El Machete — What do we know about the APT targeting Latin America?

By Veronica Valeros

Published: 2017-06-26 · Archived: 2026-04-05 16:58:34 UTC

‘Machete’ or ‘El Machete’ is a targeted attack campaign that was first documented in 2014 [1] by Kaspersky GReAT team. Early this year, Cylance SPEAR team reported how after all these years El Machete is still active [2]. Let’s walk through what we know about this targeted campaign.

Machete: A Cyber-Espionage Tool

Machete is a piece of malware that has standard characteristics of a cyber-espionage tool. According to previous reports [1] [2], the malware capabilities include: capturing keystrokes, capturing screenshots, capturing audio, capturing webcam pictures, stealing information from the clipboard and documents from local and removable drives. Most of these capabilities are obtained through external modules written in Python.

The Targets: An Unusual Bunch

While not unheard of, is not common to hear Latin American countries as targets for sophisticated threat actors. Since the first report, a series of countries remain as the most common victims: Ecuador, Venezuela, Peru, Argentina, Colombia, and Cuba. According to [2], victims were also found in other countries, including Korea, the United States, the Dominican Republic, Bolivia, Guatemala, Nicaragua, Mexico, England, Canada, Germany, Russia, and Ukraine.

A Decade Of Activities?

As mentioned before the first public report about Machete is from 2014, but the article mentions that the threat is believed to be active since 2010 or even before. Indeed, from the shared indicators, the oldest sample was first submitted on VirusTotal in 2010 (b26d1aec219ce45b2e80769368310471). Thanks to Cylance, we learnt early this year that El Machete was still active. If we place its starting date around 2010 or before, then El Machete has been active for almost a decade long. As mentioned by Cylance, the threat activities have continued working during the last years without major disruption even though there are plenty of indicators published on how to detect the threat.

Delivery Mechanisms

Phishing emails are the main source of infections. The emails usually contain external links to sites where users are lured, via social engineering techniques, to download an executable masked as with a “.SCR” extension.

Kaspersky also reported back in 2014 that web infections via fake blogs websites were also used. In this case, the authors did not bother creating sophisticated web infections, and they just took pieces of code from SET (The Social Engineering Toolkit) [1].

An APT With Hispanic Roots

There are two aspects here to mention: the Spanish-speaking victims and the Spanish language used in the code of the malware.

Most victims are Spanish speaking according to the existing reports. The phishing campaigns, the name of the payload files and even the external domains used to host the payloads use Spanish words and language, confirming the findings. Even infections in external countries may be due Spanish-speaking targets are located there, like ambassadors or political representatives.

It is theorised that the threat actors are also Spanish speakers. The source code of the malware is full of Spanish terms for things like folders and name of some functions. While these facts are not enough to confirm that the threat actors are native Spanish speakers, they do suggest they have at least a basic understanding of the language.

Summary

El Machete is a very unusual piece of malware, not so much for how it is built but for its targets. Latin Americans need to start being aware that sophisticated actors are targeting them and this will not stop [3]. There is a need to increase their defensive cyber capabilities to not only avoid these types of infections but to reduce the time to detect them.

References

[1] Kaspersky GReAT Team. (2014, August 20). El Machete. Retrieved June 25, 2017, from https://securelist.com/el-machete/66108/

[2] The Cylance SPEAR Team. (2017, March 22). El Machete's Malware Attacks Cut Through LATAM. Retrieved June 25, 2017, from https://www.cylance.com/en_us/blog/el-machete-malware-attacks-cut-through-latam.html

[3] Franceschi-Bicchierai, L. (2015, August 6). Malware Hunter Finds Spyware Used Against Dead Argentine Prosecutor. Retrieved June 26, 2017, from https://motherboard.vice.com/en_us/article/d73m8y/malware-hunter-finds-spyware-used-against-dead-argentine-prosecutor

---