19:29:28,2722073	Avira.WebAppHost.exe	27952	Thread Create		SUCCESS	Thread ID: 13440
19:29:28,3053028	phantomvpn.exe	30676	TCP Send	[redacted]:DESKTOP-[redacted]:53430 -> ec2-15-161-74-208.eu-south-1.compute.amazonaws.com:https	SUCCESS	Length: 712, startime: 18693100, endtime: 18693104, seqnum: 0, connid: 0
19:29:28,3276552	NkPtpEnum.exe	5740	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
19:29:28,3276877	NkPtpEnum.exe	5740	RegOpenKey	HKCR\CLSID\{9609f541-f089-42c7-8b8f-49bf409acce7}\EnumList	SUCCESS	Desired Access: Query Value
19:29:28,3277306	NkPtpEnum.exe	5740	RegQueryValue	HKCR\CLSID\{9609f541-f089-42c7-8b8f-49bf409acce7}\EnumList\STATE	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
19:29:28,3277490	NkPtpEnum.exe	5740	RegQueryValue	HKCR\CLSID\{9609f541-f089-42c7-8b8f-49bf409acce7}\EnumList\GUID	NAME NOT FOUND	Length: 92
19:29:28,3277648	NkPtpEnum.exe	5740	RegCloseKey	HKCR\CLSID\{9609f541-f089-42c7-8b8f-49bf409acce7}\EnumList	SUCCESS	
19:29:28,3427639	phantomvpn.exe	30676	TCP TCPCopy	[redacted]:53430 -> ec2-15-161-74-208.eu-south-1.compute.amazonaws.com:https	SUCCESS	Length: 898, seqnum: 0, connid: 0
19:29:28,3431073	phantomvpn.exe	30676	TCP Receive	[redacted]:53430 -> ec2-15-161-74-208.eu-south-1.compute.amazonaws.com:https	SUCCESS	Length: 898, seqnum: 0, connid: 0
19:29:28,3433079	powershell.exe	24436	TCP Send	[redacted]:53493 -> 188.114.96.7:https	SUCCESS	Length: 646, startime: 18693100, endtime: 18693108, seqnum: 0, connid: 0
19:29:28,3433167	powershell.exe	24436	TCP TCPCopy	[redacted]:53493 -> 188.114.96.7:https	SUCCESS	Length: 832, seqnum: 0, connid: 0
19:29:28,3435045	powershell.exe	24436	TCP Receive	[redacted]:53493 -> 188.114.96.7:https	SUCCESS	Length: 5, seqnum: 0, connid: 0
19:29:28,3435096	powershell.exe	24436	TCP Receive	[redacted]:53493 -> 188.114.96.7:https	SUCCESS	Length: 827, seqnum: 0, connid: 0
19:29:28,3439483	Adobe Desktop Service.exe	5664	CreateFile	C:\Program Files (x86)\Common Files\Adobe\Adobe Desktop Common\IPCBox\AdobeIPCBroker.exe	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Wri...