Il malware come vediamo subito dal report di procmon che ci sono delle funzioni riportate nella colonna «operation» molto interessanti come «Create File», «Read file» e «Close File» con rispettivo path

Apriamo il file (il contenuto del vostro file potrebbe essere diverso) per notare che il file ha acquisito alcuni dei caratteri da tastiera utilizzati durante l'esecuzione del malware – questo comportamento è piuttosto solito dei malware Keylogger.