IMPERVA®

HACKER INTELLIGENCE INITIATIVE

Phishing Trip to Brazil

1. Executive Summary

In this report, we investigate in detail one specific malware campaign which illustrates the sophistication of the current cyber security threat landscape. The investigation starts with the analysis of a single Phishing email message, then analyzes the malware it delivers, and ultimately an analysis of the victim population.

We noticed that the same type of malware is used successfully a number of times by the same group or by a number of groups. This leads us to believe that the malware itself is off-the-shelf malware that can be purchased – from its creator on the dark web – and then used by lower skilled criminal groups that actually run the campaigns using the malware.

We were able to access multiple command and control servers. This was a rare opportunity to get a "behind the scenes" look at the malware industry. From these servers we were able to extract a lot of interesting data about the hackers and their victims. We analyzed over a dozen victims lists collected from 14 different command and control servers. The total number of records we collected amounted to 10,848. These represent 4,984 different IP addresses.

Although the malware is designed to compromise consumers, it can easily be repurposed to compromise enterprises. Analysis of the command and control (C&C) servers explicitly showed that at least 17 percent of observed victims are bound to enterprise networks.

This reveals the danger that "consumer-centric" malware and campaigns pose to enterprise security. Opportunistic hackers reviewing the command and control logs may quickly identify infected computers on corporate networks. Then, depending upon their sophistication, they may either pivot and use the malware to compromise enterprise data, or simply "sell" access to the enterprise on dark nets or other cyber crime marketplaces.

Current endpoint security postures allow even simple campaigns like the one we analyzed to run undetected over a long period of time – more than a year in some cases. When simple adjustments are made to the campaign, such as language adaptation, it becomes noticeably more successful within a target population.

All the preceding arguments illustrate how cyber crime has morphed into an industry. Through this "industrialization", experts in creating malware can sell their goods to multiple experts in running and monetizing Phishing campaigns – allowing even "low tech" criminal groups to profitably run cyber-crime businesses and monetize in multiple ways.

The Brazilian-originated malware campaign underscores how:

- Infection campaigns remain successful despite existing endpoint security measures
- Malware campaigns are successful (in terms of number of infections)
- Enterprise data security can be compromised by personal behavior and malware initially targeting consumers

2. Introduction

When one thinks about Brazil, a picture of white sandy beaches, colorful carnival, and great soccer comes to mind. What most people don't know is that Brazil is a well-known producer (and target of) banking Trojans, more commonly known as "bankers". Bankers usually infect victims in order to collect credentials for banking websites. The attackers can later use these credentials to perform transactions or simply sell them to a third party.

Recently we have observed several "bankers" originating from Brazil, which have many similarities. This report is focused on two of these bankers which we named *Comprovante-Abril* and *Comprovante_de_Transferencia*. These malwares are designed to infect the customers of major Brazilian banks.

The malwares rely on social engineering to infect a victim. An email is sent to the victim containing a link to a ZIP file. Once the victim extracts the file and clicks the executable (accidently or because he thinks it is not an executable), the targeted victim is infected. The email messages are specially crafted to look like they were sent by legitimate companies with finance related content. The malware then starts to monitor user activity. Once the user connects to a Brazilian banking site, it intercepts session data, and sends it to the cybercriminals.

During our research, we managed to find and access many of the bankers' C&C servers. This was a rare opportunity to get a "behind the scenes" look at the malware industry. From these servers, we were able to extract a lot of interesting data about the hackers and their victims such as geo-locations, infected industries, number of campaigns, and much more. The majority of our report will focus on the information retrieved from the C&C servers. We also analyzed the malware behavior on the endpoint itself.

3. Getting Infected

As with many infection campaigns, the one we describe in this report starts with Phishing. We've already mentioned in a previous blog post that modern Phishing campaigns are sometimes mistakenly considered Spear Phishing while being mostly indiscriminant.

The email messages that sparked our interest in this story are pasted here. These were clearly distributed in large quantities and ended up in the mailbox of many individuals who didn't even bother to give them a second look before deleting them altogether. However, the language (Portuguese), subject line and simple text are adapted to appeal to a relatively large population that forms the true target of this campaign: customers of Brazilian banks.

The subject line reads "Annex to the transfer voucher." The text approximately translates to "Sorry for the additional delay, only now we managed to make the transfer. The transfer voucher follows in the attached message. I'm available for any question." Even for people who do not recall making any recent online transfer or expecting an incoming transfer, it makes sense to open the attachment and see what this message is all about (assuming that they are not your average paranoid).

Figure 1: Sample Phishing email

4. High Level Malware Analysis

In this section, we will describe our analysis of the infection chain and the malware itself. In the figure below, we depict the entire infection process which starts by downloading a compressed archive, linked from the email message.

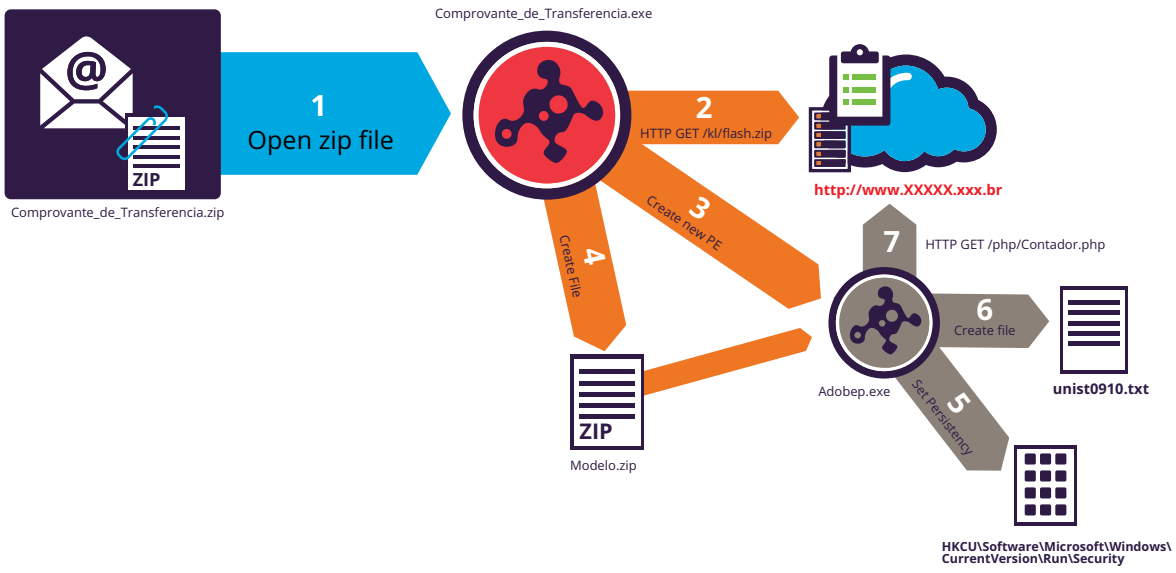


Figure 2: Infection chain

4.1 Downloader executable

Step 1 in the above figure shows the initial infection process. The name chosen for the archive and the executable it contains are in line with the theme of the message ("Comprovante de Transferencia" which means "Proof of transfer"). Thus, it can be expected that the unsuspecting user would double click and execute it.

The *Comprovante* executable is written with Borland Delphi 4.0. The Brazilian malwares are often written with Delphi, and for that reason, many anti-virus companies categorized them as "Delf Trojans". *Comprovante* has anti-sandbox capabilities and runs only on physical machines. When attempting to run samples on a virtual machine, the following message pops up:

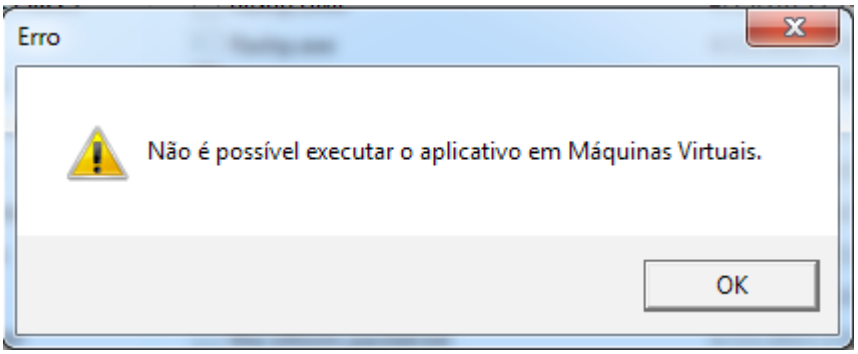


Figure 3: "You cannot run the application on virtual machines."

Steps 2-4 describe downloading of another malicious payload and the setup of auxiliary files, as *Comprovante* is a **generic** downloader. Thus, the same type of Phishing campaign can be used for distributing other types of malware, such as Key Loggers and RATs (Remote Access Trojan) – quickly shifting from a consumer focused campaign to an enterprise targeting campaign.

In Step 2, it downloads a compressed, password protected archive from an attacker controlled server, using the HTTP protocol. From this archive, in Step 3, *Comprovante* is extracting a new executable and starts it. In addition, in Step 4, the downloader generates a small compressed archive ("Modelo.zip") in a preset location ("*AppData\Roaming* directory"), which is probably used as an indicator that the computer is already infected (and avoid double infection in the future).

4.2 Banker executable

The new executable is given a misleading name like "*adobep*" and "*flashp*" which would probably be skipped and go unnoticed by most individuals. The executable is packed (wrapped) using a tool called VMProtect. This type of wrapping makes it extremely difficult for a researcher to perform static (code) analysis. VMProtect modifies the content of a binary executable file in such a way that it is extremely difficult to recover its original content. It does this by converting x86 code to a proprietary byte code. When the protected file is executed, VMProtect creates a virtual machine (VM) manager that reads the byte code and executes one instruction after another. In order to overcome this limitation we were compelled to use a dynamic, black box, analysis approach to discover the malware's functionality.

The first stage of execution of the 'banker' executable is to establish persistency by setting its path in the Windows registry under (Step 5): *HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Security*, which makes the malware start at system boot. Afterwards, in Step 6, the malware creates as small text file, called *unist0910.txt*, to be used as an indicator of infection (sometimes referred to as "mutex"). This file is located in the "%temp%" directory. The file's unique name has allowed us to find more samples of the malware in the wild and expand the research.

4.3 Registration to C&C server

Step 7 of the infection flow shows registration of the infected machine with the C&C server. Registration is done over HTTP protocol through a module called *contador.php*. The *contador.php* module adds the public IP of the infected machine to an infected machines list which is stored in *contador.txt* file on the C&C server file system. We became aware of the *contador.txt* file through a directory listing

vulnerability in the server that hosted the C&C. It allowed us to get acquainted with the general structure of C&C server, and the names of the modules and files from which it is comprised.

4.4 Ongoing malware activity

Once the malware registers to its C&C server, it waits until a user connects to one of the Brazilian banking sites.

The malware monitors online banking activity, intercepts session data, and sends the collected information to drop servers (notice that drop servers are different than C&C servers) for the cybercriminals to take advantage of. The data is sent using a raw textual protocol over TCP port 63459 to several drop servers that are located in Brazil and the USA.

Here is an example of some of protocol messages containing the collected information:

```
Malware: <|PRINCIPAL|>
C&C: <|OK|>
Malware: <|Tapa|>BRADESCO<|><|Navi|>Chrome<|><|Tapa|>BRADESCO<|>
<|Navi|>Chrome<|>
C&C: <|SocketMain|>3540624<<|
Malware: <|Info|>MY-PC<|>Windows 7 Professional<|>2.9<<|<|Tapa|>BRADESCO<|><|Navi|>Chrome<|>
Malware: <|Tapa|>BRADESCO<|>
Malware: <|Navi|>Chrome<|>
Malware: <|Tapa|>BRADESCO<|><|Navi|>Chrome<|>
C&C: <|PING|>
Malware: <|PONG|>
C&C: <|PING|>
Malware: <|PONG|>
Where the tags meaning is:
<|PRINCIPAL|> - Message header
<|Tapa|> - The bank's name
<|Navi|> - The browser used for the connection
<|Info|> - Contains infected machines computer name and OS type
<|PING|>;<|PONG|>- is a keep alive mechanism
```

5. Expanding the Research

5.1 Obtaining more data

We began our research with two emails that were sent from different origins but contained a very similar message. The samples obtained through these emails had similar (and distinctive) functionality and characteristics. For example, they both use the *unist0910.txt* file as a mutex, and they both register the victim machine's IP through a *contador.php* module on the C&C server. The aforementioned identifiers helped us expand our research and find additional samples of the same malware family and their associated C&C servers.

We used the following repositories to obtain additional samples: https://malwr.com, https://www.hybrid-analysis.com and https://www.virustotal.com. Using the new samples, we found we were able to identify more than twenty unique C&C servers, 13 of which were still active.

Additionally, we found out that C&C servers were installed on web servers vulnerable to directory listing. Thus, we were able to obtain a full list of the files that comprise the C&C server. We used this information to further look for instances of C&C servers through Google searches. This provided us with even more data to analyze.

Figure 4: Directory listing of a C&C server

5.2 Peeking into the C&C server

The C&C is comprised of text files that store information (e.g., upt.txt, atualiza.txt, Contador.txt) and PHP modules that process them (e.g., ver.php, contador.php). We tested the various modules and looked at the text files.

As mentioned earlier, the *contador.php* module adds a record to the *Contador.txt* file. Much the same way, *atualiza.php* adds a record to the *atualiza.txt* file. The Ver.php module displays a list of infected machines registered to this C&C server.

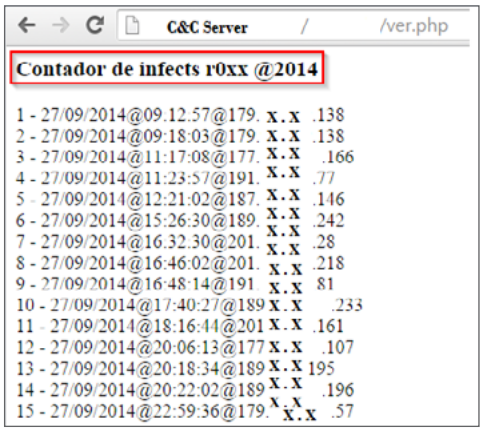


Figure 5: Output of "ver.php"

Interestingly enough, the display starts with an identification of the gang that operates the C&C. Thus, in the example above, we assume that '*r0xx*' is the name by which the gang identifies itself online. Additional information includes time and day of infection, and the source IP address of the victim.

In one of the servers, we found a text file ("auto.txt") referencing a new version of the malware for download. Hence, we assume that the malware has some sort of automatic update mechanism.

6. Analysis of the data

The information displayed by the *ver.php* module is taken from the *Contador.txt* file which contains the IP address and time of infection for each registered victim. We collected the information from all C&C servers we were able to access and used it for our analysis.

We used a number of online services in order to enrich the information we have on victim machines to include geolocation, internet service provider (ISP), and often the organization of the infected machine.

6.1 How many victims?

We analyzed **14** *contador.txt* lists collected from **13** different C&C servers (in one server we found two separate folders holding C&C files). The total number of records we collected amounts to **10,848** and represent **4,984** different IP addresses.

For our initial analysis, we split the IP addresses between those that have a single appearance in our data set and those that have multiple appearances. We assume that the first group represent actual victims, while the second group represents security research groups (see our analysis in Spotting out researchers).

IP ADDRESSES	SUMMARY
Victims	4401
Researchers	493
Total number of IP addresses	**4894**

Figure 6: IP address count

RECORDS	SUMMARY
Victims' records	4401
Researchers' records	6447
Total number of records	**10848**

Figure 7: Appearance of IP addresses in the data set

It immediately pops out from these two tables that 2/3 (two thirds) of the records were generated by the small group of IP addresses (~10% of all IPs) that we tagged as "research groups".

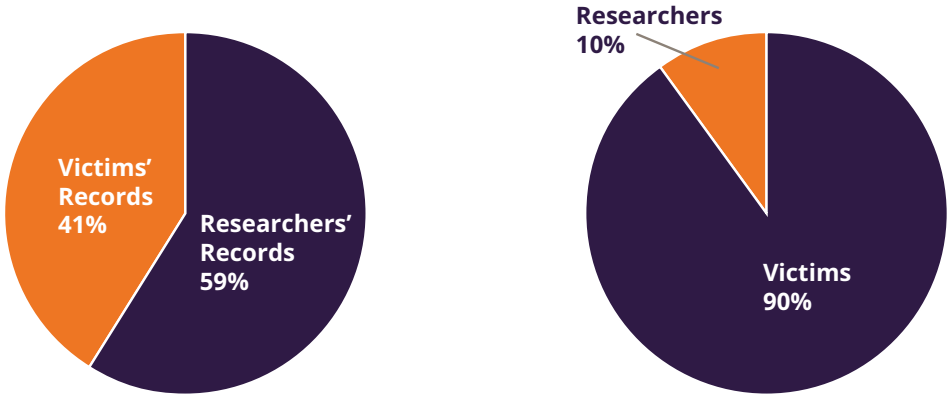


Figure 8: Contribution of Victims and Researchers to our data set

6.2 Who's behind it all?

Once we looked at our data, it became apparent that there is not one group operating behind the scenes. It appears that there are several groups of criminals, each with different technical skills (or at least a tendency towards a different attitude).

Some of the C&C servers were found on legitimate websites that had been hijacked, while others were found on servers that were set up specifically to provide C&C functionality.

Setting up a web server such as Apache or IIS typically requires basic technical skills, while hijacking websites may require more sophistication and experience. Some C&C servers are located on Web Hosting servers. In this case, the criminals use a basic web page and small-scale file hosting, where files can be uploaded easily via File Transfer Protocol (FTP) or a web interface.

Figure 9: C&C servers set up by the attacker versus hijacked legitimate sites

The cybercriminals use different operating systems and web servers. Most of the C&C servers run on a Linux distribution such as CentOS, Ubuntu, and RHEL 6 and use Apache HTTP Server.

At the time of writing this report, 7 out of 13 C&C servers are still available.

The following table contains information about C&C servers:

C&C	country	dedicated server	web server	os details	identifier (ver. php)
C&C 1	USA	Yes	Apache/2.2.3	CentOS	–
C&C 2	USA	No	Apache/2.2.9	Linux 2.6.32	–
C&C 3	Brazil	Yes	Apache/2.2.3 Locaweb (Web Hosting)	Linux 2.6.32	eCoLoGy
C&C 4	Brazil	Yes	Apache/2.2.15 (CentOS)	Linux 2.6.32	–
C&C 5	Brazil	Yes	Apache	–	–
C&C 6	Hong Kong	No	Apache/2.2.22	Ubuntu	–
C&C 7	USA	Yes	MS-wbt-Server	–	–
C&C 8	Singapore	No	IIS	Microsoft Windows Server 2003	–
C&C 9	USA	Yes	Apache/2.2.24 (Unix)	Linux 2.6.32	sysv
C&C 10	USA	Yes	Apache/2.2.24 (Unix)	Linux 2.6.32	sysv
C&C 11	Czech Republic	No	Apache/2.2.29 (FOPSI)	Linux 2.6.32	sysv
C&C 12	Romania	Yes	LiteSpeed Web Server		–
C&C 13	USA	Yes	Apache Hospedagem (Web Hosting)	Linux 2.6.32	–
C&C 13'	USA	Yes	Apache Hospedagem (Web Hosting)	Linux 2.6.32	r0xx

Figure 10: C&C servers' information

Another difference is the number of records per C&C. Some C&C servers have lists that contain hundreds (or even thousands) of records, while others contain only tens. We assume the successful C&C servers are managed by cybercriminal rings with more experience in setting up an effective spam/phishing campaigns.

This also points to industrialization, whereas the malware provided by one group is used by several different business units with differing levels of success.

The following table summarizes records information for each C&C and time of operation (a delta between first and last entry):

C&C	# records	# victim records	time of operation (days)
C&C 1	1375	695	32
C&C 2	93	91	9
C&C 3	184	60	209
C&C 4	33	27	225
C&C 5	730	710	No timestamp data
C&C 6	1331	1154	120
C&C 7	733	176	27
C&C 8	1390	119	7
C&C 9	67	36	13
C&C 10	23	18	2
C&C 11	3109	429	12
C&C 12	976	461	231
C&C 13	397	240	198

Figure 11: C&C records and time of operation

C&C servers differ substantially in the number of entries they have, as well as in time of operation:

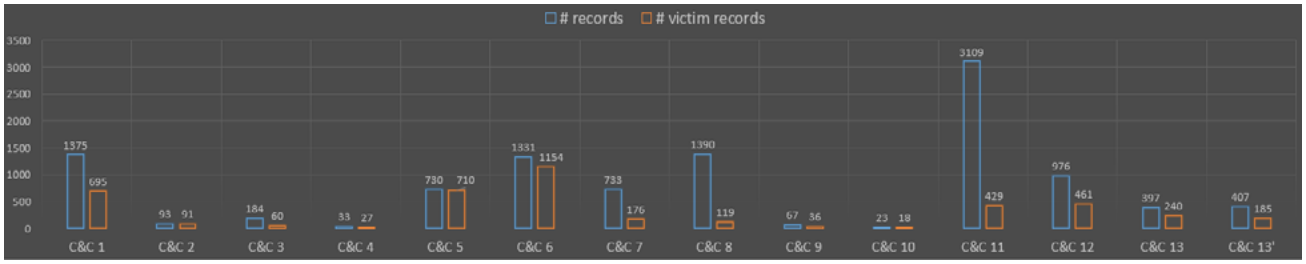


Figure 12: Records per C&C server

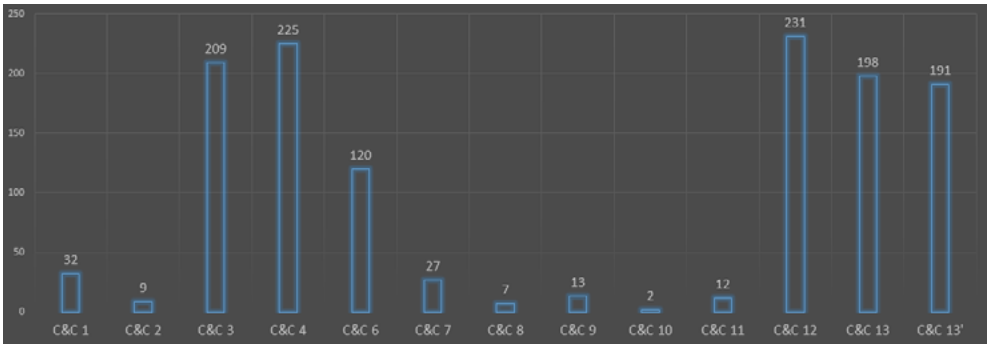


Figure 13: C&C time of operation

There is a significant difference in the average number of victims' record between dedicated servers and compromised servers:

	Dedicated Servers	Compromised Servers
Average # victim records	260.8	448.25

Figure 14: Average number of victims' records

Another difference is the average life span between dedicated servers and compromised servers. As expected, the life span of dedicated servers is much longer than of compromised servers:

	Dedicated Servers	Compromised Servers
Average time of operation (days)	125.33	37

Figure 15: Average life span (days)

As mentioned earlier, the emails we started from were adapted to Portuguese and the malware samples we inspected are targeted at Brazilian banks. It was therefore very interesting for us to check the geo aspects of this campaign. We started by looking at the geographic distribution of the C&C servers. Six of the C&C servers are located in the United States, three in Brazil, and others in Hong Kong, Singapore, Czech Republic, and Romania. As expected, there is no direct correlation between the location of C&C servers and the target geography of the malware.

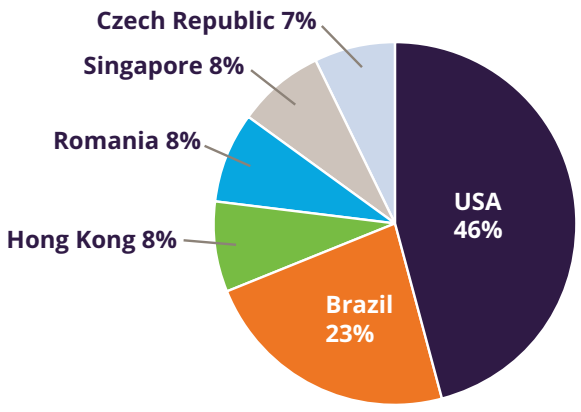


Figure 16: Geographic distribution of C&C servers

Figure 17: Geographic distribution of C&C servers (map)

6.3 Infection Campaigns

Some of the C&C servers were active over a long period of time. We noticed that the number of new victim machines fluctuates over time in a way that probably corresponds to individual infection campaigns. We therefore identified peaks on the infections timeline figures, and referred to infections between start and end of the peak as a single campaign. The following table shows the detailed campaign data we collected.

C&C	Campaign length (days	Number of Infections
C&C 1	3	81
C&C 1	2	32
C&C 1	4	156
C&C 1	5	244
C&C 1	3	98
C&C 1	3	70
C&C 1	3	18
C&C 2	2	83
C&C 3	3	31
C&C 3	2	7
C&C 3	1	5
C&C 3	1	5
C&C 4	1	3
C&C 4	2	3
C&C 4	2	3
C&C 5	No timestamp data	
C&C 6	4	571
C&C 6	6	522

C&C	Campaign length (days	Number of Infections
C&C 7	4	43
C&C 7	4	40
C&C 7	3	25
C&C 7	4	33
C&C 7	3	15
C&C 7	4	12
C&C 8	4	107
C&C 9	4	24
C&C 10	2	18
C&C 11	4	167
C&C 11	4	241
C&C 12	3	331
C&C 12	2	22
C&C 12	5	31
C&C 12	1	6
C&C 13	2	47
C&C 13	4	151
C&C 13’	5	143

Figure 18: Individual campaign data

Some general statistics on campaigns’ data:

Campaign general statistics	
Average duration (days)	3.11
Average number of infections	95.94
Max duration (days)	6
Max number of infections	571

Figure 19: General statistics on campaigns

The following figure shows number of campaigns per C&C server. Overall, we identified 36 campaigns:

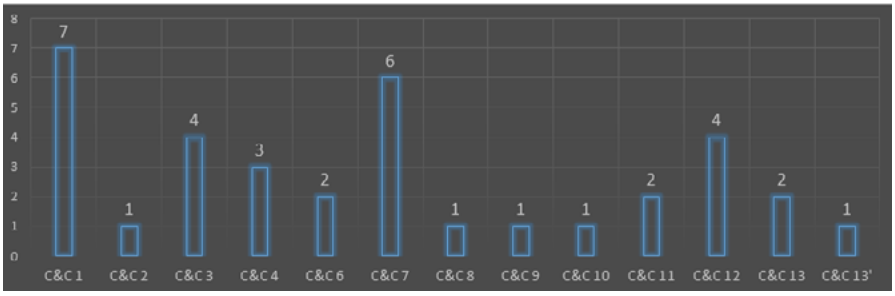
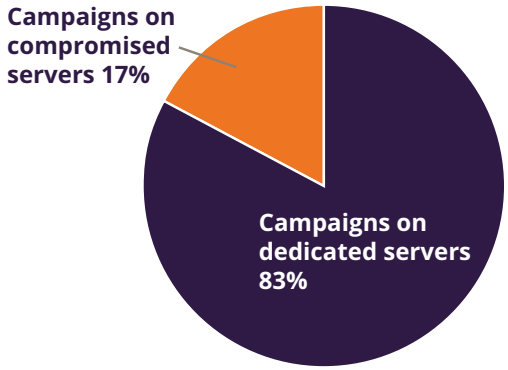


Figure 20: Campaigns per C&C server

Most of the campaigns (30 out of 36), were carried out on dedicated servers:

Figure 21: Campaigns on dedicated servers versus campaigns on compromised servers



The duration of the infection period is influenced by several parameters: the C&C lifetime, duration of spam campaigns and our timing of C&C disclosure. Some of the cybercriminals limit the timeframe the malware stores a *contador.txt* list to keep track of the most recently infected machines.

An interesting fact is that four different C&C have **only one infection in first day** of infection period. We assume the meaning of this behavior is a testing of the registration mechanism by the cybercriminals.

By spreading across multiple unrelated C&C servers, malware can remain operational for long periods of times. The following figure describes correlation of the campaign time in the calendar:

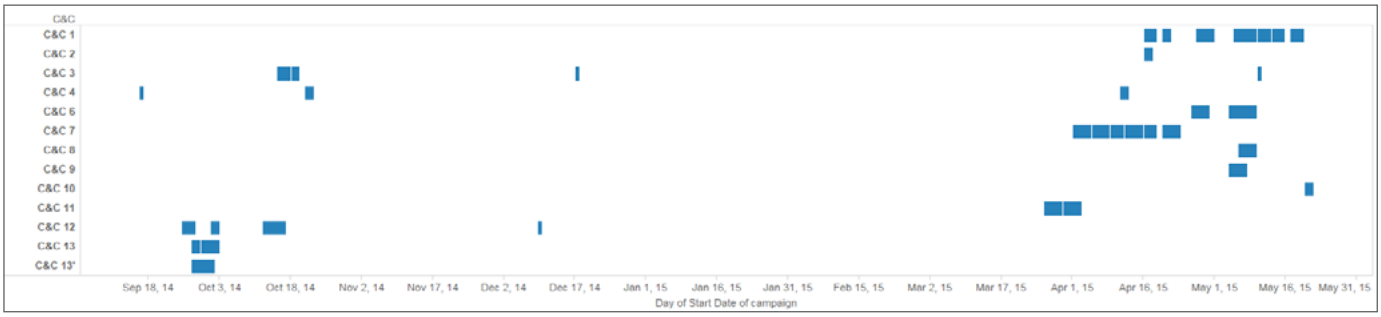


Figure 22: Correlation of the campaign time in the calendar

According to the above figure, most of the campaigns were active between September and October, 2014 and between April and May, 2015.

By analyzing the dates of individual campaigns across the different C&C servers, we see that various cybercriminal gangs started using this malware around September 2014 and have been using it ever since. 25 percent of all infections took place in 2014, and the rest in 2015.

It is important to note that campaigns data is a subset of all infections data. Thus, the campaigns on figure 22 are not consecutive.

The following area chart shows infections trend over the full time period and based on complete infections data. According to this figure, the peak of infections was in April 2015.

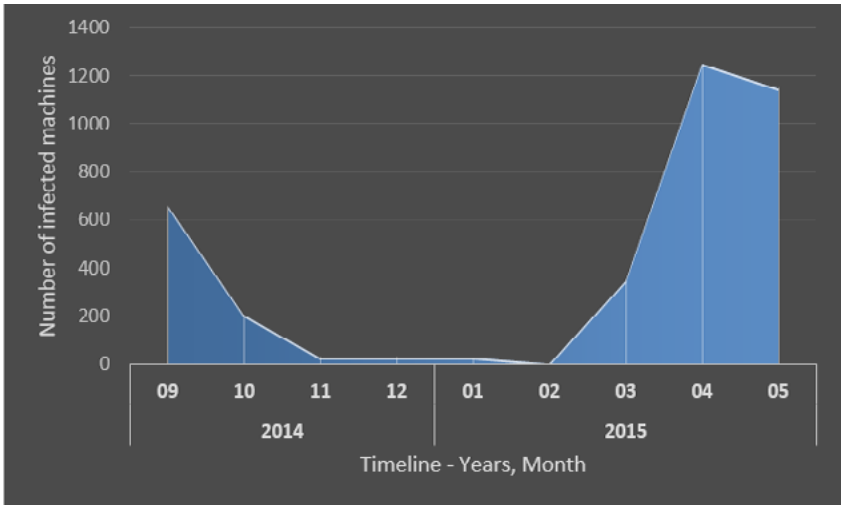


Figure 23: Infection trend 2014-2015

6.4 Implications for Enterprise

Analyzing the timestamps of individual infections (as reflected in the C&C server log) reveals interesting results. Prior to analyzing the data, we normalized the timestamps according to the local time zone, based on the IP address of the victim's machine. What we found out was that 74 percent of infections took place during work hours (07:00–19:00, victim's local time). These are the times we expect people to read emails and therefore are more likely to be infected. The following figure shows number of infections on a timeline – grouped by 6 hours range and 4 hours range.

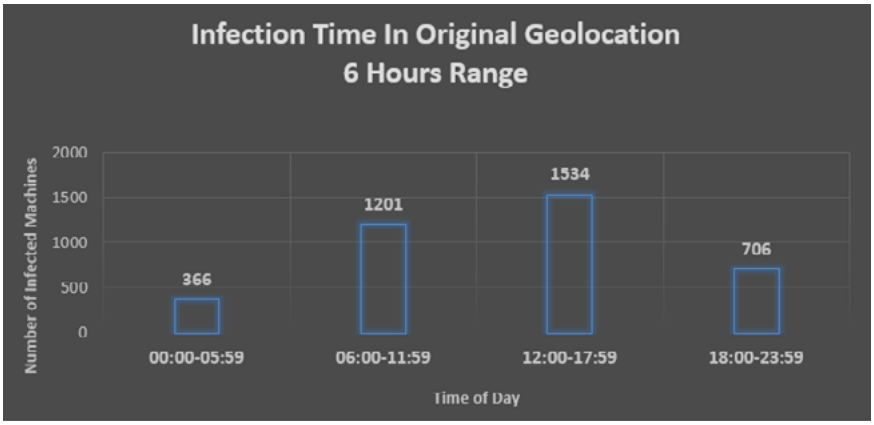


Figure 24: Infection time – 6 hour window

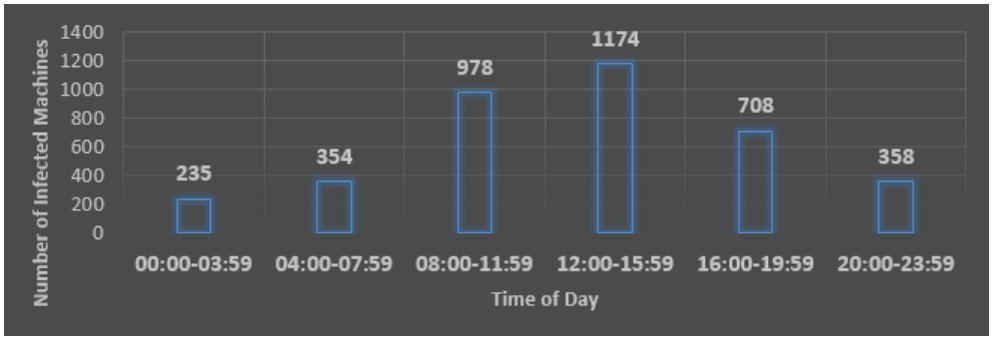


Figure 25: Infection time – 4 hour window

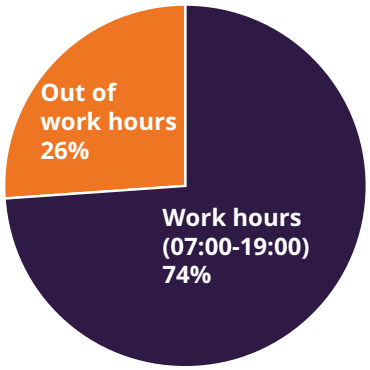


Figure 26: Infection time within / outside work hours

The malware originates from Brazil and targets Brazilian banks, so it was no surprise that most of its victims – 88 percent of the infected machines – are located in Brazil. The following figure shows geolocation of infected machines:

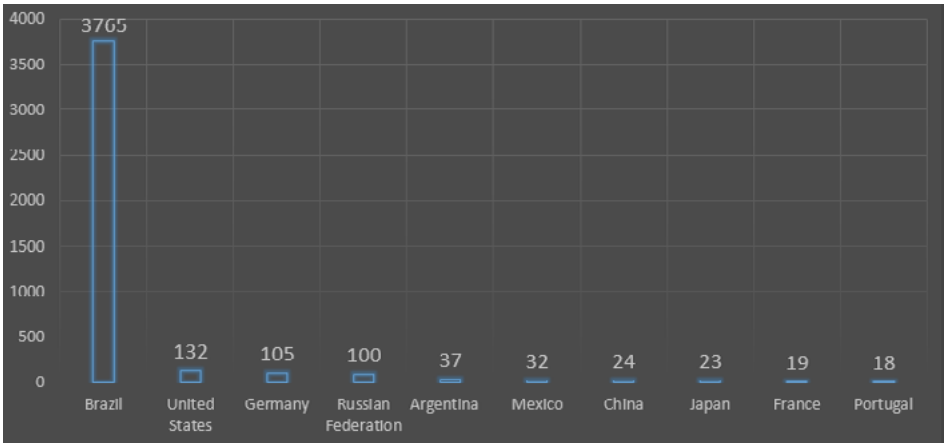


Figure 27: Geographic distribution of victim machines

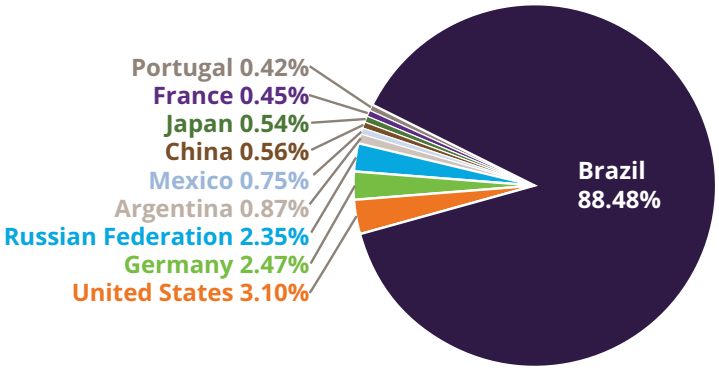


Figure 28: Geographic distribution of victim machines (%)

We found that 17 percent of the infected machines were directly tied to corporate networks. Coupled with the infection time-of-day analysis, it is reasonable to believe that infection actually occurred when machines were attached to a corporate network.

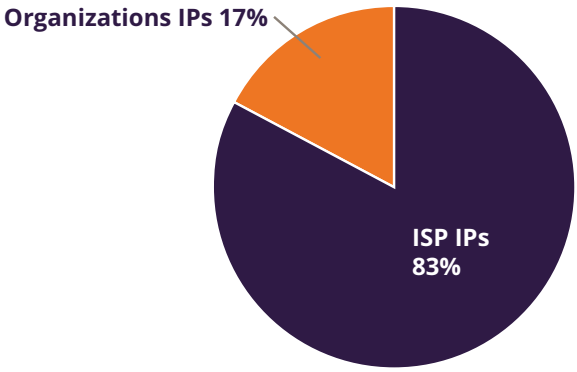


Figure 29: Infected machines within corporate networks

As expected, 72 percent of infections inside corporate network occurred during work hours (07:00–19:00, victim's local time).

This is an important data point to notice from an enterprise security perspective. It is in fact the point where personal compromise starts to become a corporate breach. Attackers that analyze their C&C logs will quickly realize that an infected computer is based off a corporate network and will spin their original intent into a persistent attack against the enterprise. The online banking Trojan "Swatbanker" that was recently detected at the German Federal Parliament (Bundestag) is an excellent example of such a threat. When detected, this alleged banking Trojan had an embedded configuration file that contained URLs for "Bundestag.btg" domain, which is the address of the German parliament's intranet. The banker used the internal URLs in order to target **forms and credentials used internally** by this government agency. There is no doubt in our mind that this attack started off as a standard generic Phishing campaign for distributing banker Trojans and only later was spun off to become an attack against internal government resources.

6.5 Spotting researchers

We removed from our previous analysis machines (IP addresses) that showed up multiple times in our data set. We assumed that these were research machines. In this section, we provide the basis for this assumption and show some anecdotal evidence to support its accuracy.

In our data, we found **493** machines with multiple hits. These machines account for a total of **6,447** hits. We divide these hits into three groups:

- Repetitive hits on a single C&C server
- Repetitive hits on more than one C&C server
- Repetitive hits from TOR exit nodes

The first group includes about **341** infected computers, accounting for **2,480** hits. While we noticed that an infected machine may create multiple hits to the same C&C server if rebooted, it does seem odd for a machine to create multiple such hits on a single day. Some of the machines in this group account for tens of hits. This is in line with the behavior of a research lab that repeatedly infects a machine with the same malware (or various samples of the same malware). Based on the criteria above, we marked **112** machines from this group as research machines (counting off a total of **1,940** hits).

The second group includes **152** machines, accounting for **3,967** hits. These computers were found in more than one C&C server log ('contador.txt' file). Such a behavior is not typical to infected machines as we have not seen in our lab a machine normally leaping between C&C servers. It is, however, in line with the expected behavior of research lab machines, testing multiple samples of a malware family.

The third group, which includes **33** machines, use TOR exit node IP addresses. It does not seem like the malware itself is designed to work through the TOR network, but researchers are frequently using the TOR network to hide the true source of activity.

By enriching the IP address information with "whois" lookup data, we were able to recognize **12** security companies accounting for **26** of the machines and **138** of the hits. It should be noted that if we were able to uncover other researchers, so can the hackers. A more sophisticated hacker can choose to blacklist researchers, a practice we have in fact seen in some C&C servers related to other malware families.

The following figure demonstrates the proportion of research machines from the entire population:

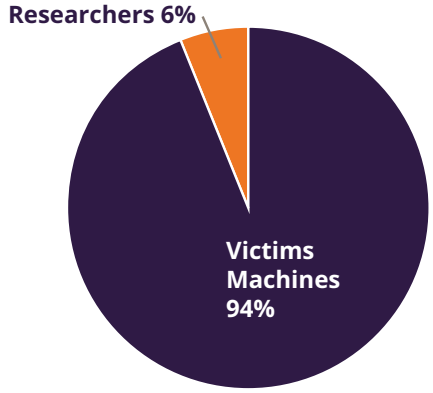


Figure 30: Proportion of research machines from the entire population

7. Summary and Conclusions

We began our research by analyzing a banker Trojan that monitors online banking activity of major Brazilian banks. During the analysis process, we uncovered several C&C servers used by multiple hacker groups in separate campaigns based on the same malware family. We were able to obtain a list of infected machines from these C&C servers and analyze their attributes.

The information we collected provided us with the following insights about malware and infection campaigns:

- Use of packing engine lets the malware remain undetected by standard AV software for enough time. While the original downloader detection rate by VirusTotal.com is relatively high (16/56 and 31/56 for the samples we had), the banker executables detection rate is significantly lower: 6/56 for *flashp.exe* and 3/56 for *adobep.exe*
- By spreading across multiple unrelated C&C servers, malware can remain operational for long periods of time. In our case, each C&C server accounted for a small proportion of the victims, and some of them lasted continuously since September 2014 to June 2015
- Malware infection campaigns can be made extremely effective if customized (with little effort) to the target population. In our case, the use of Portuguese in the email messages and the format of the message ensured a high rate of success among Brazilian recipients (88 percent of infected machines
  were in Brazil)
- The same type of malware (probably packaged differently each time) is used successfully multiple times by the same group or by a number of groups. It leads us to believe that this is an off-the-shelf malware that can be purchased from its creator on the dark web, and then used by lower-skilled criminal groups
- While the malware is primarily targeted at banking customers, it has a side effect of compromising machines within corporate networks. Given the modular nature of the malware, it is safe to assume that once the owners of the C&C perform the same analysis we did regarding the ownership of the infected machine, they'll quickly turn this around into a persistent attack against the compromised enterprises – going after business data directly, or simply selling access to these enterprises (directly or via the dark net).

While at the consumer level, there is not much one can do to defend against such attacks other than the minimal protection provided by an AV software, at the corporate level organizations must implement controls that quickly detect any activity that implies a compromised machine being turned into an attack launch pad against internal resources and business data stores. While enterprise sandboxing solutions might have detected and stopped the specific sample, those are only applied to machines inside the "enterprise perimeter". As the malware is primarily targeted at consumers, the infection is likely to happen outside the enterprise perimeter while an employee makes personal use of enterprise-issued machines (mobile workforce), or if infected employees use their own devices inside enterprise perimeter (BYOD).

Hacker Intelligence Initiative Overview

The Imperva Hacker Intelligence Initiative goes inside the cyber-underground and provides analysis of the trending hacking techniques and interesting attack campaigns from the past month. A part of the Imperva Application Defense Center research arm, the Hacker Intelligence Initiative (HII), is focused on tracking the latest trends in attacks, web application security and cyber-crime business models with the goal of improving security controls and risk management processes.