WebDAV Traffic To Malicious Sites

Published: 2017-11-13 · Archived: 2026-04-05 20:28:42 UTC

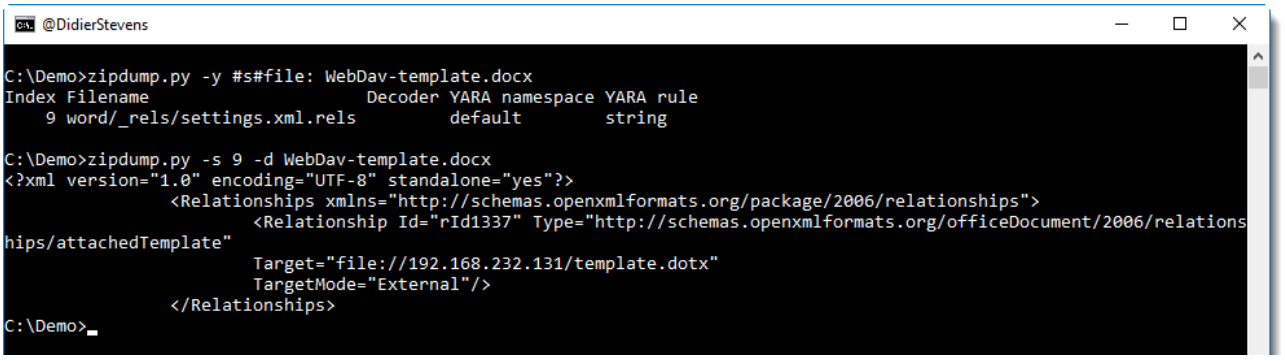
I observed WebDAV traffic to malicious sites in the past (in proxy logs), and recently I took some time to take a closer look.

TL;DR: when files are retrieved remotely with the file:// URI scheme on Windows, Windows will fallback to WebDAV when SMB connections can not be established.

I did my tests with 2 Windows 7 VMs on the same subnet, one Windows 7 machine with IIS/WebDAV, and the other Windows 7 machine with Word 2016 and a .docx document with a remote template (template.dotx) (using the file:// URI scheme). The Windows firewall on the IIS machine was configured to block ports 139 and 445.

When the .docx document is opened, Word will retrieve the template:

Here is the URI:



First we see attempts to connect on ports 445 and 139 on the IIS machine (SYN packets):

No.	Time	Source	Destination	Protocol	Length	Stream index	Info
22	2017-11-12 12:56:54.507127	192.168.232.132	192.168.232.131	TCP	66	1	49161 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
23	2017-11-12 12:56:55.591381	192.168.232.132	192.168.232.131	TCP	66	2	49162 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
24	2017-11-12 12:56:55.595856	192.168.232.132	192.168.232.131	TCP	66	3	49163 → 139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
26	2017-11-12 12:56:57.507948	192.168.232.132	192.168.232.131	TCP	66	1	[TCP Retransmission] 49161 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
27	2017-11-12 12:56:58.599926	192.168.232.132	192.168.232.131	TCP	66	3	[TCP Retransmission] 49163 → 139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
28	2017-11-12 12:56:58.599926	192.168.232.132	192.168.232.131	TCP	66	2	[TCP Retransmission] 49162 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
30	2017-11-12 12:56:59.712117	Vmware_ec:ee:3a	Broadcast	ARP	60		Who has 192.168.232.132? Tell 192.168.232.2
31	2017-11-12 12:56:59.712152	Vmware_70:62:a6	Vmware_ec:ee:3a	ARP	42		192.168.232.132 is at 00:0c:29:70:62:a6
37	2017-11-12 12:57:00.021239	192.168.232.132	192.168.232.131	NBNS	92		Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
38	2017-11-12 12:57:01.532884	192.168.232.132	192.168.232.131	NBNS	92		Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
39	2017-11-12 12:57:03.040789	192.168.232.132	192.168.232.131	NBNS	92		Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
40	2017-11-12 12:57:03.509006	192.168.232.132	192.168.232.131	TCP	62	1	[TCP Retransmission] 49161 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
41	2017-11-12 12:57:04.257992	Vmware_70:62:a6	Vmware_ec:ee:3a	ARP	42		Who has 192.168.232.2? Tell 192.168.232.132
42	2017-11-12 12:57:04.258141	Vmware_ec:ee:3a	Vmware_70:62:a6	ARP	60		192.168.232.2 is at 00:50:56:ec:ee:3a
43	2017-11-12 12:57:04.601193	192.168.232.132	192.168.232.131	TCP	62	3	[TCP Retransmission] 49163 → 139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
44	2017-11-12 12:57:04.601195	192.168.232.132	192.168.232.131	TCP	62	2	[TCP Retransmission] 49162 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
45	2017-11-12 12:57:16.605796	192.168.232.132	192.168.232.131	NBNS	92		Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
46	2017-11-12 12:57:18.116529	192.168.232.132	192.168.232.131	NBNS	92		Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
47	2017-11-12 12:57:19.621426	192.168.232.132	192.168.232.131	NBNS	92		Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>

These come from the “System process”:

Time of Day	Process Name	PID	Operation	Path	Result	Detail
12:56:57.5079582 PM	System	4	TCP Reconnect	WIN-DFGODF5ES9C.localdomain:49161 -> 192.168.232.131:microsoft-ds	SUCCESS	Length: 0, seqnum:...
12:56:58.5999341 PM	System	4	TCP Reconnect	WIN-DFGODF5ES9C.localdomain:49163 -> 192.168.232.131:netbios-ssn	SUCCESS	Length: 0, seqnum:...
12:56:58.5999381 PM	System	4	TCP Reconnect	WIN-DFGODF5ES9C.localdomain:49162 -> 192.168.232.131:microsoft-ds	SUCCESS	Length: 0, seqnum:...
12:57:03.5090295 PM	System	4	TCP Reconnect	WIN-DFGODF5ES9C.localdomain:49161 -> 192.168.232.131:microsoft-ds	SUCCESS	Length: 0, seqnum:...
12:57:04.6011758 PM	System	4	TCP Reconnect	WIN-DFGODF5ES9C.localdomain:49163 -> 192.168.232.131:netbios-ssn	SUCCESS	Length: 0, seqnum:...
12:57:04.6012115 PM	System	4	TCP Reconnect	WIN-DFGODF5ES9C.localdomain:49162 -> 192.168.232.131:microsoft-ds	SUCCESS	Length: 0, seqnum:...

There are no packets coming back from the IIS machine (I blocked port 139 and 445), and after almost 30 seconds we see an HTTP request to port 80 on the IIS machine:

48	2017-11-12 12:57:21.769201	192.168.232.132	192.168.232.131	TCP	66	4	49165 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
49	2017-11-12 12:57:21.769987	Vmware_06:d3:0e	Broadcast	ARP	60		Who has 192.168.232.132? Tell 192.168.232.131
50	2017-11-12 12:57:21.770013	Vmware_70:62:a6	Vmware_06:d3:0e	ARP	42		192.168.232.132 is at 00:0c:29:70:62:a6
51	2017-11-12 12:57:21.770367	192.168.232.131	192.168.232.132	TCP	66	4	80 → 49165 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
52	2017-11-12 12:57:21.770481	192.168.232.132	192.168.232.131	TCP	54	4	49165 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
53	2017-11-12 12:57:21.771627	192.168.232.132	192.168.232.131	HTTP	158	4	OPTIONS / HTTP/1.1
54	2017-11-12 12:57:21.772796	192.168.232.131	192.168.232.132	TCP	1514	4	80 → 49165 [ACK] Seq=1 Ack=105 Win=65536 Len=1460 [TCP segment of a reassembled PDU]

This is a WebDAV request, notice the User Agent string “DavClnt”:

```
OPTIONS / HTTP/1.1
Connection: Keep-Alive
User-Agent: DavClnt
translate: f
Host: 192.168.232.131
```

This TCP connection originates from the Word process:

12:57:21.7704892 PM	WINWORD.EXE	3056	TCP Connect	WIN-DFGODF5ES9C.localdomain:49165 -> 192.168.232.131:http	SUCCESS	Length: 0, mss: 14...
12:57:21.7728881 PM	WINWORD.EXE	3056	TCP Send	WIN-DFGODF5ES9C.localdomain:49165 -> 192.168.232.131:http	SUCCESS	Length: 104, starti...
12:57:21.7729850 PM	WINWORD.EXE	3056	TCP Receive	WIN-DFGODF5ES9C.localdomain:49165 -> 192.168.232.131:http	SUCCESS	Length: 1486, seq...

And about 3 seconds after this request, we get another WebDAV request:

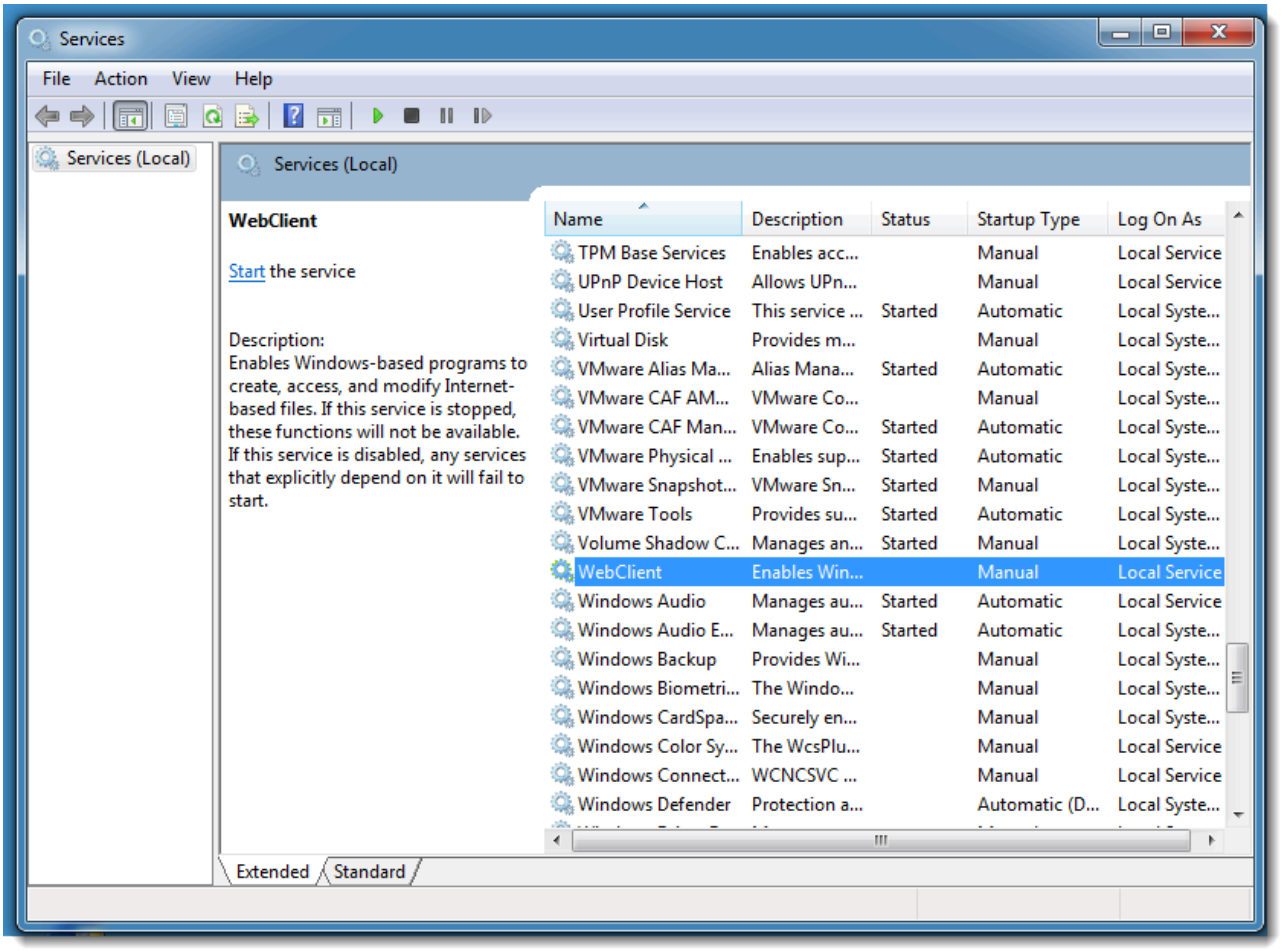
59	2017-11-12 12:57:24.844761	192.168.232.132	192.168.232.131	TCP	66	5	49166 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
60	2017-11-12 12:57:24.845420	192.168.232.131	192.168.232.132	TCP	66	5	80 → 49166 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
61	2017-11-12 12:57:24.845571	192.168.232.132	192.168.232.131	TCP	54	5	49166 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
62	2017-11-12 12:57:24.845843	192.168.232.132	192.168.232.131	HTTP	186	5	OPTIONS / HTTP/1.1
63	2017-11-12 12:57:24.846732	192.168.232.131	192.168.232.132	TCP	1514	5	80 → 49166 [ACK] Seq=1 Ack=133 Win=65536 Len=1460 [TCP segment of a reassembled PDU]

For this request, the User Agent string is “Microsoft-WebDAV-MiniRedir/6.1.7601”.

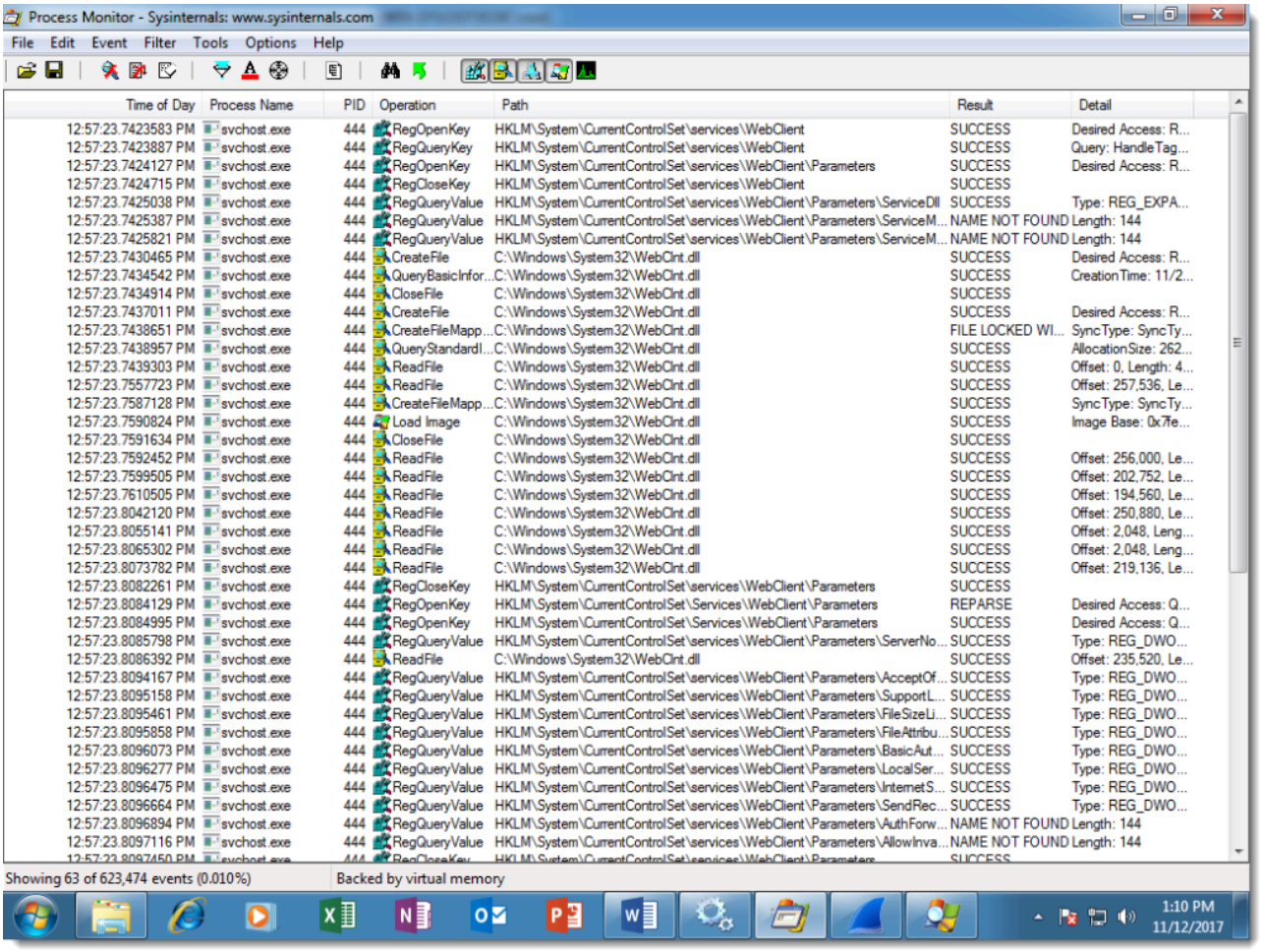
This TCP connection originates from the WebClient service:

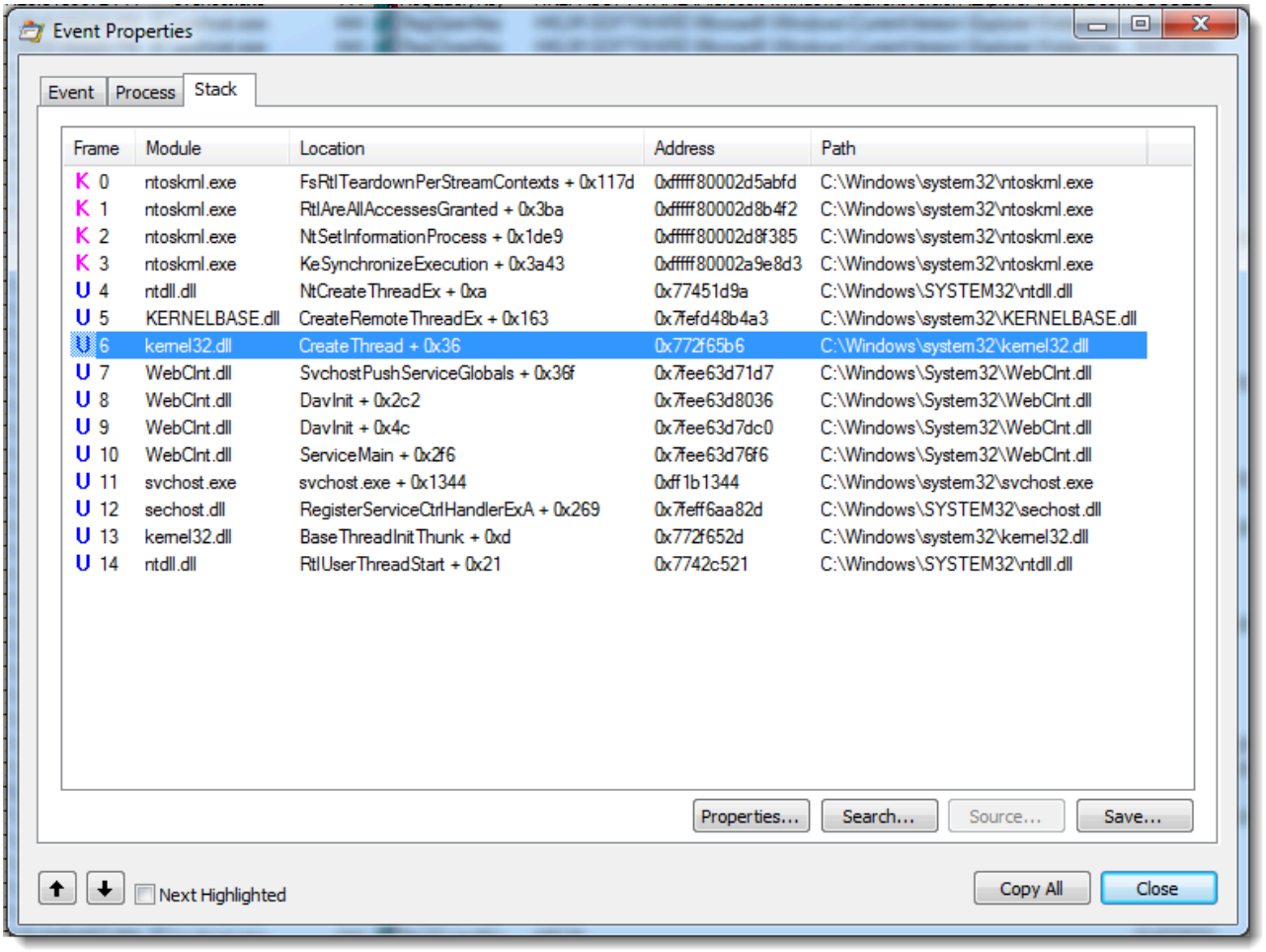
12:57:24.8455447 PM	svchost.exe	444	TCP Connect	WIN-DFGODF5ES9C.localdomain:49166 -> 192.168.232.131:http	SUCCESS	Length: 0, mss: 14...
12:57:24.8468242 PM	svchost.exe	444	TCP Send	WIN-DFGODF5ES9C.localdomain:49166 -> 192.168.232.131:http	SUCCESS	Length: 132, starti...
12:57:24.8469142 PM	svchost.exe	444	TCP Receive	WIN-DFGODF5ES9C.localdomain:49166 -> 192.168.232.131:http	SUCCESS	Length: 1486, seq...

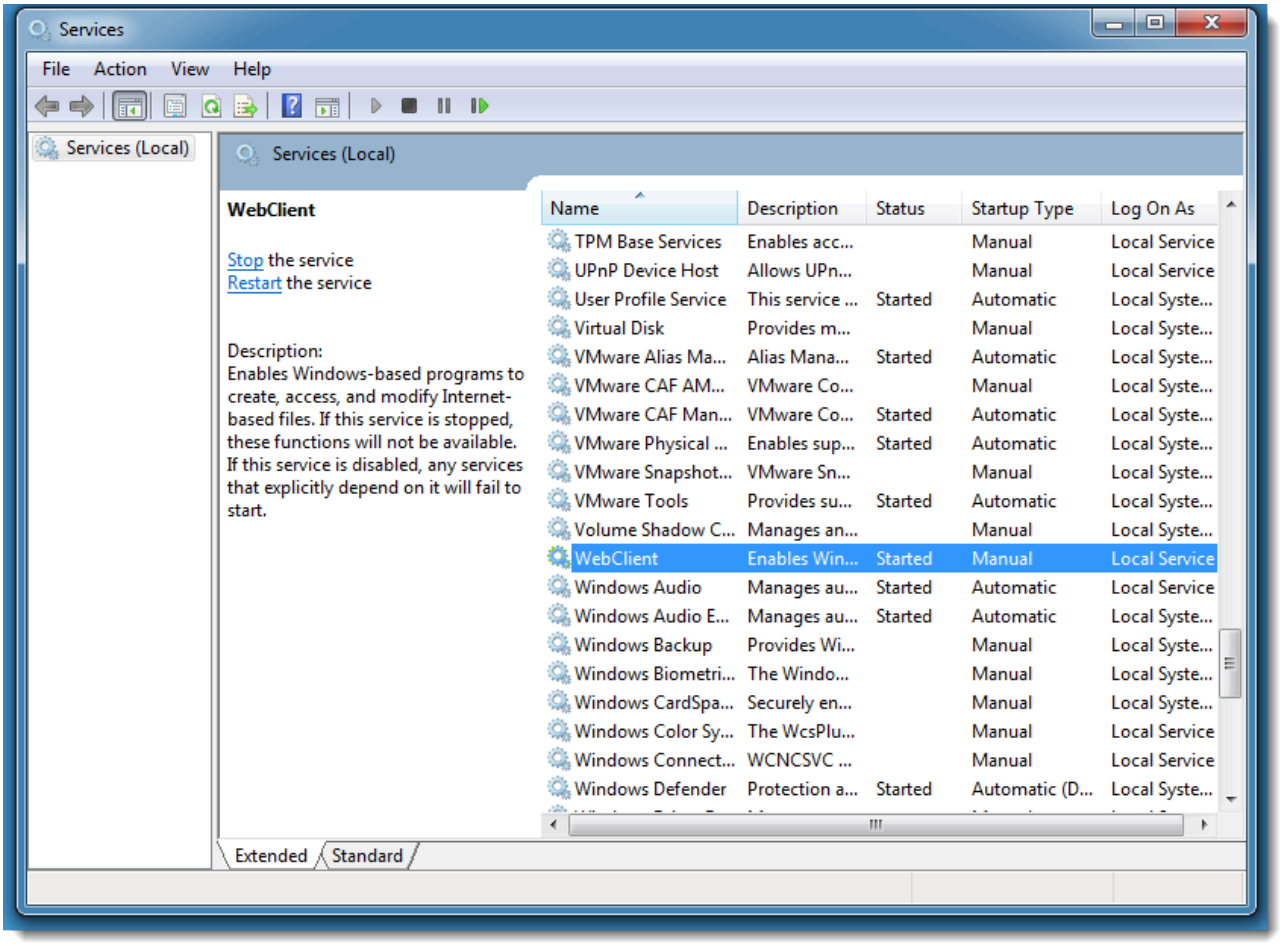
This service was not started:



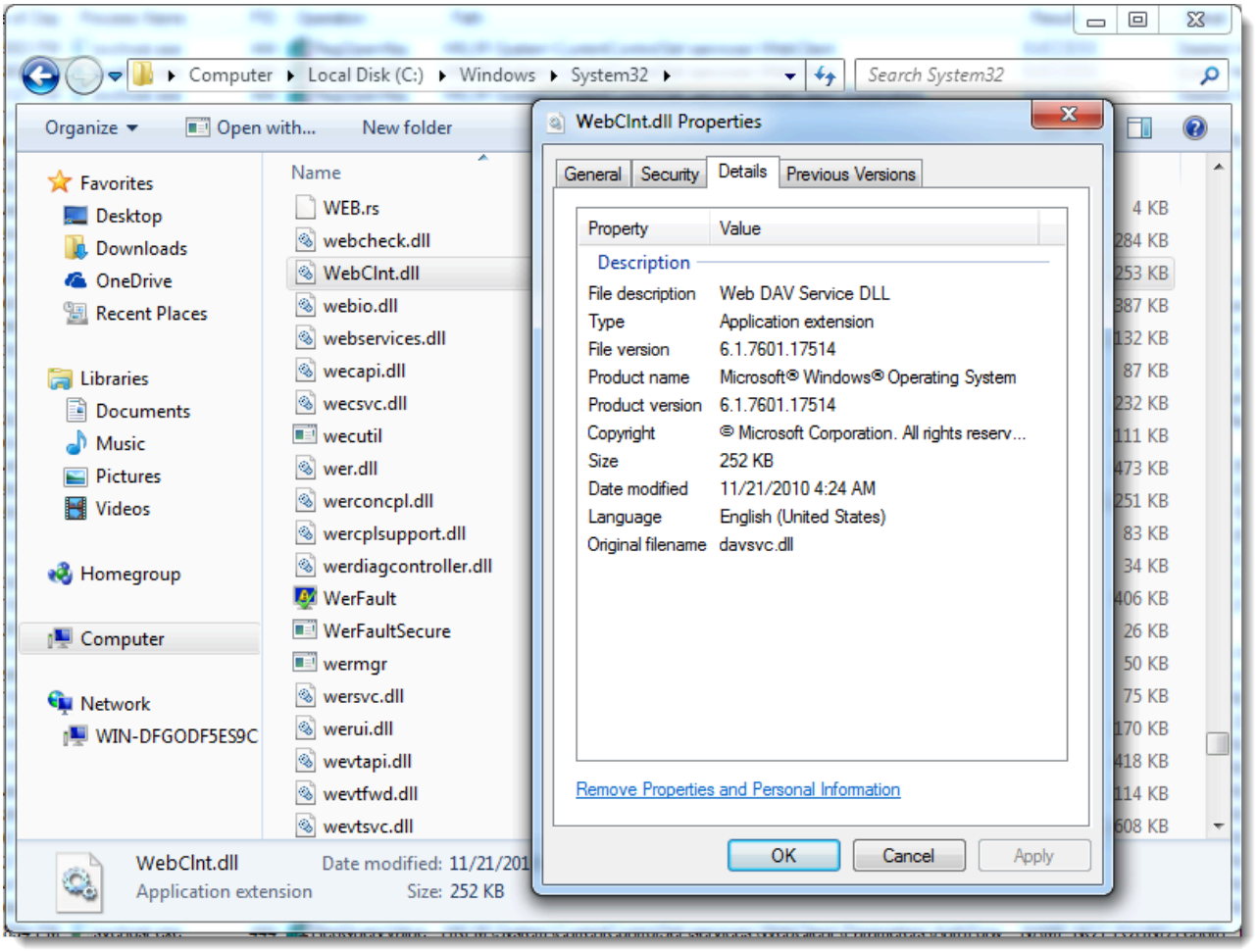
The svchost service host process will load and start the WebClient service:


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day | Process Name | PID | Operation | Path | Result | Detail
12:57:23.7423583 PM | svchost.exe | 444 | RegOpenKey | HKLM\System\CurrentControlSet\services\WebClient | SUCCESS | Desired Access: R...
12:57:23.7423887 PM | svchost.exe | 444 | RegQueryKey | HKLM\System\CurrentControlSet\services\WebClient | SUCCESS | Query: HandleTag...
12:57:23.7424127 PM | svchost.exe | 444 | RegOpenKey | HKLM\System\CurrentControlSet\services\WebClient\Parameters | SUCCESS | Desired Access: R...
12:57:23.7424715 PM | svchost.exe | 444 | RegCloseKey | HKLM\System\CurrentControlSet\services\WebClient | SUCCESS
12:57:23.7425038 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\ServiceDll | SUCCESS | Type: REG_EXPA...
12:57:23.7425387 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\ServiceM... | NAME NOT FOUND | Length: 144
12:57:23.7425821 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\ServiceM... | NAME NOT FOUND | Length: 144
12:57:23.7430465 PM | svchost.exe | 444 | CreateFile | C:\Windows\System32\WebClnt.dll | SUCCESS | Desired Access: R...
12:57:23.7434542 PM | svchost.exe | 444 | QueryBasicInfor... | C:\Windows\System32\WebClnt.dll | SUCCESS | CreationTime: 11/2...
12:57:23.7434914 PM | svchost.exe | 444 | CloseFile | C:\Windows\System32\WebClnt.dll | SUCCESS
12:57:23.7437011 PM | svchost.exe | 444 | CreateFile | C:\Windows\System32\WebClnt.dll | SUCCESS | Desired Access: R...
12:57:23.7438651 PM | svchost.exe | 444 | CreateFileMapp... | C:\Windows\System32\WebClnt.dll | FILE LOCKED WI... | SyncType: SyncTy...
12:57:23.7438957 PM | svchost.exe | 444 | QueryStandardI... | C:\Windows\System32\WebClnt.dll | SUCCESS | AllocationSize: 262...
12:57:23.7439303 PM | svchost.exe | 444 | ReadFile | C:\Windows\System32\WebClnt.dll | SUCCESS | Offset: 0, Length: 4...
12:57:23.7557723 PM | svchost.exe | 444 | ReadFile | C:\Windows\System32\WebClnt.dll | SUCCESS | Offset: 257,536, Le...
12:57:23.7587128 PM | svchost.exe | 444 | CreateFileMapp... | C:\Windows\System32\WebClnt.dll | SUCCESS | SyncType: SyncTy...
12:57:23.7590824 PM | svchost.exe | 444 | Load Image | C:\Windows\System32\WebClnt.dll | SUCCESS | Image Base: 0x7fe...
12:57:23.7591634 PM | svchost.exe | 444 | CloseFile | C:\Windows\System32\WebClnt.dll | SUCCESS
12:57:23.7592452 PM | svchost.exe | 444 | ReadFile | C:\Windows\System32\WebClnt.dll | SUCCESS | Offset: 256,000, Le...
12:57:23.7599505 PM | svchost.exe | 444 | ReadFile | C:\Windows\System32\WebClnt.dll | SUCCESS | Offset: 202,752, Le...
12:57:23.7610505 PM | svchost.exe | 444 | ReadFile | C:\Windows\System32\WebClnt.dll | SUCCESS | Offset: 194,560, Le...
12:57:23.8042120 PM | svchost.exe | 444 | ReadFile | C:\Windows\System32\WebClnt.dll | SUCCESS | Offset: 250,880, Le...
12:57:23.8055141 PM | svchost.exe | 444 | ReadFile | C:\Windows\System32\WebClnt.dll | SUCCESS | Offset: 2,048, Leng...
12:57:23.8065302 PM | svchost.exe | 444 | ReadFile | C:\Windows\System32\WebClnt.dll | SUCCESS | Offset: 2,048, Leng...
12:57:23.8073782 PM | svchost.exe | 444 | ReadFile | C:\Windows\System32\WebClnt.dll | SUCCESS | Offset: 219,136, Le...
12:57:23.8082261 PM | svchost.exe | 444 | RegCloseKey | HKLM\System\CurrentControlSet\services\WebClient\Parameters | SUCCESS
12:57:23.8084129 PM | svchost.exe | 444 | RegOpenKey | HKLM\System\CurrentControlSet\Services\WebClient\Parameters | REPARSE | Desired Access: Q...
12:57:23.8084995 PM | svchost.exe | 444 | RegOpenKey | HKLM\System\CurrentControlSet\Services\WebClient\Parameters | SUCCESS | Desired Access: Q...
12:57:23.8085798 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\ServerNo... | SUCCESS | Type: REG_DWO...
12:57:23.8086392 PM | svchost.exe | 444 | ReadFile | C:\Windows\System32\WebClnt.dll | SUCCESS | Offset: 235,520, Le...
12:57:23.8094167 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\AcceptOf... | SUCCESS | Type: REG_DWO...
12:57:23.8095158 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\SupportL... | SUCCESS | Type: REG_DWO...
12:57:23.8095461 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\FileSizeLi... | SUCCESS | Type: REG_DWO...
12:57:23.8095858 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\FileAttribu... | SUCCESS | Type: REG_DWO...
12:57:23.8096073 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\BasicAut... | SUCCESS | Type: REG_DWO...
12:57:23.8096277 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\LocalSer... | SUCCESS | Type: REG_DWO...
12:57:23.8096475 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\InternetS... | SUCCESS | Type: REG_DWO...
12:57:23.8096664 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\SendRec... | SUCCESS | Type: REG_DWO...
12:57:23.8096894 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\AuthForw... | NAME NOT FOUND | Length: 144
12:57:23.8097116 PM | svchost.exe | 444 | RegQueryValue | HKLM\System\CurrentControlSet\services\WebClient\Parameters\AllowInva... | NAME NOT FOUND | Length: 144
Showing 63 of 623,474 events (0.010%)
Backed by virtual memory
1:10 PM
11/12/2017


Event Properties
Event
Process
Stack
Frame Module Location Address Path
K 0 ntoskrnl.exe FsRtlTeardownPerStreamContexts + 0x117d 0xfffff80002d5abfd C:\Windows\system32\ntoskrnl.exe
K 1 ntoskrnl.exe RtlAreAllAccessesGranted + 0x3ba 0xfffff80002d8b4f2 C:\Windows\system32\ntoskrnl.exe
K 2 ntoskrnl.exe NtSetInformationProcess + 0x1de9 0xfffff80002d8f385 C:\Windows\system32\ntoskrnl.exe
K 3 ntoskrnl.exe KeSynchronizeExecution + 0x3a43 0xfffff80002a9e8d3 C:\Windows\system32\ntoskrnl.exe
U 4 ntdll.dll NtCreateThreadEx + 0xa 0x77451d9a C:\Windows\SYSTEM32\ntdll.dll
U 5 KERNELBASE.dll CreateRemoteThreadEx + 0x163 0x7fefd48b4a3 C:\Windows\system32\KERNELBASE.dll
U 6 kernel32.dll CreateThread + 0x36 0x772f65b6 C:\Windows\system32\kernel32.dll
U 7 WebClnt.dll SvchostPushServiceGlobals + 0x36f 0x7fee63d71d7 C:\Windows\System32\WebClnt.dll
U 8 WebClnt.dll DavInit + 0x2c2 0x7fee63d8036 C:\Windows\System32\WebClnt.dll
U 9 WebClnt.dll DavInit + 0x4c 0x7fee63d7dc0 C:\Windows\System32\WebClnt.dll
U 10 WebClnt.dll ServiceMain + 0x2f6 0x7fee63d76f6 C:\Windows\System32\WebClnt.dll
U 11 svchost.exe svchost.exe + 0x1344 0xff1b1344 C:\Windows\system32\svchost.exe
U 12 sechost.dll RegisterServiceCtrlHandlerExA + 0x269 0x7feff6aa82d C:\Windows\SYSTEM32\sechost.dll
U 13 kernel32.dll BaseThreadInitThunk + 0xd 0x772f652d C:\Windows\system32\kernel32.dll
U 14 ntdll.dll RtlUserThreadStart + 0x21 0x7742c521 C:\Windows\SYSTEM32\ntdll.dll
Properties...
Search...
Source...
Save...
Next Highlighted
Copy All
Close



WebClient (WebClnt.dll) is the WebDAV service:



To summarize, when the file:// URI scheme is used in a Word document and SMB connections can not be established, we will see WebDAV requests from:

1. Word (DavClnt)
2. WebClient service (Microsoft-WebDAV-MiniRedir/6.1.7601)

I've observed the same behavior with Windows 10 (with a different version number for the WebClient User Agent string).

When the document is opened a second time, there is no WebDAV request from Word (1), only requests from the WebClient service (2).

When I stop the WebClient service and reopen the document, there is first a WebDAV request from Word (1) followed by requests from the WebClient service (2).

When I disable the WebClient service and reopen the document, there are no more WebDAV requests at all.

Source: https://blog.didierstevens.com/2017/11/13/webdav-traffic-to-malicious-sites/