





Edit Event	Filter Tools Options Help			
9 9	# 2 @ A 🗢 CI	* x B & x B		
	PID Operation	Path	Flesut	Detail
2.exe	3564 MillegCloseKey	HKLM\SDFT\VARE\Policies\Microsoft\Windows\SafenCode/dentifers\UV lashes\(dc97\ce5-44eb-4fe4-ae2e-b0	(1490411bic) SUCCESS	
exe	3554 EFRegEnumKey	HKLM\SDFT\VARE\Policies\Microsoft\Windows\Safer\Codeldentliers\CV!\ashes	NO MORE ENTRIES	Index: 5, Length: 200
2.exe	3554 MRegCloseKey	HKLM\SDRT\VARE\Policies\Microsoft\Windows\Safer\Codeldentifiers\DV fashes	SUCCESS	
2.exe	3564 MRegDperKey	HKLM/Software/Policies/Microsoft/Windows/Saler/Codeldentifiers/O/LitZones	NAME NOT FOUND	Desired Access: Read
2.exe	3554 KRegOperKey	HKLM\Software\Policies\Microsoft\Windows\Saler\Codeldentifiers\4006\Paths	NAME NOT FOUND	Desired Access: Reed
.exe	3564 KRegDperKey	HKLM\Software\Policies\Microroft\Windows\Saler\Codeldentifiers\4006\Hashes	NAME NOT FOUND	Pesited Access: Reed
i.exe	3554 KRegOperKey	HKLM\Software\Policies\Microsoft\Windows\Saler\Codeldentifiers\4006\UriZones	NAME NOT FOUND	Desired Access: Reed
i.exe	3564 TRegDeerKey	HKLM\Software\Policies\Microsoft\Windows\Saler\Codeldentifiers\65536\Paths	NAME NOT FOUND	Pesited Access: Reed
i.exe	3564 KRegOperKey	HKLM\Software\Policies\Microsoft\Windows\Saler\Codeldenlifers\69500\lank	NAME NOT FOUND	Desired Access Read
2.exe	3564 ERegOperKey	HKLM\Softwere\Policies\Microsoft\Windows\Seler\Codeldenlifers\69536\UizCones	NAME NOT FOUND	Desired Access Read
2.exe	3564 KRegDperKey	HKLM\Software\Policies\Microsoft\Windows\Saler\Codeldenlifiers\131072\Paths	NAME NOT FOUND	Desired Access: Read
2.exe	3564 A ReaDperKey	HKLM\Software\Policies\Microsoft\Windows\Saler\Codeldentifiers\131072\Hashes	NAME NOT FOUND	Desired Access Read
2.exe	3564 RegOpenkey	HKLM/Software/Policies/Microsoft/Windows/Saler/Eodeldentifiers/13/07Z/Ut/Zones	NAME NOT FOUND	Desired Access: Read
.exe	3564 KRegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Selen\Codeldentifiers\262144\Paths	NAME NOT FOUND	Desired Access: Read
2.exe	3554 ≰ RegOperKey	HKLM\Satware\Policies\Microsoft\Windows\Seller\Codeldentifiers\262144\Hashes	NAME NOT FOUND	Desired Access: Read
2.exe	3564 KRegOperKey	HKLM\Software\Policies\Microsoft\Windows\Saler\Ecdeldenlifiers\262144\UriZones	NAME NOT FOUND	Desired Access: Read
2.exe	3554 KRegOperKey	HKEU\Software\Policies\Microsoft\Windows\Selen\Eodeldenlifiers\O\Paths	NAME NOT FOUND	Desired Access: Read
exe	3564 KRegOperKey	HKEU\Software\Policies\Microsoft\Windows\Saler\Ecdeldentiliers\0\Hashes	NAME NOT FOUND	Desired Access: Read
exe.	3564 KRegOperKey	HKCU\Satware\Palaies\Microsoft\Windows\Sater\Codeldentifiers\0\U\uZones	NAME NOT FOUND	Desired Access: Read
2.exe	3564 KRegOperKey	HKCU\Software\Policies\Microsoft\Windows\Saler\Codeldentiliers\4096\Paths	NAME NOT FOUND	Desired Access: Read
exe	3554 KRegOperKey	HKCU\Software\Policies\Microsoft\Windows\Saler\Codeldentifiers\4090\Hashes	NAME NOT FOUND	Desired Access: Read
.exe	3564 MRegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Sales\Codeldentifiers\4096\UrlZones	NAME NOT FOUND	Desired Access: Read
.exe	3554 MRegOperKey	HKCU\Software\Policies\Microsoft\Windows\Saler\Codeldentifiers\65536\Paths	NAME NOT FOUND	Desired Access: Read
2.exe	3564 KRegOperKey	HKCU\Software\Folicies\Microsoft\Windows\Saler\Codeldentifiers\65530\Hashes	NAME NOT FOUND	Desired Access: Read
2.exe	3554 KRegOperKey	HKCU\Sahware\Policies\Microsoft\\windows\Saler\Codeldenlifers\09530\UIZones	NAME NOT FOUND	Desired Access: Read
2.exe	3564 MRegOpenKey	HKCU\Software\Policies\Microsoft\\windows\Saler\Codeldentifiers\131072\Paths	NAME NOT FOUND	Desired Access: Read
2.exe	3554 RegDeerKey	HKCU\Sphware\Policies\Microsoft\Windows\Sater\Codeldentifiers\131072\Hashes	NAME NOT FOUND	Desired Access: Read
2.exe	3564 KRegDeerKey	HKCU\SatxvareVioloies\Microsoft\Windows\Sater\Codeldentifiers\131072\UiZones	NAME NOT FOUND	Desired Access: Read
2.exe	0554 KRegOperKey	HKCU\Software\Policies\Microsoft\Windows\Saler\Codeldentifiers\262144\Paths	NAME NOT FOUND	Pesited Access: Reed
i.exe	3564 KRegDperKey	HKCU\Software\Policies\Microsoft\Windows\Saler\Codeldentifiers\202144\Hashes	NAME NOT FOUND	Pesited Access: Reed
2.exe	3564 TRegOperKey	HKCU\Softwere\Policies\Microsoft\Windows\Seler\Codeldenlifiers\262144\UiZones	NAME NOT FOUND	Desired Access: Read
2.exe	3564 TReaDperKey	HKLM\Software\Policies\Microsoft\Windows\Saler\Codeldentifiers	SUCCESS	Desired Access Read
2.exe	3564 RegDuenValue	HKLM\SDFT\VARE\Policies\Microsoft\windows\SafenCodeIdentifers\DefaultLevel	SUCCESS	
c.exe c.exe	3564 ATRegDiseKey	HKLM/SDFTWARE\Policies\Microsoft/Windows\SafenCode/dentilers	SUCCESS	Type: REG_DWORD, Length: 4, Dete: 262144
				52.00 (MAC) (MAC) (MAC)
2.exe	3564 KRegOperKey	HKCU\Satware\Policies\Microsoft\Windows\Selen\Codeldentifiers	NAME NOT FOUND	Desired Access: Read
2.exe	3564 KRegOperKey	HKLM\Software\Policies\Microsoft\Windows\Seller\Ecdeldenlifiers	SUCCESS	Desired Access: Query Value
exe.	3554 KRegQuenWelue	HKLM\SDFT\WARE\Palicies\Microsoft\Windows\SalenEadeldentliers\PalicyScope	SUCCESS	Type: REG_BWORD, Length: 4, Date: 6
exe	3564 KRegCloseKey	HKLM\SDFT\WARE\Policies\Microsott\Windows\SalenEodeldentliers	SUCCESS	NEW 2017 (1977)
2.exe	3554 KRegOperKey	HKCU	SUCCESS	Desired Access: Read
2.exe	3564 KRegOperKey	HKCU\Software\Microsoft\Windows\Eument\fersion\Explorer\Shell Folders	SUCCESS	Desired Access: Read
exe.	3564 KRegCloseKey	HKCU	SUCCESS	
exe	3564 KRegQueryValue	HKCU\SoftwareVMicrosoff\Windows\Current/fersion\Explorer\Shell Folders\Cache	BUFFER OVERFLOW	Length 144
2.exe	3564 RegQueryValue	HKCU\Software\Microsoft\Windows\Current\fracerent\Explorer\Shell Folders\Cache	SUCCESS	Type: REG_SZ, Length: 160, Data: C:\Documents and Settings\Administrato\Local Settings\Temporary Internet Files
2.exe	3564 MRegCloseKey	HKCU\Software\Microsoft\Windows\Eurrent/fersion\Explorer\Shell Folders	SUCCESS	
.exe	3554 RegOperKey	HKLM\Sahware\Policies\Microsoft\Windows\Salen\Codeldentifiers	SUCCESS	Desired Access: Query Value
exe	3554 MRegQuenValue	HKLM\SDFT\VARE\Policies\Microsoft\Windows\Saler\Codeldentillers\LocFieName	NAME NOT FOUND	Lengin 536
.exe	3554 MRegCloseKey	HKLM\SDRT\VARE\Policies\Microsoft\Windows\Safer\Codeldentifiers	SUCCESS	
2.exe	3564 KRegDeerKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Distion	NAME NOT FOUND	Desired Access: Query Value, Set Value
exe	3564 KRegOperKey	HKLM\Software\Microsoft\Windows NT\Current/ferricn\Image File Execution Options\sychost exe	NAME NOT FOUND	Desired Access Read
i.exe	3564 AV Process Create	C:\VINDOWS\sustem32\syschost eve	SUCCESS	PD 3572. Commend fine "C \WINDOWS\sweem32\unchost.exe"
2.exe	3564 AT Thread Exit	W. CO. HILL S. P. S. STANISH ST. STANISH ST. STANISH ST.	SUCCESS	Thread ID 3550, User Time 0.0000003, Semel Time 0.0012500
2.exe	3564 A Process Exit		SUCCESS	Ext Status: 0. User Time: 0.0156250 seconds. Kernel Time: 0.0012500 seconds. Private Bytes: 274 422 Peak Private Bytes: 107 200. Working Set: 1,052,072, Pe
	Jose all Lincols Chi		JOCCESS	En 2007, V. V. 1100, 007, 2007, 000700, 10070, 10070, 10070, 10070, 274, 412, 1707, 277, 277, 270, 10070, 277,
	E		J.	

