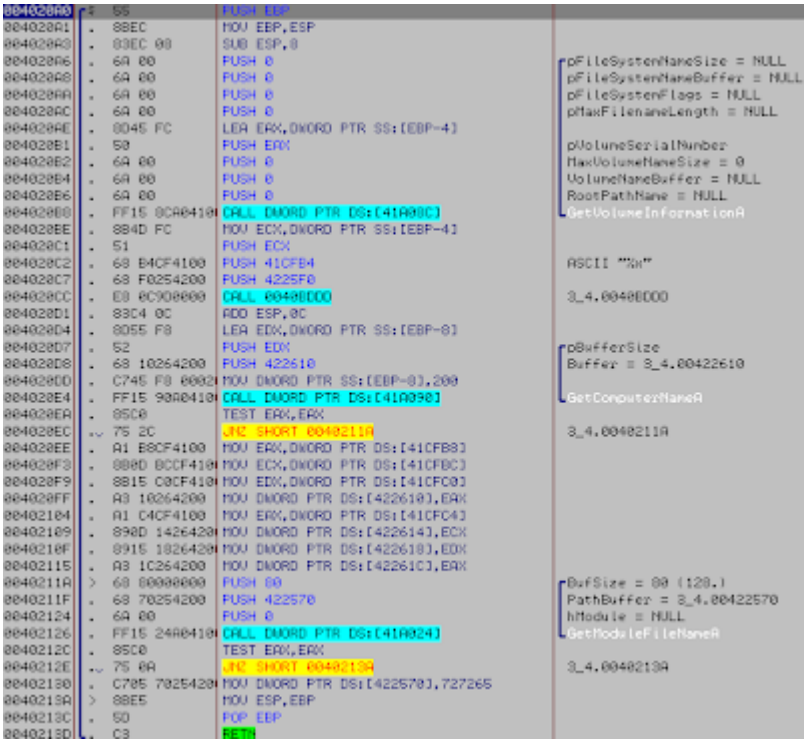
Alina 3.4 (POS Malware)

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:



Create a mutex:

```
0040228E  .  68 C0CF4100  PUSH 41CFC0                 ; MutexName = "Mad3yghhuju9Sggqd906790hFv9.4"
00402293  .  6A 01        PUSH 1                      ; InitialOwner = TRUE
00402295  .  6A 00        PUSH 0                      ; pSecurity = NULL
00402297  .  FF15 5CA0410 CALL DWORD PTR DS:[41A05C]  ; CreateMutexA
```

Create /%appdata%/java.exe

```
0040286A  .  6A 00        PUSH 0                      ; hTemplateFile = NULL
0040286C  .  6A 00        PUSH 0                      ; Attributes = 0
0040286E  .  6A 02        PUSH 2                      ; Mode = CREATE_ALWAYS
00402870  .  6A 00        PUSH 0                      ; pSecurity = NULL
00402872  .  6A 01        PUSH 1                      ; ShareMode = FILE_SHARE_READ
00402874  .  68 00000040  PUSH 40000000               ; Access = GENERIC_WRITE
00402879  .  8D95 E8FEFFF LEA EDX,DWORD PTR SS:[EBP-118]
0040287F  .  52           PUSH EDX                    ; FileName
00402880  .  FF15 28A0410 CALL DWORD PTR DS:[41A028]  ; 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:

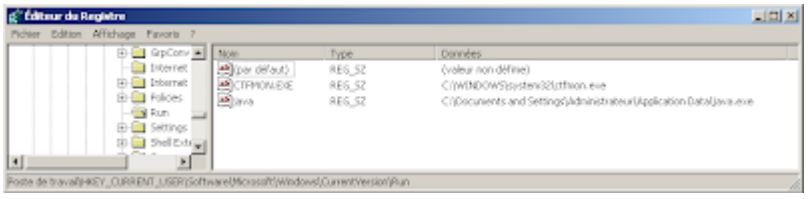
```
0040295B  .  6A 00        PUSH 0                      ; pOverlapped = NULL
0040295D  .  8D8D 30FBFFF LEA ECX,DWORD PTR SS:[EBP-4D0]
00402963  .  51           PUSH ECX                    ; pBytesRead
00402964  .  53           PUSH EBX                    ; BytesToRead
00402965  .  50           PUSH EAX                    ; Buffer
00402966  .  57           PUSH EDI                    ; hFile
00402967  .  8985 3CFBFFF MOV DWORD PTR SS:[EBP-4C4],EAX
0040296D  .  FF15 50A0410 CALL DWORD PTR DS:[41A050]  ; ReadFile
00402973  .  85C0         TEST EAX,EAX
00402975  .v 74 40        JE SHORT 00402987           ; 3_4.00402987
00402977  .  399D 30FBFFF CMP DWORD PTR SS:[EBP-4D0],EBX
0040297D  .v 75 38        JNZ SHORT 004029B7          ; 3_4.00402987
0040297F  .  8B85 3CFBFFF MOV EAX,DWORD PTR SS:[EBP-4C4]
00402985  .  6A 00        PUSH 0                      ; pOverlapped = NULL
00402987  .  8D95 30FBFFF LEA EDX,DWORD PTR SS:[EBP-4D0]
0040298D  .  52           PUSH EDX                    ; pBytesWritten
0040298E  .  53           PUSH EBX                    ; nBytesToWrite
0040298F  .  50           PUSH EAX                    ; Buffer
00402990  .  56           PUSH ESI                    ; hFile
00402991  .  FF15 38A0410 CALL DWORD PTR DS:[41A038]  ; WriteFile
```

and if he fail to write he will Copy it:

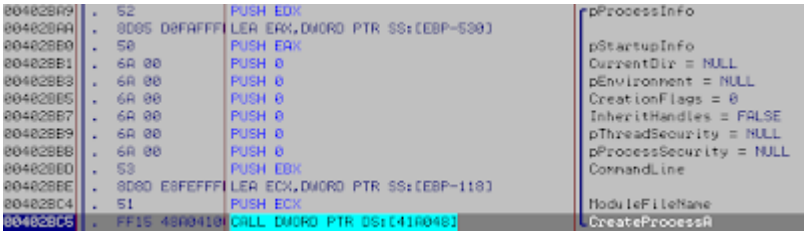
```
00402A17  .  6A 00        PUSH 0                      ; FailIfExists = FALSE
00402A19  .  8D8D E8FEFFF LEA ECX,DWORD PTR SS:[EBP-118]
00402A1F  .  51           PUSH ECX                    ; NewFileName
00402A20  .  8D95 E0FDFFF LEA EDX,DWORD PTR SS:[EBP-220]
00402A26  .  52           PUSH EDX                    ; ExistingFileName
00402A27  .  FF15 54A0410 CALL DWORD PTR DS:[41A054]  ; CopyFileA
```

Add a registry persistence:

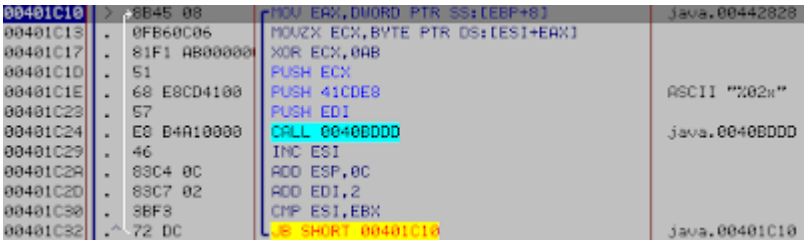
```
004014E9  .  52           PUSH EDX                    ; BufSize
004014EA  .  51           PUSH ECX                    ; Buffer
004014EB  .  6A 01        PUSH 1                      ; ValueType = REG_SZ
004014ED  .  53           PUSH EBX                    ; Reserved
004014EE  .  50           PUSH EAX                    ; ValueName
004014EF  .  8B45 FC      MOV EAX,DWORD PTR SS:[EBP-4]
004014F2  .  50           PUSH EAX                    ; hKey
004014F3  .  FF15 14A0410 CALL DWORD PTR DS:[41A014]  ; RegSetValueExA
```



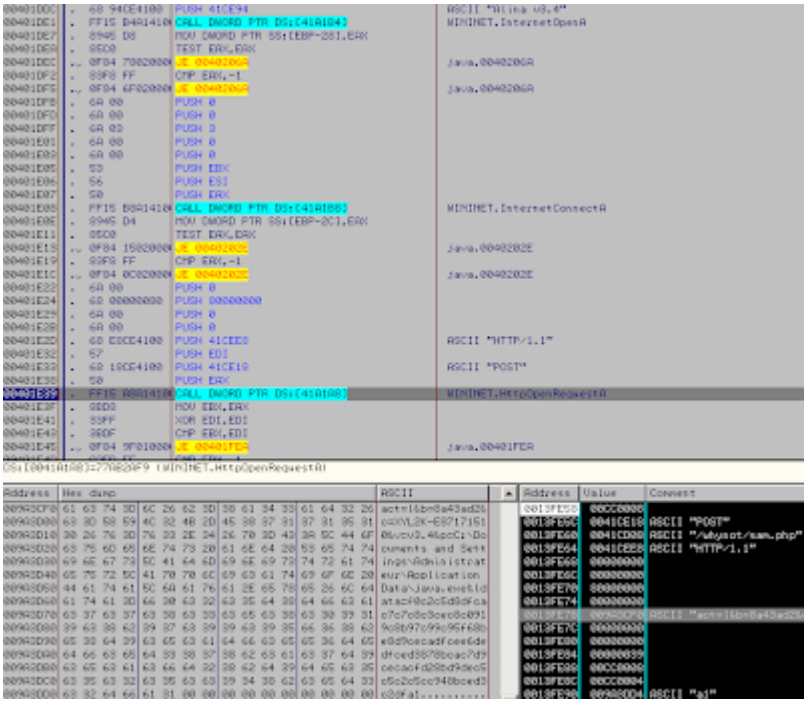
Launch the process:



Encode something (i've not checked what)



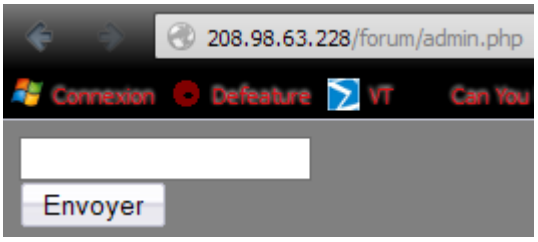
Call the C&C



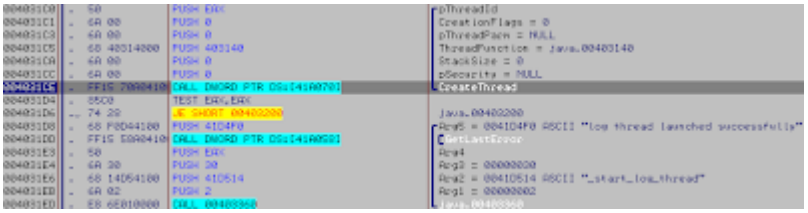
And fail because the first is dead, so retry with 208.98.63.228
Backend info:

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...



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.
