A STUDY OF MACHETE CYBER ESPIONAGE OPERATIONS IN LATIN AMERICA

Veronica Valeros, Maria Rigaki, Kamila Babayeva & Sebastian Garcia
Czech Technical University in Prague, Czech Republic

{veronica.valeros; maria.rigaki}@aic.fel.cvut.cz; babaykam@fel.cvut.cz;
sebastian.garcia@agents.fel.cvut.cz

ABSTRACT

Reports on cyber espionage operations have been on the rise in the last decade. However, operations in Latin America are heavily under-researched and potentially underestimated. In this paper we analyse and dissect a cyber espionage tool known as Machete. The results presented in this work are based on the collection, reversing and analysis of Machete samples from 2011 to 2019. The large collection of samples allowed us to analyse the malware's evolution in detail and track changes in its functionality and structure, including modifications introduced as late as January 2019.

Our research shows that Machete is operated by a highly coordinated and organized group that focuses on Latin American targets. We describe the five phases of the APT operations from delivery to exfiltration of information and we show why Machete is considered a cyber espionage tool. Furthermore, our analysis indicates that the targeted victims belong to military, political or diplomatic sectors. The review of the almost eight years of Machete operations shows that it is probably operated by a single group whose activities may be state-sponsored. Machete is still active and operational to this day.

INTRODUCTION

Cyber espionage is understood as the act of obtaining restricted information without permission using software tools, such as malware. While traditional espionage [1] activities are difficult to detect and study as they are typically covert operations, cyber espionage operations have more often been disclosed and studied. There is, however, a lack of research in this area in Latin America. Very few cyber espionage campaigns have been discovered and studied in this region in the last decade.

Nowadays, cyber espionage is conducted by groups often referred to as Advanced Persistent Threats (APTs). APT is the technical term used to identify economic or politically motivated groups that conduct cyber attacks persistently and effectively against a specific target. What distinguishes APTs from traditional attacks are their clear goals, specific targets, and long-term, highly organized campaigns [2].

In this paper we present an in-depth analysis of the espionage activities of an APT group in Latin America through the analysis of one of its cyber espionage tools known as Machete or Ragua. Reports about Machete have been published previously in [3] and [4], however their results are based on a subset of Machete samples, leaving unanswered questions about its long-term operations, the functionality of the malware in detail, and the attackers' capabilities and operations as a whole. We

aim to provide an extensive overview of the malware and actors by analysing their operations from their beginning until today.

Our research is based on a large corpus of Machete malware binaries that span eight years of operation. The malware corpus was processed, reverse engineered and dissected in order to obtain the malware configurations, command-and-control servers and decoy documents used in the campaigns. This information was used to identify the profile of the targets, the regions affected by the malware, and details of the malware infrastructure.

We show that the group behind Machete fits the description of an APT as it is running a long-term operation, it attacks specific targets and aims at strategic benefits. Based on the information extracted from the malware binaries we have been able to understand that Machete is targeting political and military-related victims. The victims appear to be located in Central and South America and are primarily Spanish speakers. Furthermore, our research indicates – due to the sharing of encryption keys and overlapping network infrastructure – that there is likely one group operating the malware.

The main contributions of this paper include:

- An in-depth analysis of Machete that complements and goes beyond previous reports. The analysis is based on the largest collection of Machete binaries to date, which is three times as large as reported in previous work. The time span of the analysed samples is also broader and has allowed the study of the attackers' methods over time.
- The most comprehensive collection to date of Machete hashes and decoy documents spanning eight years of operations.
- Discovery of new functionality based on reverse engineering analysis of Machete samples. Until now it was not known that Machete was able to perform lateral movement within an infected organization. Our analysis showed that Machete can propagate via infection of USB drives. The use of *Dropbox* as an exfiltration method is also first reported in this paper.
- A qualitative analysis of the decoy documents based on language, topics and countries that sheds light on potential victims and helps highlight the interests of the attackers when choosing their targets.
- A case study of the operations of an APT group that is active in a largely understudied part of the world, namely Latin America.

PREVIOUS WORK

This paper focuses on the cyber espionage activities of an APT group conducted in Latin America[1]. The study of this group is conducted by the analysis of one of its tools, known as Machete or Ragua.

Machete was first reported in 2014 [3], and subsequently in 2017 [4]. These reports give a general overview of the malware's functionality, but they both focus on a small corpus of malware samples. Both reports provide numbers of victims and countries, but no information is provided to verify these claims. There is no supporting information as to where, when and how data about the victims was collected. Additionally, while many of the sample hashes provided in these reports are publicly available, not all of the samples can be accessed to verify the analysis.

[1] Latin America refers to territories in the Americas where the Spanish, Portuguese and French languages prevail. Commonly understood as all countries south of the United States.

Machete was not the first cyber espionage campaign in Latin America. In 2012, a report [5] described a targeted attack dubbed 'Operation Medre'. This targeted attack attempted to steal *AutoCAD* files from victim computers. The victims were primarily located in Peru, but other countries in the region were also targeted. The type of espionage conducted by this APT group is considerably different from that conducted by the group behind Machete.

In 2015, a report [6] uncovered an APT group dubbed 'Packrat' targeting Latin American politicians, journalists and others. This group is believed to have been operating since 2008. There are similarities with Machete in the way this actor operates, the type of infrastructure used, and the use and themes of decoy documents. However, there are significant differences in the tools used for espionage – in this case, known existing malware. There's no evidence that the two actors are the same. In 2018, a new report disclosed the use of remote access tools for espionage in Latin America [7]. While this attack presents some similarities with the Packrat group, the targeted audience and the tactics used were substantially different.

In early 2019, researchers uncovered a new ATP group, dubbed APT-C-36 [8], targeting companies and government agencies in Colombia. The tactics and techniques used differ significantly from those used by Machete.

Several studies focus on the delivery mechanism used by APT groups. In [9], researchers present a study of decoy documents. The study shows how documents are socially engineered to match native language, regional and thematic interests of the targets. This seems to be a common factor in all the APTs targeting Latin America. Other studies of targeted attacks against NGOs [10] and individuals [11] also show the preference among attackers for using socially engineered suspicious links and documents.

METHODOLOGY

For this research we used malware binaries, or samples, that contain Machete. In the first stage of the research we aimed to obtain valid Machete samples to analyse. These samples were reverse engineered and studied to determine the malware characteristics, how they targeted their victims, and how the malware evolved over time.

This research is based on a corpus of 105 Machete binaries and 63 decoy documents. The following steps were carried out in order to obtain and create this large corpus of validated samples: first, we searched for and collected all possible Machete samples from public and private repositories; second, we manually verified that these samples were Machete samples; third, we identified the structure and nesting of files to differentiate between first-stage and second-stage binaries, their parents, and the individual modules; fourth, we reversed engineered each file to obtain the source code of the malware written in Python, its configuration files, encryption keys, and the decoy documents used, when available.

In order to obtain samples of Machete, we first relied on hashes from previous work [3, 4]. A total of eight hashes were available from the first report, and 27 initial decoys from the second report. However, not all of these were publicly available. An initial analysis of the files led to the identification of specific characteristics in the binaries, such as number of Portable Executable (PE) sections, PE comments, file structure, and the final modules' source code. These characteristics, combined with specific anti-virus signatures, IP addresses and domain names, were used to expand the search and identify more potential Machete samples in public and private repositories. Every

binary matching our indicators was downloaded for further manual classification by a human analyst. At the end of this stage the corpus of samples at our disposal had tripled the number of files reported in previous work.

The samples positively classified as Machete were further processed. This workflow is illustrated in Figure 1.

1. The first step in this process consisted of identifying the parent. The malware is typically distributed as an email attachment, therefore the attachment is considered a parent.
2. Next, the parent was uncompressed to identify the first stage of Machete.
3. In the third step, the first-stage malware was uncompressed to extract the second-stage malware and the second-stage decoy document.
4. The second-stage malware was further uncompressed to identify the malware libraries, modules and configuration files.
5. Next, the modules were reverse engineered from PE files to Python compiled code.
6. Finally, the Python compiled modules were decompiled to obtain the source code of the malware, in Python.

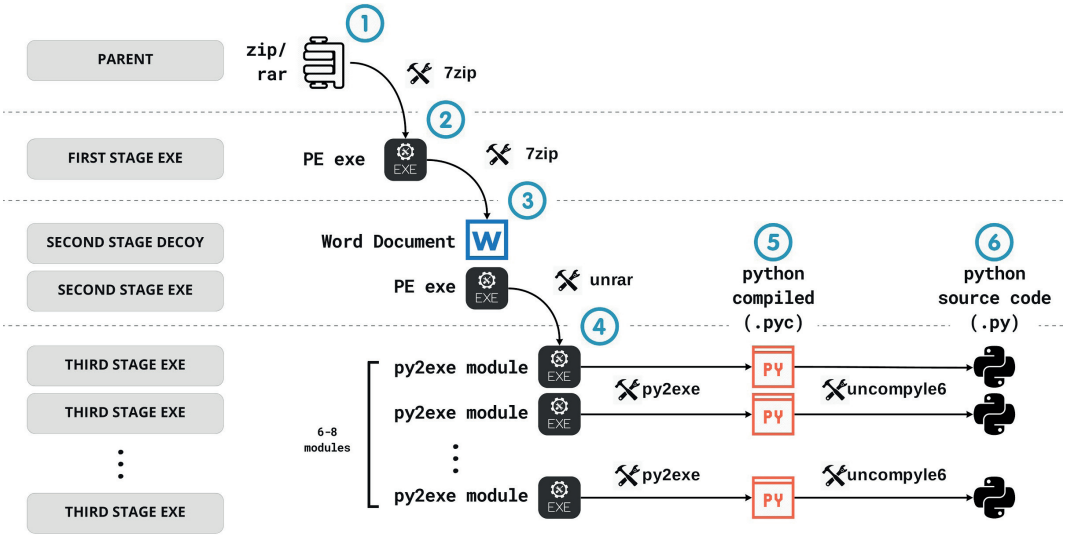

Figure 1: Machete has a nested structure. The parent is what the victim receives (1). This file contains a first executable file (2). The first executable file contains the payload and the decoy document (3). The payload consists of six to eight modules (4), which can be further reverse engineered to obtain their source code (6).

The reverse engineering of the modules consisted of obtaining the Python compiled code from the PE module using a tool called *unpy2exe* [12]. Once the Python compiled code (.pyc) was obtained,

we used a tool called *uncompyle6* [13] to obtain the Python source code. This process is known as decompilation.

In most cases the Python source code was obfuscated using a tool such as *pyobfuscate* [14], which makes the source code difficult to read by renaming variables to nonsensical names and adding dummy clauses to increase 'noise'. Reversing the obfuscation is a process known as deobfuscation. In this case, deobfuscation was still possible, given that external library calls were not obfuscated and the code was still able to run. No other anti-analysis or anti-debugging techniques were used among the examined samples.

At the end of this process, an exhaustive corpus of 105 stage 2 Machete samples, along with 63 decoy documents and the source code of all modules for every sample, was available to continue the analysis and research. The list of SHA256 hashes of decoy documents is shown in Appendix A; the list of SHA256 hashes of stage 2 Machete samples is shown in Appendix B.

MALWARE OPERATIONS

Machete is a piece of malicious software designed for *Windows* operating systems (32-bit). It is distributed as a Portable Executable file compressed as a ZIP or RAR file. Machete is written in Python.

APT operations are highly coordinated and organized. They typically follow a common structure, often known as a kill chain [15]. Machete APT operations are no exception. The five phases of the operation are illustrated in Figure 2, namely: delivery, installation, action on objectives, lateral movement and exfiltration. This section describes these phases, the encryption used to protect the stolen information, and finally, why we consider Machete to be a cyber espionage tool.

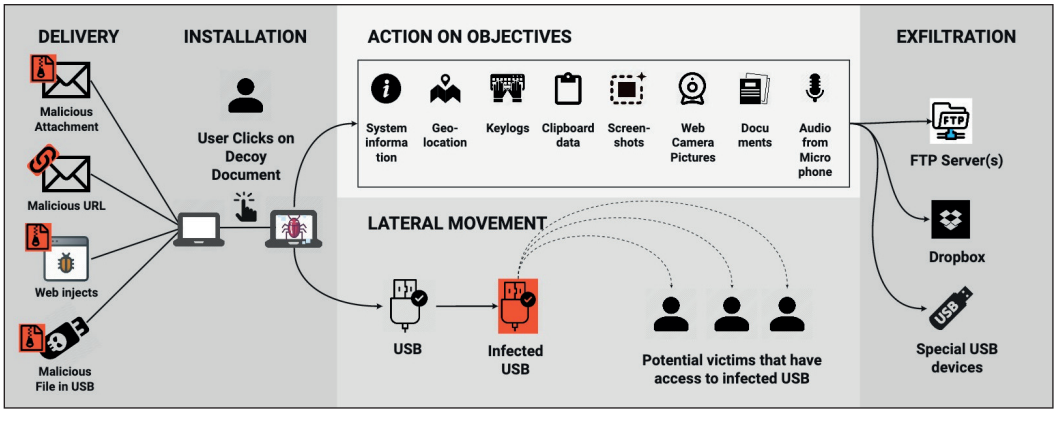

Figure 2: Machete operations are structured in five phases: delivery, installation, action on objectives, lateral movement and exfiltration.

Delivery

There are four known methods for distributing Machete: (i) as a malicious attachment in a phishing email, (ii) as a linked file (URL) in a phishing email, (iii) as an executable file in an infected USB

drive, and (iv) via web injections. The first two methods are the most likely to be used for the initial compromise according to previous work [3, 4].

The third method of delivery, discovered during this investigation, is commonly used by attackers in order to jump air-gapped secured systems and to move laterally within an already compromised organization. No exploits or zero-day vulnerabilities are needed for the delivery of this malware.

Installation

Targeted victims are lured into downloading and opening the Machete malware via well-crafted social engineering techniques. As previously mentioned, no vulnerabilities are exploited in the operating system in order to execute the malware. Once the victim clicks to open the decoy file, the malware is executed and the decoy document is displayed to the victim.

Action on objectives

Machete is an espionage tool designed to steal information such as keystrokes, clipboard content, screenshots, web camera captures, audio from the computer's microphone, system information and geolocation of the target. These functionalities are described in full in the next section.

Lateral movement

Compromised victims can be used to spread the malware further within the same organization. Through reverse engineering of the samples, we discovered that Machete has specific instructions on how to spread automatically via USB drives. In the presence of an external drive, Machete will copy itself to the drive, then proceed to copy any important documents to the computer in order to steal them. This spreading gives attackers the ability to strengthen their foothold in an organization, maximizing their effectiveness.

Exfiltration

We use the term 'exfiltration' to refer to the act of 'unauthorized copying and transmission of information by any means', as defined in [16]. Machete has three main methods of exfiltrating the stolen information from its victims. First, it uploads the collected data to a designated File Transfer Protocol (FTP) server. While the documents are encrypted, the FTP communication is not encrypted. The FTP server is secured with a username and password, however the credentials can be found either in the source code of the malware or, in newer versions of the malware, in a configuration file.

The second method for exfiltrating the information from the victim is via USB devices. Machete is able to recognize special USB devices, and if they are present the malware will copy the collected information to the USB drive. This latter feature suggests that the attackers may have physical access to some of the victim computers.

The third method for data exfiltration was observed only in a few cases. In those cases, Machete was using *Dropbox* [17] as an exfiltration server.

Encryption

Machete encrypts the files using symmetric encryption. In particular, it uses the Advanced Encryption Standard (AES) algorithm, and the encryption key is embedded in the source code of the malware. (Encryption is further discussed in the 'malware infrastructure' subsection.)

Machete cyber espionage capabilities

Machete shares some capabilities with other APT groups such as remote access tools, and information-stealing malware. This raises some questions, such as 'Why is Machete different?' and 'What makes it an espionage tool?'

Machete differentiates itself from other malware thanks to its combined capabilities. The recording of audio, capture of web camera photographs and collecting of documents from the victim's computer over long periods of time is something that can be directly linked to possible extortion, surveillance or espionage activities.

The intent and specific data-stealing functionality is what defines Machete as a cyber espionage tool. The information stolen does not appear to have monetary value for the threat actors. The tool is not designed to steal credit card information, usernames and passwords – the sort of information that anyone can easily profit from. The information stolen by Machete seems valuable only to actors that would use this information themselves, along with their own information, to influence decisions and gain strategic advantage at a government or political level.

MALWARE CAPABILITIES

The purpose of Machete is to steal information about its victims, specifically documents or data they may possess and information about their current behaviour. During the analysis of Machete samples over a period of eight years we observed the APT group adding and removing functionality. Considering the complete malware corpus, we found functions designed to steal the following information:

- **System information**: who the target is and information about the computer being used.
- **Geolocation**: where the target is located.
- **Keystrokes**: what the target writes.
- **Clipboard content**: what the target copies and pastes.
- **Screen captures**: what the target is seeing on the screen.
- **Web camera captures**: who or what is in front of the computer's web camera field of view.
- **Audio**: what the victim is saying, or conversations from the surrounding environment.
- **Documents**: specific documents in the target's computer.

In the following subsections each function is described in detail.

System information

The type and amount of information collected from the targets varies as well as the method. In early versions of Machete, the extraction was field by field using the *platform* [21] library, which is part of the Python standard library. As illustrated in Figure 3, the information collected consisted of public IP, operating system name, operating system release, the computer network name (node), system version, architecture and processor. The public IP is retrieved after contacting the C&C server. Information about local network cards, local IPs and MAC addresses is obtained using the *Windows* command `ipconfig`. The collected information is stored in a text file for later exfiltration.

```
try:
    web = urllib.urlopen('http://190.60.245.28/mi.asp')
    f = open(appdata + 'Info.txt', 'w')
    f.write('\n--------------------------\n')
    f.write('\n Start-Up: ' + time.asctime() + '\n')
    f.write('\n--------------------------\n')
    f.write('IP        :' + web.read(17) + '\n')
    f.write('system    :' + platform.system() + '\n')
    f.write('release   :' + platform.release() + '\n')
    f.write('node      :' + platform.node() + '\n')
    f.write('version   :' + platform.version() + '\n')
    f.write('machine   :' + platform.machine() + '\n')
    f.write('processor:' + platform.processor() + '\n')
    f.close()
except Exception as e:
    pass
```

Figure 3: Gathering system information using the platform library.

This Python library was later replaced with the *Windows* `systeminfo` function. In later versions of Machete the information collected in this step was reduced considerably.

Geolocation

There are fewer than a dozen samples of Machete that incorporate the functionality to geographically locate the target using Wi-Fi MAC addresses. The oldest sample to implement this functionality is from 2012, and the latest one is from 2019. The malware has two modes of retrieving geo location: the first uses only the MAC address, while the second uses MAC address, channel, and signal strength. In both cases the malware first collects the information from the infected device using the *Windows* `netsh` command. There are several attempts at determining the geo location based on the information available using a *Google* API[2]. The information the malware is retrieving is the accuracy, latitude, longitude, and a link to *Google Maps*.

```
a = open(appdata + '\\' + file_Geo, 'w')
a.write('     Geolocalizacion por MAC \n')
a.write('Accuracy ---------- %d' % wg.getAccuracy() + '\n')
a.write('Latitude ---------- %s' % wg.getLatitude() + '\n')
a.write('Longitude --------- %s' % wg.getLongitude() + '\n')
a.write('Google Maps Link -- %s' % wg.getGoogleMapsLink() + '\n')
a.close()
```

Figure 4: Gathering geolocation information.

It is important to note here that the link to *Google Maps* is regionalized to Argentina (com.ar). The link is created as follows:

`http://maps.google.com.ar/maps?f=q&source=s_q&hl=en&geocode=&q=%s+%s`

Keystrokes

For the stealing of keystrokes, the malware has a keylogger functionality in one of its modules. The malware defines a series of keys in which it is interested, and defines what to do when one of these keys is pressed in the operating system. Machete creates a log file formatted as Hyper Text Markup Language (.htm). The log contains the date and time of the keystrokes, name of the opened application, and the keystrokes typed by the user. In this manner, the attackers not only know *what*

[2] The API used by the malware was deprecated in early 2012, and discontinued by the end of 2012.

the victim was typing, but also *when* and *where*. This provides context and an added value to the stolen information.

This module has suffered minor changes since its first development. One change highlight occurred in mid-2012 when the names of the key IDs were re-written. In this change a typo was introduced that has been present in all the Machete samples that have come since then. The keys 160 and 161 were renamed from *lshift* and *rshift* to *Shitf(Izq)* and *Shitf(Dcha).*

Clipboard content

Similarly, the malware has a clipboard monitor, which logs everything that the victim copies in a special log file named 'Clip.html'. The malware logs the clipboard content, data and time, and the name of the open window.

Screen captures

Another vital functionality of Machete is screen capture. Machete is able to take screenshots from the victim computer. These images are indexed by date and time, and provide high value to the attackers in their intelligence analysis due to their rich and detailed content.

Web camera captures

Another of the functions is web camera capture, in which the malware routinely takes pictures using the web camera of the computer (if such a device exists). The web camera capture can tell the attackers who is using the computer, what the victim looks like, or reveal the identity of other individuals. Not only that, it also shows when the computer is unattended, which can be vital if the attackers have physical access to the infected machine.

Audio

Machete is also able to record sound using the microphone of the computer. This functionality has been added and removed multiple times. The Python library *pyaudio* is used to record the audio in .WAV files. The malware then uses the *LAME MP3* audio encoder to convert the files to MP3.

Documents

The last core functionality is document stealing. The malware is able to find, encrypt, and steal interesting documents found on the victim computer. Attackers define files as interesting based on the type of document. In the oldest sample of Machete from 2011, the malware was looking for a small collection of file extensions: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .jpg, .pgp, .skr and .asc. The interest in retrieving new documents increased, and the list expanded to include the additional file extensions: .db, .mdb, .pkr, .gpg, .drw, .lpt, .shp, .rte, .sda, .odp, .sxi, .odt, .sxw, .ods, .sxc, .odg, .sxd, .odb, .odf, .sxm, .txt, and specific files such as key3.db and signons.sqlite used by *Firefox* to store user credentials. The files are encrypted before they are exfiltrated.

Apart from well-known document formats, is worth noting the attackers' interest in databases (.db, .mdb, .odb), encryption files (.gpg, .pgp, .asc, .skr, .pkr), maps and design files (.drw, .lpt, .shp, .sda, .sxd), and business applications' source code (.os).

MALWARE INFRASTRUCTURE

The analysis of Machete and its functionality also provided some insights into the attackers' own operational capabilities. With the information obtained from the samples we tried to answer the following questions:

- What are the attackers' capabilities in terms of infrastructure?
- Are there multiple attackers that use Machete?
- How did the malware evolve over time?

Infrastructure

Machete exfiltrates information primarily via FTP servers. This information is embedded in the Machete samples, namely: domain name, username and password, routes, version, and encryption key. Table 1 provides a summary of the above information along with the software versions found in the malware. Passwords are not displayed for security reasons. Figure 5 shows the distribution of the FTP users, routes and malware versions among the malware samples analysed.

List of servers	FTP user	FTP routes	Malware versions
190.60.245.28	administrador andryu	Cancer AND Arkantos Equipos GANADEROS_4 SII	-
190.60.245.29	administrador	AND SII SII/AGM MARQUETALIA GANADEROS_2 GANADEROS_4 GANADEROS_6 set SET and Arkantos Equipos	-
ftp.agaliarept.com	Manizales	huanuco	-
ftp.alquimedes.net	admin1	Buenaventura	13.1
ftp.blogwhereyou.com	administrador	bitec	-
ftp.Grannegral.com	grannadmin	-	-

Table 1: Attacker infrastructure summary.

List of servers	FTP user	FTP routes	Malware versions
derte.ddns.net	ahy860	Amazona Apoyos EL FRA1 HUM11 Otros Pro SIS TE TRANS	2.0 2.2 39.0
skdier.ddns.net	bafer	Otros	75.0
idrt.gotdns.ch	ad856	Amazona Buenaventura Cali Guajira Huila Monteria Vichada	2.2 3.0 21.3 27.1 27.9
mcsi.gotdns.ch	mager	-	-
jristr.hopto.org	ad856	Huila	20.1
maers.hopto.org	mkier	Armenia Buenaventura Cali Casanare Guajira Risaralda Vichada	4.0 84.0
java-mail.servepics.com	administrador	bitec	-
java.dyndns-mail.com	administrador	Marquetalia Rimex	-
java.serveblog.net	admin1	-	14.0 14.2
javath.myftp.org	administrador	Marquetalia	-
wbgs.3utilities.com	custom97	Risaralda	4.0
Grannegral.com[3]	-	-	-
agaliarept.com[3]	-	-	-
blogwhereyou.com[3]	-	-	-

Table 1: Attacker infrastructure summary (contd.).

[3] These sites are used as HTTP C&C servers, therefore no credentials are associated with them.

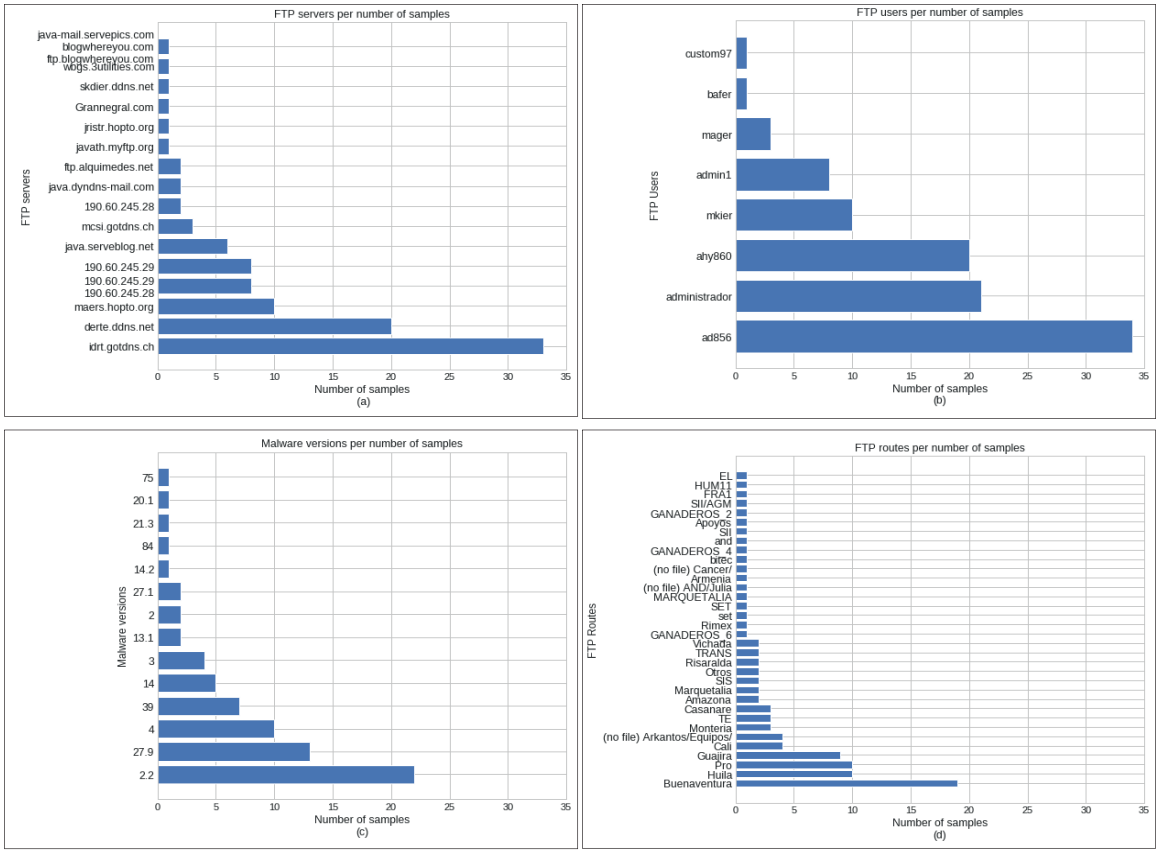

Figure 5: Distributon of (a) FTP servers; (b) FTP users; (c) malware versions; and (d) FTP routes.

- **FTP servers**. Machete used multiple FTP server domains for its campaigns. For the most part the domain names do not overlap with the malware versions. A total of 14 FTP server domains were identified. Machete used dynamic DNS services such as ddns.net or serveblog.net in many cases. Dynamic DNS gives flexibility to their operations.
- **FTP credentials**. From 2013, the group used one set of usernames per FTP server. However, in older samples the attackers were using the same username across multiple FTP servers. The same password was reused in multiple accounts. Attackers evolved to use multiple versions as a way to separate functionality and/or targets.
- **FTP routes**. The most used FTP servers contain several *routes*. These are folders in the FTP server where the stolen information is stored. Every Machete sample has a route defined. Routes are often named after Colombian cities or areas, e.g. Buenaventura, Guajira, Huila, etc. This might be an indication of where the attack operators are stationed.

- **IP addresses**. A total of 13 unique IP addresses have been found associated with Machete FTP servers since its origin. These IPs were obtained via a public passive DNS service [18]. Passive DNS is a system that stores DNS resolution data along with time period. Further analysis showed that different domain names shared IP addresses, even during overlapping periods of time.

  The earliest date that an FTP domain was seen is early 2012. Before this time, attackers relied on IP addresses.

- **Encryption keys**. Machete uses symmetric encryption to encrypt the stolen data before exfiltrating it. The encryption key is embedded in the binary. Three distinct AES keys were shared among all analysed samples. This is a strong indication that there was only one group involved in the malware operation as it is very unlikely that different organizations would choose to encrypt their documents with the same keys and store them on the same servers.

MALWARE EVOLUTION

The oldest Machete binary in our corpus dates back to 2011. This is confirmed by the sample's submission date to *VirusTotal* [20], which was also in the same year. The most recent sample of Machete was observed in early 2019. Through our reverse engineering and code analysis we have been able to identify three major changes in the last eight years of Machete activity. The first major change was to split Machete functionality into different smaller modules – this happened in early 2011, bringing more flexibility to the malware. The second major change was in 2014 when the obfuscation of the Python source code was added in an effort to bypass detection. The third major change was in early 2019 when the unpacking of the malware code changed considerably, also to hinder detection efforts.

Machete's authors used multiple versions of the malware mainly to differentiate between campaigns and targets. Modules and functionality were added or removed over time. However, the underlying code structure did not change dramatically until late 2018.

The initial versions of the malware showed how its authors were putting together the malware, building up new functionality, testing libraries, fine tuning parameters. Modularity was added later. In early samples the malware had hard-coded IPs and credentials for the FTP server to exfiltrate data. The IPs were later changed to dynamic DNS domain names, but were still in plain text in the code. The malware later evolved to obfuscate the credentials, and later stored them in a text file, obfuscated. All the changes observed gave Machete modularity and flexibility, allowing new campaigns to be created with the minimum modification of the code.

In terms of anti-analysis techniques, the vast majority of the samples were obfuscated at the Python source code level, probably as an attempt to slow down malware analysts. Earlier versions of Machete were not obfuscated at all.

ANALYSIS OF TARGETS

To understand the purpose of Machete, and the goals of the actors operating it, we analysed the targeted victims. The analysis of possible victims is performed through the analysis of the decoy documents used. Decoy documents were obtained from Machete parent samples, which contained both decoy and malware. By looking at the decoys used in the campaigns through the years we try to infer the profiles of the targets. Information about victims obtained from previous work [3, 4] was not taken into account as it was impossible to validate it.

Manual annotation of decoy documents

A total of 75 unique decoy documents were identified, each of which was used in one or more malicious campaigns. The decoy documents were embedded and compressed in the Machete malware – however, they were only used as decoys and not as an exploitation tool. In this section we present an analysis of 40 documents observed between 2013 and 2018.

We manually analysed each decoy document used by Machete, noting the language, country, dates, and theme covered. The first phase consisted of noting the type of document used (PDF, *Word*, images, etc.). The second phase consisted of identifying the language used in the documents, to establish a target group. The third phase focused on assigning each document to a theme category based on the content (political, economic, military, etc.). The fourth phase consisted of identifying the country or countries targeted by the document.

Type of decoy documents

The type of documents used were predominantly *Microsoft Word* documents, followed by PDF, *PowerPoint* documents, and JPG images (see Figure 6). Two versions of *Microsoft* documents were used: .docx and .doc. The .docx format was introduced in *Word 2007*. PDF documents were the second most commonly used type of document. In third place, different *Microsoft PowerPoint* documents were used: .pps, .ppt and .pptx. Lastly, one image in JPG format was used.

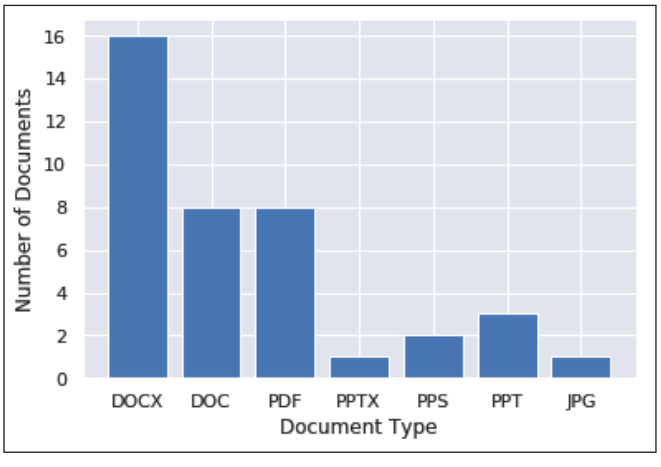

Figure 6: Breakdown of decoy documents used by Machete.

The majority of the documents appear to be documents that have been stolen and re-purposed for the spear-phishing attacks. They could have been manually crafted for the purpose of the attacks, but there are indicators which point to our first hypothesis. In particular, many of the *Microsoft Word* documents still contained metadata about date of creation, author, organization, and last time printed, which appeared to be real. Typically, a manually crafted document will have this data removed or replaced with fake data. This doesn't seem to be the case in the corpus of documents we analysed. A subgroup of documents contained information, names, stamps and references that would also be hard to fake.

Languages, countries, regions

Spanish speakers are the primary targets of Machete, but not the only ones as previous work suggested [4]. Of all the decoy documents analysed, one document was written in Portuguese and the rest were written in Spanish. All Spanish- and Portuguese-speaking countries could be targeted by these decoys, irrespective of the country or region. Spanish is the official language in 21 countries, the majority of which are located in Central and South America [19].

After careful analysis of the content of the documents, it was possible to observe that each one made specific reference to certain countries. It was possible then, again through careful analysis, to identify the affected countries in each document. The content of each document was read and examined by native Spanish speakers in order to identify the theme and the country. For instance, in a military personnel reassignment decoy document, all personnel mentioned were from Venezuela. In this case, the annotated country was Venezuela. This process was repeated for all decoy documents that contained enough context. The annotated country is just an indication of where the document was stolen or crafted from, but it doesn't limit the target audience, as any military official from neighbouring countries would also be interested in this information.

In Figure 7 we show the number of decoy documents per country, while in Figure 8 we emphasize the geographical regions from which the documents were stolen. While previous work mentioned targeted victims outside Latin America, we could not confirm that by looking at the data obtained from the Machete samples.

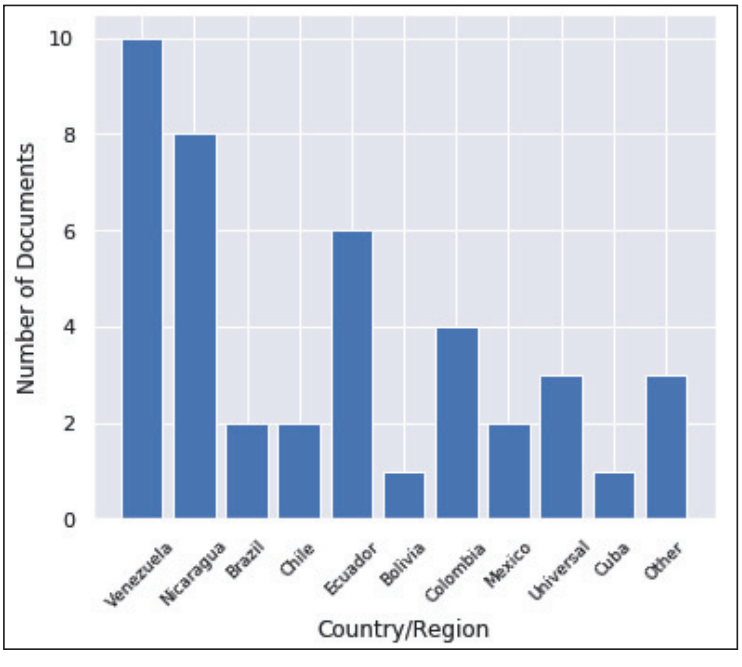

Figure 7: Number of decoys per country used by Machete.

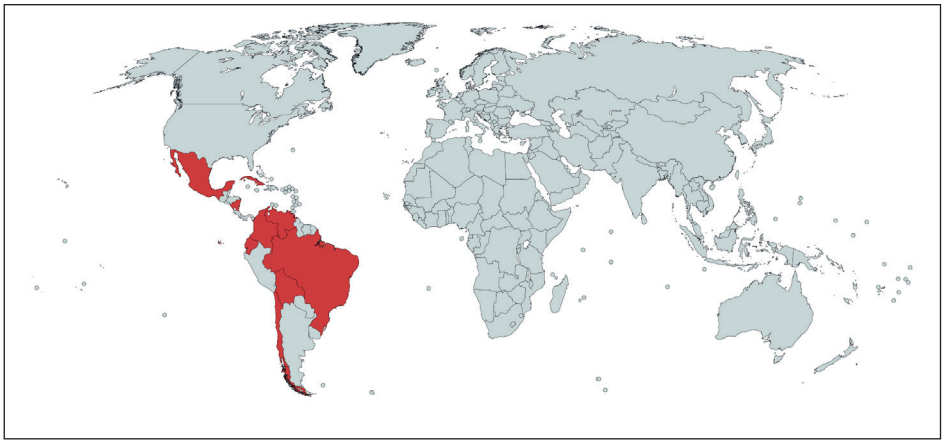

Figure 8: The content of the decoy documents show countries targeted by Machete.

Topics

The themes of the decoy documents indicate that the potential victims are heavily interested in political topics at national levels, and in military information, ranging from the movement of troops to personnel reassignments. Other decoys appealed to the sense of fear in the victim, using themes such as debt collection and legal subpoenas. In a minority of cases the attackers used generic themes such as sexual content to lure victims into opening the documents; in this case the targets were primarily male. Each document focuses on a specific theme or topic that is highly alluring and attractive for the targets. The number of documents per topic used by Machete is shown in Figure 9.

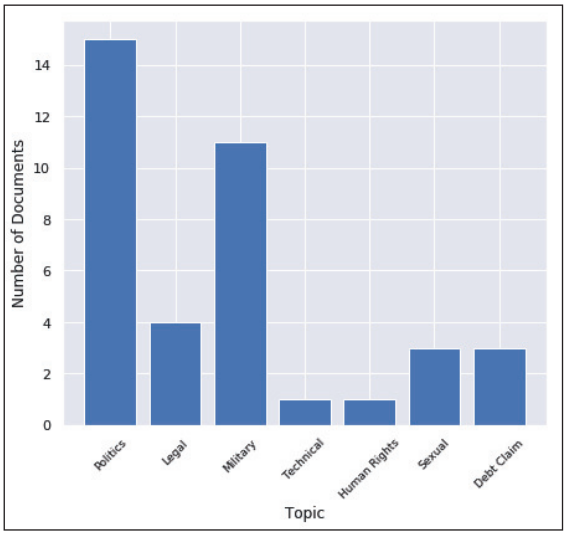

Figure 9: Breakdown of topics used by Machete in decoy documents.

Decoy documents used in targeted attacks must have certain characteristics. According to the work of [10], attackers use documents that are (1) believable, (2) enticing and (3) conspicuous. The decoy documents used in this espionage activity are believable, due to their nature: they are real, existing documents, not crafted or artificially created. The documents are enticing, as the topics covered are highly attractive and lure victims into opening them. Finally, they are conspicuous as they attract attention and are easily observable by the victim.

Dates

The creation date was extracted from the metadata of each document. Metadata can be altered, so this date is taken as an initial reference of document creation. These dates show that the documents were created in the years 2000, 2006, 2011, 2013, 2014, 2015, 2016 and 2017.

CONCLUSIONS

This paper has presented an analysis of eight years of operations of an APT group targeting Latin America using a cyber espionage tool known as Machete. Spear phishing through the use of real and enticing documents seems the most effective way to compromise their targets. The functionality of Machete has fluctuated considerably in the last eight years, however the main core functionality of the malware remains: keylogging, screen capture, and document stealing. The oldest Machete sample was observed in early 2011, which suggests that the group's activities started earlier. Machete is still active today.

Our analysis of decoy documents showed that the targeted victims are mainly located in Latin America. However, in this work we could not arrive at the same conclusions as were drawn in previous work regarding the number of victims and their countries. Additionally, the majority of the decoy documents are written in Spanish, but there is a minority of documents in Portuguese, confirming that the victims are located all across Latin America. The documents' topics are mostly military and political in nature, which points to military and politically motivated targets.

Our investigation suggests that APT sophistication is directly related to the socioeconomics of the targeted regions. Machete is sophisticated considering the region in which it operates. Compared to other APTs it does lack sophistication in terms of the programming language used, the lack of vulnerabilities exploited, and its anti-analysis techniques. However, failing to investigate threats like this based on their apparent lack of sophistication leaves victims in the dark and unprotected.

Our research has also shown that Machete does not rely on zero-day exploits. This confirms previous research that also shows that APT groups rely more on spear-phishing techniques.

Machete continues to evolve and new malware samples are being observed every month. As part of our future work we plan to continue monitoring it and reporting on its activities in order to help stop this threat.

ACKNOWLEDGEMENT

The authors would like to thank Ross Gibb for his assistance with malware reversing; *Reversing Labs* for access to their malware repository; and Luciano Martins for providing additional Machete samples. This research was partially supported by an *Avast Foundation* grant for the protection of civil society.

REFERENCES

[1] Espionage. https://www.mi5.gov.uk/espionage.

[2] Chen, P.; Desmet, L.; Huygens, C. A study on advanced persistent threats. In IFIP International Conference on Communications and Multimedia Security. Springer, 2014, pp.63–72.

[3] El machete. https://securelist.com/el-machete/66108/.

[4] El machete malware attacks cut through latam. https://threatvector.cylance.com/enus/home/el-machete-malware-attacks-cut-through-latam.html.

[5] Acad/medre. 10000s of autocad designs leaked in suspected industrial espionage. https://www.welivesecurity.com/media\files/white-papers/ESET\ACAD\Medre\A\whitepaper.pdf.

[6] Packrat, Seven Years of a South American Threat Actor. https://citizenlab.ca/2015/12/packrat-report/.

[7] CannibalRAT targets Brazil. https://blog.talosintelligence.com/2018/02/cannibalrat-targets-brazil.html.

[8] APT-C-36: Continuous Attacks Targeting Colombian Government Institutions and Corporations. https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/.

[9] Le Blond, S.; Gilbert, C.; Upadhyay, U.; Gomez-Rodriguez, M.; Choffnes, D. R. A broad view of the ecosystem of socially engineered exploit documents. in NDSS, 2017.

[10] Le Blond, S.; Uritesc, A.; Gilbert, C.; Chua, Z. L.; Saxena, P.; Kirda, E. A look at targeted attacks through the lense of an NGO. in USENIX Security Symposium, 2014, pp.543–558.

[11] Marczak, W. R.; Scott-Railton, J.; Marquis-Boire, M.; Paxson, V. When governments hack opponents: A look at actors and technology. In USENIX Security Symposium, 2014, pp.511–525.

[12] unpy2exe - Extract .pyc files from executables created with py2exe. https://github.com/matiasb/unpy2exe.

[13] uncompyle6 - A cross-version python bytecode decompiler. https://github.com/rocky/python-uncompyle6.

[14] pyobfuscate- Python source code obfuscator. https://github.com/astrand/pyobfuscate.

[15] Hutchins, E.M.; Cloppert, M.J.; Amin, R.M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. 2011. Leading Issues in Information Warfare & Security Research, 1(1), p.80.

[16] Bowen, B. M.; Hershkop, S.; Keromytis, A. D.; Stolfo, S. J. Baiting inside attackers using decoy documents. In Security and Privacy in Communication Networks, Y. Chen, T. D. Dimitriou, and J. Zhou, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp.51–70.

[17] Dropbox. https://www.dropbox.com.

[18] Risk IQ. https://community.riskiq.com/.

[19] The world factbook. https://www.cia.gov/library/publications/the-world-factbook/fields/402.html.

[20] VirusTotal. https://www.virustotal.com.

[21] Platform – Access to underlying platform's identifying data. https://docs.python.org/2.7/library/platform.html.

APPENDIX A: LIST OF DECOY HASHES

Hash	File type	Names
013cfbe82080762aaa97cb774fe084131e6a94ee5f6604fc5c975d56b03cd086	GPG	calii.gpg
025d161e9907d858195cf22f0fb00b94adf6861b9957afb8a663307cb262bf3e	WORD	Cuestionario.docx
03d2ae661f30d94a1da07697084b62e7329ccb63d59152e5d151d6202cb36dee	MP3	001_fiebre_de_amor.mp3
13a0090019a4f4f36d22647a0870fdb121070d6927e287d88ddac4179c252ae2	JPG	saradesnuda.jpg
1493413566d3b959cf95e46e47c629f656a19b93ead3500b183ec9f7c431ed3c	PPS	HotBrazilianX.pps
1e3c73dbafe5e5fd9d66ff8a187e2ee3a42a643badbc2ab251ee58883b302ebc	DOC	Deuda_del_Estado_con_Instituto_de_Seguridad_Social_de_las_FF.AA.docx
267aec2b429bc40e283d105adcede8702a201df4bf852abbf126555111bada67	JPG	LISTA_DEL_RADG_N_0931208.jpg
2c4ade7c7d275f15cacb09f5fc2ec72596317c852f0ae04b4c8a743d6fc192e8	PPS	Curriculum_vitae.pps
3092cc06a4f12ae61d25bdca845e713e08ae2aa73a07f976a7036af1eba92fde	WORD	Nicaragua_denuncia_ante_la_CIJ_las.docx
346f38711eba3d960c7d58f2d555f16249a3107d2cbc26b39af34cb61912e4bd	PPS	ProfeciadeMariaenFatima.pps
36f08af4592f3582aa1793e703e4baa5f196c2937f5de659721a26922c04a4db	WORD	Aniversario_de_cascos_azules_ecuatorianos.docx
3d955a4ed6eaba916ac680d9a0dcc8ff3bd83eec7d97a73c5f66b5a13f0e80d4	WORD	verifica_em_Dourados_MS.docx
48a0aed89d68aac81d0bf9b49470e8fc9019d1c586648e0440c99420215c8edd	PPT	INSTRUCTIVO_LOGISTICO.pptx
4b6aaaa21a2abaf031d17d73e1f6f87f0103d743c25295feaf3e084c4cb7cef9	PDF	ramadan.pdf
55179cbd95e7e25ce793cd55dc49dc44aacc0177f2a968507ebdf5641c4ff76d	PDF	Para_su_analisis.pdf
57b39ba4303fcea2ff00f7c5a584dfb1a675ae42459fc6147819f718966027e2	WORD	REINCORPORACION.docx
5acb4d7af14690a5034fc9c52b387259b0e2bd232eab86bdd46bdc2bf3d89ad6	DOC	Notificacion_Judicial_No_121523_2017.docx

Hash	File type	Names
5c004089feb719a9be2b614b02f4c46d463b26f0d9f1f119d7b45fba39618e7b	PDF	Semanario_En_Marcha_1756_11.pdf
5dfce01e5fbd03cbb3e3e6a9d1e59438b8af66a679e9726dce3908db76e701d1	PDF	RDGMA_07_4432.pdf
5ecef1e042a477d36dec2e01e6bcc2e6109e5b0be94719c52d15783cb9ae11d0	WORD	Notificacion_Judicial_No_8030923_2015.doc
6321163ece7fb3dded6a499a45169a8b43aa70331ae6dcb322f2ff2b1b06bc7d	WORD	Informe_Derechos_Humanos_en_Nicaragua.docx
65a960932315239c8ead7bee7c3668aa19465aab4448ac07ae9d4b6eca97685c	PPT	El_Arte_De_La_Guerra.ppt
66a996b13c801e6785a1b5817665f4c6dd88128b20fd044fdb04b858aa1aabbd	DOC	INFORME_DE_PRENSA_NACIONAL.docx
70d2b415883670922075c237be320857b065ec09cd9bcee6c00c663add408a38	JPG	01.JPG
7392207affc0d3fb15c8d466739aec9ae2ab0c80f29024c1ddcf881ef97fd94a	PDF	Justicia_transicional.pdf
7433e606673c795d8168e73221903723af4fc0cdf2185a4c2585eef7b04a8323	WORD	Notificacion_Judicial_No_8030923_2014.doc
7477348b41e3eaf22c9b97237a42bc32538ea676e8e5855872a8a95791ea9a71	WORD	Bolet?n_PAT_034_UADMNE_Visita_de_Guardianes_del_Mar_a_repartos_navales.doc
74a3ff07154e48bcf040105a786e1a59dc74f3e81eea729c3aff2ee356df8d7e	WORD	mandado.docx
7519b655a60d139176c287571ba0ccb39e87bc844b8d9a14878e2482b725f671	PDF	ORDENES_GENERALES.pdf
7682fc44a44e6daf94489348d0ac2789ccbeeae01a598f231d654a65abf562a2	JPG	1.jpg
7bc86c143d949d58793916c757b5e08ae97f1cd1cc5c657e7167816560094fb1	WORD	carta_social_de_las_americas.doc
7fba2b9a65193af775cd30fa9d0a79ac4419a7bec6d6b94dc43d5956e1e7fc16	DOC	Requisitos A?o 2017 Ayudas Socioeconomicas.docx
8415300b1c02db9463a7b090412a5d9133ef33b8b26414c437d5a8d498a0de4a	JPG	l.jpg
8711b9da265a9a676b05d223452af8a9709f6f5074d1ecaaede6e9d9d708377f	WORD	DIRECTIVA_MANDO_OPERACIONAL.docx
8aa29fe700a2d5416e1755dbd6c98174c43e9fe04a7644115b84dc5c4090f44e	WORD	Parte_Diairio _065.doc
8f2c6b065f84cfea969caa0bce19a3b0651623c3f7f1a6c0f3f8c06bc766da66	WORD	Notificacion_Judicial_No_121123_2016.doc
94daefde7908a6649cf5194eb0dbc1c4df2fb095e1c18a9cf1b340ecc04f1c8e	DOC	Notificacion_Judicial_No_121523_2017.docx
953bc952120c6d2a167e3952787e1279ee8ec839b976531cde549612a504e53f	JPG	NinaBonita.jpg
9a7c680560c581b54961f37aad5cb50d1d29559811b1291e0c4a7c1a182a0d84	PDF	Mensaje_de_un_preso_pol?tico_Mando_de_las_Farc_Ep.pdf

Hash	File type	Names
9aa15c6ebef8f5c4c5b2fa3d6e420f9202b979cca010c13bb415be48f8f923b2	DOC	Cambio_de_inmueble.docx
9af59e63dd4f7e110684bca9d30fbf3c06b83bc461588e4e322a2f35e4c75cbe	WORD	Padrino_Lopez_Hay_un_golpe_de_Estado_en_desarrollo.docx
9b9ae069f858bf3576c1e46d74ea2e695dba18a10a0962686686d0c31aa51d59	PPT	Suntzu.ppt
aa89947c1d50ae7eeeae10b2d14ca0e72e9059d48800981372584f6891dc23fa	PDF	713751_mc505_15.pdf
ac5aae0e3f5ac96890f656f30463d55f5969bb9c1054b3f9d0a8d3cb0b64bcf8	WORD	05_10_2016_INFORME_DE_PRENSA_NACIONAL.docx
b034ff67b04a5c358c35be8d227e0af9de13fc9133b64e22ee1448d1b408bbc8	WORD	ROSARIO_EN_MULTINOTICIAS_13_ABRIL_2016.zip
b16c7693df3870c1ac8e3e7e221a96282b4a55bfef5977f57672ba7707c3ba56	PDF	Citacion_Judicial_expediente_10388.pdf
b2c40e192d3ae727ac5b9775480736e5f0a856c7aba8c1d368044afe37543d81	WORD	Denuncia_penal_o_querella.docx
bd7f20549ef7456251c8ae6720fcd19a61e7e8b7a3fadc5a4e94ee634e913fb0	WORD	DECRETO_No_18_Duelo_Virgilio_Godoy.docx
c49d8e2ab1709974668660f8445144cd0f4b68f076fde8be929126d3453bacf5	PPS	Terremoto.pps
d9e393350a9ac0604d5f6eb1dbd5c5417615b847e8ad684eb9d5fe2745e47f14	PDF	RAD-0677-CEOFANB.pdf
dad6de8b3ce07bfdf113497b4028e2bc7fdebb297de4fe59283a033873ec9588	WORD	Articulo_sobre_funcionarias_de_Nicaragua.docx
dcd67236a22f2cedef26146ad7314c594463ef3ef5ea278a23cefeccaf3010bd	PDF	NOTA_020_NY_Coordinadores_Nacionales.pdf
df80bc45ce8fdc23c01b581d6adf50d79945f1d81d473af3ceefa70cdae2f2bf	WORD	Articulo_de_Opinion_Heinz_Dieterich.docx
e2e6449711d9a7e0734a3754059a10b2fbd377a2e527e151cbcff064324cea8b	PDF	partes_2010_farc.pdf
e5521e9cf04fc97addb169b0a87bedf9eb0c4884270eafb6962380ec8f2662b6	WORD	CIRCULAR_8_OCT_2016.doc
e97c49fbc77642c8c655192612b3d0e7ddba1580e969cddbf0e964aecb3f3fdc	PDF	FOLLETO_semblanzamono.pdf
ee8c3f5150b33dacbe2372057face554a95fa79ae607dfd5ab2c71a5b3db34e7	WORD	PARTE_ESPECIAL_COMANDANCIA_GENERAL_DE_LA_AVIACI?N_20SEP15.doc
f01139eba43147557faaae5e6353faf5862f4a6615ef47143742799145b68f54	PDF	semanario_en_marcha_1758_1.pdf
f21099e550f2cdee99c5f40267c6d4bac0f608f047ecd81dc89516c16fc87d25	PPS	Hermosa_XXX.pps
f65621214898033320f18921dfb6c21f07b0ee2e8dbcb93effd496f02e279c089	WORD	Mision_Secreta_de_la_DINA_en_Washigton.docx

Hash	File type	Names
f9570bd13528468e15013f3518db836b00861d5085b94e61541024e20cd28395	WORD	Ministerio_de_Defensa_ordena_al_Issfa_que_no_suspenda_tres_prestaciones.docx
fba6700308e7a6213104c03058ed60c9fc83e06871a28a01896cebf0185b38c8	WORD	977_REG_IN_CO_012_V1.doc
fdeeb297ac54b7e77f76ea1e2259491e5827752fe797bb41b5284c5047f87fbf	WORD	2016_00109_01.doc

APPENDIX B: LIST OF MACHETE STAGE 2 HASHES

Hash	First submission	File type
01a1e15d0c96a0d24127d70db5c9afb8e2161bfade0f83d5cf84185294f4e789	2017-09-06 04:55:41	EXE
0754b184f6639614350c293309a1beaac8b138981b93f66c7ca204dccd60ba9d	2019-05-02 21:47:46	EXE
085b80120b564a0e1abe8b9c6f060fd2a6f235cfa04b5e6edf49880a69505350	2017-07-12 17:57:07	EXE
092fcc90317dd683791776e92b56dafb0ba826803f60001c0283b5fabcee9375	2018-11-19 11:43:00	EXE
0972e075b70ea6f43b4a6f2c5e7f9329c3f4b382d7327b556131587142a3751f	2016-02-06 18:26:21	EXE
0ace83a066992a4d9155c1884361f68309759a9ccb7b8c660c9d90cbcb7d58d9	2013-08-23 12:04:57	EXE
0b11a0994b25ce03c90dab61facccd106bbe67dc2f040db12d34b831331f8d93	2016-12-11 02:01:23	EXE
0e5ec0e1f27d64f0876f77f28701dcaf417a3793c1b6052d18ed65fdcb9fdf8e	2018-04-26 23:44:05	EXE
0f96d5ecbfde8222510e926438be192f583ec4622acd72bf8649d38fe8121510	2016-02-19 17:24:25	EXE
1206f315415dd7bb07ac4a1b0107215bc3c081a34bf1f4b78d6f9bb5167afcd3	-	EXE
12140cec8e75fc291aecda570f26c4375c633c373d5590ee8baea6f54996f757	2018-10-10 14:41:50	EXE
14e3053393d9b3845cec621cd79b0c5d7cd7cf656be0f5a78bb16fd0439c9917	2016-12-07 19:52:25	EXE
158c55f56a37e93f957a2b359917b4fb7886d5ca6fe1c44eab4ea8fd1542edc7	2018-09-26 02:23:47	EXE
18d2730ccf0dad92efe9ff2789af3c36b220e87f691d1cd421faf2c572edb89c	2019-04-18 16:57:14	EXE
1c0f253b91b651e8cb61ea5dc6f0bf077bec3ab9612e78f9a30c3026e39bf8a8	2016-10-05 03:01:31	EXE
22f52e4421134fa334270ff15b2726d7781ad84f1ce76d6ca0b7afe4223bcb57	2017-02-09 18:20:39	EXE

Hash	First submission	File type
242a1b8f9253b678c03507f137ade7a369c43964a9e2ee21b88289feeb61d208	2019-01-03 09:16:25	EXE
257723b1bd9f77a6d134393f3abf8423cc4cff534e260b1f928d6d2c6c81e4dc	2011-03-10 16:02:31	EXE
27c2a5dafc976e9c0b71e6ad80a3584a50a5e6bda0edaee1292a7aa9bc052816	-	EXE
28131cea5009f680064a7962279ebdff7728463a6d0a30ef2077999abe27bee7	2016-03-28 10:55:28	EXE
282651843b51a1c81fb4c2d94f319439c66101d2a0d10552940ede5c382dc995	2015-11-12 21:04:02	EXE
2f878a3043d8f506fa53265afcea40b622e82806d1438cf4a07f92fb01d9962f	2016-11-23 17:33:46	EXE
3156023a48135a5c64c09e5da2aa47bfa624edf16d9b357df45022e0d9a9039e	-	EXE
34a05e770220e4011dc73d018d89c16d69e2e974135ecd1ed91f90436f887c5c	2017-06-22 01:19:04	EXE
3937a4679abd97fe7e692b134b494cf823fa2d58f84aeccad86da11d15332016	2013-08-14 20:21:02	EXE
3b326f99ce3f4d8fa86135a567ba236fcc0eb308cd5bbfc74404a5fe3737682a	2016-12-05 19:42:52	EXE
3db990554b6bee43a2057e5ceb892ea8f048a86044ff61647ac967b0827fc832	2018-05-06 00:01:43	EXE
3fa4defac48a14e983a5d224bffbc81206561a559f4e393bcd6c232b0450fd23	2017-08-15 16:37:59	EXE
3fc825099c216decf842604e48346c7d56cfb7b796a82b308556111c3e117d91	2011-03-25 16:33:31	EXE
40f46b60e6fd74b01c7b6dee4070e8647e2ff39c19bab09cd874872c28008093	-	EXE
4367aadb5325cf7ee134e33ae806efaf5d555ce02ad02fc80659e9bc08995d32	2019-04-18 16:57:16	EXE
52cec92c27d99c397e6104e89923aa126b94d3b1cf3afa1c49b353494219162e	2013-10-30 15:09:27	EXE
57a40d6a7db3f5ca56458d73b74051f57f2f9fb32d9d8e792647ba65f22866f6	2017-05-27 08:05:38	EXE
581ccee516a8cfeb64dd5feb881a3d294da3adc3f4afe506fef4852452441a7d	2019-05-16 15:00:46	EXE
58c0179ae3da711df0df5669618c9e32ea7a86eb4de849a008c72372e0b89ffd	2017-02-04 16:26:24	EXE
590bfc6b7fbd89e629e551fa9d70f1cdc0773d73dfea503d204a05014a8f0191	2019-02-23 00:34:22	EXE
5add76389e065a538bb097caa8637c4fe398f9d140d54e68df8c6ca536cf745a	2017-05-09 16:18:46	EXE
5c84ee01eacd2abb44b8a8945bfa0349a0804e3243931cc3277f469d3142abd6	2012-11-29 05:31:13	EXE
5d524fad6fbc403476b2e845c9449aa1018fbc8573b1ecb13a8f548b7b2ed62d	2018-04-26 23:44:33	EXE

Hash	First submission	File type
5fed1bda348468eddbdd3cdefd03b6add327ff4d9cf5d2300201e08724b24c9a	2017-02-28 03:14:27	EXE
613351824cabdb3932ab0709138de1fcff63f3f8926d51b23291ebf345df4471	2016-09-18 18:46:49	EXE
635f974fe32ada66247a47d422a3e9315efaeac6eecf08d27f5957c696ae8b9f	2017-03-31 15:04:10	EXE
661901d87ffc4bd83d1410b9be0e9020fca6798eda1c4444fe6f13242cf2f347	2017-01-13 00:53:04	EXE
672ab713d09aee8ca98b12a16c799f74dabc4767daf370d7d959c40c17d1ad49	2014-11-30 17:27:03	EXE
6917db24c61e6de8be08d02febe764fe7e63218b37e4a22e9d7e8691eee38dcb	2016-11-25 22:01:58	EXE
702f804cf9672ef6aa1c1d99d6a2b0702a17434c3ecf049ebaf582a202e24654	-	EXE
704db74937d0e136527167c85ffe13be87671d8adfd11fa9132830cf1deba3af	2018-09-05 23:19:37	EXE
708ea731a9e26eff26edc6d175f478a1b2936dc9f09bbd445ed3598212e12bf6	2018-10-10 14:41:27	EXE
732ceaf2ce6f233bb4a305edc8d2bb59587a92bd6f03ea748bef6dd13bf38499	2016-07-09 14:35:09	EXE
767ae90931eee786efcec22105d0faa7ba629fec6b926ba898d50c2085bce727	2011-03-18 15:20:24	EXE
76af6661f95bf45537c961d4446d924a70b9b053ddbf02c8bfda2918d5ac90f5	2016-05-12 08:41:15	EXE
7d7e175d5d8cd2ba50c005bdcb7691b8abbd9cbf23b3823484bbf447a8f8df05	2015-10-22 17:05:19	EXE
7dba07fe71a868714e81c672b78f0caef05142ee0f0b32fb5945831e235fccf4	2018-09-27 16:27:21	EXE
819351fa37aa0701325f92c904cde147b06fd61ee161fdf77e9946f96774e841	2017-03-16 16:09:57	EXE
83b0444e856ccd72e3a5fa98189499a0c8c69765845c68471ad6552d07070712	2018-10-02 20:30:35	EXE
8444103dac4c2b559e8dbd6b6984b943868ffb11141ebee50d4faa022d8948a5	2019-05-16 14:51:53	EXE
8aee80339609393cf745213bd079bb8793086ed585d84744085c28a0885cc053	2016-10-08 11:34:45	EXE
8c6053476681aabed32cf9fa5eec5a7e34c0d4413501a22bce8754c6ebc2c13a	2017-05-05 14:06:48	EXE
93348d6dffd45a4c01b10fc90501c666f7a5360547e2a025d5980f235e815cc9	2017-01-31 18:38:25	EXE
93d21d1810e83fc703e02db9e1fc71e82f9bd7f9a04a83a5a0d621ab830d8572	2019-05-17 03:32:29	EXE
96c88cf46b041476954fe7a63aecb9972dc42b1b91bf6e5186cc4857fc3c8840	2015-09-12 22:39:54	EXE
9c09d32be276498a5a82a875b19d3fb9bf2e5fb39a7790df4fa335aa69f41721	2011-04-18 19:13:19	EXE

Hash	First submission	File type
9cbcbcf748b59191c1e219975fabf97e0034217c3bec25453d7a74131c59161b	-	EXE
9d1247333783333e556d29684eb05060e8c88eb476a5803d0879c41f4344f6bd9	2016-05-01 18:58:51	EXE
a089ebe39128ba4db0ac88d41ea7222f0b6ea6dc5fa14d32a811454647e76555	2011-08-22 17:34:51	EXE
a13bf3977f173389848b24ea7ee3b516217f63d58b8a67c3a02958d6cd521caa	2011-09-08 19:36:10	EXE
a316348ca9bec675fa0601a18403ad27948591f63c82b9e262e3b1fb65c3b3ce	2013-09-03 16:57:36	EXE
a45004be7c9dd3f194b21ff097fbb38c908917fb6222caa9e7fcbd8ee9734472	2016-04-15 01:51:56	EXE
a997b1c8c0e720399a2e042b2cfb9e43a06bf7aeb073d3b9b111653b79ef13f1	2016-10-09 11:02:54	EXE
ac0cc80cbad209e37d63ad3f9ce4d79d3c0b31e24be08303bf5b2acb104a5008	2011-03-18 02:30:46	EXE
aceb2194737884cf2dccd805611390b5c0fb43c67a38af9d95fc9794bc44b5a8	2017-03-22 19:48:49	EXE
b50f908ddf754ba269c0982fbd14d6ea85741282bd08473b1175394cf21fdbd6	2019-05-07 17:47:19	EXE
b5ac86677c6059c37c3b6888ab2849b1750463af822642bfb1db8855f0bba06a	2016-12-17 06:51:12	EXE
b635e99e5a68766aa4cbd9fbb26173d4ecfc80ece4adc16f7ad6552db5009c12	2017-03-10 17:49:16	EXE
b8341d72c3b2ecd90a18d428a7ea81a267eb105a36692042fe8904b0b0ea6b07	2016-04-28 15:57:36	EXE
bbaf6c934df8eae63922b49daed665200a53107c2f6fdf19b5d99f7ccc508f28	2015-10-01 18:32:55	EXE
bc3cedfa6a2c05717116b29c2b387a985a504a97ce0e0a43212b3bc89ac9cf95	2015-10-23 07:00:36	EXE
be7249b73a8783b7d3105e8d3904f492e0e3b2116ebdbf7fb893a2de3d301854	2019-05-08 05:15:41	EXE
c156212dc079992c3ccbe06410ba8d48fe1144b09c36f600162da5ccb80f3f12	2011-05-18 11:56:47	EXE
c1d8e730c01827d5425ab6c6ae41929b4b9e61459d07ec1771c3c0e6f706e0fb	-	EXE
c463a4c933a28090d04663ce007a7ae0a8dedadf8ede063ccf0b3c6a659e909d	2016-02-06 04:35:50	EXE
c634f10a475df833c55610e38e947dda278b474b6650bb8570ab3801be43739f	2016-05-02 13:13:45	EXE
c7dfb4f774aa2b72e17501e43c49b131eb502cb8a8ef1812b1cda5773abe345f	2015-10-08 00:35:10	EXE
ca38869a6c455b56429c9a5c38ba4ce244da1312d650c71420d062820a3aa563	-	EXE
cd7b8b4bbcfbbcdf0034cc21b022ddaf0cefef11fd288a134b42737e54ca16ba	2019-04-26 11:20:25	EXE

Hash	First submission	File type
ce4e407b32f77300c4ea12e578575a486af3b4182d6738e226dc77b1965d0c95	2018-03-21 05:14:24	EXE
cf18f4f24f0ebab20620c32ab5755f58585d2e1363153c96a926fa284dada606	2017-03-06 20:53:53	EXE
d07f6dcfd654eb8cba55aa06d91757872d10f72acf34e915318564151fc7456e	2017-09-20 12:14:03	EXE
d0dcd14ffdadec81e23de6034f1d012d1b1c4f54f3f3f3d492a13274a316ac31	2017-06-16 21:04:44	EXE
d2b81d32ceb61640c72d2af241527e942218e2067c7a0ae4ff5b6eabe659255e	2016-10-12 04:21:07	EXE
d44288a48327bc7dd88e3ce5e755881b9b04f59f1a180fc6f51b85f231d6ebdf	2017-03-31 14:00:16	EXE
dc316fb6000da33d0b42db4036031f0abf4e82791bd5d2c1c803adc6a4ed4106	2011-05-03 22:23:55	EXE
dc91c604bd680a8e49fd38d3e6aab3e8114d2e08ba6467597c846da6c1d1095d	2019-05-04 22:07:39	EXE
dccfc0700608a2d2a8c1a2bfde560347ce62b4a989524e87687b17dbc6447117	-	EXE
df8e038a95c2f40f04354ab0f9f5d86253b690cb0ce89e10124c879814912f07	2011-09-12 16:29:32	EXE
e427c7026c7cb2e62c13333508543230c26f7ac92ccf8796f6c4dcf9f15350f9	2018-06-09 01:48:34	EXE
e55cdfb5779749152c54be708f037d8fdca3b5378dfbebf6616f377bc4958dd1	2017-03-23 13:14:04	EXE
e65b921bf81a04a973cb62891fdc6cd1c877fec1e29c16442689ea118e06b019	2011-03-16 17:33:54	EXE
ed3fb28c4ca3349877b389c6b165a5408a8e749ec67e55e706182c2c483fee44	2016-07-09 14:46:59	EXE
f143fb756c03f403ce1388343d6646d391ba0864c520aacecbaa8fa67dd3f436	2017-01-27 21:01:11	EXE
f5c88b38183d170656aaa88655fafa6d282338e708dd09281bb96eab0fb24ba4	2017-06-13 03:28:26	EXE
f78466d0d24e11c67277c8714d3060295ca264b83322834a51c0e9658ef970f7	-	EXE
f8f76827e0c7afcb8cf2bdae43e14e265568857fee145f38d31d23c89d58a465	-	EXE
f98ef639797013d6eddfcc00f7d208510ac02ca49bed1eb9250156081d5ed0ab	2016-07-09 14:40:09	EXE
fabd49d071d0ef11e65e45416e90440f68d680ac1089b71424bfeff4589f4bbb	2019-04-28 10:51:59	EXE