

REVERSING MRXSMB.SYS CHAPTER I

"Getting Ring0"

Rubén Santamarta ruben@reversemode.com www.reversemode.com

May 15, 2006

Index

1.Introduction	2
2.Cscdll.dll and mrxsmb.sys	2
3.Flaw	5
4.Last Words	8
5.Testing With Kartoffel	9
6.References & GPG Key	10

1.INTRODUCTION

"Client Side Caching" briefly

"*Client Side Caching*" aka "*Offline Files*" provides to Windows 2000 and Windows XP (Windows Vista?) the proper infrastructure which facilitates a seamless operation across connectivity states between client and remote server.

It is employed to safeguard the user and the client applications across connectivity interruptions ,bandwidth changes, etc. This is accomplished in part by caching the desirable file or files together with the appropriate protocol information to a local data store. It is located in the hidden "*%systemroot%**csc*" directory . In addition, access rights and share access rights are also cached.

Cut and paste from *Windows XP Resource online* :

"The CSC directory contains all offline files that are requested by any user on the computer. The database mimics the network resource while it is offline so that files are accessed as though the network resource is still available. File permissions and system permissions on the files are preserved. For example, a Microsoft® Word document created by Bob, given a password, and saved to a share on which only Bob has Full Control, cannot be opened from the CSC directory by Alice, because she has neither the share permissions to open the file nor the password required to open the file in Microsoft Word. You can also maintain the security of sensitive files by using Encrypting File System (EFS) to encrypt the Offline Files cache."

2.CSCDLL.DLL AND MRXSMB.SYS

The CSC infrastructure comprises user-mode components. One of them is the undocumented system dll, *cscdll.dll*.

It exports synchronization functions, online/offline states, offline store, file handling, cache operations, etc.

For example, Cscdll.dll is used by Windows Media Player or Internet Explorer . When the user is trying to access to a remote share file or share directory content, the CSC mechanism is activated.

Cscdll.dll is not alone, there is a driver waiting it...mrxsmb.sys.

Mrxsmb.sys is the Microsoft Server Message Block Redirector Driver. According to Microsoft Installable File System Documentation, the basic software components required as part of a Network Redirector are:

- A kernel-mode file system device driver (SYS) that provides the network redirector functions.
- A user-mode dynamic link library (DLL) that provides access for client user-applications to the Network Provider interface for non-file operations and enables communication with the kernel-mode file system driver providing the network redirector functions.

The user-mode component is easily identified, as well as its associated kernel-mode component , *mrxsmb.sys.* It does not mean that *mrxsmb.sys* only "serves" to *cscdll.dll* although we will focus on that communication.

Sometimes, there is a service between the dll and the driver which acts as "intermediary", i.e. both *ntlanman.dll* and *svchost.exe* communicate with *mrxsmb.sys* in order to perform certain operations, however it is "surveiled" by svchost.exe

Cscdll.dll "talks" directly with *mrxsmb.sys.* There is a well known api which is used by user-mode applications to communicate with drivers:

BOOL DeviceloControl(HANDLE hDevice, DWORD dwloControlCode, LPVOID lpInBuffer, DWORD nInBufferSize, LPVOID lpOutBuffer, DWORD nOutBufferSize, LPDWORD lpBytesReturned, LPOVERLAPPED lpOverlapped):

The way in which the IOM will handle input and output buffers is determined by the IOCTL . IOCTLs are generated using the following macro defined in *ddk.h*

#define CTL_CODE(DeviceType, Function, Method, Access) (
 ((DeviceType) << 16) | ((Access) << 14) | ((Function) << 2) | (Method)</pre>

<u>DeviceType</u> 0x0000-0x7FFF Reserved for Microsoft. 0x8000-0xFFFF Reserved for OEMs and IHVs Interesting: #define FILE_DEVICE_NETWORK_FILE_SYSTEM <u>0x00000014</u>

Function

0x000-0x7FF Reserved for Microsoft 0x800-0xFFF Reserved for OEMs and IHVs.

<u>Method</u>

#define METHOD_BUFFERED	0
#define METHOD_IN_DIRECT	1
#define METHOD_OUT_DIRECT	2
#define METHOD NEITHER	3

<u>Access</u>	
#define FILE_ANY_ACCESS	0x00000000
#define FILE_READ_ACCESS	0x0000001
#define FILE_WRITE_ACCESS	0x0000002
Having a look at DDK one more time :	

METHOD_NEITHER

"The I/O manager does not provide any system buffers or MDLs. The IRP supplies the <u>user-mode virtual addresses</u> of the input and <u>output buffers</u> that were specified to DeviceIoControl or IoBuildDeviceIoControlRequest, <u>without validating</u> or mapping them.

This method can be used only if the driver can be guaranteed to be running in the context of the thread that originated the I/O control request. Only a highest-level kernel-mode driver is guaranteed to meet this condition, so METHOD_NEITHER is seldom used for the I/O control codes that are passed to low-level device drivers.

With this method, the highest-level driver must determine whether to set up buffered or direct access to user data on receipt of the request, possibly must lock down the user buffer, and must wrap its access to the user buffer in a structured exception handler[...]"



So IOCTLs potentially dangerous would like as follows:

0x14xxx3 - 0x14xxx7 - 0x14xxxB - 0x14xxxF

3.FLAW

Just the most important steps and code snippets are explained

DeviceIoControl is heavily used.

[...] sub_770A972C+53 call ds:DeviceIoControl sub_770A97AA+57 call ds:DeviceIoControl sub_770A983D+57 call ds:DeviceIoControl sub_770A98C9+83 call ds:DeviceIoControl sub_770A99CA+42 call ds:DeviceIoControl [...]

cscdll.dll

We are seeking certain parameters, OutBuffer != NULL && OutBufferSize != 0

Potentially dangerous Call **RING 3**

.text:770A9D53	push	[ebp+lpInBuffer]
.text:770A9D56	call	sub_770A9700 - Returns Input Buffer length
.text:770A9D5B	рор	ecx
.text:770A9D5C	mov	edx, [ebp+arg_C]
.text:770A9D5F	mov	ecx, [ebp+lpOutBuffer]
.text:770A9D62	push	0 ; IpOverlapped
.text:770A9D64	push	offset BytesReturned ; lpBytesReturned
.text:770A9D69	push	18h ; nOutBufferSize-Sizeof(OBJECT_ATTRIBUTES)
.text:770A9D6B	shl	eax, 1
.text:770A9D6D	push	ecx ; lpOutBuffer -Any memory address
.text:770A9D6E	push	eax ; nInBufferSize
.text:770A9D6F	push	[ebp+lpInBuffer] ; lpInBuffer
.text:770A9D72	mov	[ecx+10h], edx
.text:770A9D75	push	141043h ; dwloControlCode- 0x14xxx3h match!
.text:770A9D7A	push	esi ; hDevice – Later
.text:770A9D7B	call ds:De	eviceIoControl
.text:770A9D81	test edi, e	di
.text:770A9D83	mov	ebx, eax
.text:770A9D85	jz	short loc_770A9D8D
.text:770A9D87	push	esi ; hObject

cscdll.dll

What about the device?... CreateFileA help us.

.text:770AA9A6	push 0 ; hTemplateFile	
.text:770AA9A8	push [esp+4+dwFlagsAndAttributes] ;	
.text:770AA9AC	push 3 ; dwCreationDisposition	
.text:770AA9AE	push 0 ; IpSecurityAttributes	
.text:770AA9B0	push 3 ; dwShareMode	
.text:770AA9B2	push 20h ; dwDesiredAccess	
.text:770AA9B4	<pre>push offset a_Shadow ; "\\\\.\\shadow" ; Nice device name.</pre>	
.text:770AA9B9	call ds:CreateFileA	
cscdll.dll		

RING0

mrxsmb.sys handling our request....

Firstly...

PAGE:00060AC2	cmp [esp+arg_4], 141043h	;Our "Magic" IOCTL
PAGE:00060ACA	mov eax, [esp+arg_0]	· · · · · · · · · · · · · · · · · · ·
PAGE:00060ACE	jnz short loc_60B12	
PAGE:00060AD0	mov ecx, [eax+0FCh]	
PAGE:00060AD6	mov eax, [eax+0F8h]	;Input Buffer length
PAGE:00060ADC	dec eax	;'\0' out!
PAGE:00060ADD	cmp eax, 288h	;Max length
PAGE:00060AE2	ja short loc_60AEF	;Bad, Bad, Bad
PAGE:00060AE4	push eax ; Length	
PAGE:00060AE5	push ecx ; Address	
PAGE:00060AE6	call sub_3B45C	;ProbeForWrite & ProbeForRead check [Inbuff]

mrxsmb.sys

Finally...

PAGE:00064CA4 mov [ebp+ObjectAttributes.ObjectName], eax; Very important! PAGE:00064CA7 pop ecx, eax PAGE:00064CA8 kor eax, eax PAGE:00064CA1 lea edi, [ebp+tEaBuffer] PAGE:00064CA2 mov eax, [ebp+var_54], al PAGE:00064CB2 mov eax, [ebp+var_14+2], bx PAGE:00064CB3 xor edx, edx PAGE:00064CB4 mov word ptr [ebp+var_14], bx PAGE:00064CB2 mov word ptr [ebp+var_14], bx PAGE:00064CB4 mov word ptr [ebp+var_14], bx PAGE:00064CC2 mov [ebp+ObjectAttributes.Length], 18h ; 18h==OutBufferSize PAGE:00064CC3 mov [ebp+ObjectAttributes.RootDirectory], edx PAGE:00064CC6 mov [ebp+ObjectAttributes.SecurityQualityOfService], edx PAGE:00064CC6 mov [ebp+var_52], 4 PAGE:00064CC6 mov [ebp+var_38], 1 PAGE:00064CC6 mov [ebp+var_38], 1 PAGE:00064CC6 mov [ebp+var_38], 1 PAGE:00064CC7 pop ecx PAGE:00064CC7 pop ecx PAGE			
PAGE:00064CA7 pop ecx PAGE:00064CA8 lea edi. [ebp+EaBuffer] PAGE:00064CA1 rep stosd PAGE:00064CA2 mov eax, [ebp+var_54], al PAGE:00064CB3 add ebx, 0Ch PAGE:00064CB4 mov word ptr [ebp+var_14], bx PAGE:00064CB5 add ebx, 0Ch PAGE:00064CB4 mov word ptr [ebp+var_14], bx PAGE:00064CC2 mov (ebp+0bjectAttributes.Length], 18h ; 18h==OutBufferSize PAGE:00064CC3 mov [ebp+0bjectAttributes.RootDirectory], edx PAGE:00064CC6 mov [ebp+0bjectAttributes.SecurityQualityOfService], edx PAGE:00064CD6 mov [ebp+0bjectAttributes.SecurityQualityOfService], edx PAGE:00064CD6 mov [ebp+var_52], 4 PAGE:00064CD6 mov [ebp+var_38], 1 PAGE:00064CE1 mov [ebp+var_38], 1 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 <td>PAGE:00064CA4</td> <td>mov</td> <td>[ebp+ObjectAttributes.ObjectName], eax ;Very important!</td>	PAGE:00064CA4	mov	[ebp+ObjectAttributes.ObjectName], eax ;Very important!
PAGE:00064CAA lea edi, [ebp+EaBuffer] PAGE:00064CAF and [ebp+var_54], al PAGE:00064CBF and [ebp+var_54], al PAGE:00064CB5 add ebx, 0Ch PAGE:00064CB8 xor edx, edx PAGE:00064CB8 mov word ptr [ebp+var_14], bx PAGE:00064CB8 mov word ptr [ebp+var_14], bx PAGE:00064CC2 mov [ebp+ObjectAttributes.length], 18h ; 18h==OutBufferSize PAGE:00064CC2 mov [ebp+ObjectAttributes.length], 18h ; 18h==OutBufferSize PAGE:00064CC2 mov [ebp+ObjectAttributes.length], 18h ; 18h==OutBufferSize PAGE:00064CC3 mov [ebp+ObjectAttributes.SecurityDecriptor], edx PAGE:00064CC6 mov [ebp+ObjectAttributes.SecurityQecriptor], edx PAGE:00064CC6 mov [ebp+Var_52], 4 PAGE:00064CC9 mov [ebp+Var_52], 4 PAGE:00064CC6 mov [ebp+var_53], 15h PAGE:00064CC6 mov [ebp+var_53], 15h PAGE:00064CC8 mov [ebp+var_53], 1 PAGE:00064CC8 mov [ebp+var_53], 1 PAGE:00064CC8 mov [ebp+var_53], 1 PAGE:00064CC8 mov [ebp+var_53], 1 PAGE:00064CC7 pp ecx PAGE:00064CC7 pp ecx PAGE:00064CF4 lea eax.[ebp+EaBuffer] PAGE:00064CF4 push 5 PAGE:00064CF4 push 5 PAGE:00064CF4 push 5 PAGE:00064CF4 push 5 PAGE:00064CF4 push 68h ; CreateOptions PAGE:00064CF4 push 68h ; CreateOptions PAGE:00064CF5 push 68h ; CreateOptions PAGE:00064CF6 push 68h ; CreateOptions PAGE:00064D00 push 68h ; CreateOptions PAGE:00064D01 push 68h ; CreateOptions PAGE:00064D04 push 7 ; ShareAccess PAGE:00064D05 push 68h ; CreateOptions PAGE:00064D06 push 80h ; FileAttributes PAGE:00064D06 push 80h ; FileAttributes PAGE:00064D06 push 80h ; DesiredAccess PAGE:00064D07 push eax ; ObjectAttributes] PAGE:00064D08 lea eax,[ebp+IOEtatusBlock] PAGE:00064D09 push 68h ; CreateOptions PAGE:00064D09 push eax ; ObjectAttributes] PAGE:00064D01 lea eax,[ebp+IOEtatusBlock] PAGE:00064D01 push eax ; ObjectAttributes] PAGE:00064D01 push eax ; ObjectAttributes] PAGE:00064D01 push eax ; ObjectAttributes] PAGE:00064D10 lea eax,[ebp+IOEtatusBlock] PAGE:00064D11 lea edi,[ebp+IOEtatusBlock] PAGE:00064D11 lea edi,[ebp+IOEtatusBlock] PAGE:00064D11 push eax ; ObjectAttributes] PAGE:00064D11 lea edi,[PAGE:00064CA7	рор	ecx
PAGE:00064CAA lea edi, [ebp+tEaBuffer] PAGE:00064CAF and [ebp+tar_54], al PAGE:00064CB2 mov eax, [ebp+tar_54], al PAGE:00064CB3 add ebx, 0Ch PAGE:00064CB3 mov eax, [ebp+tar_14+2], bx PAGE:00064CB4 mov word ptr [ebp+var_14+2], bx PAGE:00064CC2 mov [ebp+ObjectAttributes.Length], 18h ; 18h==OutBufferSize PAGE:00064CC2 mov [ebp+ObjectAttributes.Attributes], 40h PAGE:00064CC3 mov [ebp+ObjectAttributes.SecurityDescriptor], edx PAGE:00064CC3 mov [ebp+ObjectAttributes.SecurityDescriptor], edx PAGE:00064CC6 mov [ebp+CaBuffer], edx PAGE:00064CC6 mov [ebp+var_53], 15h PAGE:00064CC6 mov [ebp+var_53], 15h PAGE:00064CC6 mov [ebp+var_53], 15h PAGE:00064CC6 test byte ptr [eax], 1 PAGE:00064CC7 pup [z short loc_64CF2 PAGE:00064CC7 pup ecx PAGE:00064CC7 pup ecx PAGE:00064CC7 pup ecx PAGE:00064CC7 pup ecx PAGE:00064CC7 pup ecx PAGE:00064CC7 pup ecx PAGE:00064CF1 lea eax, [ebp+tEaBuffer] PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF3 push 24h ; EaLength PAGE:00064CF4 lea eax, [ebp+tEaBuffer] PAGE:00064CF5 push 24h ; EaLength PAGE:00064CF5 push 24h ; EaLength PAGE:00064CF5 push 24h ; EaLength PAGE:00064CF5 push 24h ; EaLength PAGE:00064D0 push 88h ; CreateOptions PAGE:00064D0 push 88h ; CreateOptions PAGE:00064D1 push eax ; AllocationSize PAGE:00064D1 push eax ; ObjectAttributes PAGE:00064D1 push eax ; ObjectA	PAGE:00064CA8	xor	eax, eax
PAGE:00064CAD rep stosd PAGE:00064CAF and [ebp+var_54], al PAGE:00064CBS add ebx, 0Ch PAGE:00064CBS add ebx, 0Ch PAGE:00064CBE mov word ptr [ebp+var_14+2], bx PAGE:00064CCB mov word ptr [ebp+var_14+2], bx PAGE:00064CC2 mov [ebp+ObjectAttributes.Length], 18h ; 18h==OutBufferSize PAGE:00064CC2 mov [ebp+ObjectAttributes.RotDirectory], edx PAGE:00064CC3 mov [ebp+ObjectAttributes.SecurityDescriptor], edx PAGE:00064CC6 mov [ebp+ObjectAttributes.SecurityDescriptor], edx PAGE:00064CD6 mov [ebp+ADjectAttributes.SecurityDescriptor], edx PAGE:00064CD6 mov [ebp+ADjectAttributes.SecurityDescriptor], edx PAGE:00064CD6 mov [ebp+ADjectAttributes.SecurityDescriptor], edx PAGE:00064CD6 mov [ebp+ar_52], 4 PAGE:00064CD6 mov [ebp+ar_52], 4 PAGE:00064CE6 test byte ptr [eax], 1 PAGE:00064CE8 mov [ebp+var_38], 1 PAGE:00064CE9 jz short loc_64CF2 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF4 lea eax, [ebp+EaBuffer] PAGE:00064CF7 pop ecx PAGE:00064CF7 pop ecx PAGE:00064CF7 pop ecx PAGE:00064CF7 pop ecx PAGE:00064CF7 push 8ak ; EaBuffer PAGE:00064CF7 push 8ak ; CreateOptions PAGE:00064CF7 push 8ak ; CreateOptions PAGE:00064D04 push 7 ; ShareAccess PAGE:00064D05 push 88h ; CreateOptions PAGE:00064D06 push 80h ; FileAttributes PAGE:00064D06 push 80h ; FileAttributes PAGE:00064D07 push eax ; AllocationSize PAGE:00064D08 lea eax, [ebp+HoStatusBlock] PAGE:00064D09 push 62k ; AllocationSize PAGE:00064D09 push eax ; ObjectAttributes PAGE:00064D09 push eax ; ObjectAttributes PAGE:00064D10 lea eax, [ebp+ObjectAttributes] PAGE:00064D10 lea eax, [ebp+ObjectAttributes] PAGE:00064D10 lea eax; [ebp+ObjectAttributes] PAGE:00064D10 lea eax; [ebp+ObjectAttributes] PAGE:00064D11 lea edi, [ebp+FileHandle] ; FileHandle===OutBuffer+0xC PAGE:00064D15 lea edi, [ebp+var_50] PAGE:00064D15 lea edi, [e	PAGE:00064CAA	lea	edi, [ebp+EaBuffer]
PAGE:00064CBF and [ebp+var_54], al PAGE:00064CB2 mov eax, [ebp+var_8] PAGE:00064CB8 xor edx, edx PAGE:00064CB8 mov word ptr [ebp+var_14+2], bx PAGE:00064CC2 mov [ebp+ObjectAttributes.ReotDirectory], edx PAGE:00064CC2 mov [ebp+ObjectAttributes.RootDirectory], edx PAGE:00064CC3 mov [ebp+ObjectAttributes.RootDirectory], edx PAGE:00064CC3 mov [ebp+ObjectAttributes.SecurityOescriptor], edx PAGE:00064CD3 mov [ebp+be]ctAttributes.SecurityOescriptor], edx PAGE:00064CD9 mov [ebp+tasBuffer], edx PAGE:00064CD9 mov [ebp+tasBuffer], edx PAGE:00064CE6 test byte ptr [eax], 1 PAGE:00064CE6 test byte ptr [eax], 1 PAGE:00064CE8 mov [ebp+var_52], 4 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF1 lea eax, [ebp+EaBuffer] PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF1 lea eax, [ebp+EaBuffer] PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF1 lea eax, [ebp+EaBuffer] PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF1 lea eax, [ebp+EaBuffer] PAGE:00064CF2 push 5 PAGE:00064CF1 push 24h ; EaLength PAGE:00064CF1 push 24h ; EaLength PAGE:00064CF1 push 24h ; EaLength PAGE:00064CF1 push 24h ; EaLength PAGE:00064D02 push 68h ; CreateOptions PAGE:00064D04 push 7 ; ShareAccess PAGE:00064D04 push 7 ; ShareAccess PAGE:00064D05 push 80h ; FileAttributes PAGE:00064D06 push 80h ; FileAttributes PAGE:00064D06 push 80h ; FileAttributes PAGE:00064D07 push eax ; loStatusBlock PAGE:00064D08 lea eax, [ebp+ObjectAttributes] PAGE:00064D10 push eax ; loStatusBlock PAGE:00064D10 push eax ; loStatusBlock PAGE:00064D10 push eax ; loStatusBlock PAGE:00064D11 push eax ;	PAGE:00064CAD	rep s	tosd
PAGE:00064CB2 mov eax. [ebp+var_8] PAGE:00064CB3 add ebx, 0Ch PAGE:00064CBA mov word ptr [ebp+var_14+2], bx PAGE:00064CBE mov word ptr [ebp+var_14+2], bx PAGE:00064CC2 mov [ebp+ObjectAttributes.Length], 18h ; 18h==OutBufferSize PAGE:00064CC2 mov [ebp+ObjectAttributes.RootDirectory], edx PAGE:00064CC6 mov [ebp+ObjectAttributes.SecurityOualityOfService], edx PAGE:00064CD6 mov [ebp+ObjectAttributes.SecurityOualityOfService], edx PAGE:00064CD6 mov [ebp+var_53], 15h PAGE:00064CE0 mov [ebp+var_53], 15h PAGE:00064CE6 test byte ptr [eax], 1 PAGE:00064CE8 mov [ebp+var_38], 1 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF7 pop ecx PAGE:00064CF8 mov esi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$" PAGE:00064CFF push eax ; EaBuffer] PAGE:00064CFF push eax ; EaBuffer PAGE:00064CFF push eax ; EaBuffer PAGE:00064D0 push 68h ; CreateOptions PAGE:00064D0 push 68h ; CreateOptions PAGE:00064D1 push 68h ; CreateFileHandle; FileHandle=FileHandle=FileHandle	PAGE:00064CAF	and	[ebp+var_54], al
PAGE:00064CB5 add ebx, 0Ch PAGE:00064CB8 xor edx, edx PAGE:00064CBA mov word ptr [ebp+var_14+2], bx PAGE:00064CBE mov word ptr [ebp+var_14], bx PAGE:00064CC2 mov [ebp+ObjectAttributes.Length], 18h ; 18h==OutBufferSize PAGE:00064CC2 mov [ebp+ObjectAttributes.RootDirectory], edx PAGE:00064CC3 mov [ebp+ObjectAttributes.RootDirectory], edx PAGE:00064CD3 mov [ebp+DetetAttributes.SecurityOcscriptor], edx PAGE:00064CD9 mov [ebp+eabuffer], edx PAGE:00064CD0 mov [ebp+var_52], 4 PAGE:00064CE8 mov [ebp+var_53], 15h PAGE:00064CE6 test byte ptr [eax], 1 PAGE:00064CE8 mov [ebp+var_38], 1 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF4 lea eax, [ebp+EaBuffer] PAGE:00064CF5 mov esi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$" PAGE:00064CF5 mov esi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$" PAGE:00064CF7 pop ecx PAGE:00064CF7 push eax ; EaBuffer] PAGE:00064D0 push 68h ; CreateOptions PAGE:00064D0 push 68h ; CreateOptions PAGE:00064D0 push eax ; loStatusBlock] PAGE:00064D1	PAGE:00064CB2	mov	eax, [ebp+var_8]
PAGE:00064CB8 xor edx, edx PAGE:00064CBA mov word ptr [ebp+var_14+2], bx PAGE:00064CC2 mov [ebp+ObjectAttributes.Length], 18h ; 18h==OutBufferSize PAGE:00064CC3 mov [ebp+ObjectAttributes.RootDirectory], edx PAGE:00064CD3 mov [ebp+ObjectAttributes.SecurityDescriptor], edx PAGE:00064CD6 mov [ebp+VojectAttributes.SecurityDescriptor], edx PAGE:00064CD6 mov [ebp+Var_53], 15h PAGE:00064CDC mov [ebp+var_52], 4 PAGE:00064CD6 mov [ebp+var_52], 4 PAGE:00064CD6 mov [ebp+var_52], 4 PAGE:00064CE9 jz short loc_64CF2 PAGE:00064CE8 mov [ebp+var_38], 1 PAGE:00064CF2 piz short loc_64CF2 PAGE:00064CF2 piz short loc_64CF2 PAGE:00064CF2 piz short loc_64CF2 PAGE:00064CF2 pix short loc_64CF2 PAGE:00064CF2 pix short loc_64CF2 PAGE:00064CF5 pix short loc_64CF2 PAGE:00064CF7 pop ecx PAGE:00064CF7 pop ecx PAGE:00064CF7 pop ecx PAGE:00064CF7 pop ecx PAGE:00064CF7 pop ecx PAGE:00064CF7 pop ex ; CODE XREF: sub_64B98+151#j PAGE:00064CF7 pop ex ; CODE XREF: sub_64B98+151#j PAGE:00064CF7 pop ex ; [ebp+EaBuffer] PAGE:00064CF7 pop ex ; [ebp+EaBuffer] PAGE:00064CF7 pop ex ; [ebp+EaBuffer] PAGE:00064CF5 push 24h ; EaLength PAGE:00064CF5 push 24h ; EaLength PAGE:00064D00 push 68h ; CreateOptions PAGE:00064D02 push 1 ; CreateDisposition PAGE:00064D04 push 7 ; ShareAccess PAGE:00064D05 push 80h ; FileAttributes PAGE:00064D06 push 80h ; FileAttributes PAGE:00064D06 push eax ; LoStatusBlock PAGE:00064D07 push eax ; IoStatusBlock PAGE:00064D08 lea eax, [ebp+HoStatusBlock] PAGE:00064D01 lea eax, [ebp+HoExtatusBlock PAGE:00064D01 push eax ; ObjectAttributes PAGE:00064D01 push eax ; ObjectAttributes PAGE:00064D01 push eax ; ObjectAttributes PAGE:00064D13 push eax ; ObjectAttributes PAGE:00064D14 push 100080h ; DesiredAccess PAGE:00064D15 push [ea edi, [ebp+HieHandle]; FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D16 lea edi, [ebp+HieHandle]; FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D17 rep movxd PAGE:00064D17 call ds:ZwCreateFile ; jtfZwCreateFile) Overwrite();	PAGE:00064CB5	add	ebx, 0Ch
PAGE:00064CBA mov word ptr [ebp+var_14+2], bx PAGE:00064CC2 mov [ebp+ObjectAttributes.Length], 18h ; 18h==OutBufferSize PAGE:00064CC3 mov [ebp+ObjectAttributes.RootDirectory], edx PAGE:00064CD6 mov [ebp+ObjectAttributes.SecurityQualityOfService], edx PAGE:00064CD6 mov [ebp+DobjectAttributes.SecurityQualityOfService], edx PAGE:00064CD9 mov [ebp+EaBuffer], edx PAGE:00064CD0 mov [ebp+var_52], 4 PAGE:00064CC6 test byte ptr [eax], 1 PAGE:00064CC6 test byte ptr [eax], 1 PAGE:00064CC2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF4 lea eax, [ebp+EaBuffer] PAGE:00064CF5 push 24h ; EaLength PAGE:00064CF5 push 24h ; EaLength PAGE:00064CFF push eax ; EaBuffer PAGE:00064CFF push eax ; EaBuffer PAGE:00064DFF push eax ; CreateOptions PAGE:00064DFF push eax ; IoStatusBlock] PAGE:00064D01 push 24h ; FileHandle; FileHandle==OutBuffer+0xC PAGE:00064D05 push eax ; IoStatusBlock] PAGE:00064D06 push eax ; ObjectAttributes PAGE:00064D06 push eax ; ObjectAttributes PAGE:00064D07 push eax ; IoStatusBlock] PAGE:00064D08 lea eax, [ebp+ObjectAttributes] PAGE:00064D09 push eax ; ObjectAttributes] PAGE:00064D01 lea eax, [ebp+ObjectAttributes] PAGE:00064D05 push eax ; ObjectAttributes] PAGE:00064D06 push eax ; ObjectAttributes] PAGE:00064D07 push eax ; ObjectAttributes] PAGE:00064D08 lea eax, [ebp+ObjectAttributes] PAGE:00064D01 lea eax, [ebp+ObjectAttributes] PAGE:00064D13 push eax ; ObjectAttributes] PAGE:00064D14 push 100080h ; DesiredAcceass PAGE:00064D15 repmovsd PAGE:00064D16 lea ed, [ebp+va_50] PAGE:00064D17 repmovsd PAGE:00064D17 repmovsd	PAGE:00064CB8	xor	edx, edx
PAGE:00064CEE mov word ptr [ebp+var_14], bx PAGE:00064CC2 mov [ebp+ObjectAttributes.Length], 18h ; 18h==OutBufferSize PAGE:00064CC3 mov [ebp+ObjectAttributes.RotDirectory], edx PAGE:00064CD3 mov [ebp+ObjectAttributes.SecurityDescriptor], edx PAGE:00064CD6 mov [ebp+CbjectAttributes.SecurityDescriptor], edx PAGE:00064CD6 mov [ebp+var_53], 15h PAGE:00064CCE mov [ebp+var_52], 4 PAGE:00064CE6 test byte ptr [eax], 1 PAGE:00064CE8 mov [ebp+var_38], 1 PAGE:00064CE9 jz short loc_64CF2 PAGE:00064CF2 mov [ebp+var_38], 1 PAGE:00064CF2 push 5 PAGE:00064CF4 lea eax, [ebp+EaBuffer] PAGE:00064CF5 mov esi, offset aRxcsccopychu_0; "\$RxCscCopyChunkOpen\$" PAGE:00064CF5 push 5 PAGE:00064CF7 pop ecx PAGE:00064CF7 push 24h ; EaLength PAGE:00064CFF push eax ; EaBuffer PAGE:00064CFF push 86h ; CreateOptions PAGE:00064D02 push 1 ; CreateOptions PAGE:00064D04 push 7 ; ShareAccess PAGE:00064D05 push eax ; loStausBlock PAGE:00064D05 push eax ; loStausBlock PAGE:00064D06 push 80h ; FileAttributes PAGE:00064D07 push eax ; loStausBlock PAGE:00064D07 push eax ; ObjectAttributes PAGE:00064D06 push 80h ; FileAttributes PAGE:00064D07 push eax ; loStausBlock PAGE:00064D07 push eax ; ObjectAttributes PAGE:00064D06 push eax ; ObjectAttributes PAGE:00064D07 push eax ; IoStausBlock PAGE:00064D07 push eax ; ObjectAttributes PAGE:00064D07 push eax ; ObjectAttributes PAGE:00064D13 push eax ; ObjectAttributes PAGE:00064D14 push 100080h ; DesiredAccess PAGE:00064D15 repmovsd PAGE:00064D16 lea ed.[ebp+var_50] PAGE:00064D17 repmovsd PAGE:00064D17 repmovsd	PAGE:00064CBA	mov	word ptr [ebp+var_14+2], bx
PAGE:00064CC2mov[ebp+ObjectAttributes.Length], 18h; 18h==OutBufferSizePAGE:00064CC3mov[ebp+ObjectAttributes.RotoDirectory], edxPAGE:00064CD6mov[ebp+ObjectAttributes.Attributes], 40hPAGE:00064CD6mov[ebp+ObjectAttributes.SecurityDescriptor], edxPAGE:00064CD6mov[ebp+Var_53], 15hPAGE:00064CD6mov[ebp+var_52], 4PAGE:00064CE6testbyte tr [eax], 1PAGE:00064CE6mov[ebp+var_52], 4PAGE:00064CE8mov[ebp+var_38], 1PAGE:00064CF2push5PAGE:00064CF2push5PAGE:00064CF2push5PAGE:00064CF2push5PAGE:00064CF8movesi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$"PAGE:00064CF7push24h; EaleungthPAGE:00064CF7pusheax; EaBufferPAGE:00064CF7pusheax; ShareAccessPAGE:00064CF1push68h; CreateOptionsPAGE:00064D02push7; ShareAccessPAGE:00064D04push7; ShareAccessPAGE:00064D05pusheax; IoStatusBlockPAGE:00064D06pusheax; IoStatusBlockPAGE:00064D07pusheax; IoStatusBlockPAGE:00064D08leaeax; IoStatusBlockPAGE:00064D10leaeax; IoStatusBlockPAGE:00064D10leaeax; IoStatusBlockPAGE:00064D11pushio	PAGE:00064CBE	mov	word ptr [ebp+var_14], bx
PAGE:00064CC9 mov [ebp+ObjectAttributes.RootDirectory], edx PAGE:00064CD3 mov [ebp+ObjectAttributes.Attributes], 40h PAGE:00064CD6 mov [ebp+ObjectAttributes.SecurityDescriptor], edx PAGE:00064CD0 mov [ebp+Var_53], 15h PAGE:00064CE0 mov [ebp+var_52], 4 PAGE:00064CE6 test byte ptr [eax], 1 PAGE:00064CE6 test byte ptr [eax], 1 PAGE:00064CE8 mov [ebp+var_38], 1 PAGE:00064CF2 mov [ebp+tar_38], 1 PAGE:00064CF2 loc_64CF2: ; CODE XREF: sub_64B98+151#j PAGE:00064CF2 push 5 PAGE:00064CF4 lea eax. [ebp+EaBuffer] PAGE:00064CF5 mov esi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$" PAGE:00064CFF push 24h ; EaLength PAGE:00064CFF push 68h ; CreateOptions PAGE:00064D0 push 68h ; StreatAccess PAGE:00064D0 push 68h ; CreateOptions PAGE:00064D0 push 68h ; StreatAccess PAGE:00064D0 push 68h ; FileAttributes PAGE:00064D0 push 64x ; AllocationSize PAGE:00064D0 push 64x ; ObjectAttributes PAGE:00064D1 lea eax. [ebp+ObjectAttributes PAGE:00064D1 push eax ; ObjectAttributes PAGE:00064D1 push eax ; DistatusBlock PAGE:00064D1 push eax ; DistatusBlock PAGE:00064D1 push [ebp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D1 push [ebp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D1 push [ebp+var_50] PAGE:00064D1 push [ebp+var_50] PAGE:00064D1 push [ebp+var_50] PAGE:00064D1 push [ebp+var_50] PAGE:00064D1 push [ebp+var_50] PAGE:00064D1 push [ebp+var_50] PAGE:00064D1 push [ea eax]; [ebp+var_50] PAGE:00064D1 push [ebp+var_50] P	PAGE:00064CC2	mov	[ebp+ObjectAttributes.Length], 18h ; 18h==OutBufferSize
PAGE:00064CCC mov [ebp+ObjectAttributes.Attributes].40h PAGE:00064CD3 mov [ebp+ObjectAttributes.SecurityDescriptor], edx PAGE:00064CD6 mov [ebp+Var_53], 15h PAGE:00064CDC mov [ebp+var_52], 4 PAGE:00064CE6 test byte ptr [eax], 1 PAGE:00064CE9 jz short loc_64CF2 PAGE:00064CF2 jz short loc_64CF2 PAGE:00064CF2 mov [ebp+var_38], 1 PAGE:00064CF2 ptr [eax], 1 PAGE:00064CF4 lea eax, [ebp+EaBuffer] PAGE:00064CF5 mov esi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$" PAGE:00064CF7 pop ecx PAGE:00064CFF push eax ; EaBuffer PAGE:00064CFF push eax ; CreateOptions PAGE:00064D00 push 68h ; CreateOptions PAGE:00064D04 push 7 ; ShareAccess PAGE:00064D04 push 7; ShareAccess PAGE:00064D05 push eax ; IoStatusBlock] PAGE:00064D06 push eax ; IoStatusBlock PAGE:00064D06 push eax ; IoStatusBlock PAGE:00064D07 push eax ; IoStatusBlock PAGE:00064D08 lea eax, [ebp+ObjectAttributes] PAGE:00064D09 push eax ; IoStatusBlock PAGE:00064D01 lea eax, [ebp+ObjectAttributes] PAGE:00064D14 push 7 cshareAccess PAGE:00064D14 push 100080h ; DesiredAccess PAGE:00064D14 push 100080h ; DesiredAccess PAGE:00064D15 push [ebp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D16 lea edit [ebp+var_50] PAGE:00064D17 rep movsd PAGE:00064D17 rep movsd PAGE:00064D14 call ds:ZwCreateFile ; if(ZwCreateFile) Overwrite();	PAGE:00064CC9	mov	[ebp+ObjectAttributes.RootDirectory], edx
PAGE:00064CD3 mov [ebp+ObjectAttributes.SecurityDescriptor], edx PAGE:00064CD6 mov [ebp+EaBuffer], edx PAGE:00064CE0 mov [ebp+var_53], 15h PAGE:00064CE6 test byte ptr [eax], 1 PAGE:00064CE9 jz short loc_64CF2 PAGE:00064CF2 pz short loc_64CF2 PAGE:00064CF2 push 5 PAGE:00064CF7 pop ecx PAGE:00064CF7 pop ecx PAGE:00064CF8 mov esi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$" PAGE:00064CF7 push 24h ; EaLength PAGE:00064CF7 push 68h ; CreateDptions PAGE:00064CFF push 68h ; CreateDptions PAGE:00064CFF push 68h ; FileAttributes PAGE:00064D0 push 80h ; FileAttributes PAGE:00064D0 push 80h ; FileAttributes PAGE:00064D0 push eax ; LaBuffer PAGE:00064D0 push 68h ; CreateDptions PAGE:00064D0 push 68h ; CreateDptions PAGE:00064D0 push 68h ; FileAttributes PAGE:00064D0 push eax ; LaBuffer PAGE:00064D0 push 68h ; CreateDptions PAGE:00064D0 push 68h ; CreateDptions PAGE:00064D0 push 68h ; FileAttributes PAGE:00064D0 push 80h ; FileAttributes PAGE:00064D0 push eax ; loStatusBlock] PAGE:00064D0 push eax ; loStatusBlock] PAGE:00064D10 lea eax, [ebp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D11 lea eat, [cbp+roljectAttributes] PAGE:00064D12 push [cbp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D14 push 100080h ; DesiredAccess PAGE:00064D15 push [cbp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D16 lea eat, [cbp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D17 lea edt, [cbp+var_50] PAGE:00064D16 lea eath [cbp+var_50] PAGE:00064D17 rep movsd PAGE:00064D16 lea eath [cbp+var_50] PAGE:00064D16 lea eath [cbp+var_50] PAGE:00064D17 rep movsd PAGE:00064D16 lea eath [cbp+var_50] PAGE:00064D17 call ds:ZwCreateFile ; if(ZwCreateFile) Overwrite();	PAGE:00064CCC	mov	[ebp+ObjectAttributes.Attributes], 40h
PAGE:00064CD6 mov [ebp+ObjectAttributes.SecurityQualityOfService], edx PAGE:00064CD9 mov [ebp+var_53], 15h PAGE:00064CE0 mov [ebp+var_52], 4 PAGE:00064CE9 jz short loc_64CF2 PAGE:00064CE8 mov [ebp+var_53], 1 PAGE:00064CE9 jz short loc_64CF2 PAGE:00064CE9 jz short loc_64CF2 PAGE:00064CF2 mov [ebp+var_38], 1 PAGE:00064CF2 push 5 PAGE:00064CF4 lea eax, [ebp+EaBuffer] PAGE:00064CF7 pop ecx PAGE:00064CF8 mov esi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$" PAGE:00064CFF push eax ; Ealength PAGE:00064CFF push eax ; Ealength PAGE:00064CFF push 68h ; CreateOptions PAGE:00064D00 push 68h ; CreateOptions PAGE:00064D01 push 7 ; ShareAccess PAGE:00064D04 push 7 ; ShareAccess PAGE:00064D05 push eax, [ebp+loStatusBlock]	PAGE:00064CD3	mov	[ebp+ObjectAttributes.SecurityDescriptor], edx
PAGE:00064CD9 mov [ebp+EaBuffer], edx PAGE:00064CDC mov [ebp+var_53], 15h PAGE:00064CE0 mov [ebp+var_52], 4 PAGE:00064CE9 jz short loc_64CF2 PAGE:00064CF2 jz short loc_64CF2 PAGE:00064CF2 push 5 PAGE:00064CF2 push 5 PAGE:00064CF4 lea eax, [ebp+EaBuffer] PAGE:00064CF4 lea eax, [ebp+EaBuffer] PAGE:00064CF7 pop ecx PAGE:00064CF8 mov esi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$" PAGE:00064CF7 push eax ; EaBuffer PAGE:00064CFF push eax ; EaBuffer PAGE:00064CFF push eax ; EaBuffer PAGE:00064D01 push 24h ; EaLength PAGE:00064D02 push 1 ; CreateOptions PAGE:00064D04 push 7 ; ShareAccess PAGE:00064D04 push 7 ; ShareAccess PAGE:00064D05 lea eax, [ebp+loStatusBlock] PAGE:00064D05 push eax ; IoStatusBlock PAGE:00064D06 push eax ; ObjectAttributes PAGE:00064D07 push eax ; ObjectAttributes PAGE:00064D08 lea eax, [ebp+ObjectAttributes] PAGE:00064D01 lea eax, [obp+Chitributes] PAGE:00064D10 lea eax ; ObjectAttributes] PAGE:00064D11 lea eax ; ObjectAttributes] PAGE:00064D13 push eax ; ObjectAttributes] PAGE:00064D14 push 100080h ; DesiredAccess PAGE:00064D15 push eax ; ObjectAttributes] PAGE:00064D14 push 100080h ; DesiredAccess PAGE:00064D15 push eax ; ObjectAttributes] PAGE:00064D14 push 100080h ; DesiredAccess PAGE:00064D15 push eax ; ObjectAttributes] PAGE:00064D16 lea eax, [ebp+Var_50] PAGE:00064D17 rep movsd PAGE:00064D16 lea eat, [cbp+Var_50] PAGE:00064D16 lea eat, [cbp+Var_50] PAGE:00064D16 lea eat, [cbp+Var_50] PAGE:00064D16 cattributes] PAGE:00064D16 lea eat, [cbp+Var_50] PAGE:00064D16 cattributes] PAGE:00064D16 cattributes] PAGE:00064D16 lea eat, [cbp+Var_50] PAGE:00064D16 cattributes] PAGE:00064D16 cattributes] PAGE:00064D11 cattribute	PAGE:00064CD6	mov	[ebp+ObjectAttributes.SecurityQualityOfService], edx
PAGE:00064CDC mov [ebp+var_53], 15h PAGE:00064CE0 mov [ebp+var_52], 4 PAGE:00064CE6 test byte ptr [eax], 1 PAGE:00064CE9 jz short loc_64CF2 PAGE:00064CF2 mov [ebp+var_38], 1 PAGE:00064CF2 por ebp+var_38], 1 PAGE:00064CF2 por ebp+var_38], 1 PAGE:00064CF2 por ebp+var_38], 1 PAGE:00064CF2 por ebp+var_38], 1 PAGE:00064CF4 lea eax, [ebp+EaBuffer] PAGE:00064CF7 pop ecx PAGE:00064CF7 pop ecx PAGE:00064CF7 pop ecx PAGE:00064CFF push eax ; EaBuffer PAGE:00064CFF push eax ; EaBuffer PAGE:00064D00 push 68h ; CreateOptions PAGE:00064D02 push 1 ; CreateOptions PAGE:00064D02 push 1 ; CreateOptions PAGE:00064D04 push 7 ; ShareAccess PAGE:00064D06 push 80h ; FileAttributes PAGE:00064D06 push eax ; loStatusBlock] PAGE:00064D0F push eax ; ObjectAttributes] PAGE:00064D0F push eax ; ObjectAttributes PAGE:00064D10 lea eax, [ebp+ObjectAttributes] PAGE:00064D11 push (bp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D14 push 7 ; DiseredAccess PAGE:00064D15 push (bp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D16 push [ebp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D17 push eax ; ObjectAttributes PAGE:00064D19 push [ebp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D11 push [ebp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D12 push [ebp+FileHandle]; FileHandle==OutBuffer+0xC PAGE:00064D14 push 7 rep movsd PAGE:00064D15 call ds:ZwCreateFile ; jf(ZwCreateFile) Overwrite();	PAGE:00064CD9	mov	[ebp+EaBuffer], edx
PAGE:00064CE0mov[ebp+var_52], 4PAGE:00064CE6testbyte ptr [eax], 1PAGE:00064CE9jzshort loc_64CF2PAGE:00064CF2mov[ebp+var_38], 1PAGE:00064CF2push5PAGE:00064CF4leaeax, [ebp+EaBuffer]PAGE:00064CF5popecxPAGE:00064CF6movesi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$"PAGE:00064CF7popecxPAGE:00064CF8movesi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$"PAGE:00064CF7push24hPAGE:00064CF7pusheax ; EaBufferPAGE:00064D6push68hPAGE:00064D00push68hPAGE:00064D02push1PAGE:00064D04pushPAGE:00064D05pushPAGE:00064D06pushPAGE:00064D07pushPAGE:00064D08leaeax, [ebp+loStatusBlock]PAGE:00064D07pushPAGE:00064D07pushPAGE:00064D07pushPAGE:00064D07pushPAGE:00064D07pushPAGE:00064D08leaPAGE:00064D09pushPAGE:00064D10leaPAGE:00064D11pushPAGE:00064D14pushPAGE:00064D14pushPAGE:00064D14pushPAGE:00064D14pushPAGE:00064D15rep movsdPAGE:00064D16leaPAGE:00064D17rep movsdPAGE:00064D16leaPAGE:00064D17<	PAGE:00064CDC	mov	[ebp+var_53], 15h
PAGE:00064CE6testbyte ptr [eax], 1PAGE:00064CE9jzshort loc_64CF2PAGE:00064CF4mov[ebp+var_38], 1PAGE:00064CF2push 5PAGE:00064CF2push 5PAGE:00064CF4leaeax, [ebp+EaBuffer]PAGE:00064CF7popecxPAGE:00064CF8movesi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$"PAGE:00064CF7push 24h; EaLengthPAGE:00064CF7push eax; EaBufferPAGE:00064CF7push 68h; CreateOptionsPAGE:00064D00push 68h; CreateOptionsPAGE:00064D01push 7; ShareAccessPAGE:00064D02push 1; CreateOptionsPAGE:00064D03push 68h; FileAttributesPAGE:00064D04push 7; ShareAccessPAGE:00064D05push edx; AllocationSizePAGE:00064D06push edx; IoStatusBlock]PAGE:00064D07push eax; ObjectAttributes]PAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D11push (ebp+FileHandle]; FileHandle==OutBuffer+0xCPAGE:00064D14push 100080h; DesiredAccessPAGE:00064D15rep movsdPAGE:00064D16leaedi, [ebp+var_50]PAGE:00064D17leaedi, [ebp+var_50]PAGE:00064D16leaedi, [ebp+var_50]PAGE:00064D17callds:ZwCreateFilePAGE:00064D21callds:ZwCreateFilePAGE:00064D21callds:ZwCreateFilePAGE:00064D21c	PAGE:00064CE0	mov	[ebp+var_52], 4
PAGE:00064CE9jzshort loc_64CF2PAGE:00064CE8mov[ebp+var_38], 1PAGE:00064CF2page:00064CF2colored colored color	PAGE:00064CE6	test	byte ptr [eax], 1
PAGE:00064CEBmov[ebp+var_38], 1PAGE:00064CF2push 5PAGE:00064CF2push 5PAGE:00064CF4leaeax, [ebp+EaBuffer]PAGE:00064CF7popecxPAGE:00064CF8movesi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$"PAGE:00064CFBpush 24h ; EaLengthPAGE:00064CFFpush eax ; EaBufferPAGE:00064CFFpush 68h ; CreateOptionsPAGE:00064D00push 68h ; CreateOptionsPAGE:00064D01push 7 ; ShareAccessPAGE:00064D02push 80h ; FileAttributesPAGE:00064D05push eax ; loStatusBlock]PAGE:00064D06push eax ; loStatusBlockPAGE:00064D07push eax ; ObjectAttributes]PAGE:00064D10leaPAGE:00064D11push eax ; ObjectAttributesPAGE:00064D12push eax ; ObjectAttributes]PAGE:00064D13push eax ; ObjectAttributes]PAGE:00064D14push 100080h ; DesiredAccessPAGE:00064D15rep movsdPAGE:00064D16lea edi, [ebp+rar_50]PAGE:00064D17rep movsdPAGE:00064D16cal edi, SzwCreateFile ; if(ZwCreateFile) Overwrite();	PAGE:00064CE9	jz :	short loc_64CF2
PAGE:00064CF2PAGE:00064CF2 loc_64CF2:; CODE XREF: sub_64B98+151#jPAGE:00064CF2push 5PAGE:00064CF4leaPAGE:00064CF7popPAGE:00064CF8movPAGE:00064CF7push 24hPAGE:00064CFFpush 24hPAGE:00064CFFpush eaxPAGE:00064D00push 68hPAGE:00064D02push 1CreateOptionsPAGE:00064D04push 7PAGE:00064D05push 80hPAGE:00064D06push 7PAGE:00064D07push 7PAGE:00064D08leaeax, [ebp+loStatusBlock]PAGE:00064D05push eaxPAGE:00064D06push eaxPAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D14push eaxPAGE:00064D15push eaxPAGE:00064D14push followingPAGE:00064D15push eaxPAGE:00064D16leaPAGE:00064D17leaPAGE:00064D18leaPAGE:00064D14push followingPAGE:00064D15push [ebp+FileHandle]; FileHandle; FileHandle==OutBuffer+0xCPAGE:00064D17leaPAGE:00064D16leaPAGE:00064D17rep movsdPAGE:00064D15rep movsdPAGE:00064D21call ds:ZwCreateFilePAGE:00064D21call ds:ZwCreateFilePAGE:00064D21call ds:ZwCreateFile	PAGE:00064CEB	mov	[ebp+var_38], 1
PAGE:00064CF2 loc_64CF2:; CODE XREF: sub_64B98+151#jPAGE:00064CF2push 5PAGE:00064CF4leaPAGE:00064CF7popPAGE:00064CF8movmovesi, offset aRxcsccopychu_0; "\$RxCscCopyChunkOpen\$"PAGE:00064CFDpush 24hPAGE:00064CFFpush eaxPAGE:00064D00push 68hPAGE:00064D02push 1PAGE:00064D04push 7PAGE:00064D05push 80hPAGE:00064D06push 80hFileAttributesPAGE:00064D07push eaxPAGE:00064D08leaeax, [ebp+loStatusBlock]PAGE:00064D10push eaxPAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D13push eaxPAGE:00064D14push 100080hPAGE:00064D15push [ebp+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D16push [ebp+tra_50]PAGE:00064D17leaPAGE:00064D16push [ebp+tra[]PAGE:00064D17rep movsdPAGE:00064D15rep movsdPAGE:00064D16call ds:ZwCreateFile ; if(ZwCreateFile) Overwrite();	PAGE:00064CF2		
PAGE:00064CF2push 5PAGE:00064CF4leaeax, [ebp+EaBuffer]PAGE:00064CF7popecxPAGE:00064CF8movesi, offset aRxcsccopychu_0; "\$RxCscCopyChunkOpen\$"PAGE:00064CFDpush 24h; EaLengthPAGE:00064CFFpush eax; EaBufferPAGE:00064D00push 68h; CreateOptionsPAGE:00064D02push 1; CreateDispositionPAGE:00064D04push 7; ShareAccessPAGE:00064D05push 80h; FileAttributesPAGE:00064D06push eax; IoStatusBlock]PAGE:00064D07push eax; IoStatusBlockPAGE:00064D08leaeax, [ebp+lobjectAttributes]PAGE:00064D10leaeax, [obje+Chtributes]PAGE:00064D11push eax; ObjectAttributesPAGE:00064D12push (bep+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D17leaedi, [ebp+var_50]PAGE:00064D17rep movsdPAGE:00064D17callds:ZwCreateFilePAGE:00064D21callds:ZwCreateFilePAGE:00064D21callds:ZwCreateFile	PAGE:00064CF2 loc_64CF	-2:	; CODE XREF: sub_64B98+151#j
PAGE:00064CF4leaeax, [ebp+EaBuffer]PAGE:00064CF7popecxPAGE:00064CF8movesi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$"PAGE:00064CFDpush24h; EaLengthPAGE:00064CFFpusheax; EaBufferPAGE:00064D00push68h; CreateOptionsPAGE:00064D02push1; CreateOispositionPAGE:00064D04push7; ShareAccessPAGE:00064D05push80h; FileAttributesPAGE:00064D06push80h; FileAttributesPAGE:00064D07pusheax; AllocationSizePAGE:00064D08leaeax, [ebp+ObjectAttributes]PAGE:00064D10leaeax; ObjectAttributesPAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D15push[ebp+FileHandle]; FileHandle; FileHandle==OutBuffer+0xCPAGE:00064D17leaedi, [ebp+var_50]PAGE:00064D18callds:ZwCreateFilePAGE:00064D17callds:ZwCreateFilePAGE:00064D21callds:ZwCreateFilePAGE:00064D21callds:ZwCreateFile	PAGE:00064CF2	push	5
PAGE:00064CF7popecxPAGE:00064CF8movesi, offset aRxcsccopychu_0; "\$RxCscCopyChunkOpen\$"PAGE:00064CFDpush24h; EaLengthPAGE:00064CFFpusheax; EaBufferPAGE:00064D00push68h; CreateOptionsPAGE:00064D02push1; CreateOispositionPAGE:00064D04push7; ShareAccessPAGE:00064D06push80h; FileAttributesPAGE:00064D08leaeax, [ebp+loStatusBlock]PAGE:00064D09pusheax; IoStatusBlockPAGE:00064D07pusheax; ObjectAttributes]PAGE:00064D10leaeax, [cbp+ObjectAttributes]PAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D15push[ebp+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D17leaedi, [ebp+var_50]PAGE:00064D18callds:ZwCreateFilePAGE:00064D14callds:ZwCreateFile	PAGE:00064CF4	lea	eax, [ebp+EaBuffer]
PAGE:00064CF8movesi, offset aRxcsccopychu_0; "\$RxCscCopyChunkOpen\$"PAGE:00064CFDpush24h; EaLengthPAGE:00064D00pusheax; EaBufferPAGE:00064D02push68h; CreateOptionsPAGE:00064D04push7; ShareAccessPAGE:00064D06push80h; FileAttributesPAGE:00064D07push80h; FileAttributesPAGE:00064D08leaeax, [ebp+loStatusBlock]PAGE:00064D0Fpushedx; AllocationSizePAGE:00064D0Fpusheax, [bp+ObjectAttributes]PAGE:00064D10leaeax, [cbp+ObjectAttributes]PAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D15push[ebp+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D1Cleaedi, [ebp+var_50]PAGE:00064D1Frep movsd; if(ZwCreateFile) Overwrite();	PAGE:00064CF7	рор	ecx
PAGE:00064CFDpush24h; EaLengthPAGE:00064D00pusheax; EaBufferPAGE:00064D00push68h; CreateOptionsPAGE:00064D02push1; CreateDispositionPAGE:00064D04push7; ShareAccessPAGE:00064D06push80h; FileAttributesPAGE:00064D08leaeax, [ebp+loStatusBlock]PAGE:00064D0Fpushedx; AllocationSizePAGE:00064D0Fpusheax; loStatusBlockPAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D15push[ebp+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D1Cleaedi, [ebp+var_50]PAGE:00064D1Frep movsd; if(ZwCreateFile) Overwrite();	PAGE:00064CF8	mov	esi, offset aRxcsccopychu_0 ; "\$RxCscCopyChunkOpen\$"
PAGE:00064CFFpusheax; EaBufferPAGE:00064D00push68h; CreateOptionsPAGE:00064D02push1; CreateDispositionPAGE:00064D04push7; ShareAccessPAGE:00064D06push80h; FileAttributesPAGE:00064D0Bleaeax, [ebp+loStatusBlock]PAGE:00064D0Fpushedx; AllocationSizePAGE:00064D0Fpusheax, [ebp+ObjectAttributes]PAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D15push[ebp+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D16leaedi, [ebp+var_50]PAGE:00064D17rep movsd; all ds:ZwCreateFilePAGE:00064D21call ds:ZwCreateFile; if(ZwCreateFile) Overwrite();	PAGE:00064CFD	push	24h ; EaLength
PAGE:00064D00push68h; CreateOptionsPAGE:00064D02push1; CreateDispositionPAGE:00064D04push7; ShareAccessPAGE:00064D06push80h; FileAttributesPAGE:00064D0Bleaeax, [ebp+IoStatusBlock]PAGE:00064D0Fpushedx; AllocationSizePAGE:00064D0Fpusheax; loStatusBlockPAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D15push[ebp+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D1Cleaedi, [ebp+var_50]PAGE:00064D1Frep movsdcallCallds:ZwCreateFile; if(ZwCreateFile) Overwrite();	PAGE:00064CFF	push	eax ; EaBuffer
PAGE:00064D02push 1; CreateDispositionPAGE:00064D04push 7; ShareAccessPAGE:00064D06push 80h; FileAttributesPAGE:00064D0Bleaeax, [ebp+loStatusBlock]PAGE:00064D0Fpush edx; AllocationSizePAGE:00064D0Fpush eax; loStatusBlockPAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D13push eax; ObjectAttributesPAGE:00064D14push 100080h; DesiredAccessPAGE:00064D19push [ebp+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D17leaedi, [ebp+var_50]PAGE:00064D18rep movsdCallds:ZwCreateFile; if(ZwCreateFile) Overwrite();	PAGE:00064D00	push	68h ; CreateOptions
PAGE:00064D04push7; ShareAccessPAGE:00064D06push80h; FileAttributesPAGE:00064D0Bleaeax, [ebp+loStatusBlock]PAGE:00064D0Fpushedx; AllocationSizePAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D19push[ebp+FileHandle]; FileHandle ; FileHandle==OutBuffer+0xCPAGE:00064D17leaedi, [ebp+var_50]PAGE:00064D18rep movsdcallCharles:00064D21callds:ZwCreateFileCharles:00064D21callcall	PAGE:00064D02	push	1 ; CreateDisposition
PAGE:00064D06push80h; FileAttributesPAGE:00064D0Bleaeax, [ebp+loStatusBlock]PAGE:00064D0Epushedx; AllocationSizePAGE:00064D0Fpusheax; loStatusBlockPAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D19push[ebp+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D1Cleaedi, [ebp+var_50]PAGE:00064D1Frep movsdcallCallds:ZwCreateFile; if(ZwCreateFile) Overwrite();	PAGE:00064D04	push	7 ; ShareAccess
PAGE:00064D0Bleaeax, [ebp+loStatusBlock]PAGE:00064D0Epushedx; AllocationSizePAGE:00064D0Fpusheax; loStatusBlockPAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D19push[ebp+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D1Cleaedi, [ebp+var_50]PAGE:00064D1Frep movsdcallCallds:ZwCreateFile; if(ZwCreateFile) Overwrite();	PAGE:00064D06	push	80h ; FileAttributes
PAGE:00064D0Epushedx; AllocationSizePAGE:00064D0Fpusheax; loStatusBlockPAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D19push[ebp+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D1Cleaedi, [ebp+var_50]PAGE:00064D1Frep movsdcallCallds:ZwCreateFile; if(ZwCreateFile) Overwrite();	PAGE:00064D0B	lea	eax, [ebp+loStatusBlock]
PAGE:00064D0Fpusheax; loStatusBlockPAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D19push[ebp+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D1Cleaedi, [ebp+var_50]PAGE:00064D1Frep movsdcallCallds:ZwCreateFile; if(ZwCreateFile) Overwrite();	PAGE:00064D0E	push	edx ; AllocationSize
PAGE:00064D10leaeax, [ebp+ObjectAttributes]PAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D19push[ebp+FileHandle] ; FileHandle ; FileHandle == OutBuffer+0xCPAGE:00064D1Cleaedi, [ebp+var_50]PAGE:00064D1Frep movsdPAGE:00064D21callds:ZwCreateFile; if(ZwCreateFile)Overwrite();	PAGE:00064D0F	push	eax ; loStatusBlock
PAGE:00064D13pusheax; ObjectAttributesPAGE:00064D14push100080h; DesiredAccessPAGE:00064D19push[ebp+FileHandle] ; FileHandle ; FileHandle == OutBuffer+0xCPAGE:00064D1Cleaedi, [ebp+var_50]PAGE:00064D1Frep movsdPAGE:00064D21callds:ZwCreateFile; if(ZwCreateFile)Overwrite();	PAGE:00064D10	lea	eax, [ebp+ObjectAttributes]
PAGE:00064D14push100080h; DesiredAccessPAGE:00064D19push[ebp+FileHandle] ; FileHandle ; FileHandle == OutBuffer+0xCPAGE:00064D1Cleaedi, [ebp+var_50]PAGE:00064D1Frep movsdPAGE:00064D21callds:ZwCreateFile; if(ZwCreateFile)Overwrite();	PAGE:00064D13	push	eax ; ObjectAttributes
PAGE:00064D19push [ebp+FileHandle]; FileHandle ;FileHandle==OutBuffer+0xCPAGE:00064D1Clea edi, [ebp+var_50]PAGE:00064D1Frep movsdPAGE:00064D21call ds:ZwCreateFile; if(ZwCreateFile) Overwrite();	PAGE:00064D14	push	100080h ; DesiredAccess
PAGE:00064D1Cleaedi, [ebp+var_50]PAGE:00064D1Frep movsdPAGE:00064D21call ds:ZwCreateFile; if(ZwCreateFile) Overwrite();	PAGE:00064D19	push	[ebp+FileHandle] ; FileHandle ;FileHandle==OutBuffer+0xC
PAGE:00064D1F rep movsd PAGE:00064D21 call ds:ZwCreateFile ; if(ZwCreateFile) Overwrite();	PAGE:00064D1C	lea	edi, [ebp+var_50]
PAGE:00064D21 call ds:ZwCreateFile ; if(ZwCreateFile) Overwrite();	PAGE:00064D1F	rep m	ovsd
	PAGE:00064D21	call	ds:ZwCreateFile ; if(ZwCreateFile) Overwrite();

mrxsmb.sys

Cscdll.dll is requesting to *mrxsmb.sys* a handle to a file. The mrxsmb.sys routine which handles this IOCTL, trusts on the caller. Error. Unfortunatly, the world is not perfect, there are Bush people, oops!, bad people I mean.

PAGE:00064D19 push [ebp+FileHandle] ; FileHandle ;**FileHandle==OutBuffer+0xC** ProbeForWrite had avoided headaches

Checking for max length (288h)...

0	<u> </u>			
PAGE:00060AD6	mov	eax, [eax+0F8h]	;Input Buffer Length	
PAGE:00060ADC	dec	eax	;'len-1	
PAGE:00060ADD	cmp	eax, 288h	;Max length	
PAGE:00060AE2	ја	short loc_60AEF	;Bad, Bad, Bad	

mrxsmb.sys

Nevertheless, ZwCreateFile is still returning -1 and we should generate valid handle values.

Tip ZwCreateFile returns a handle to the own caller if ObjectName is equal to NULL.

So...pretty simple:

InputBuffer filled with zeroes

+ InputBuffSize = 2

PAGE:00060ADC dec eax ; **2-1** = **1**

ObjectAttributes.ObjectName==NULL

PAGE:00064CA4 mov [ebp+ObjectAttributes.ObjectName], eax; eax==NULL mrxsmb.sys

This structure is passed to ZwCreateFile, thus it will always return a handle to the own caller so the memory address pointed by OutBuffer+0xC will be overwritten with this value.

It seems that *mrxsmb.sys* is filling a pseudo-OBJECT_ATTRIBUTES structure in user-mode, I guess that it is performed in order to speed up file operations.

SHADOW DEVICE

"What about "\\.\shadow" device?" "It's really obscure ,isn't it?" "What the f**** is this?" perhaps questions like these are in your mind at this moment.

Shadow Devices are usually implemented in order to deal with reentrancy issues during IRP_MJ_CREATE operations. It builts a "second device path" in the driver, (\Device\LanmanRedirector is the one of the main devices). This is the goal of the Shadow device in this case.

PAGE:000429DF	push offset a??Shadow ; "\\??\\Shadow"	
PAGE:000429E4	lea eax, [ebp+SymbolicLinkName]	
PAGE:000429E7	push eax ; DestinationString	
PAGE:000429E8	mov esi, ds:RtlInitUnicodeString	

PAGE:000429EE	call esi ; RtIInitUnicodeString
PAGE:000429F0	lea eax, [ebp+SymbolicLinkName]
PAGE:000429F3	push eax ; SymbolicLinkName
PAGE:000429F4	call ds:IoDeleteSymbolicLink
PAGE:000429FA	push [ebp+DeviceName] ; DeviceName
PAGE:000429FD	lea eax, [ebp+SymbolicLinkName]
PAGE:00042A00	push eax ; SymbolicLinkName
PAGE:00042A01	call ds:IoCreateSymbolicLink

mrxsmb.sys

The Shadow device is the device used by the CSC components. Every action performed by CSC has assigned this device.

GENERATING VALUES

One of the most important characteristic of this vulnerability is the chance to generate controlled values.

The value of the handle grows toward higher or lower values, this behaviour could be modeled using a simple linear equation:

y= ax +/- b where y=Desired/obtained value b=First handle obtained. x=Number of Calls needed/executed a=sizeof(HANDLE)

Calling successively DeviceIoControl in the way we have previously explained, we are generating any value, with the condition of being a multiple of sizeof(HANDLE) and limited by the max number of handles permitted by Windows.

Important

Handles are process specific

4.LAST WORDS

Unprivileged users can execute arbitrary code with kernel privileges.

5. TESTING WITH Kartoffel

Kartoffel is an Open Source (GPL) Driver Verification Tool that I have developed.

Using Kartoffel you can test this vulnerability quickly. 1.Load Kartoffel Driver- i.e > kartoffel -q c:\windows\system32\Drivers\Kartoffeldriver.sys 2.Query Device > kartoffel -s \\.\Shadow -n 0x10 -o 0x10 -z 0x2 -Z 0x18 -I 141043 -v Output – Added amazing FX ;) Input Size: [0x0002] Ouput Size: [0x0018] IOCTL:[0x00141043] -> Response received [IOM notified] [RESULTS] _____ Test ID [0x0001] ------[FUZZING] Input Buffer Size: (0x0002) Method: "" Submethod: "" Output Buffer Size: (0x0018) Method: "" Submethod: "" - IOCTL [0x00141043] => DEVICE: FILE_DEVICE_NETWORK_FILE_SYSTEM => ACCESS: ANY ACCESS => FUNCTION: 0x0410 => METHOD: METHOD_NEITHER [FLAW] - RING 0 ACCESS - // Flaw Identified [BUFFERS] Response Received [OUTPUT BUFFER] [0x000]: 00000000 00000000 000007D4 // The handle previously explained. 00000000 Original Data [OUTPUT BUFFER] 00000000 [0x000]: 00000000 0000000 0000000 Original Data [INPUT BUFFER] [0x000]: 00000000 00000000 0000000 0000000 Kartoffel is available for download at <u>www.reversemode.com</u>

6. REFERENCES

1.Microsoft Developers Network Online <http://msdn.microsoft.com> June 8, 2006

2.Sk. Windows Local Kernel Exploitation.

<http://www.xfocus.net/projects/Xcon/2004/Xcon2004_sk.pdf> June 8, 2006

3.Mrxsmb.sys Privilege Scalation Exploit Code

<http://www.reversemode.com/index.php?option=com_remository&Itemid=2&func=select&id =9> June 8, 2006

-----BEGIN PGP PUBLIC KEY BLOCK-----Version: GnuPG v1.4.2 (MingW32)

mQGiBEOLXR8RBAC+CP5OBdAnccP6H3Sy9YwPDA2AUJ6d0tTfYWQVWNLKcbF12tQp tCNqPJlR6Gx2UZMphdUlPwEZ1PwuENSmJuabuN09GZ4/cr+VVXPOHh2cHfYej/W3 JOpSVhPH539noSxAwQrojU6EpKvHcunfLT431N9qSsYSizohgMqISEs2BwCgzMJM 8tmc8I7m0kIocnNd+gH0uu0EAIxgH9oauDiWVSRJYvpdi6YKGRwV9Zuu05Cx4bts VucKhVLXatDYsUuMvrIsd3palCI90dMA0wEK8XpemMqXA91bXpyrZHwVLRcUWlrH WJCA53zgPTHRg77GT004gLkdzrmcljiq8kglJo7EM2ICGEQ4UYU1gyu6r84NeLSn dXI0A/9ZJDdIASAmoC7+uuVv+tA/9kqXwQGVJYwu137H/A3m5RWdNAVusOEhpOdR YZwYGuLojgoy9j5zUfy+tc9JtKPjUGPth7YGSQycOwr4symlKx9W4/LagJk5ZBQW C+Oq33oELl48EqjIvIHm3h2P6vUZaP2R8wVJe1bcOE6OCty/U7QoUnViZW4gU2Fu dGFtYXJ0YSA8cnViZW5AcmV2ZXJzZW1vZGUuY29tPohmBBMRAgAmBQJDi10fAhsD BQkDwmcABgsJCAcDAgQVAggDBBYCAwECHgECF4AACgkQ2pGo2fjs103RfwCZAfdi rSY+jD040scd+BKZKFScQhIAoKXKIp7DWKESjEGiXjQYPl1FBUdFuQINBEOLXUMQ CAC5M6M0uH+xk5SouFur7FXhOXOlNFGHa7ADI5CRIfiTyFdjuLb5vZTWFdevSEm/ oEVh0pEHY0uPv8B+f8bwdBljdZn/MCkfT4Y4Q4jLyKKJAYrYHJamxeCZxlCvF68/ YRucXryohGIP1YsXz0w2v4cNPALbAUV9hD5DaD933G2rJZ1POHjwkTUWF17upwT9 yfGgf0w3oL1oyQsD0hgqyqzFXtVepH4wZgt/yodDcPrZjXwPV9pGtEdTZQXn8NXC p90GfVIAeh86j8RCOuoMkejx1/5w/9bxjCmQlCLtDdcs62hX2cpdgRkMzod83egV J5pQy2orWsEb7SMRXUGn6JrHAAQNB/0fGGszanhz047AuJM/GTaXpiOlCHIOqFAz X9/Tt0mRWwF0f/fv4HrTH5TJGqXpnMTC3bizAXRmDh1NThqQ9iTXJCi7iwVOtt0x G55VYuIUEwJ0WNJ4sy/MEE1qoyqW7MgGOtHZ2vkxiJKsraBiJdK/n1oePKh06u2z 9Y213PJtB7+nlVITkehCTlJ5VNhDgQ8D44cyxaxTZD6bDqaE+NX2lcqUM1dKNm0W qkVOyjNXlYp/sFiQXYGUApYsMIbubQOI67YS5ReHAUKjPuZGswqbN+4eiwfCuyeM zxWWq4wtEGpVcH1jqZ53QQNiBYm4Xw5WHbN+nxb86xxagabBikeBiE8EGBECAA8F AkOLXUMCGwwFCQPCZwAACgkQ2pGo2fjs103M0wCfUVbtbjwRbmgAvXOGrv38alEI p6UAoILzgf6ktJwUchyuxwuEZzhMNqEL =iSHC

----END PGP PUBLIC KEY BLOCK-----

