Machete (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:17:22 UTC

Machete

aka: El Machete

According to ESET, 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.
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.
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.
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.

References

There is no Yara-Signature yet.
