

Alina 3.4 (POS Malware)

Archived: 2026-04-05 18:39:36 UTC

The malware come from: <http://vxvault.siri-urz.net/ViriFiche.php?ID=23179>

Hosted on the site of a deputy.



GetPCName:

```

004020A0 . 85      PUSH EBP
004020A1 . 8BEC   MOV EBP,ESP
004020A3 . 03EC   SUB ESP,0
004020A6 . 6A 00   PUSH 0
004020A8 . 6A 00   PUSH 0
004020AA . 6A 00   PUSH 0
004020AC . 6A 00   PUSH 0
004020AE . 0045 FC LEA EDI,00000045 PTR SS:[EBP-4]
004020B1 . 50      PUSH EDI
004020B2 . 6A 00   PUSH 0
004020B4 . 6A 00   PUSH 0
004020B6 . 6A 00   PUSH 0
004020B8 . FF15 0C804100 CALL DWORD PTR DS:[41000C]
004020BE . 8B4D FC MOV ECX,0000004D PTR SS:[EBP-4]
004020C1 . 51      PUSH ECX
004020C2 . 68 B4CF4100 PUSH 41CFB4
004020C7 . 68 F0254200 PUSH 4225F0
004020CC . E8 0C308000 CALL 00408000
004020D1 . 83C4 0C ADD ESP,0C
004020D4 . 0055 F8 LEA EDI,00000055 PTR SS:[EBP-8]
004020D7 . 52      PUSH EDI
004020D8 . 68 10264200 PUSH 422610
004020DD . C745 F8 0002 MOV DWORD PTR SS:[EBP-0],200
004020E4 . FF15 90004100 CALL DWORD PTR DS:[410090]
004020EA . 85C8   TEST EAX,EAX
004020EC . 75 2C   JNZ SHORT 0040211A
004020EE . A1 B0CF4100 MOV EAX,000000B0 PTR DS:[41CFB0]
004020F3 . 8B8D BCF4100 MOV ECX,0000008D PTR DS:[41CFBC]
004020F9 . 8B15 C0CF4100 MOV EDI,00000015 PTR DS:[41CF00]
004020FF . A3 10264200 MOV DWORD PTR DS:[422610],EDI
00402104 . A1 C4CF4100 MOV EAX,000000C4 PTR DS:[41CF40]
00402109 . 898D 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 PUSH 0
0040211F . 68 70254200 PUSH 422570
00402124 . 6A 00   PUSH 0
00402126 . FF15 24004100 CALL DWORD PTR DS:[410024]
0040212C . 85C8   TEST EAX,EAX
0040212E . 75 0A   JNZ SHORT 00402134
00402130 . C705 70254200 MOV DWORD PTR DS:[422570],727265
0040213A . 8BE5   MOV ESP,EBP
0040213C . 50      POP EBP
0040213D . C3      RETN

```

Create a mutex:

```

0040228E . 68 C8F4100 PUSH 410F08
00402293 . 6A 01 PUSH 1
00402295 . 6A 00 PUSH 0
00402297 . FF15 50A04100 CALL DWORD PTR DS:[41A050]
    FileName = "Hdd3yghu9u9ggjd96796hfv0.4"
    InitialOwner = TRUE
    pSecurity = NULL
    CreateFile
    
```

Create %appdata%/java.exe

```

0040286A . 6A 00 PUSH 0
0040286C . 6A 00 PUSH 0
0040286E . 6A 02 PUSH 2
00402870 . 6A 00 PUSH 0
00402872 . 6A 01 PUSH 1
00402874 . 68 00000000 PUSH 00000000
00402879 . 8D95 E8FEFF LEA EDX, DWORD PTR SS:[EBP-110]
0040287F . 52 PUSH EDI
00402880 . FF15 26A04100 CALL DWORD PTR DS:[41A020]
    hTemplateFile = NULL
    Attributes = 0
    Mode = CREATE_ALWAYS
    pSecurity = NULL
    ShareMode = FILE_SHARE_READ
    Access = GENERIC_WRITE
    FileName
    CreateFile
    
```

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 PUSH 0
0040295D . 000D 30FBFFF LEA ECK, DWORD PTR SS:[EBP-4D0]
00402963 . 51 PUSH ECK
00402964 . 53 PUSH EBK
00402965 . 58 PUSH EAK
00402966 . 57 PUSH EDI
00402967 . 8905 3CFBFFF MOV DWORD PTR SS:[EBP-4C4], EAK
0040296D . FF15 50A04100 CALL DWORD PTR DS:[41A050]
00402973 . 85C0 TEST EAK, EAK
00402975 . 74 40 JZ SHORT 00402987
00402977 . 399D 30FBFFF CMP DWORD PTR SS:[EBP-4D0], EBK
0040297D . 75 38 JNZ SHORT 00402987
0040297F . 8885 3CFBFFF MOV EAK, DWORD PTR SS:[EBP-4C4]
00402985 . 6A 00 PUSH 0
00402987 . 8D95 30FBFFF LEA EDX, DWORD PTR SS:[EBP-4D0]
0040298D . 52 PUSH EDK
0040298E . 53 PUSH EBK
0040298F . 58 PUSH EAK
00402990 . 56 PUSH ESI
00402991 . FF15 38A04100 CALL DWORD PTR DS:[41A030]
    pOverlapped = NULL
    pBytesRead
    BytesToRead
    Buffer
    hFile
    ReadFile
    3_4.00402987
    3_4.00402987
    pOverlapped = NULL
    pBytesWritten
    nBytesToWrite
    Buffer
    hFile
    WriteFile
    
```

and if he fail to write he will Copy it:

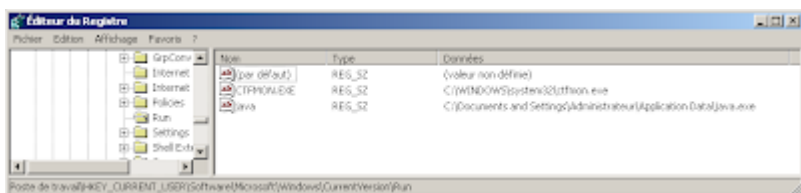
```

00402A17 . 6A 00 PUSH 0
00402A19 . 8D8D E8FEFF LEA ECK, DWORD PTR SS:[EBP-110]
00402A1F . 51 PUSH ECK
00402A20 . 8D95 E0FDFFF LEA EDX, DWORD PTR SS:[EBP-220]
00402A26 . 52 PUSH EDX
00402A27 . FF15 54A04100 CALL DWORD PTR DS:[41A054]
    FailIfExists = FALSE
    NewFileName
    ExistingFileName
    CopyFile
    
```

Add a registry persistence:

```

004014E9 . 52 PUSH EDX
004014EA . 51 PUSH ECK
004014EB . 6A 01 PUSH 1
004014ED . 53 PUSH EBK
004014EE . 58 PUSH EAK
004014EF . 8845 FC MOV EAK, DWORD PTR SS:[EBP-4]
004014F2 . 58 PUSH EAK
004014F3 . FF15 14A04100 CALL DWORD PTR DS:[41A014]
    BufSize
    Buffer
    ValueType = REG_SZ
    Reserved
    ValueName
    hKey
    RegSetValueEx
    
```

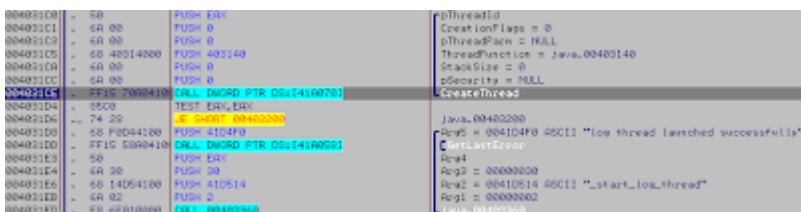


Launch the process:

- 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...



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.

Source: <http://www.xylibox.com/2013/02/alina-34-pos-malware.html>