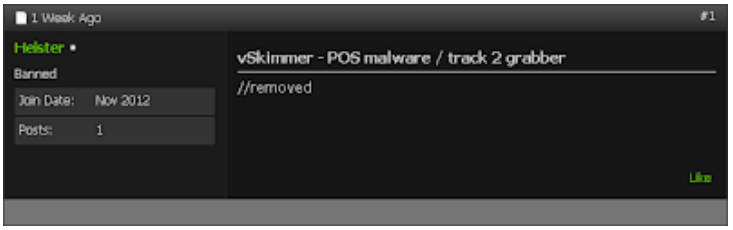
vSkimmer, Another POS malware

Archived: 2026-04-05 17:56:41 UTC

When i've view this post, content was already removed and member Banned.



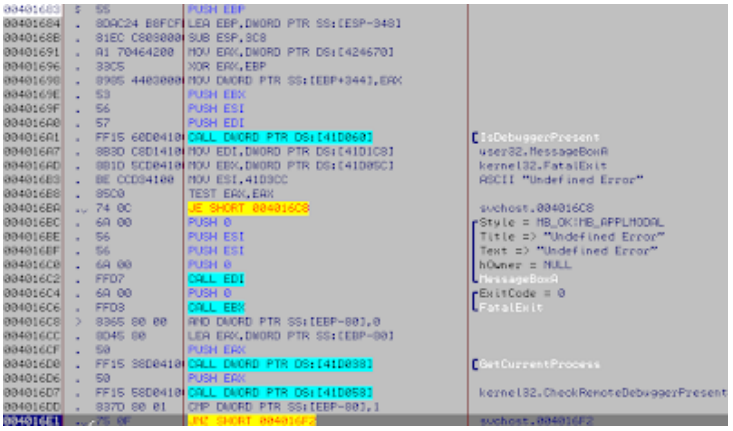
vSkimmer - Virtual Skimmer

Functions:
- Track 2 grabber
- HTTP Loader (Download & Execute)
- Update bot itself

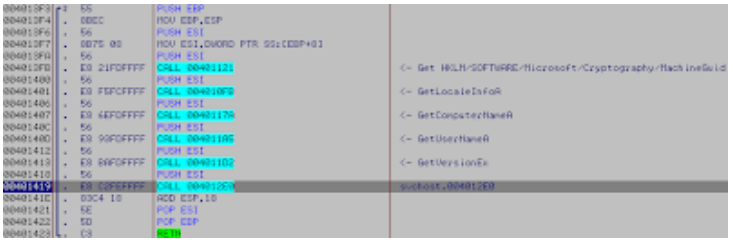
Working Modes:
- Online: If internet is reachable it will try to bypass firewalls and communicate to a the control panel.
- Offline: If internet is not reachable it wait for a specific pendrive/flashdrive plugged in and copy logs to it.

Server coded in PHP (can be modified on request to send logs to remote server, via smtp, etc..)
Client coded in C++ no dependencies, 66kb, cryptable. (can be customized)

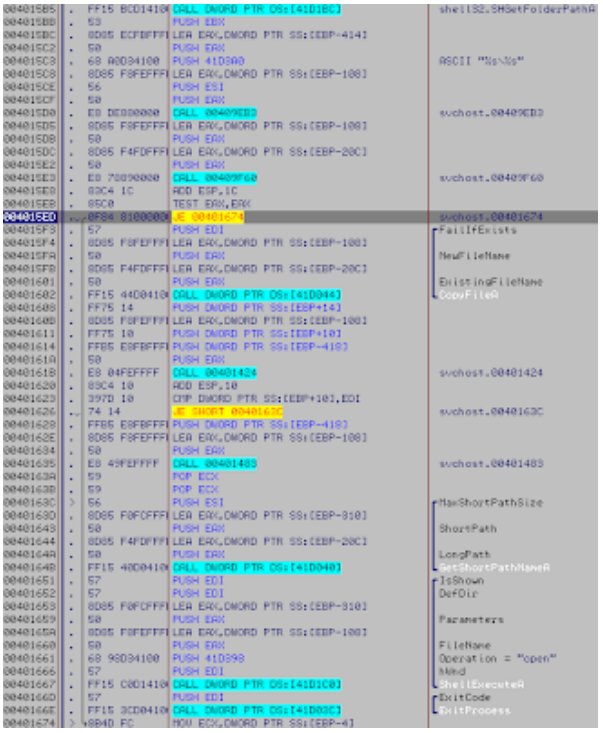
The malware check the presence of debugger:



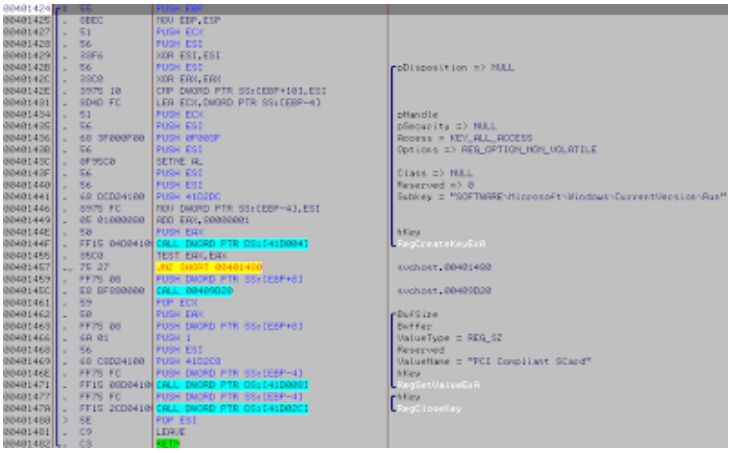
Get PC details (OS,Computer name, GUID for identify you in the POS botnet, etc..)



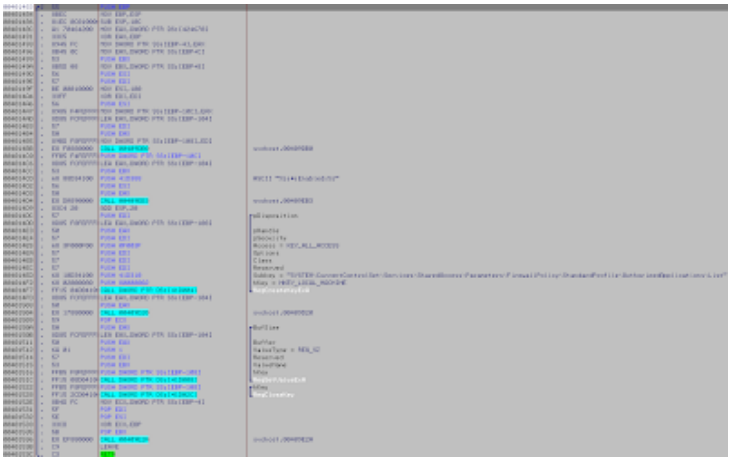
Check if the file is executed from %APPDATA% if not add registry persistence, firewall rule, make a copy and execute the copy:



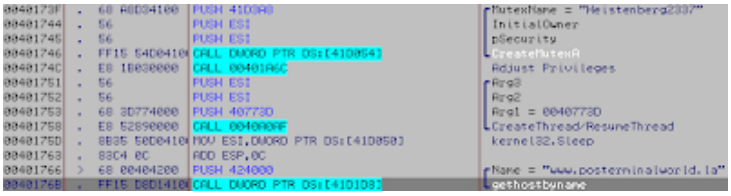
Detail of the registry persistence:



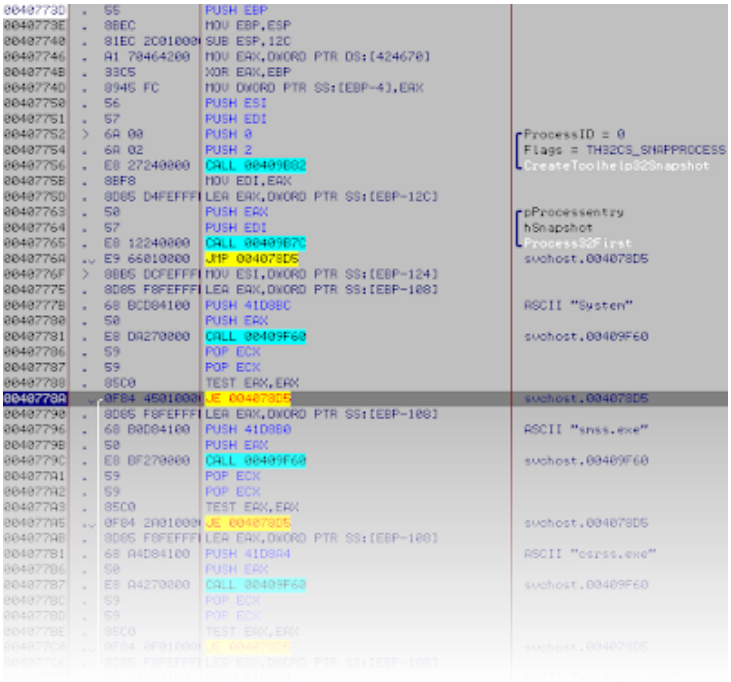
Firewall rule to allow the malware:



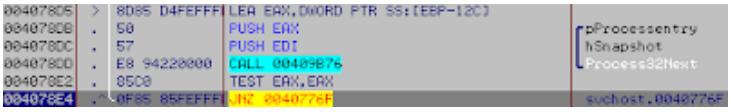
Create a mutex, thread and get host information:



Check for process:

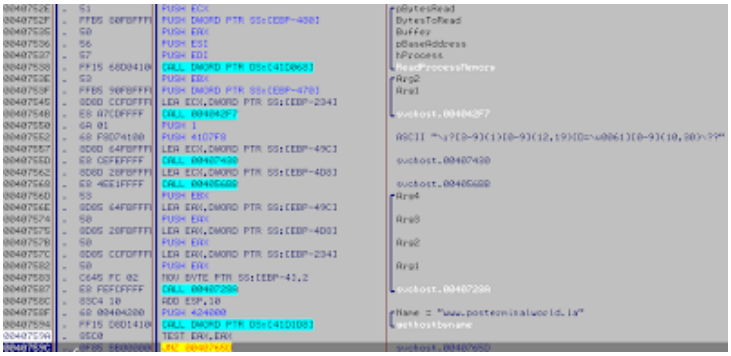


Some are whitlisted: "System", smss.exe, csrss.exe, winlogon.exe, services.exe, lsass.exe, svchost.exe, spoolsv.exe, wscntfy.exe, alg.exe, mscorsvw.exe, ctfmon.exe, explorer.exe:

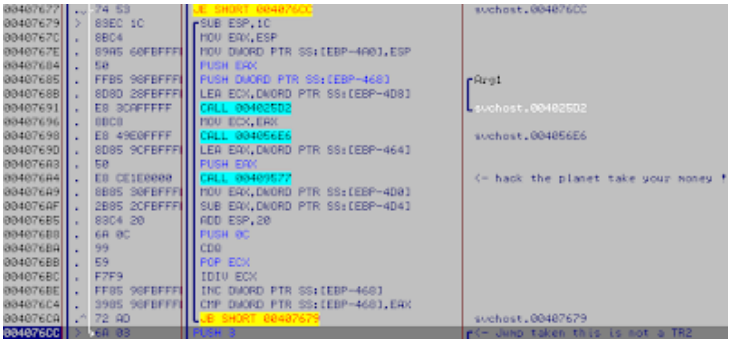


And when finally a process is found:

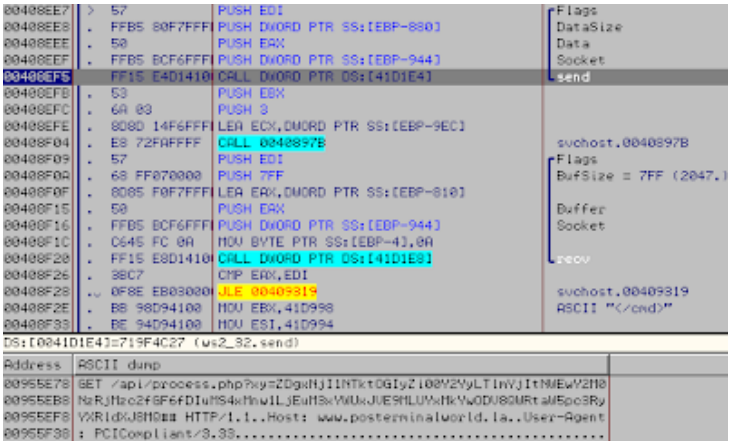
Read the process and search for pattern:



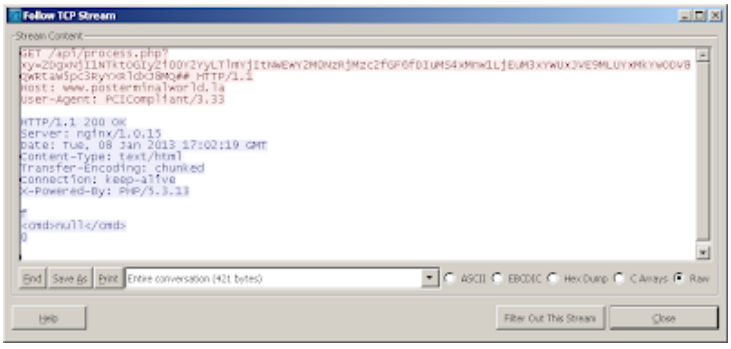
If nothing found:



Get infos, Base64 and call the gate via GET request:

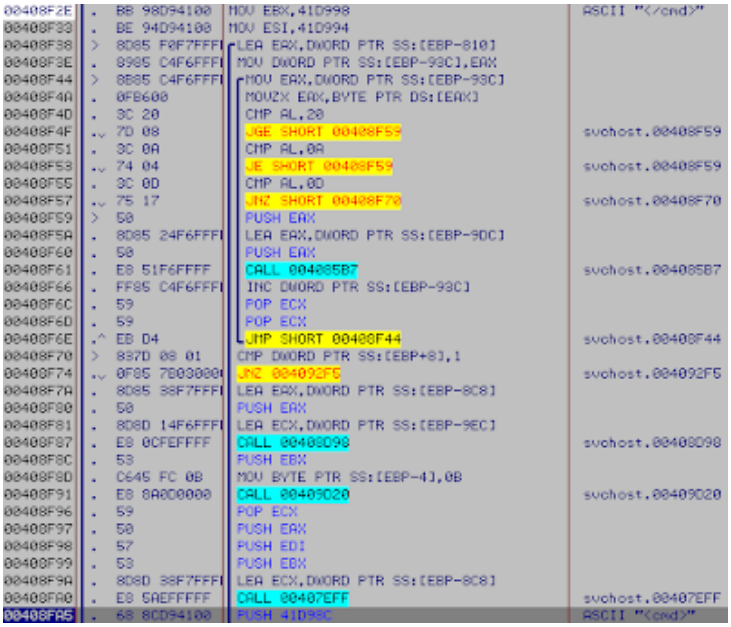


Answer:



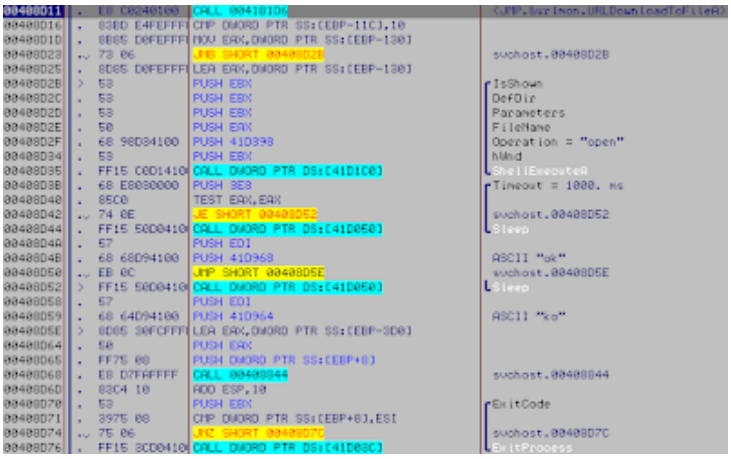
• dns: 1 ›› ip: 31.31.196.44 - adresse: WWW.POSTERMINALWORLD.LA

Parse the answer:

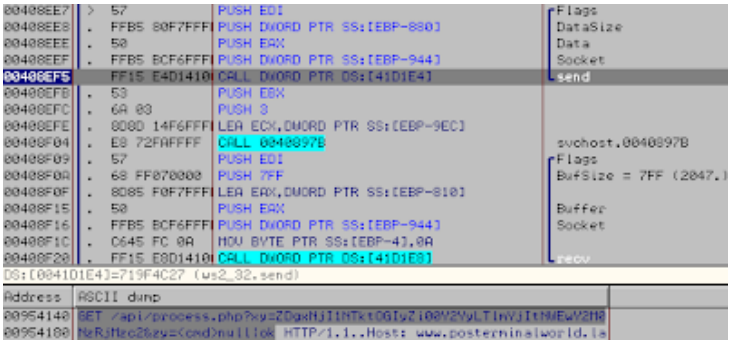


Answer is reduced to first 3 letters and compared with 'dlx' (Download & Execute) and 'upd' (Update) if one of these are found that mean the bad guys send us an order.

For example dlx:

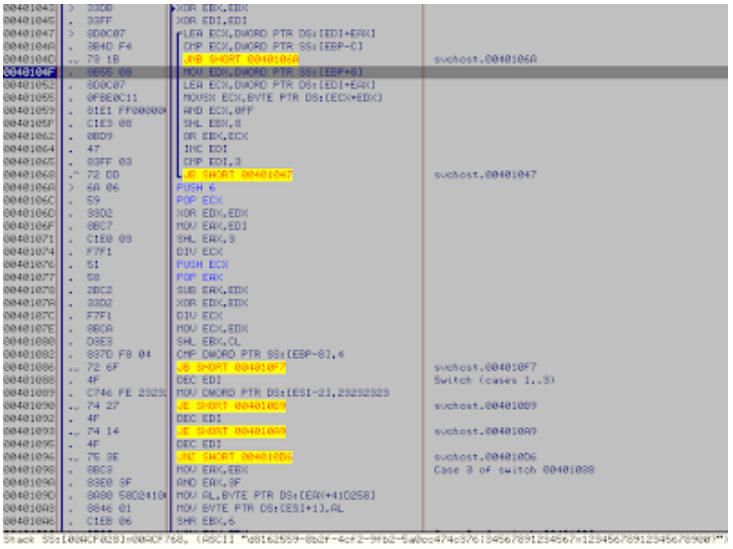


Order is executed and a response is send to the server:

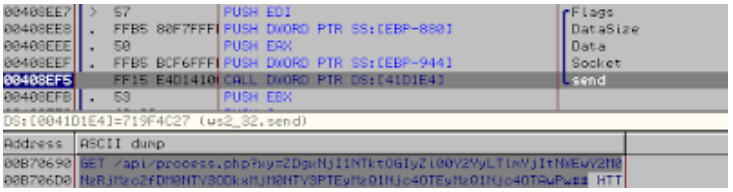


The part i love with pos malware:

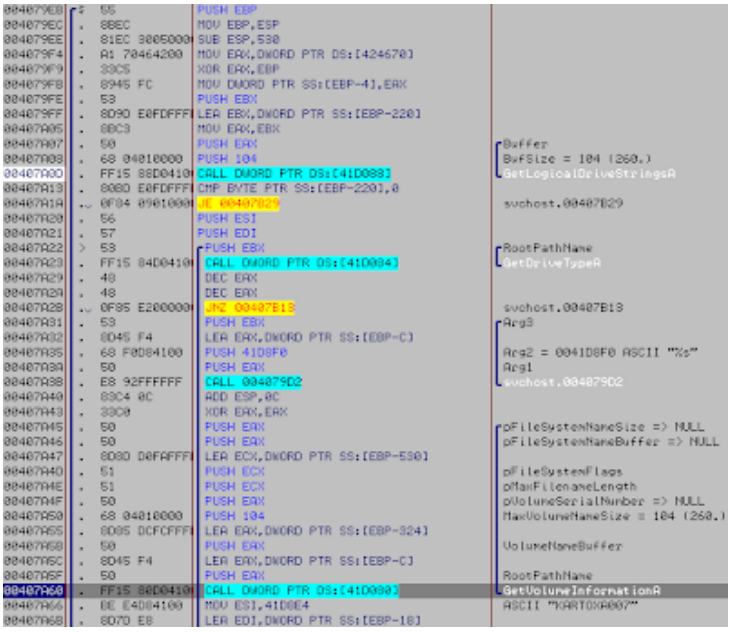
Or just a simple ";1234567891234567=12345678912345678900?" in a txt but it's more gangsta to swipe a card.
So the algo detect the pattern, the track2 is encoded to base64



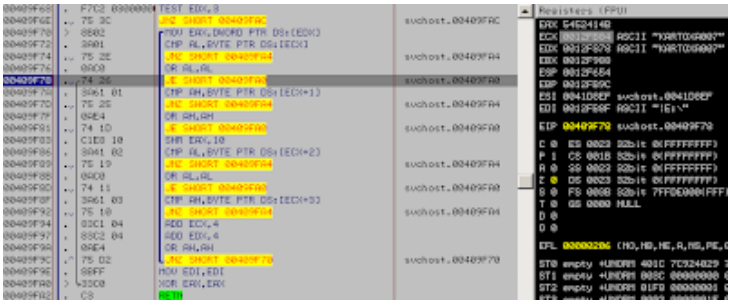
And sent to the panel:

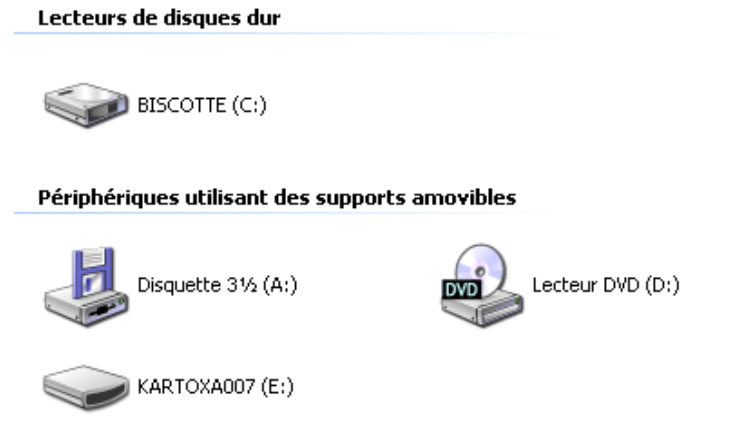


Now for the offline mode, get drive:

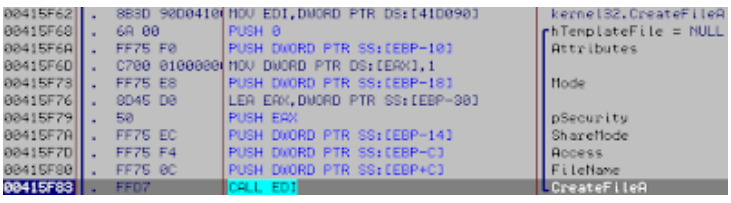


The flash drive must be named "KARTOXA007" (dumps in russian)

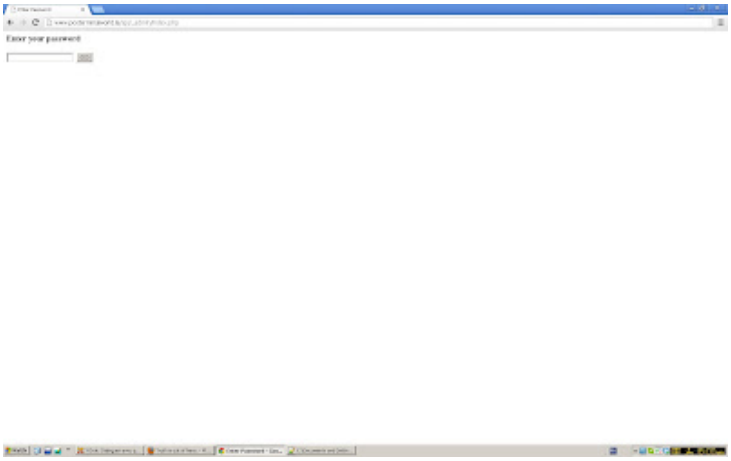




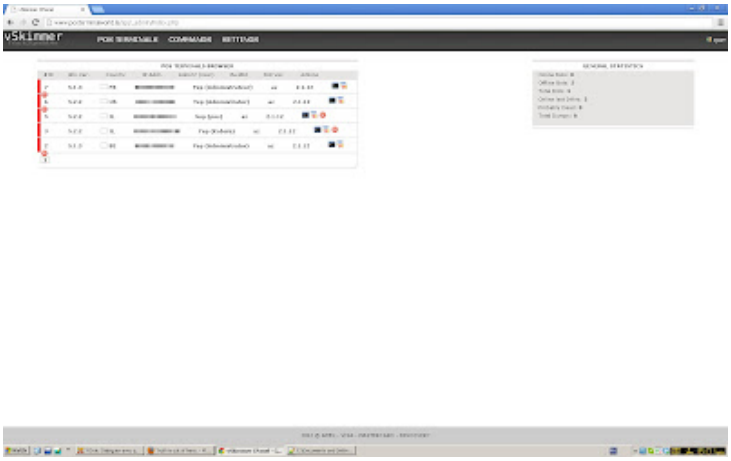
Create dmpz.log:



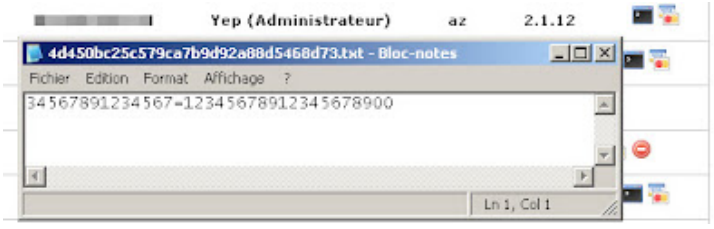
Now let's have a look on the panel:



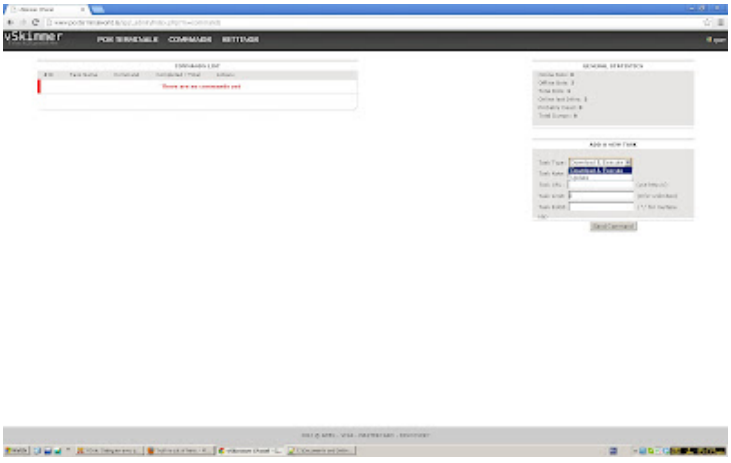
POS Terminals:



Dump download:

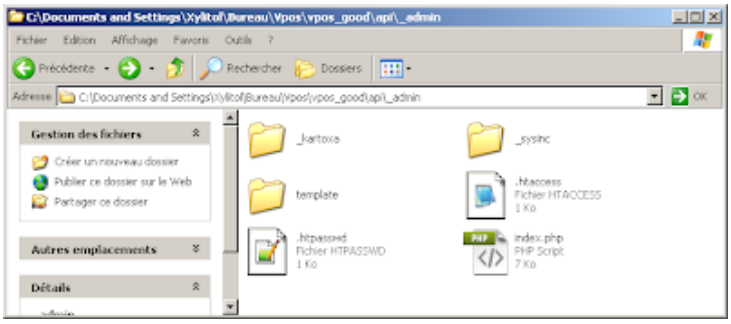


Commands:



Settings:

Dumped.. :)



Sample:
https://www.virustotal.com/file/bb12fc4943857d8b8df1ea67eecc60a8791257ac3be12ae44634ee559da91bc0/analysis/135823759
Unpack:
https://www.virustotal.com/file/4fba64ad3a7e1daf8ca2d65c3f9b03a49083b7af339b995422c01a1a96532ca3/analysis/1358238314
Thanks Zora for the sample :)

Source: https://www.xylibox.com/2013/01/vskimmer.html