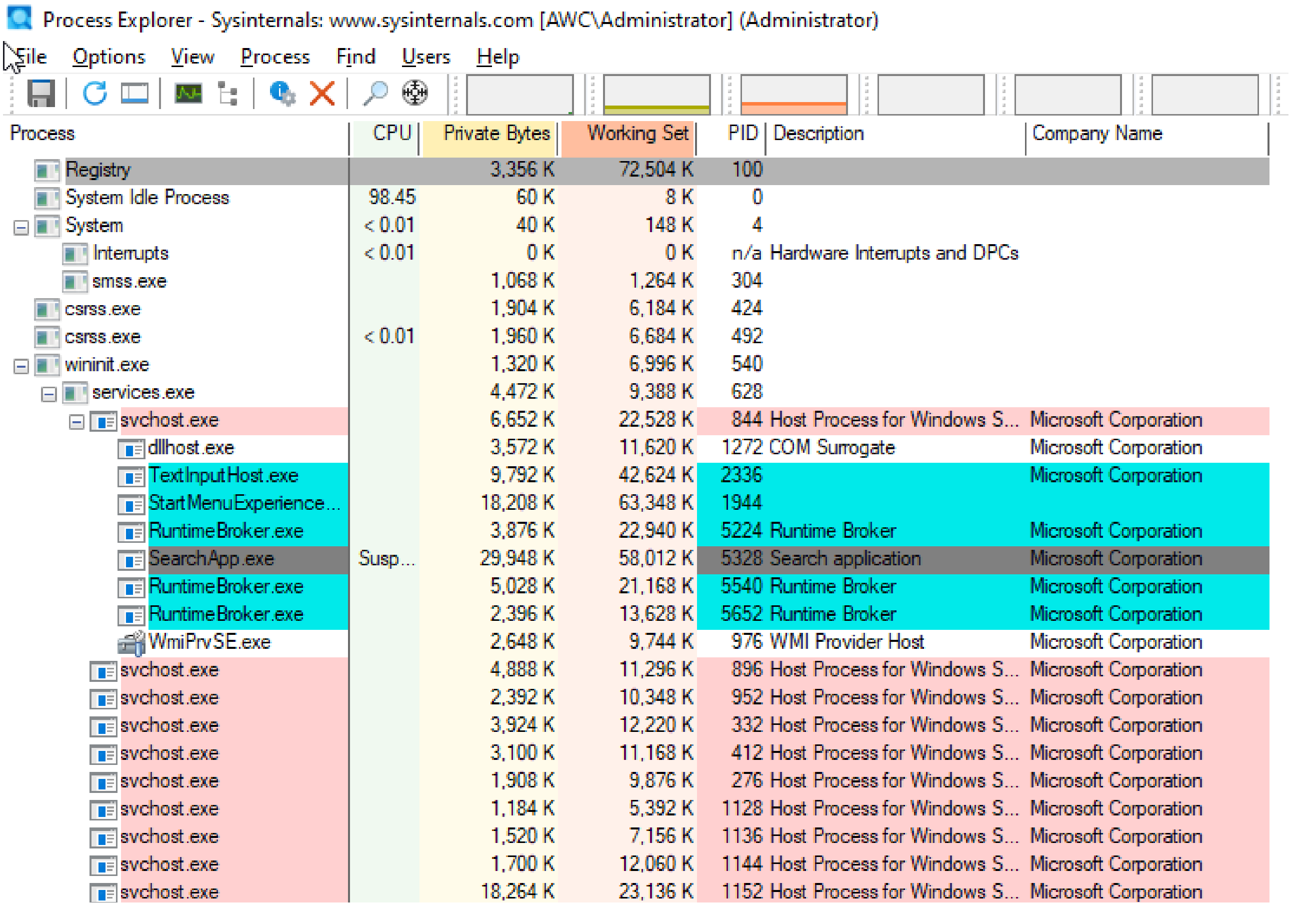
OUTPUT:

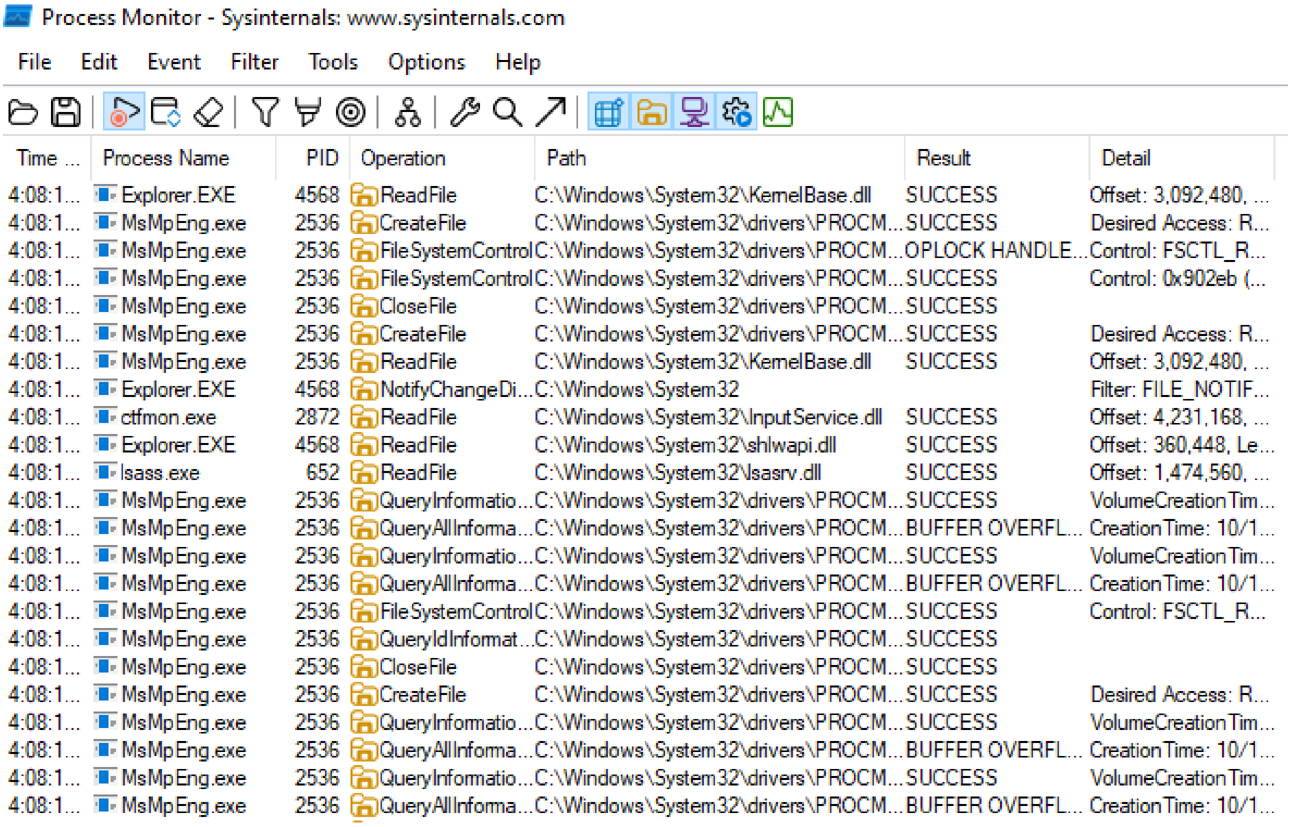
Normal:

Proc Explorer


Process Explorer - Sysinternals: www.sysinternals.com [AWC\Administrator] (Administrator)
File
Options
View
Process
Find
Users
Help

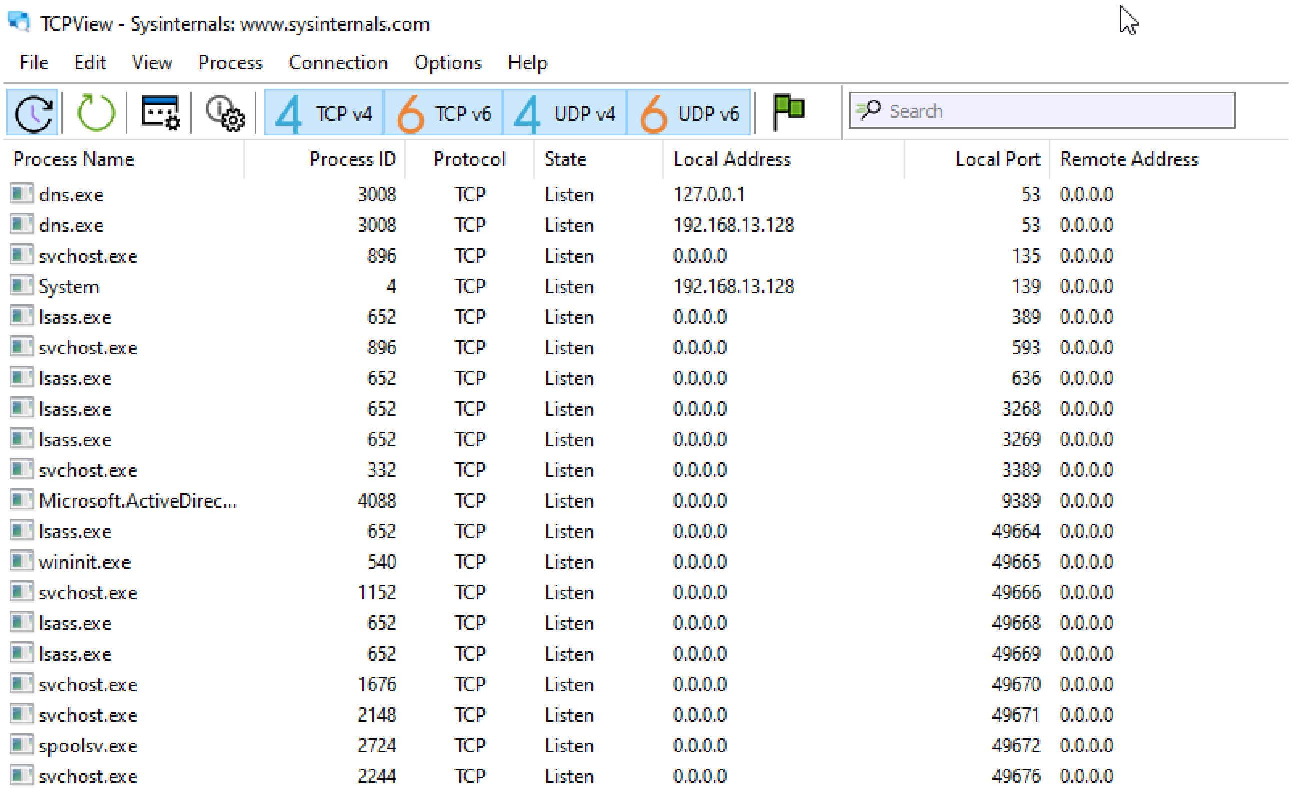
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		3,356 K	72,504 K	100		
System Idle Process	98.45	60 K	8 K	0		
System	< 0.01	40 K	148 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,068 K	1,264 K	304		
csrss.exe		1,904 K	6,184 K	424		
csrss.exe	< 0.01	1,960 K	6,684 K	492		
wininit.exe		1,320 K	6,996 K	540		
services.exe		4,472 K	9,388 K	628		
svchost.exe		6,652 K	22,528 K	844	Host Process for Windows S...	Microsoft Corporation
dllhost.exe		3,572 K	11,620 K	1272	COM Surrogate	Microsoft Corporation
TextInputHost.exe		9,792 K	42,624 K	2336		Microsoft Corporation
StartMenuExperience...		18,208 K	63,348 K	1944		
RuntimeBroker.exe		3,876 K	22,940 K	5224	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	29,948 K	58,012 K	5328	Search application	Microsoft Corporation
RuntimeBroker.exe		5,028 K	21,168 K	5540	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2,396 K	13,628 K	5652	Runtime Broker	Microsoft Corporation
WmiPrvSE.exe		2,648 K	9,744 K	976	WMI Provider Host	Microsoft Corporation
svchost.exe		4,888 K	11,296 K	896	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,392 K	10,348 K	952	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,924 K	12,220 K	332	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,100 K	11,168 K	412	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,908 K	9,876 K	276	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,184 K	5,392 K	1128	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,520 K	7,156 K	1136	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,700 K	12,060 K	1144	Host Process for Windows S...	Microsoft Corporation
svchost.exe		18,264 K	23,136 K	1152	Host Process for Windows S...	Microsoft Corporation

Proc Mon:



Time ...	Process Name	PID	Operation	Path	Result	Detail
4:08:1...	Explorer.EXE	4568	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 3,092,480, ...
4:08:1...	MsMpEng.exe	2536	CreateFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	Desired Access: R...
4:08:1...	MsMpEng.exe	2536	FileSystemControl	C:\Windows\System32\drivers\PROCM...	OPLOCK HANDLE...	Control: FSCTL_R...
4:08:1...	MsMpEng.exe	2536	FileSystemControl	C:\Windows\System32\drivers\PROCM...	SUCCESS	Control: 0x902eb (...
4:08:1...	MsMpEng.exe	2536	CloseFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	
4:08:1...	MsMpEng.exe	2536	CreateFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	Desired Access: R...
4:08:1...	MsMpEng.exe	2536	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 3,092,480, ...
4:08:1...	Explorer.EXE	4568	NotifyChangeDi...	C:\Windows\System32		Filter: FILE_NOTIF...
4:08:1...	ctfmon.exe	2872	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS	Offset: 4,231,168, ...
4:08:1...	Explorer.EXE	4568	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset: 360,448, Le...
4:08:1...	lsass.exe	652	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1,474,560, ...
4:08:1...	MsMpEng.exe	2536	QueryInformatio...	C:\Windows\System32\drivers\PROCM...	SUCCESS	VolumeCreationTim...
4:08:1...	MsMpEng.exe	2536	QueryAllInforma...	C:\Windows\System32\drivers\PROCM...	BUFFER OVERFL...	CreationTime: 10/1...
4:08:1...	MsMpEng.exe	2536	QueryInformatio...	C:\Windows\System32\drivers\PROCM...	SUCCESS	VolumeCreationTim...
4:08:1...	MsMpEng.exe	2536	QueryAllInforma...	C:\Windows\System32\drivers\PROCM...	BUFFER OVERFL...	CreationTime: 10/1...
4:08:1...	MsMpEng.exe	2536	FileSystemControl	C:\Windows\System32\drivers\PROCM...	SUCCESS	Control: FSCTL_R...
4:08:1...	MsMpEng.exe	2536	QueryIdInformat...	C:\Windows\System32\drivers\PROCM...	SUCCESS	
4:08:1...	MsMpEng.exe	2536	CloseFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	
4:08:1...	MsMpEng.exe	2536	CreateFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	Desired Access: R...
4:08:1...	MsMpEng.exe	2536	QueryInformatio...	C:\Windows\System32\drivers\PROCM...	SUCCESS	VolumeCreationTim...
4:08:1...	MsMpEng.exe	2536	QueryAllInforma...	C:\Windows\System32\drivers\PROCM...	BUFFER OVERFL...	CreationTime: 10/1...
4:08:1...	MsMpEng.exe	2536	QueryInformatio...	C:\Windows\System32\drivers\PROCM...	SUCCESS	VolumeCreationTim...
4:08:1...	MsMpEng.exe	2536	QueryAllInforma...	C:\Windows\System32\drivers\PROCM...	BUFFER OVERFL...	CreationTime: 10/1...

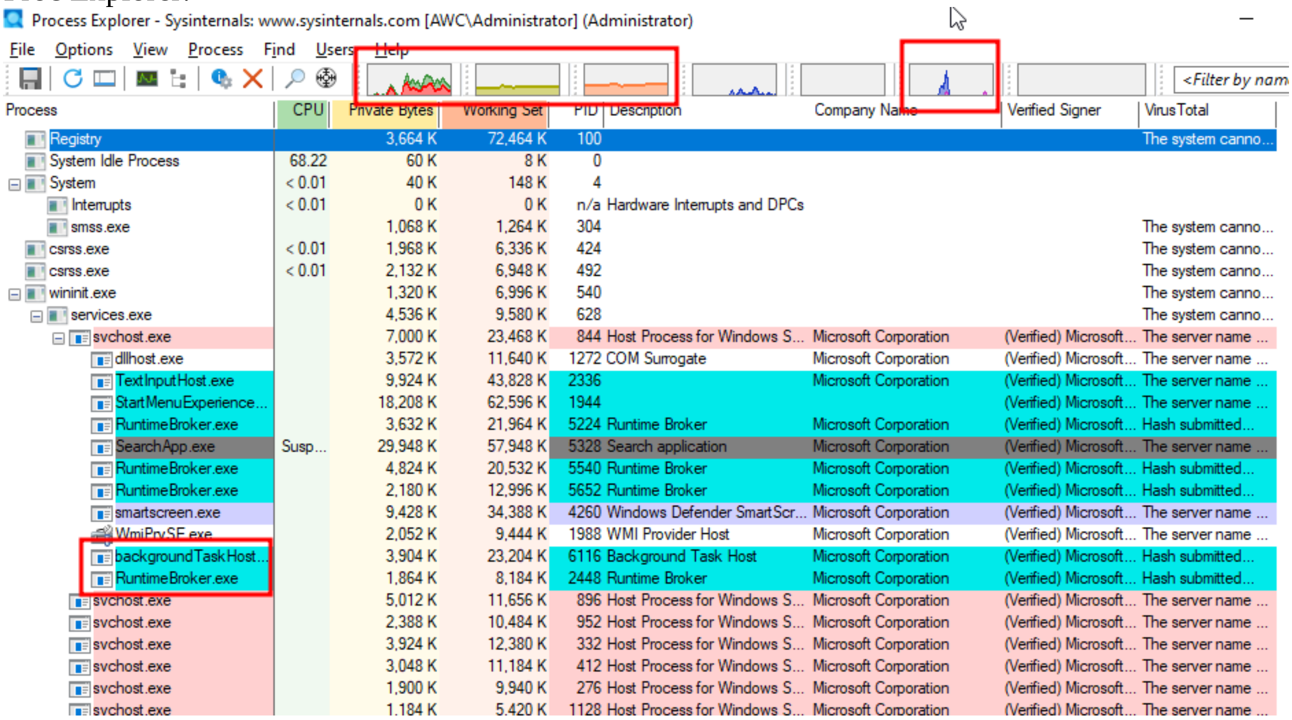
TCP View:



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address
dns.exe	3008	TCP	Listen	127.0.0.1	53	0.0.0.0
dns.exe	3008	TCP	Listen	192.168.13.128	53	0.0.0.0
svchost.exe	896	TCP	Listen	0.0.0.0	135	0.0.0.0
System	4	TCP	Listen	192.168.13.128	139	0.0.0.0
lsass.exe	652	TCP	Listen	0.0.0.0	389	0.0.0.0
svchost.exe	896	TCP	Listen	0.0.0.0	593	0.0.0.0
lsass.exe	652	TCP	Listen	0.0.0.0	636	0.0.0.0
lsass.exe	652	TCP	Listen	0.0.0.0	3268	0.0.0.0
lsass.exe	652	TCP	Listen	0.0.0.0	3269	0.0.0.0
svchost.exe	332	TCP	Listen	0.0.0.0	3389	0.0.0.0
Microsoft.ActiveDirec...	4088	TCP	Listen	0.0.0.0	9389	0.0.0.0
lsass.exe	652	TCP	Listen	0.0.0.0	49664	0.0.0.0
wininit.exe	540	TCP	Listen	0.0.0.0	49665	0.0.0.0
svchost.exe	1152	TCP	Listen	0.0.0.0	49666	0.0.0.0
lsass.exe	652	TCP	Listen	0.0.0.0	49668	0.0.0.0
lsass.exe	652	TCP	Listen	0.0.0.0	49669	0.0.0.0
svchost.exe	1676	TCP	Listen	0.0.0.0	49670	0.0.0.0
svchost.exe	2148	TCP	Listen	0.0.0.0	49671	0.0.0.0
spoolsv.exe	2724	TCP	Listen	0.0.0.0	49672	0.0.0.0
svchost.exe	2244	TCP	Listen	0.0.0.0	49676	0.0.0.0

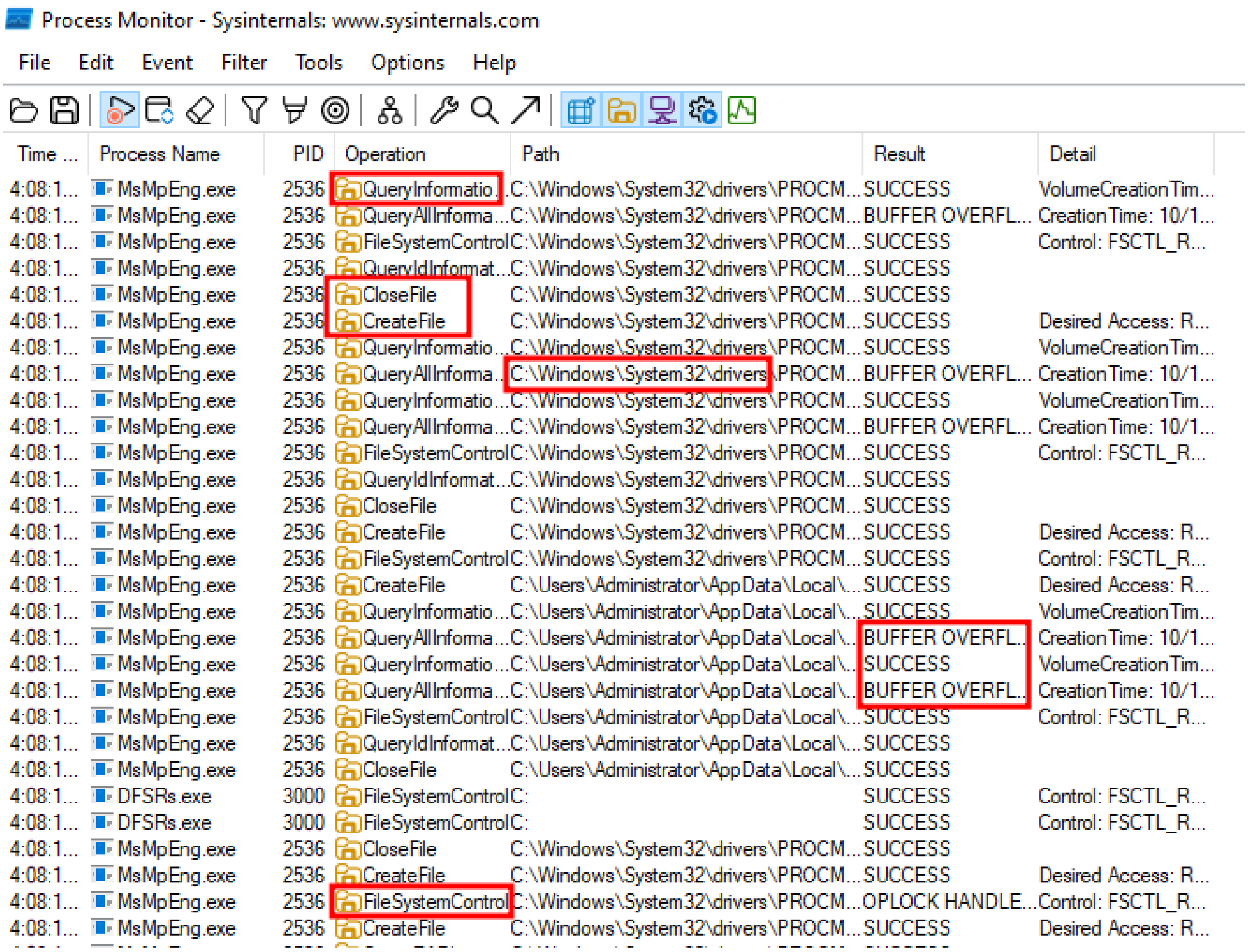
Analysis after malware run:

Proc Explorer:


Process Explorer - Sysinternals: www.sysinternals.com [AWC\Administrator] (Administrator)
File
Options
View
Process
Find
Users
Help
<Filter by nam

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
Registry		3,664 K	72,464 K	100				The system canno...
System Idle Process	68.22	60 K	8 K	0				
System	< 0.01	40 K	148 K	4				
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs			
smss.exe		1,068 K	1,264 K	304				The system canno...
csrss.exe	< 0.01	1,968 K	6,336 K	424				The system canno...
csrss.exe	< 0.01	2,132 K	6,948 K	492				The system canno...
wininit.exe		1,320 K	6,996 K	540				The system canno...
services.exe		4,536 K	9,580 K	628				The system canno...
svchost.exe		7,000 K	23,468 K	844	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	The server name ...
dllhost.exe		3,572 K	11,640 K	1272	COM Surrogate	Microsoft Corporation	(Verified) Microsoft...	The server name ...
TextInputHost.exe		9,924 K	43,828 K	2336		Microsoft Corporation	(Verified) Microsoft...	The server name ...
StartMenuExperience...		18,208 K	62,596 K	1944			(Verified) Microsoft...	The server name ...
RuntimeBroker.exe		3,632 K	21,964 K	5224	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...	Hash submitted...
SearchApp.exe	Susp...	29,948 K	57,948 K	5328	Search application	Microsoft Corporation	(Verified) Microsoft...	The server name ...
RuntimeBroker.exe		4,824 K	20,532 K	5540	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...	Hash submitted...
RuntimeBroker.exe		2,180 K	12,996 K	5652	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...	Hash submitted...
smartscreen.exe		9,428 K	34,388 K	4260	Windows Defender SmartScr...	Microsoft Corporation	(Verified) Microsoft...	The server name ...
WmiPrvSE.exe		2,052 K	9,444 K	1988	WMI Provider Host	Microsoft Corporation	(Verified) Microsoft...	The server name ...
backgroundTaskHost...		3,904 K	23,204 K	6116	Background Task Host	Microsoft Corporation	(Verified) Microsoft...	Hash submitted...
RuntimeBroker.exe		1,864 K	8,184 K	2448	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...	Hash submitted...
svchost.exe		5,012 K	11,656 K	896	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	The server name ...
svchost.exe		2,388 K	10,484 K	952	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	The server name ...
svchost.exe		3,924 K	12,380 K	332	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	The server name ...
svchost.exe		3,048 K	11,184 K	412	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	The server name ...
svchost.exe		1,900 K	9,940 K	276	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	The server name ...
svchost.exe		1,184 K	5,420 K	1128	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	The server name ...

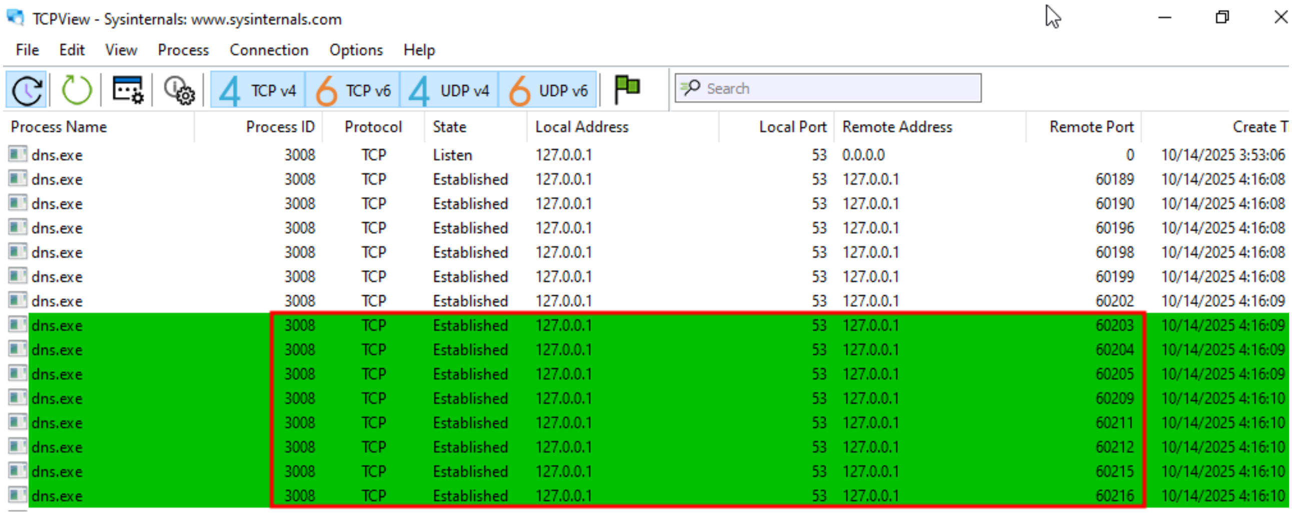
Proc Mon:



Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
4:08:1...	MsMpEng.exe	2536	QueryInformatio...	C:\Windows\System32\drivers\PROCM...	SUCCESS	VolumeCreationTim...
4:08:1...	MsMpEng.exe	2536	QueryAllInforma...	C:\Windows\System32\drivers\PROCM...	BUFFER OVERFL...	CreationTime: 10/1...
4:08:1...	MsMpEng.exe	2536	FileSystemControl	C:\Windows\System32\drivers\PROCM...	SUCCESS	Control: FSCTL_R...
4:08:1...	MsMpEng.exe	2536	QueryIdInformat...	C:\Windows\System32\drivers\PROCM...	SUCCESS	
4:08:1...	MsMpEng.exe	2536	CloseFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	
4:08:1...	MsMpEng.exe	2536	CreateFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	Desired Access: R...
4:08:1...	MsMpEng.exe	2536	QueryInformatio...	C:\Windows\System32\drivers\PROCM...	SUCCESS	VolumeCreationTim...
4:08:1...	MsMpEng.exe	2536	QueryAllInforma...	C:\Windows\System32\drivers\PROCM...	BUFFER OVERFL...	CreationTime: 10/1...
4:08:1...	MsMpEng.exe	2536	QueryInformatio...	C:\Windows\System32\drivers\PROCM...	SUCCESS	VolumeCreationTim...
4:08:1...	MsMpEng.exe	2536	QueryAllInforma...	C:\Windows\System32\drivers\PROCM...	BUFFER OVERFL...	CreationTime: 10/1...
4:08:1...	MsMpEng.exe	2536	FileSystemControl	C:\Windows\System32\drivers\PROCM...	SUCCESS	Control: FSCTL_R...
4:08:1...	MsMpEng.exe	2536	QueryIdInformat...	C:\Windows\System32\drivers\PROCM...	SUCCESS	
4:08:1...	MsMpEng.exe	2536	CloseFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	
4:08:1...	MsMpEng.exe	2536	CreateFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	Desired Access: R...
4:08:1...	MsMpEng.exe	2536	FileSystemControl	C:\Windows\System32\drivers\PROCM...	SUCCESS	Control: FSCTL_R...
4:08:1...	MsMpEng.exe	2536	CreateFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Desired Access: R...
4:08:1...	MsMpEng.exe	2536	QueryInformatio...	C:\Users\Administrator\AppData\Local\...	SUCCESS	VolumeCreationTim...
4:08:1...	MsMpEng.exe	2536	QueryAllInforma...	C:\Users\Administrator\AppData\Local\...	BUFFER OVERFL...	CreationTime: 10/1...
4:08:1...	MsMpEng.exe	2536	QueryInformatio...	C:\Users\Administrator\AppData\Local\...	SUCCESS	VolumeCreationTim...
4:08:1...	MsMpEng.exe	2536	QueryAllInforma...	C:\Users\Administrator\AppData\Local\...	BUFFER OVERFL...	CreationTime: 10/1...
4:08:1...	MsMpEng.exe	2536	FileSystemControl	C:\Users\Administrator\AppData\Local\...	SUCCESS	Control: FSCTL_R...
4:08:1...	MsMpEng.exe	2536	QueryIdInformat...	C:\Users\Administrator\AppData\Local\...	SUCCESS	
4:08:1...	MsMpEng.exe	2536	CloseFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	
4:08:1...	DFSRs.exe	3000	FileSystemControl	C:	SUCCESS	Control: FSCTL_R...
4:08:1...	DFSRs.exe	3000	FileSystemControl	C:	SUCCESS	Control: FSCTL_R...
4:08:1...	MsMpEng.exe	2536	CloseFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	
4:08:1...	MsMpEng.exe	2536	CreateFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	Desired Access: R...
4:08:1...	MsMpEng.exe	2536	FileSystemControl	C:\Windows\System32\drivers\PROCM...	OPLOCK HANDLE...	Control: FSCTL_R...
4:08:1...	MsMpEng.exe	2536	CreateFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	Desired Access: R...

TCP View:



TCPView - Sysinternals: www.sysinternals.com

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create T
dns.exe	3008	TCP	Listen	127.0.0.1	53	0.0.0.0	0	10/14/2025 3:53:06
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60189	10/14/2025 4:16:08
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60190	10/14/2025 4:16:08
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60196	10/14/2025 4:16:08
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60198	10/14/2025 4:16:08
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60199	10/14/2025 4:16:08
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60202	10/14/2025 4:16:09
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60203	10/14/2025 4:16:09
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60204	10/14/2025 4:16:09
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60205	10/14/2025 4:16:09
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60209	10/14/2025 4:16:10
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60211	10/14/2025 4:16:10
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60212	10/14/2025 4:16:10
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60215	10/14/2025 4:16:10
dns.exe	3008	TCP	Established	127.0.0.1	53	127.0.0.1	60216	10/14/2025 4:16:10