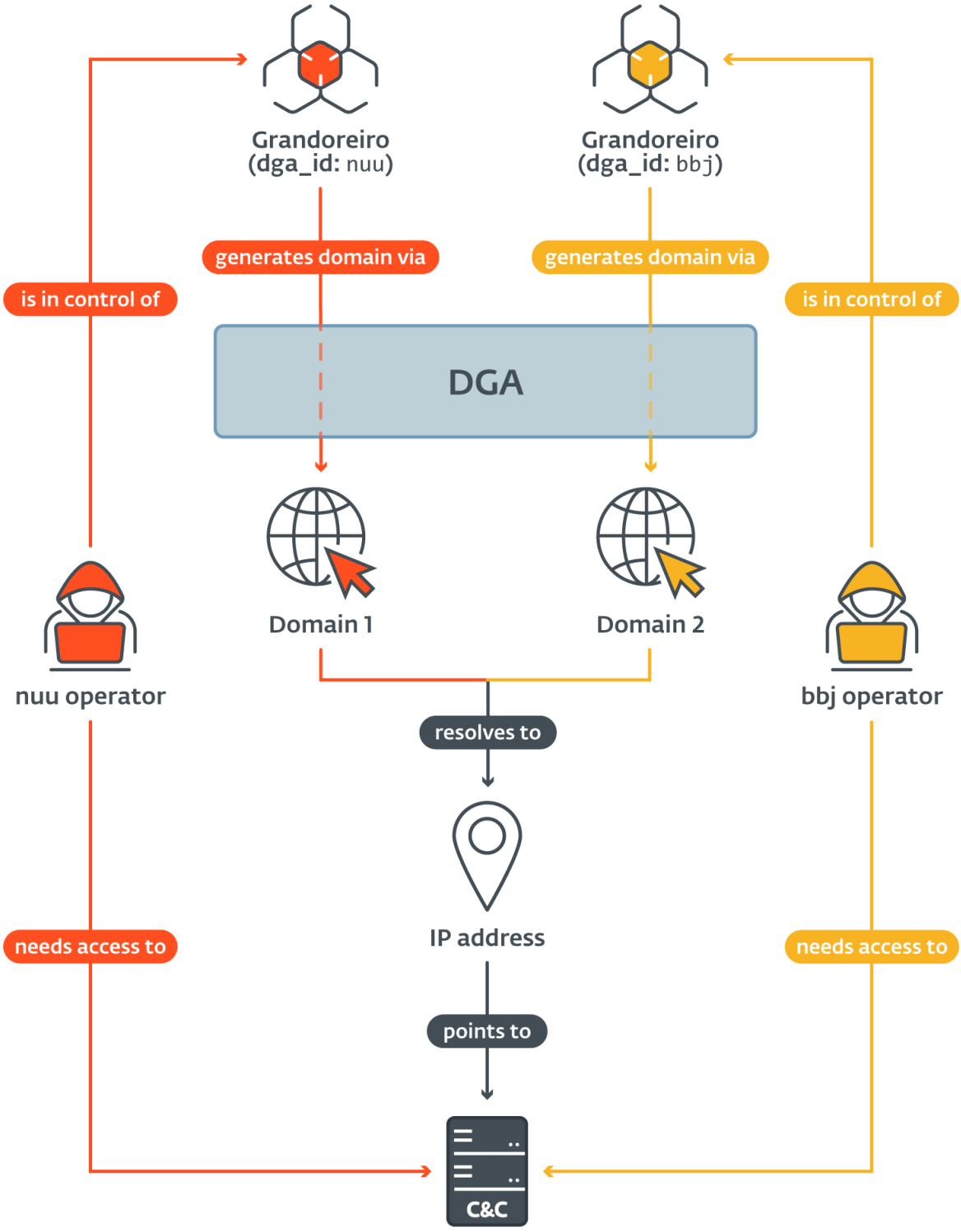


Figure 3. Schema of an IP overlap in two different Grandoreiro DGA configurations

On much rarer occasions, we have also observed an IP address being reused by a different dga_id a few days later. Only this time, the parameters Grandoreiro used to establish a connection (explained later in the text) changed as well. This means that, in the meantime, the C&C server side must have been reinstalled or reconfigured.

Our initial assumption was that the dga_id is unique for each DGA configuration. This later proved to be incorrect – we have observed two sets of different configurations sharing the same dga_id. Table 2 shows both of them, “jjk” and “gh”, where “jjk” and “jjk(2)” correspond to two different DGA configurations, same as “gh” and “gh(2)”.

Table 2 shows the clusters we were able to observe. All DGA configurations that shared at least one IP address are in the same cluster and their associated dga_ids are listed. Clusters that account for less than 1% of all victims are disregarded.

Table 2. Grandoreiro DGA clusters

Cluster ID	dga_id list	Cluster size	% of all C&C servers	% of all victims
1	b, bbh, bbj, bbn, bhg, cfb, cm, cob, cwe, dee, dnv, dvg, dzr, E, eeo, eri, ess, fhg, fox, gh, gh(2), hjo, ika, jam, jjk, jjk(2), JKM, jpy, k, kcy, kWn, md7, md9, MRx, mtb, n, Nkk, nsw, nuu, occ, p, PCV, pif, rfg, rox3, s, sdd, sdg, sop, tkk, twr, tyj, u, ur4, vfg, vgy, vki, wtt, ykl, Z, zaf, zhf	62	93.6%	94%
2	jl2, jly	2	2.4%	2.5%
3	ibr	1	0.8%	1.6%
4	JYY	1	1.6%	1.1%

The biggest cluster contains 78% of all active dga_ids. It is responsible for 93.6% of all C&C server IP addresses and 94% of all victims we've seen. The only other cluster consisting of more than 1 dga_id is cluster 2.

Some sources claim that Grandoreiro operates as malware-as-a-service (MaaS). The Grandoreiro C&C server backend does not allow simultaneous activity of more than one operator at once. Based on Table 2, the vast majority of DGA-produced IP addresses can be clustered together with no clear distribution pattern. Finally, considering the network protocol's heavy bandwidth requirements (we dive into that at the end of the blogpost), we believe that the different C&C servers are used as a primitive load-balancing system and that it is more likely that Grandoreiro is operated by a single group or by a few groups closely cooperating with one another.

C&C tracking

Grandoreiro's implementation of its network protocol allowed ESET researchers to take a peek behind the curtain and get a glimpse of the victimology. Grandoreiro C&C servers give away information about the connected victims *at the time of the initial request* to each newly connected victim. That said, the data is biased by the number of requests, their intervals, and the validity of the data provided by the C&C servers.

Each victim connected to the Grandoreiro C&C server is identified by a login_string – a string Grandoreiro constructs upon establishing the connection. Different builds use different formats and different formats contain different information. We summarize the information that can be obtained from the login_string in Table 3. The Occurrence column shows a percentage of all the formats we've seen that hold the corresponding kind of information.

Table 3. Overview of information that can be obtained from a Grandoreiro victim's login_string

Information	Occurrence	Description
Operating system	100%	OS of victim's machine.
Computer name	100%	Name of victim's machine.
Country	100%	Country that the Grandoreiro sample targets (hardcoded in the malware sample).
Version	100%	Version (version_string) of the Grandoreiro sample.
Bank codename	92%	Codename of the bank that triggered the C&C connection (assigned by Grandoreiro's developers).
Uptime	25%	Time (in hours) that the victim's machine has been running.
Screen resolution	8%	Screen resolution of the victim's main monitor.
Username	8%	Username of the victim.

Three of the fields deserve a closer explanation. Country is a string hardcoded in the Grandoreiro binary rather than information obtained via appropriate services. Therefore, it serves more like an *intended* country of the victim.

Bank codename is a string Grandoreiro's developers associated with a certain bank or other financial institution. The victim visited that bank's website, which triggered the C&C connection.

The version_string is a string identifying a specific Grandoreiro build. It is hardcoded in the malware and holds a string that identifies a specific build series, a version (which we already talked about in the introduction), and a timestamp. Table 4 illustrates the different formats and the information they hold. Notice that some of the timestamps contain only month and day, while others contain the year as well.

Table 4. List of different version_string *formats and their parsing*

Version string	Build ID	Version	Timestamp
DANILO	DANILO	N/A	N/A
(V37)(P1X)1207	P1X	V37	12/07
(MX)2006	MX	N/A	20/06
fox50.28102020	fox50	N/A	28/10/2020
MADMX(RELOAD)EMAIL2607	MADMX(RELOAD)EMAIL	N/A	26/07

One may be tempted to say that the Build ID actually identifies the operator. However, we don't think that is the case. The format of this string is very chaotic, sometimes it refers only to a month in which the binary probably was built (like (AGOSTO)2708). Additionally, we strongly believe that P1X refers to a console used by Grandoreiro operator(s) called PIXLOGGER.

C&C server tracking – findings

In this section, we focus on what we've found by querying the C&C servers. All the statistical data listed in this section has been obtained directly from Grandoreiro C&C servers, not from ESET telemetry.

Old samples are still active

Each login_string we observed contains the version_string and the vast majority of those contain the timestamp information (see Table 3 and Table 4). While a lot of them contain only day and month, as seems to be the developer's choice occassionally, the oldest communicating sample was timestamped 15/09/2020 – that is from the time this DGA was first introduced to Grandoreiro. The most recent sample was timestamped 12/23/2023.

Operating system distribution

Since all of the login_string formats contain OS information, we can paint an accurate picture of what operating systems fell victim, as illustrated in Figure 4.

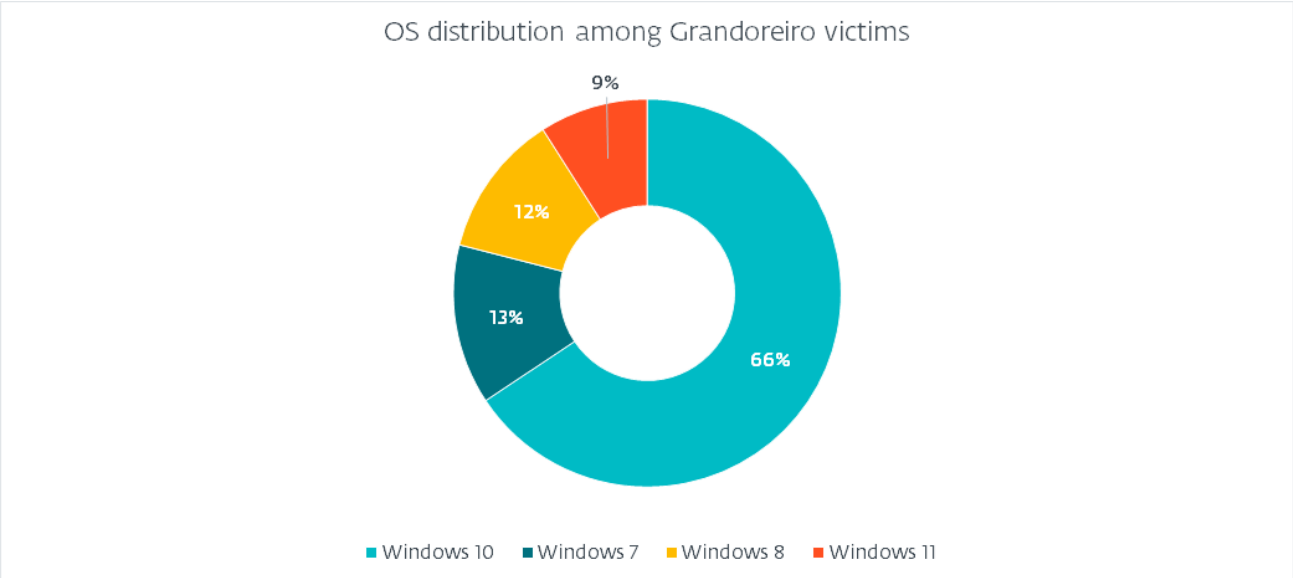


Figure 4. Operating system distribution among Grandoreiro victims

(Intended) country distribution

We already mentioned that Grandoreiro uses a hardcoded value instead of querying a service to obtain the country of the victim. Figure 5 shows the distribution that we have observed.

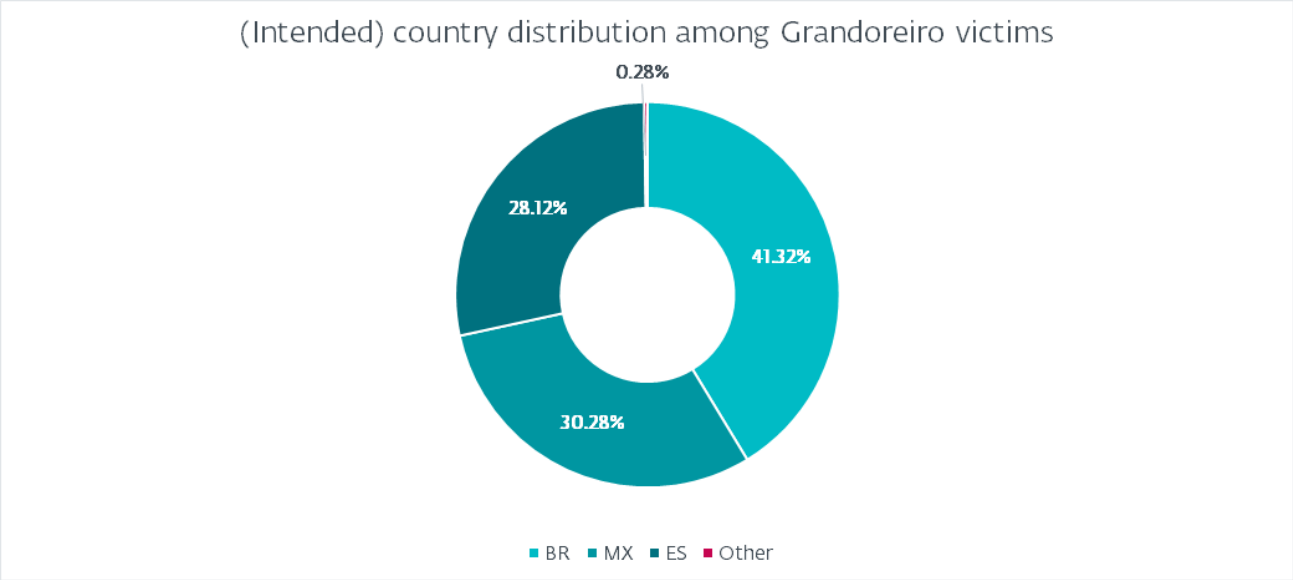


Figure 5. (Intended) country codes distribution among Grandoreiro victims

This distribution is to be expected of Grandoreiro. Interestingly, it does not correlate with the heatmap depicted in Figure 1. The most logical explanation is that the builds are not marked properly to resemble their intended targets. For example, the increase in attacks in Argentina is not reflected at all by the hardcoded marking. Brazil accounts for almost 41% of all victims, followed by Mexico with 30% and Spain with 28%. Argentina, Portugal, and Peru account for less than 1%. Interestingly, we have seen a few (fewer than 10) victims marked as PM (Saint Pierre and Miquelon), GR (Greece), or FR (France). We believe those are either typos or have other meanings rather than aiming at those countries.

Also note that while Grandoreiro added targets from many countries outside of Latin America as early as 2020, we have observed few to no campaigns targeting those countries and Figure 5 supports this.

Number of victims

We have observed that the average number of victims connected in a day is 563. However, this number certainly contains duplicates, because if a victim stays connected for a long time, which we've observed is often the case, then the Grandoreiro C&C server will report it on multiple requests.

Trying to address this issue, we defined a *unique* victim as one with a unique set of identifying characteristics (like computer name, username, etc.) while omitting those that are subject to change (like uptime). With that, we ended up with 551 *unique* victims connected in a day on average.

Taking into account that we have observed victims who were connecting to the C&C servers constantly for over a year's period, we calculated an average number of 114 *new unique* victims connecting to the C&C servers each day. We came to this number by disregarding *unique* victims that we have already observed before.

Grandoreiro internals

Let us focus, in depth, on the two most crucial features of Grandoreiro: the DGA and the network protocol.

DGA

Grandoreiro's operators have implemented several kinds of DGAs over the years, with the most recent one appearing in July 2020. While we noticed a few minor changes, the core of the algorithm hasn't change since.

The DGA utilizes a specific configuration that is hardcoded in the binary, stored as multiple strings. Figure 6 displays one such configuration (with dga_id "bbj"), reformatted in JSON for better readability.


```
{
  "base_domain": ".freedynamicdns.org",
  "base64_alpha": "ghijklmnopqrstuvwxyABCDEFGHIJKLMNOPQRSTUVWXYZabcdefz0123456789+/",
  "dga_table": [
    "bbj|1|afjq|pswb|insg|hmrw|svzj|hkpu|seva|knqe|vycm|ilqv|vydi|knqe|wafk|qthy|yblq|mqty|ehyd|zclq|beho|tfuz|ckpd|rsxc|xakp|impu|vzch|knre|dgvc|vycm|gkpt|nqtv|ains|ejov|1",
    "bbj|2|nrwi|guxc|puzj|dins|xafk|uxah|gvze|rdgz|knrg|ains|uxch|nqvc|glqv|qtxi|hybg|tfwb|bejo|ybgl|ehwd|reuz|orfw|yclq|inqv|fins|fwze|xbfk|ordu|bjmr|mpsx|aejn|uxch|psgx|2",
    "bbj|3|foub|uvzi|qdua|txbm|kpdh|vydj|pdhy|vain|psev|dgxc|dgxc|sehy|qdhy|nqdh|bkpt|adin|vydi|dgko|thwb|gvaf|fvyf|qthy|bjnt|inqe|bjnr|qtyi|rvaj|orwb|hlqv|zdhm|rfuz|wzej|3",
    "bbj|4|vcms|qthx|vafm|uycn|lqva|uzch|fins|zchm|vych|psgx|qtyi|filq|ehwb|yblq|puzk|ckpd|ckpd|nrdw|nrfw|vzcn|svak|psvc|filq|dhkp|vzdi|qeuy|imqv|ychl|seva|xain|vyin|fins|4",
    "bbj|5|mqvj|abkp|kpta|cmpf|osev|dgxc|uxcm|sxbk|hkns|vaej|sfuz|knsg|xaip|akns|ilqv|ehxd|vyb1|tyb1|adin|reva|yblq|zchm|orfw|uzcm|wbjo|fjms|wbjo|hkpu|sfva|ains|dh1q|qdhy|5",
    "bbj|6|rwbm|filq|fknu|rduz|otfw|ruxj|otyk|otfx|xblq|bjot|cmpd|psxc|rfuz|ckod|ruzj|puxc|cfkp|xcfk|uxah|ckns|uxak|knsx|ckns|svyi|vycl|ilqv|adin|xadi|wakp|bejo|vydi|orev|6",
    "bbj|7|lqew|mnrv|wafm|bglq|xafk|hxcg|thxc|qthy|akns|vybn|dilq|tfwb|uzin|cglq|uxaf|fuze|orfw|mquz|hxaf|vyci|psex|svyk|ilot|yaej|jnrf|iloe|xbls|cglr|lqth|dglq|mqty|mqtz|7",
    "bbj|8|lqdw|wzch|orwc|inqe|kpsu|seva|aimr|psva|gvyd|ilqe|lqty|hwae|ilqe|jmqu|ydgl|gjot|reuz|orwb|xbgk|mptu|fjmr|sfva|mquz|cfin|ilpe|chkq|thyd|fins|loth|wadi|rfvz|wzim|8",
    "bbj|9|ekpw|ckns|ylqf|ejms|fuze|cmpd|vzjo|mrdu|vzjn|hkpu|qduy|fins|adin|psev|nsva|hwbg|seva|twbl|lqty|uybg|yblq|jmrw|pthy|zjmr|mpuz|xafk|xbjo|jmrw|fuze|vain|fins|evyd|9",
    "bbj|10|rzjp|nsgy|pdua|xbgk|evyd|cfkp|uxah|ordu|ruxj|mpsz|aehm|fins|duzf|ruzj|behm|twbl|bejo|dglq|vydi|mqty|uydi|ehyd|ruzj|ehmr|gwbg|ajmr|sxxe|uycm|ruzj|zchm|wzej|cmpd|10",
    "bbj|11|nsgy|jnqv|cfkq|kosg|psgx|ckpd|mptu|fjmr|nrfv|dhmq|nqev|fins|qtgy|twbl|tfvb|ruyi|cgjo|fuze|ybjo|xbej|jmpf|aehm|sfua|knqv|seuy|yclq|qtxi|ycgl|tgxc|svyi|ehyd|twzj|11",
    "bbj|12|fkov|hjmt|dgls|sgva|dhkq|hkpu|chkp|xcfk|ehxc|kpdv|gwbg|evai|vbiq|cmrg|hybh|ydgl|dgxc|adh1|fins|imqv|nqva|uxcm|uxcm|nqva|knsx|knsx|xakp|yclq|cknd|mrdu|mpty|jmrw|12"
  ],
  "month_substitution": "N,S,L,W,B,K,Z,O,D,E,P,V"
}
```


Figure 6. Grandoreiro DGA configuration, reformatted in JSON

In the vast majority of cases, the base_domain field is freedynamicdns.org or zapto.org. As already mentioned, Grandoreiro utilizes No-IP for its domain registration. The base64_alpha field corresponds to the custom base64 alphabet the DGA uses. The month_substitution is used to substitute a month number for a character.

The dga_table forms the main part of the configuration. It consists of 12 strings, each with 35 fields delimited by |. The first entry of each line is the dga_id. The second and last entry represent the month the line is intended for. The remaining 32 fields each represent a value for a different day of the month (leaving at least one field unused).

The logic of the DGA is shown in Figure 7. The algorithm first selects the correct line and the correct entry from it, treating it as a four-byte key. It then formats the current date into a string and encrypts it with the key using a simple XOR. It then prepends the dga_id to the result, encodes the result using base64 with a custom alphabet, and then removes any = padding characters. The final result is the subdomain that, together with base_domain, is to be used as the C&C server for the current day. The part highlighted in red is a failsafe mechanism and we discuss it next.

```python
def dga(dt, cfg=None, cfg_backup=None):
    # choose entry from dga_table based on current month
    cfg_line_entries = cfg["dga_table"][dt.month - 1].split('|')

    # substitute month for its letter
    m = (cfg["month_substitution"].split(","))[dt.month - 1]

    # convert date into string (decimal day + substituted month + year % 10)
    dts = dt.strftime("%d") + m + str(dt.year % 10)

    # get the xor key for the day
    key = cfg_line_entries[dt.day + 1]

    # get the dga_id
    dga_id = cfg_line_entries[0]

    # xor dts with key using xor and format result as uppercase hex string
    data = ''.join('{:02X}'.format(x) for x in [ord(c) ^ ord(key[i % len(key)]) for (i, c) in enumerate(dts)])

    # prepend dga_id
    data = dga_id + data

    # base64 encode with custom alphabet and remove '='
    custom_b64_alpha = cfg["base64_alpha"]
    data = base64.b64encode(data.encode()).decode('utf-8')
    tr = data.maketrans(STD_B64_ALPHA, custom_b64_alpha)
    data = data.translate(tr).replace("=", "")

    # transform into lowercase
    subdomain = data.lower()

    # concatenate into the main C&C server address
    yield "http://" + subdomain + cfg["base_domain"]

    if cfg_backup is not None:
        # take part of the main C&C domain that will be used to generate the backups
        subdomain_part = subdomain[8:]

        # for each entry in the backup config
        for key, pfx, dom in cfg_backup:
            # xor the relevant part using the key, prepent the prefix and append the base domain
            data = pfx + ''.join('{:02X}'.format(x) for x in [ord(c) ^ ord(key[i % len(key)]) for (i, c) in enumerate(subdomain_part)])
            yield "http://" + data.lower() + dom
```

Figure 7. Grandoreiro DGA computation reimplemented in Python

Grandoreiro has implemented, in some builds, a failsafe mechanism for when the main domain fails to resolve. This mechanism is not present in all builds and its logic has changed a few times, but the basic idea is illustrated in Figure 7. It uses a configuration that is constant in the samples we analyzed and can be generated by the simple code shown in Figure 8. Each entry consists of a key, a prefix, and a base domain.

The failsafe algorithm takes a part of the main C&C subdomain. It then iterates over all configuration entries, encrypts it using XOR and prepends a prefix, similar to the main algorithm part.

```python
def generate_backup_config():
    domains = ["zapto.org", "servequake.com", "servehalflife.com", "serveconterstrike.com",
     "redirectme.net", "myftp.org", "hopto.org", "ddnsking.com", "gotdns.ch", "myftp.biz"]
    counter = 1
    for pfx in "abcdefgh":
        for dom in domains:
            yield (counter, pfx, dom)
            counter += 1
```

Figure 8. Failsafe DGA configuration generator reimplemented in Python

Since September 2022, we have started to observe samples that utilize a slightly modified DGA. The algorithm remains almost identical, but rather than base64 encoding the subdomain in the final step, a hardcoded prefix is prepended to it. Based on our tracking, this method has become the dominant one since approximately July 2023.

Network protocol

Grandoreiro utilizes RTC Portal, a set of Delphi components built on top of the RealThinClient SDK which is built on top of HTTP(S). The RTC Portal was discontinued in 2017 and its source code published on GitHub. Essentially, RTC Portal allows one or more Controls to remotely access one or more Hosts. Hosts and Controls are separated by a mediator component called Gateway.

Grandoreiro operators use a console (acting as the Control) to connect to the C&C server (acting as Gateway) and to communicate with the compromised machines (acting as Hosts). To connect to Gateway, three parameters are required: a secret key, the key length, and a login.

The secret key is used to encrypt the initial request sent to the server. Therefore, the server also needs to know the secret key so as to decrypt the initial client request.

The key length determines the length of the keys to encrypt the traffic, established during the handshake. The traffic is encrypted using a custom stream cipher. Two different keys are established – one for inbound and one for outbound traffic.

The login can be any string. The Gateway requires each connected component to have a unique login.

Grandoreiro uses two different combinations of secret key and key length values, always hardcoded in the binary, and we already discussed the login_string that is used as the login.

The RTC documentation states that it can only handle a limited number of connections at once. Considering that each connected Host needs to send at least one request per second or else its connection is dropped, we believe that the reason Grandoreiro utilizes multiple C&C servers is an attempt not to overwhelm any one of them.

Conclusion

In this blogpost, we have provided a peek behind the curtain of our long-term tracking of Grandoreiro that helped to make this disruption operation possible. We have described in depth how Grandoreiro's DGA works, how many different configurations exist simultaneously, and how we were able to spot many IP address overlaps among them.

We have also provided statistical information obtained from the C&C servers. This information provides an excellent overview of the victimology and targeting, while also allowing us to see the actual level of impact.

The disruption operation led by the Federal Police of Brazil aimed at individuals who are believed to be high up in the Grandoreiro operation hierarchy. ESET will continue to track other Latin American banking trojans while closely monitoring for any Grandoreiro activity following this disruption operation.

> For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.
> ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.

IoCs

Files

SHA-1	Filename	Detection	Description
FB32344292AB36080F2D040294F17D39F8B4F3A8	Notif.FEL.RHKVYIIPFVBCGQJPOQÃ.msi	Win32/Spy.Grandoreiro.DB	MSI downlo
08C7453BD36DE1B9E0D921D45AEF6D393659FDF5	RYCB79H7B-7DVH76Y3-67DVHC6T20-CH377DFHVO-6264704.msi	Win32/Spy.Grandoreiro.DB	MSI downlo
A99A72D323AB5911ADA7762FBC725665AE01FDF9	pcre.dll	Win32/Spy.Grandoreiro.BM	Grandoreiro
4CDF7883C8A0A83EB381E935CD95A288505AA8B8	iconv.dll	Win32/Spy.Grandoreiro.BM	Grandoreiro

Network

IP	Domain	Hosting provider	First seen	Details
20.237.166[.]161	DGA-generated	Azure	2024-01-12	C&C server.
20.120.249[.]43	DGA-generated	Azure	2024-01-16	C&C server.
52.161.154[.]239	DGA-generated	Azure	2024-01-18	C&C server.
167.114.138[.]249	DGA-generated	OVH	2024-01-02	C&C server.
66.70.160[.]251	DGA-generated	OVH	2024-01-05	C&C server.
167.114.4[.]175	DGA-generated	OVH	2024-01-09	C&C server.
18.215.238[.]53	DGA-generated	AWS	2024-01-03	C&C server.
54.219.169[.]167	DGA-generated	AWS	2024-01-09	C&C server.

IP	Domain	Hosting provider	First seen	Details
3.144.135[.]247	DGA-generated	AWS	2024-01-12	C&C server.
77.246.96[.]204	DGA-generated	VDSina	2024-01-11	C&C server.
185.228.72[.]38	DGA-generated	Master da Web	2024-01-02	C&C server.
62.84.100[.]225	N/A	VDSina	2024-01-18	Distribution server.
20.151.89[.]252	N/A	Azure	2024-01-10	Distribution server.

MITRE ATT&CK techniques

This table was built using version 14 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1587.001	Develop Capabilities: Malware	Grandoreiro developers develop their own custom downloaders.
Initial Access	T1566	Phishing	Grandoreiro spreads through phishing emails.
Execution	T1204.002	User Execution: Malicious File	Grandoreiro pressures victims to manually execute the phishing attachment.
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Grandoreiro uses the standard Autostart locations for persistence.
	T1574.001	Hijack Execution Flow: DLL Search Order Hijacking	Grandoreiro is executed by compromising the DLL search order.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	Grandoreiro is often distributed in password-protected ZIP archives.
	T1027.001	Obfuscated Files or Information: Binary Padding	Grandoreiro EXEs used to have enlarged .rsrc sections with large BMP images.
	T1218.007	System Binary Proxy Execution: Msiexec	Grandoreiro downloaders are bundled inside MSI installers.
	T1112	Modify Registry	Grandoreiro stores part of its configuration data in the Windows registry.
Discovery	T1010	Application Window Discovery	Grandoreiro discovers online banking websites based on window names.
	T1057	Process Discovery	Grandoreiro discovers security tools based on process names.
	T1518.001	Software Discovery: 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 %COMPUTERNAME% and operating system.
Collection	T1056.002	Input Capture: GUI Input Capture	Grandoreiro can display fake pop-ups and capture text typed into them.

Tactic	ID	Name	Description
	T1056.001	Input Capture: Keylogging	Grandoreiro is capable of capturing keystrokes.
	T1114.001	Email Collection: Local Email Collection	Grandoreiro's operators developed a tool to extract email addresses from Outlook.
Command and Control	T1132.002	Data Encoding: Non-Standard Encoding	Grandoreiro uses RTC, which encrypts data with a custom stream cipher.
	T1568.002	Dynamic Resolution: Domain Generation Algorithms	Grandoreiro relies solely on DGA to obtain C&C server addresses.
	T1573.001	Encrypted Channel: Symmetric Cryptography	In RTC, encryption and decryption are done using the same key.
	T1571	Non-Standard Port	Grandoreiro often uses non-standard ports for distribution.
	T1071	Application Layer Protocol	RTC is built on top of HTTP(S).
Exfiltration	T1041	Exfiltration Over C2 Channel	Grandoreiro exfiltrates data to its C&C server.
Impact	T1529	System Shutdown/Reboot	Grandoreiro can force a system reboot.