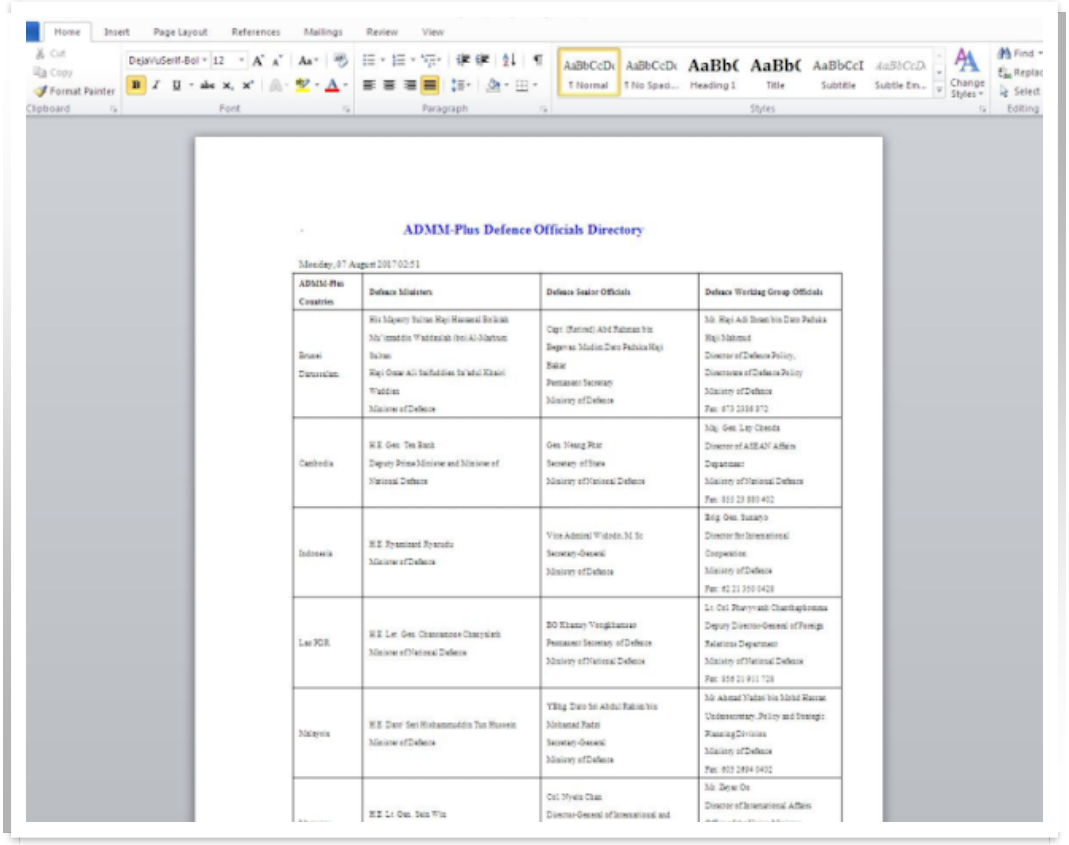
Deep Malware Analysis

Joe Security's Blog



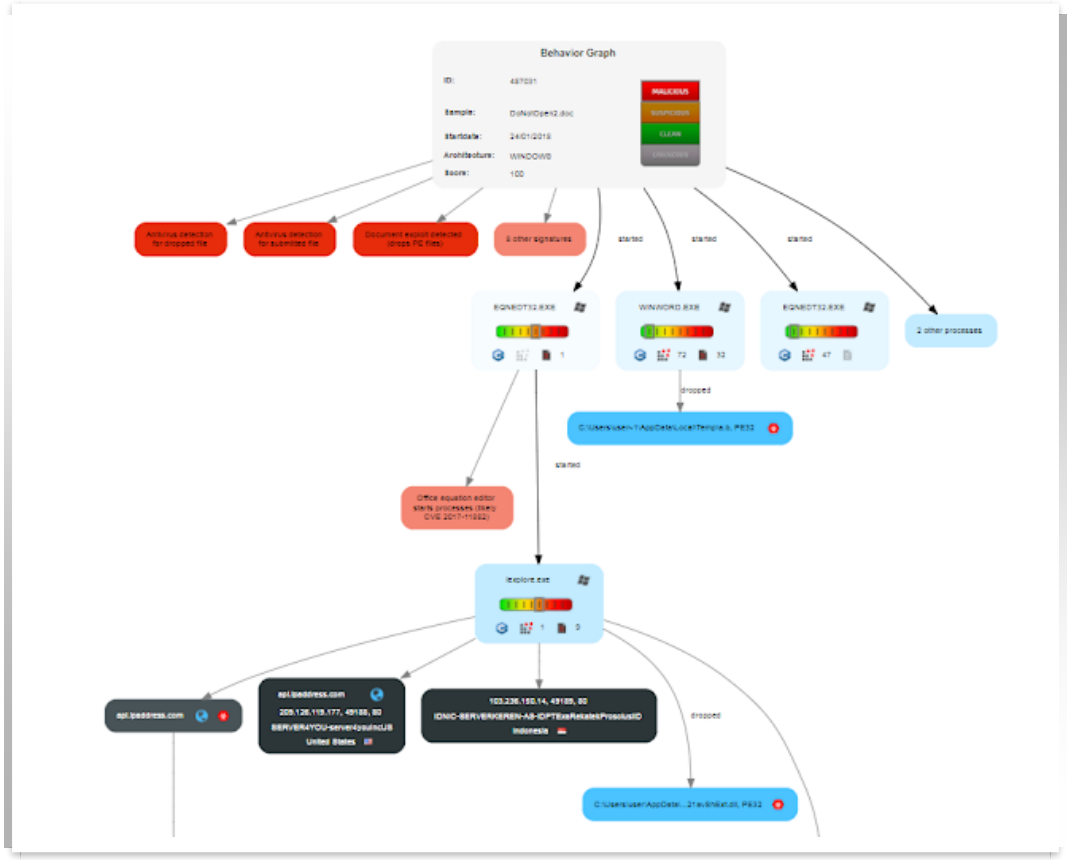
Static File Info

General

File type:	Rich Text Format data, version 1, unknown character set
Entropy (8bit):	4.652722413777991
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	DoNotOpen2.doc
File size:	261090
MD5:	f12fc711529b48bcef52c5ca0a52335a
SHA1:	5f89a6b2f1f38b581c65e9a1117c43a3060bfdc1
SHA256:	d3fc69a9f2ae2c446434abbfbe1693ef0f81a5da0a7f39d27c80d85f4a49c411
SHA512:	dcec5673653561354867fa1586a60899e4fd952fd693922aaba86c765710cd32186ca7c1c
File Content Preview:	{\rtf1\adeflang1025\ansi\ansicpg936\uc2\adeff0\deff0\stshfdbch13\stshfloch0\stshfhich0\s 2052\themelangcs0{\fonttbl{\f0\fbidi \froman\fcharset0\fprq2{*\panose 020206030504050

CVE-2018-0802

We start the analysis by having a look at the behavior graph and acknowledge that the process EQNEDT32.EXE was started among Winword.exe:

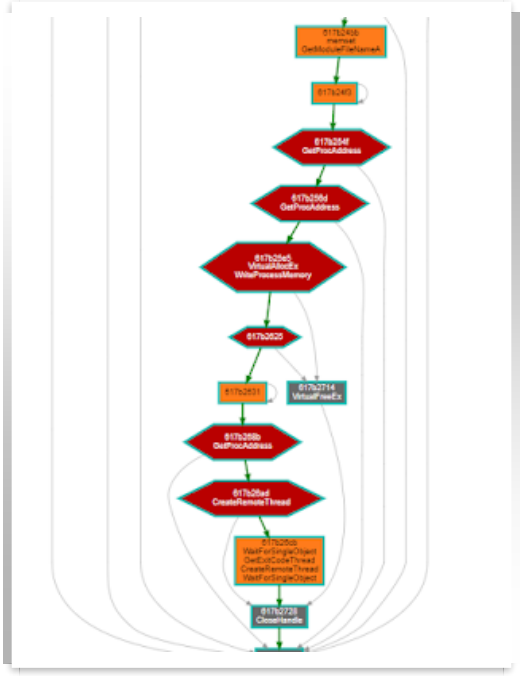


This process is the Microsoft Office Equation Editor. In November 2017 the security company Embedi detected an exploit in EQNEDT32.EXE which later got the identification CVE-2017-11882. Microsoft patched the flaw in November.

So, is Elise using this exploit? To answer this question we had a detailed look at the exploit itself. The outcome: no it is not CVE-2017-11882 but rather CVE-2018-0802. CVE-2018-0802? This a second exploit also included in EQNEDT32.EXE which was detected in later December.

We extracted the trampoline and shellcode:

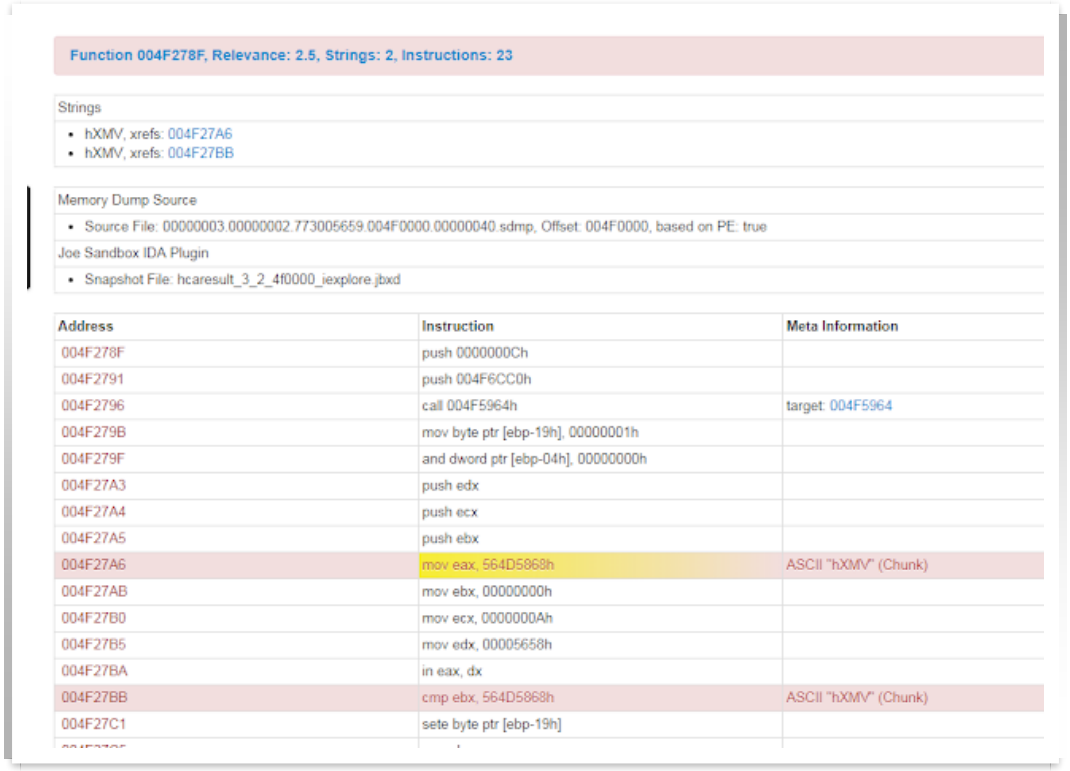
The code renames and loads the PE file (named a.b) previously dropped by Word. The newly loaded code is then injected into IExplorer.exe where the main payload is executed:



617B2700	push edx	
617B2701	push dword ptr [ebp-0000024Ch]	
617B2707	call dword ptr [ebp-00000234h]	CreateRemoteThread@KERNEL32.DLL (Import, Hidden, 7 Params) executed
617B270D	push FFFFFFFFh	executed
617B270F	push eax	
617B2710	call edi	WaitForSingleObject@KERNEL32.DLL (Import, 2 Params)
617B2712	jmp 617B2728h	target: 617B2728
617B2714	push edi	xref: 617B261F 617B262B
617B2715	push esi	
617B2716	push dword ptr [ebp-00000230h]	
617B271C	push dword ptr [ebp-0000024Ch]	
617B2722	call dword ptr [617B4048h]	VirtualFreeEx@KERNEL32.DLL (Import, Unknown Params)
617B2728	push dword ptr [ebp-0000024Ch]	xref: 617B26C9 617B2712
617B272E	call dword ptr [617B406Ch]	CloseHandle@KERNEL32.DLL (Import, 1 Params)
617B2734	pop edi	xref: 617B248E 617B24B5 617B2567 617B25DF 617B26A7

Sandbox Evasions

Elise performs a variety of sandbox checks in In IExplorer:



Function 004F278F, Relevance: 2.5, Strings: 2, Instructions: 23

Strings

- hXMV, xrefs: 004F27A6
- hXMV, xrefs: 004F27BB

Memory Dump Source

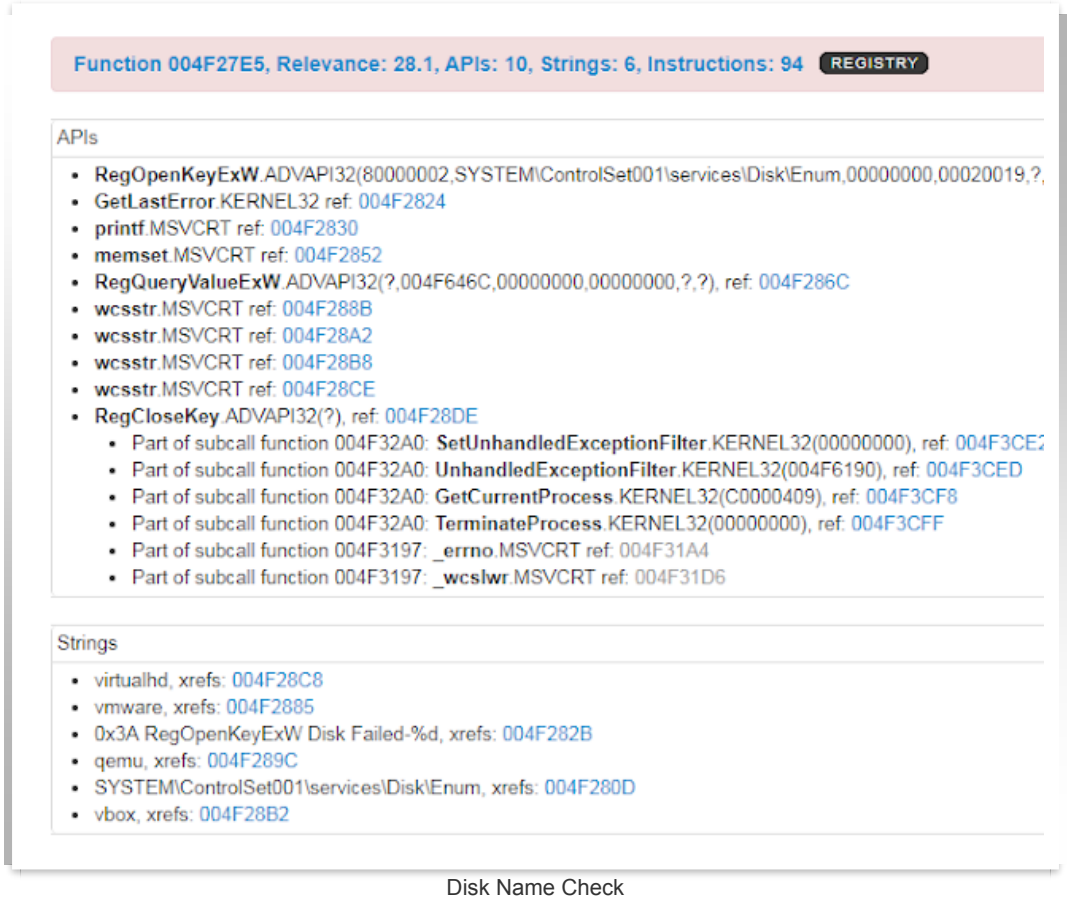
- Source File: 00000003.00000002.773005659.004F0000.00000040.sdmp, Offset: 004F0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_4f0000_iexplore.jbxd

Address	Instruction	Meta Information
004F278F	push 0000000Ch	
004F2791	push 004F6CC0h	
004F2796	call 004F5964h	target: 004F5964
004F279B	mov byte ptr [ebp-19h], 00000001h	
004F279F	and dword ptr [ebp-04h], 00000000h	
004F27A3	push edx	
004F27A4	push ecx	
004F27A5	push ebx	
004F27A6	mov eax, 564D5868h	ASCII "hXMV" (Chunk)
004F27AB	mov ebx, 00000000h	
004F27B0	mov ecx, 0000000Ah	
004F27B5	mov edx, 00005658h	
004F27BA	in eax, dx	
004F27BB	cmp ebx, 564D5868h	ASCII "hXMV" (Chunk)
004F27C1	sete byte ptr [ebp-19h]	

VMware backdoor check



Function 004F27E5, Relevance: 28.1, APIs: 10, Strings: 6, Instructions: 94 REGISTRY

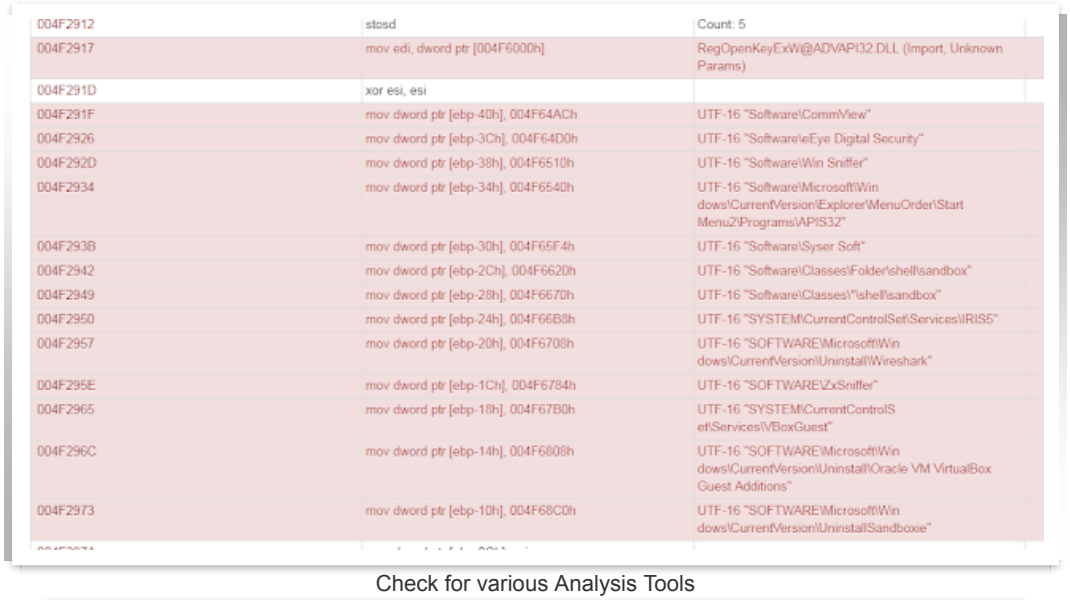
APIs

- **RegOpenKeyExW**.ADVAPI32(80000002,SYSTEM\ControlSet001\services\Disk\Enum,00000000,00020019,?,
- **GetLastError**.KERNEL32 ref: 004F2824
- **printf**.MSVCRT ref: 004F2830
- **memset**.MSVCRT ref: 004F2852
- **RegQueryValueExW**.ADVAPI32(?,004F646C,00000000,00000000,?,?), ref: 004F286C
- **wcsstr**.MSVCRT ref: 004F288B
- **wcsstr**.MSVCRT ref: 004F28A2
- **wcsstr**.MSVCRT ref: 004F28B8
- **wcsstr**.MSVCRT ref: 004F28CE
- **RegCloseKey**.ADVAPI32(?), ref: 004F28DE
  - Part of subcall function 004F32A0: **SetUnhandledExceptionFilter**.KERNEL32(00000000), ref: 004F3CE2
  - Part of subcall function 004F32A0: **UnhandledExceptionFilter**.KERNEL32(004F6190), ref: 004F3CED
  - Part of subcall function 004F32A0: **GetCurrentProcess**.KERNEL32(C0000409), ref: 004F3CF8
  - Part of subcall function 004F32A0: **TerminateProcess**.KERNEL32(00000000), ref: 004F3CFF
  - Part of subcall function 004F3197: **_errno**.MSVCRT ref: 004F31A4
  - Part of subcall function 004F3197: **_wcslwr**.MSVCRT ref: 004F31D6

Strings

- virtualhd, xrefs: 004F28C8
- vmware, xrefs: 004F2885
- 0x3A RegOpenKeyExW Disk Failed-%d, xrefs: 004F282B
- qemu, xrefs: 004F289C
- SYSTEM\ControlSet001\services\Disk\Enum, xrefs: 004F280D
- vbox, xrefs: 004F28B2

Disk Name Check



004F2912	stosd	Count: 5
004F2917	mov edi, dword ptr [004F6000h]	RegOpenKeyExW@ADVAPI32.DLL (Import, Unknown Params)
004F291D	xor esi, esi	
004F291F	mov dword ptr [ebp-40h], 004F64ACh	UTF-16 "Software\CommView"
004F2926	mov dword ptr [ebp-3Ch], 004F64D0h	UTF-16 "Software\eEye Digital Security"
004F292D	mov dword ptr [ebp-38h], 004F6510h	UTF-16 "Software\Win Sniffer"
004F2934	mov dword ptr [ebp-34h], 004F6540h	UTF-16 "Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\APIS32"
004F293B	mov dword ptr [ebp-30h], 004F65F4h	UTF-16 "Software\Syser Soft"
004F2942	mov dword ptr [ebp-2Ch], 004F6620h	UTF-16 "Software\Classes\Folder\shell\sandbox"
004F2949	mov dword ptr [ebp-28h], 004F6670h	UTF-16 "Software\Classes*\shell\sandbox"
004F2950	mov dword ptr [ebp-24h], 004F66B8h	UTF-16 "SYSTEM\CurrentControlSet\Services\IRIS5"
004F2957	mov dword ptr [ebp-20h], 004F6708h	UTF-16 "SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark"
004F295E	mov dword ptr [ebp-1Ch], 004F6784h	UTF-16 "SOFTWARE\ZxSniffer"
004F2965	mov dword ptr [ebp-18h], 004F67B0h	UTF-16 "SYSTEM\CurrentControlSet\Services\VBoxGuest"
004F296C	mov dword ptr [ebp-14h], 004F6808h	UTF-16 "SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Oracle VM VirtualBox Guest Additions"
004F2973	mov dword ptr [ebp-10h], 004F68C0h	UTF-16 "SOFTWARE\Microsoft\Windows\CurrentVersion\UninstallSandboxie"

Check for various Analysis Tools

Function 004F2A05, Relevance: 46.0, APIs: 7, Strings: 19, Instructions: 482

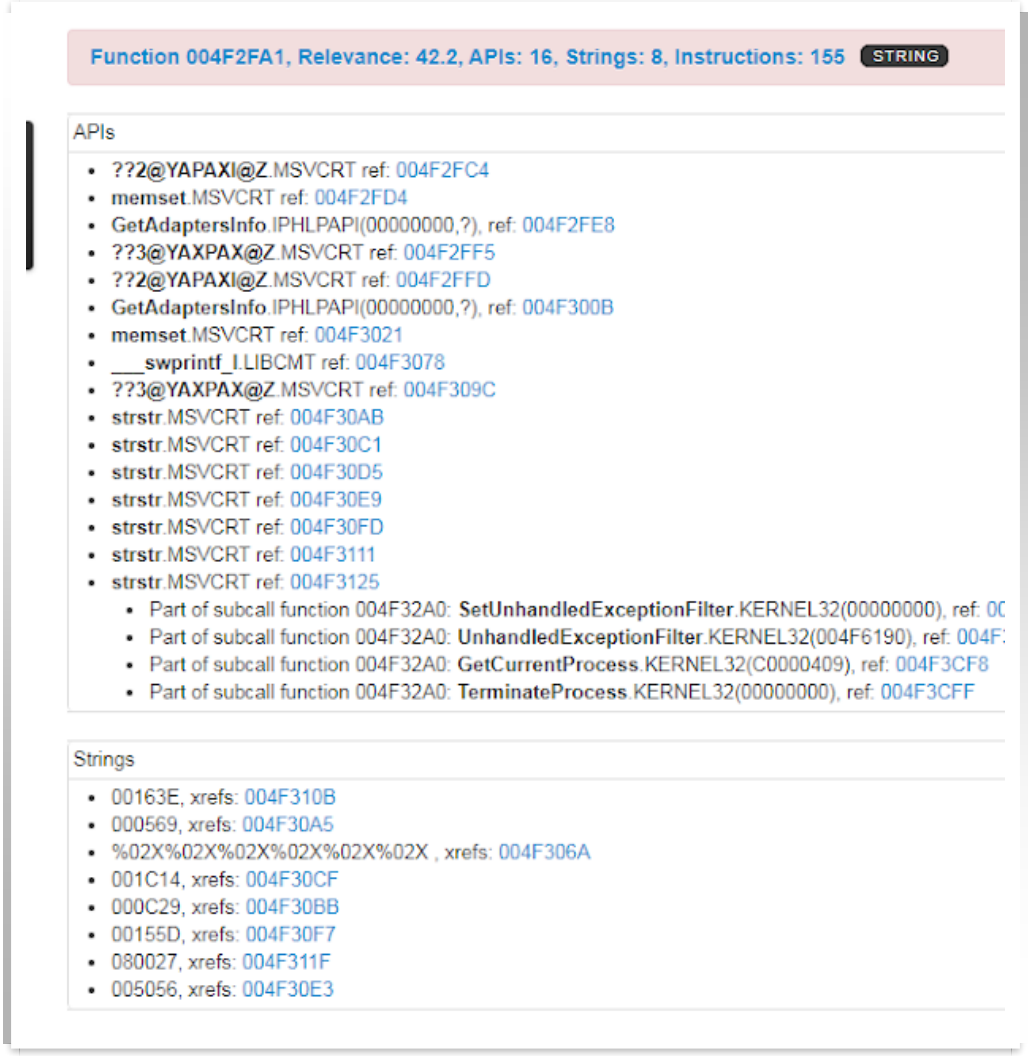
APIs

- **CreateToolhelp32Snapshot**.KERNEL32(00000002,00000000), ref: 004F2A2A
- **memset**.MSVCRT ref: 004F2A51
- **memset**.MSVCRT ref: 004F2A6C
- **Process32FirstW**.KERNEL32(?,?), ref: 004F2A7E
- **___swprintf_l**.LIBCMT ref: 004F2AA4
  - Part of subcall function 004F3197: **_errno**.MSVCRT ref: 004F31A4
  - Part of subcall function 004F3197: **_wcslwr**.MSVCRT ref: 004F31D6
- **Process32NextW**.KERNEL32(?,?), ref: 004F2F6A
- **CloseHandle**.KERNEL32(?), ref: 004F2F81
  - Part of subcall function 004F32A0: **SetUnhandledExceptionFilter**.KERNEL32(00000000), ref: 004F3CE2
  - Part of subcall function 004F32A0: **UnhandledExceptionFilter**.KERNEL32(004F6190), ref: 004F3CED
  - Part of subcall function 004F32A0: **GetCurrentProcess**.KERNEL32(C0000409), ref: 004F3CF8
  - Part of subcall function 004F32A0: **TerminateProcess**.KERNEL32(00000000), ref: 004F3CFF

Strings

- irise.exe, xrefs: 004F2C95
- vmupgradehelper.exe, xrefs: 004F2BA9
- windbg.exe, xrefs: 004F2E20
- Syser.exe, xrefs: 004F2EA8
- Regshot.exe, xrefs: 004F2D98
- SandboxieDcomLaunch.exe, xrefs: 004F2F23
- vmtools.exe, xrefs: 004F2C5A
- IrisSvc.exe, xrefs: 004F2CCC
- vmwaretray.exe, xrefs: 004F2B6E
- SandboxieRpcSs.exe, xrefs: 004F2EEC
- vmwareuser.exe, xrefs: 004F2B33
- vboxtray.exe, xrefs: 004F2ABD
- vboxservice.exe, xrefs: 004F2AF8
- wireshark.exe, xrefs: 004F2D10
- vmacthlp.exe, xrefs: 004F2C1F
- ollydbg.exe, xrefs: 004F2DDC
- ZxSniffer.exe, xrefs: 004F2D54
- vmtoolsd.exe, xrefs: 004F2BE4
- PEBrowseDbg.exe, xrefs: 004F2E64

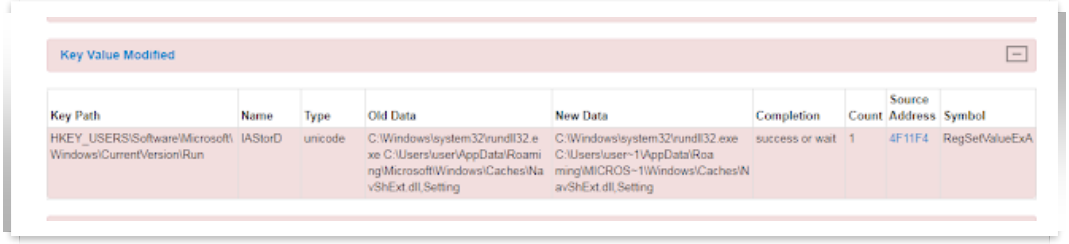
Process Check



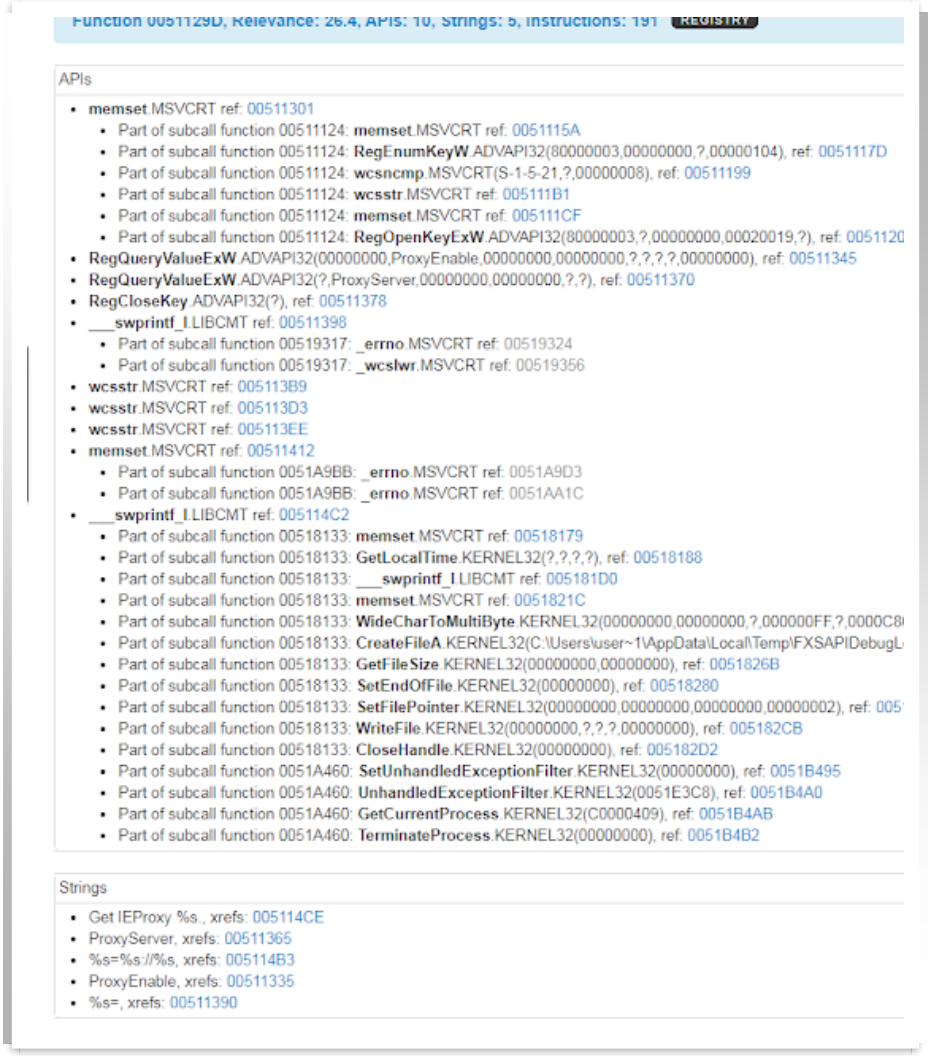
Mac Address Check

Payloads

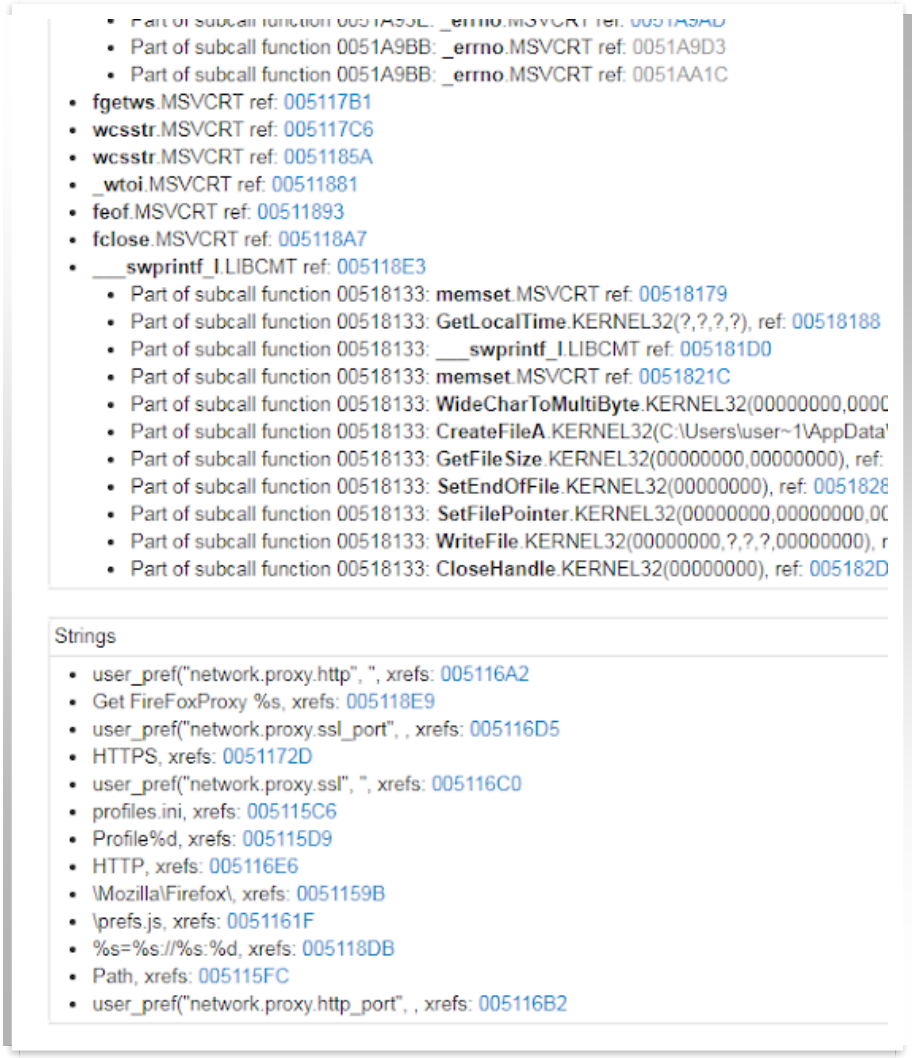
After passing all the sandbox checks Elise creates an autostart key:



Thanks to Hybrid Code Analysis we can also detect all malicious functionalities:



Add a Proxy to Internet Explorer



Add a Proxy to Firefox

Finally, in function 514D05, 5159AF and 515486 we find the download, upload and command execution handlers. Elise can collect and upload the following data:

- CPU Usage
- Ram (size/free)
- Disk space (size/free)
- Windows Version
- Username
- Locale
- Timezone
- SID
- List of tasks
- List of network adapters
- List of files on Desktop

Final Words

Elise is a very advanced piece of malware using for its distribution only the latest exploits. Before the main payload is executed many different Sandbox evasions are performed. The payload and the communication code is injected into IExplorer likely bypassing PFW and HIPS.

Interested in trying out Joe Sandbox? Register for free at Joe Sandbox Cloud Basic or contact us for an in-depth technical demo!

Full Joe Sandbox Analysis Report.

Joe Security LLC
business parc Reinach
Christoph Merian-Ring 11
4153 Reinach
Switzerland

Contact