BÁO CÁO

Phân tích, xác định Nguyên nhân sự cố An toàn thông tin

THEO CASE

CASE: Case0001

I Thông tin về case

1.1. Thông tin chung

a. Thông tin máy tính

	Properties
Computer	DESKTOP-4ER81B7
NumberSession	1
Sum	513386
SumAlert	135
Collector	Admin
Status	Success

b. Thông tin các lần thu thập

	Computer	Session	Sum	SumAlert	Collector	Status
Properties	DESKTOP-4ER81B7	2021-02-22 T10:57:16	513386	135	Admin	Success

1.2. Thông tin dữ liệu thu thập

	Computer	Session	Network	System	Log	Malware	Collector	Status
1	DESKTOP-4ER81B7	2021-02-22 T10:57:16	1401	486638	25346	1	Admin	Success

1.3. Thông tin dữ liệu cảnh báo

Computer: DESKTOP-4ER81B7

	Session	Type	Critical	High	Medium	Info	Collector	Status
1	2021-02-22 T10:57:16	Network	0	2	95	0	Admin	Success
2	2021-02-22 T10:57:16	System	0	0	0	0	Admin	Success
3	2021-02-22 T10:57:16	Logevent	0	0	37	0	Admin	Success
4	2021-02-22 T10:57:16	Malware	1	0	0	0	Admin	Success

II Phân tích, xác định nguyên nhân sự cố ATTT

2.1. Phân tích, xác định nguyên nhân sự cố ATTT qua dữ liệu truyền thông

	Properties
Risk	High
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kill tiến trình Lý do: mã độc VistaDrive.exe Nguồn: https://www.pcmatic.com/company/libraries/process/detail.asp?fn=VistaDrive.exe.html
Type	CurrentProcess
Summary	@uid: af68bf28a2cab2e30be750ea331627a6 name: csrss.exe arguments: %SystemRoot%\\\\system32\\\\csrss.exe ObjectDirectory=\\\\Windows SharedSection=102420480768 Windows=On SubSystemType=Windows ServerDll=basesrv1 ServerDll=winsrv:UserServerDllInitialization3 ServerDll=sxssrv4 ProfileControl=Off MaxRequestThreads=16 pid: 108 parentpid: 1008 path: C:\\Windows\\System32\\csrss.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:33 userTime: 3.984375 systemTime: 615.53125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	High
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16

	Properties
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kill tiến trình Lý do: mã độc VistaDrive.exe Nguồn: https://www.pcmatic.com/company/libraries/process/detail.asp?fn=VistaDrive.exe.html
Type	CurrentProcess
Summary	@uid: cf62dc088828f25a5c9062f821175465 name: csrss.exe arguments: %SystemRoot%\\\\system32\\\\csrss.exe ObjectDirectory=\\\\Windows SharedSection=102420480768 Windows=On SubSystemType=Windows ServerDll=basesrv1 ServerDll=winsrv:UserServerDllInitialization3 ServerDll=sxssrv4 ProfileControl=Off MaxRequestThreads=16 pid: 924 parentpid: 696 path: C:\\Windows\\System32\\csrss.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:32 userTime: 1.390625 systemTime: 4.765625 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: f2fdb0d4c6aa35157cc07866e60aaed1 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s UserManager pid: 916 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 8.0625 systemTime: 10.890625 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 44299a4613bf69fab66727b69124d490 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s DisplayEnhancementService pid: 1056 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.140625 systemTime: 0.15625 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 562e8490e0d376535645e416289d8b87 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k DcomLaunch -p -s PlugPlay pid: 1160 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:34 userTime: 0.015625 systemTime: 0.0 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 236f5356cc59a49bf84219acff275b47 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k DcomLaunch -p pid: 1184 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:34 userTime: 412.015625 systemTime: 257.203125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 91d7af5109c5bc2aa003b6eb2b78cb67 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k RPCSS -p pid: 1304 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\NETWORK SERVICE startTime: 2021-02-18T02:03:34 userTime: 174.359375 systemTime: 99.859375 SecurityID: S-1-5-20 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 434686c184f6c735a59425ffae8d0f51 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k DcomLaunch -p -s LSM pid: 1352 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:34 userTime: 5.921875 systemTime: 9.5625 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình winlogon.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: tiến trình winlogon.exe có thể bị giả mạo bởi mã độc trojan Nguồn: https://vi.stealthsettings.com/winlogon-exe-microsoft-windows-logon-process-vs-trojanvirus.html
Type	CurrentProcess

	Properties
Summary	@uid: a586e327b07e2fb1ec4db2feaa5dbcc1 name: winlogon.exe arguments: winlogon.exe pid: 1616 parentpid: 1008 path: C:\\Windows\\System32\\winlogon.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.625 systemTime: 7.75 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: f1ea86491b0ef5483b163e07aafcf63b name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s HvHost pid: 1836 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.0 systemTime: 0.015625 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium

	Properties
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 48f9c9ad2f66be39428157893cbe05b6 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s ProfSvc pid: 1912 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.109375 systemTime: 0.4375 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: b4ff0baf884d3cbda303d75b138e9294 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService pid: 1920 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 1.046875 systemTime: 0.96875 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: d8ddea1c4716d4f4df1bed211573213d name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s Schedule pid: 1928 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 14.828125 systemTime: 24.890625 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 13b309989ec23b6032d5f33f9e738fd1 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc pid: 1936 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 0.6875 systemTime: 0.609375 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 5d18b74263be332ecf711f90b9134ee0 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s StorSvc pid: 1996 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:05:39 userTime: 14.484375 systemTime: 29.703125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 8029f577fac0ca2f4c4b74623d0ad9ac name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s hidserv pid: 2056 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.03125 systemTime: 0.125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: f04285f7f451e8267c3a855770952c81 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog pid: 2136 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 10.59375 systemTime: 5.359375 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: cc4f4b5708052da027ae957ef141644 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalServiceNoNetwork -p pid: 2204 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 1.5625 systemTime: 1.0625 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: f4d0a6a43d43958fb5d0eed5436edc33 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalService -p -s nsi pid: 2360 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 3.859375 systemTime: 2.234375 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: fb0e546e6a0781fcf4769108a5da5525 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp pid: 2472 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 98.3125 systemTime: 54.453125 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 2a9c707879c0aad89c187253d1a3b3d6 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc pid: 2744 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 0.015625 systemTime: 0.0625 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: ad98a158c4e2f5e11978ae48f10e79fa name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k NetworkService -p -s NlaSvc pid: 2772 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\NETWORK SERVICE startTime: 2021-02-18T02:03:37 userTime: 8.390625 systemTime: 12.84375 SecurityID: S-1-5-20 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 5b3d8d7bdf59a7940e4ac7308d729c36 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalService -p -s netprofm pid: 2960 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 11.703125 systemTime: 16.734375 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 358c2253e541223e6520b47ac59d6e0a name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain pid: 3004 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 26.453125 systemTime: 1159.984375 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 1015c3ef2089c514bbe75784b1d59b95 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k netsvcs -p -s Themes pid: 3012 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.328125 systemTime: 0.8125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 7f5c10a43dec337b0dca9b41e8ae32c7 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalService -p -s EventSystem pid: 3020 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 0.921875 systemTime: 0.90625 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 84b184b6236b9021363204d171019e5c name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k appmodel -p -s StateRepository pid: 3028 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 337.078125 systemTime: 56.734375 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 24a3d1951d593bd43c9b70b1a2415122 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s SENS pid: 3124 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 1.703125 systemTime: 1.8125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 3e245ef9f18b4951a9de1c20c94f76fd name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder pid: 3204 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 1.109375 systemTime: 3.109375 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: f8ce20464fb925713674be29c581361e name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalService -p -s FontCache pid: 3220 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 3.359375 systemTime: 1.75 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 4fe6c1b38576e7c5bc56d5d48cc7ac01 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalServiceNetworkRestricted -p -s WinHttpAutoProxySvc pid: 3228 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 3.765625 systemTime: 11.609375 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: e7a8109ac846dcb12506e210f9c864e5 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k NetSvcs -p -s hns pid: 3284 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 2.03125 systemTime: 3.5 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 1df1a27ffdb2f2bfbc1daec41ca31b5f name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k NetworkService -p -s Dnscache pid: 3360 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\NETWORK SERVICE startTime: 2021-02-18T02:03:37 userTime: 77.921875 systemTime: 273.125 SecurityID: S-1-5-20 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: b84c04375a820312bbc8535e2a3f97d1 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k NetSvcs -s nvagent pid: 3452 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.109375 systemTime: 0.078125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 87c879cafb65917208afe6e2cdb3df49 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalServiceNoNetworkFirewall -p pid: 3532 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 19.34375 systemTime: 20.375 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 94204ffc9d240408615667d3148be18b name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalServiceAndNoImpersonation -p -s wcncsvc pid: 3568 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:06:06 userTime: 1.765625 systemTime: 1.015625 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 4f72c0f078eb145f0e38fed58aad81bf name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalServiceNetworkRestricted -p pid: 3600 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 115.03125 systemTime: 78.359375 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:48
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 2bcb3100c70ee7d933990b3126c25a9c name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k netsvcs -p -s SharedAccess pid: 3624 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.84375 systemTime: 3.484375 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: e7cd2d7a7233e6cb0ae272c136e7d39 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalServiceNetworkRestricted -p pid: 3708 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 6.734375 systemTime: 9.203125 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 84defddcd52b76846abc0597e71dfbd name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalServiceNetworkRestricted -p pid: 3716 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 0.734375 systemTime: 3.25 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 7f457977a47eb88b48e0b253892050db name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalSystemNetworkRestricted -p pid: 3940 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 27.859375 systemTime: 35.921875 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: b8b4d476d6a50bc286f3a7a4062cbdc9 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k netsvcs -p -s ShellHWDetection pid: 4024 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.28125 systemTime: 0.421875 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: d99b2e4a583c54afde258c6593b57ec6 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k WbioSvcGroup -s WbioSrvc pid: 4104 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.5 systemTime: 0.703125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 6ee63b0692e0ea732adef9dd08e5d475 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k NetworkService -p -s LanmanWorkstation pid: 4216 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\NETWORK SERVICE startTime: 2021-02-18T02:03:37 userTime: 0.265625 systemTime: 0.640625 SecurityID: S-1-5-20 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 694cc8ac57bf4ada4a09d6c211d33882 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k NetworkService -p -s CryptSvc pid: 4460 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\NETWORK SERVICE startTime: 2021-02-18T02:03:37 userTime: 4.875 systemTime: 7.640625 SecurityID: S-1-5-20 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 2c5aa3d12ce1d65808df15f95d2a8ea6 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k utcsvc -p pid: 4472 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 16.015625 systemTime: 10.28125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: ae56c35dd045bf9c5db3e6b9c4aebba3 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s DeviceAssociationService pid: 4532 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.171875 systemTime: 0.546875 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: a3e806b24b33b919a087bb010fc71d57 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalService -p -s SstpSvc pid: 4556 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 0.0 systemTime: 0.046875 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: fa6f6a2a94ac82db742f098ea0c9962f name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s Winmgmt pid: 4588 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 16.03125 systemTime: 6.609375 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 40eb130f06018ed32985581097e48edc name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalServiceNoNetwork -p -s DPS pid: 4596 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 348.09375 systemTime: 506.0 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: e9b059521480e3f48204dba83d71008 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s WpnService pid: 4692 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 1.296875 systemTime: 1.453125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: e79b150c53c4dff5135f63fa23c3f7d4 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k imgsvc pid: 4708 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:37 userTime: 0.421875 systemTime: 2.09375 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: f2766afd833f18463097be96a100a33a name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s TrkWks pid: 4780 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.03125 systemTime: 0.0625 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 458bd5c4fe5102606e1b3add5c748670 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s gpsvc pid: 4796 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-22T10:56:35 userTime: 0.0 systemTime: 0.03125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: c08e7158db7d8609b52b04ac946cf8ed name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalService -p -s BthAvctpSvc pid: 4828 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:04:09 userTime: 0.1875 systemTime: 0.09375 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: ffbe74579550805b51b01ce07f7aa3c4 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s LanmanServer pid: 5060 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:37 userTime: 0.796875 systemTime: 0.6875 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: fe95d491e263caebbc4a1c03dce2a006 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s wuauserv pid: 5136 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:04:09 userTime: 104.546875 systemTime: 42.0625 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: bf172adc43252f82666db9d938416727 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k NetworkService -p -s TapiSrv pid: 5156 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\NETWORK SERVICE startTime: 2021-02-18T02:03:38 userTime: 0.015625 systemTime: 0.046875 SecurityID: S-1-5-20 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: b5ca9ae330cd60f44beeb6fdc1813066 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k NetSvcs -p -s iphlpsvc pid: 5216 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:38 userTime: 1.21875 systemTime: 0.8125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 1f39ea8fe5c86e4d74a263558b360e33 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalService -p -s WdiServiceHost pid: 5880 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:38 userTime: 0.03125 systemTime: 0.1875 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 153f33d655591ced2c4d3d93f093d3aa name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k netsvcs pid: 5988 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:38 userTime: 0.1875 systemTime: 0.265625 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 83c82117ea71a4394ea13b356007fe6f name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k UnistackSvcGroup -s CDPUserSvc pid: 6360 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: DESKTOP-4ER81B7\\DangPH startTime: 2021-02-18T02:03:38 userTime: 98.453125 systemTime: 65.984375 SecurityID: S-1-5-21-28845077-1834584736-464141660-1001 SecurityType: SidTypeUser
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 75d5e174beb6908beca74d463e1c23e9 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k UnistackSvcGroup -s WpnUserService pid: 6880 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: DESKTOP-4ER81B7\\DangPH startTime: 2021-02-18T02:03:38 userTime: 19.921875 systemTime: 6.59375 SecurityID: S-1-5-21-28845077-1834584736-464141660-1001 SecurityType: SidTypeUser
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: acbded7bdf86b300ac1f3753d22620e6 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s TokenBroker pid: 6972 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:38 userTime: 16.703125 systemTime: 7.046875 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: d86354ec42723ec1b802133f70883826 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s TabletInputService pid: 7308 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:38 userTime: 0.046875 systemTime: 0.078125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: a8006bcc0aac4d0de24afddb4bf0829c name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalService -p -s CDPSvc pid: 7744 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:38 userTime: 0.8125 systemTime: 0.625 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 40b473cabb4cf8e362c32d7e165398a5 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k NetworkServiceNetworkRestricted -p -s PolicyAgent pid: 7944 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\NETWORK SERVICE startTime: 2021-02-18T02:03:38 userTime: 1.234375 systemTime: 4.515625 SecurityID: S-1-5-20 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: be4dcdcc6cebef54accf8c4b9aca950b name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalServiceNetworkRestricted -s RmSvc pid: 8232 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:39 userTime: 0.921875 systemTime: 0.453125 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 1186e031988615c05ddc64bde523f1b2 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc pid: 8336 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:44 userTime: 0.984375 systemTime: 1.578125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 2f775f34facef35af47eb36d43773bc7 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s NgcSvc pid: 8516 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:39 userTime: 0.296875 systemTime: 0.296875 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:49
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 4fa6a41189885fb855439d582f307387 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc pid: 8772 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: DESKTOP-4ER81B7\\DangPH startTime: 2021-02-18T02:03:39 userTime: 5.40625 systemTime: 4.828125 SecurityID: S-1-5-21-28845077-1834584736-464141660-1001 SecurityType: SidTypeUser
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 3205141e0f11e996ed96f63d8e9db69d name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k appmodel -p -s camsvc pid: 8880 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:47:25 userTime: 3.75 systemTime: 3.625 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 687ff29d86c4b0e836a8b7d8df0e2121 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalServiceNetworkRestricted -p -s NgcCtnrSvc pid: 9040 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:39 userTime: 4.609375 systemTime: 3.625 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: d9ca0a9e300eaea7a83eaa6e3608d68 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -s CertPropSvc pid: 9200 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:39 userTime: 2.140625 systemTime: 3.96875 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 2be68879fa22603209adb878c9df14cf name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalServiceAndNoImpersonation -s SCardSvr pid: 9208 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:39 userTime: 1.890625 systemTime: 1.03125 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 3ab4f4c80c4a33946780f90c9597c20c name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k netsvcs -p pid: 11300 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:08:09 userTime: 0.96875 systemTime: 0.796875 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 707f1551b13c4ac196ddacbe3bf25879 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalServiceAndNoImpersonation -p -s QWAVE pid: 11484 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-19T06:52:02 userTime: 0.46875 systemTime: 2.4375 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: bfbe34582050daf020145e799faebcf2 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalService -p -s fdPHost pid: 12204 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T16:29:06 userTime: 1.546875 systemTime: 2.59375 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 66b69b0208063775f43a71b82578e2fc name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s Appinfo pid: 12208 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:43 userTime: 3.828125 systemTime: 15.28125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 5f441793fa3dfec8561f55882c09e988 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s WdiSystemHost pid: 12608 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:52 userTime: 0.359375 systemTime: 0.28125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 61449ecd0cc5532f837b33d08d89143b name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s DsSvc pid: 12636 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T10:00:31 userTime: 1.5625 systemTime: 0.59375 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 4aad02440bedafafe10e2e7bb704faf name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalService -p -s LicenseManager pid: 13260 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:04:07 userTime: 2.03125 systemTime: 1.28125 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 855d22dafa09f398b16286e269bec93a name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalServiceAndNoImpersonation -p -s FDResPub pid: 13568 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:03:53 userTime: 1.34375 systemTime: 3.421875 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: aaf2c3cf99c01647ec1cfe803970e1ff name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalService -s W32Time pid: 13840 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:49:46 userTime: 4.21875 systemTime: 3.03125 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: df6d1c8ada76433950c6bf9df42c293e name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s UsoSvc pid: 14288 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:04:24 userTime: 2.421875 systemTime: 2.859375 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: d72925eba34090141f56c6345c729aa0 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s lfsvc pid: 14600 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T02:03:55 userTime: 1.703125 systemTime: 1.5 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 6fcebdeb134c844eb8be94e9ee5669a3 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k NetworkService -p -s DoSvc pid: 15316 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\NETWORK SERVICE startTime: 2021-02-18T02:05:39 userTime: 16.0625 systemTime: 30.375 SecurityID: S-1-5-20 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 1c9deaa8569ae9d3bc53ea4e4aee8618 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k AarSvcGroup -p -s AarSvc pid: 15676 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: DESKTOP-4ER81B7\\DangPH startTime: 2021-02-18T02:04:09 userTime: 3.546875 systemTime: 2.515625 SecurityID: S-1-5-21-28845077-1834584736-464141660-1001 SecurityType: SidTypeUser
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: be3a0421be5cda61670e9c73ddb293fe name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s seclogon pid: 16768 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-18T14:47:56 userTime: 0.03125 systemTime: 0.03125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: f0b774745285772fb7220d830f0d9416 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k UnistackSvcGroup pid: 17384 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: DESKTOP-4ER81B7\\DangPH startTime: 2021-02-18T02:05:38 userTime: 1.0625 systemTime: 0.6875 SecurityID: S-1-5-21-28845077-1834584736-464141660-1001 SecurityType: SidTypeUser
CreationTime	2021-02-22T11:09:50
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 18f43d1d5b09e869efa006e4275d7ef7 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k LocalService -p -s CaptureService pid: 17744 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: DESKTOP-4ER81B7\\DangPH startTime: 2021-02-18T09:58:53 userTime: 0.375 systemTime: 0.203125 SecurityID: S-1-5-21-28845077-1834584736-464141660-1001 SecurityType: SidTypeUser
CreationTime	2021-02-22T11:09:51
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 6e176041942e2d3784b4409955565f9a name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalServiceNetworkRestricted -p -s wscsvc pid: 17884 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-18T02:05:42 userTime: 0.375 systemTime: 0.53125 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:51
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 5a5a3b35842d3f326d89721077d29018 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k wsappx -p -s ClipSVC pid: 20180 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-22T11:06:24 userTime: 0.03125 systemTime: 0.015625 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:52
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: d04097a367e4c221ca0e194e4823d7e4 name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s LxssManager pid: 20324 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-21T21:02:46 userTime: 0.15625 systemTime: 0.109375 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:52
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 6b2cd222033cfc48e857aff5518b5d60 name: svchost.exe arguments: C:\\\\WINDOWS\\\\System32\\\\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts pid: 21004 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\LOCAL SERVICE startTime: 2021-02-22T07:28:18 userTime: 0.015625 systemTime: 0.0 SecurityID: S-1-5-19 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:52
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess

	Properties
Summary	@uid: 3df1f623f08201d37e9dbe171bcc12eb name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k netsvcs -p -s AppMgmt pid: 22376 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-22T11:05:38 userTime: 0.015625 systemTime: 0.015625 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:52
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Quét tiêu diệt mã độc, kiểm tra lượng tài nguyên tiến trình svchost.exe sử dụng, nếu sử dụng một lượng lớn rất có thể đó là mã độc trojan. Lý do: một số loại trojan giả dạng tiến trình svchost.exe Nguồn: https://quantrimang.com/gioi-thieu-ve-svchost-exe-54957
Type	CurrentProcess
Summary	@uid: 4ebc1ac2695c3c1e6168c2166bb34d4c name: svchost.exe arguments: C:\\\\WINDOWS\\\\system32\\\\svchost.exe -k wsappx -p -s AppXSvc pid: 24708 parentpid: 700 path: C:\\Windows\\System32\\svchost.exe Username: NT AUTHORITY\\SYSTEM startTime: 2021-02-22T11:05:52 userTime: 0.015625 systemTime: 0.078125 SecurityID: S-1-5-18 SecurityType: SidTypeWellKnownGroup
CreationTime	2021-02-22T11:09:52
Handler	admin
Status	Success

2.2. Phân tích, xác định nguyên nhân sự cố ATTT qua dữ liệu hệ thống

2.3. phân tích, xác định nguyên nhân sự cố ATTT qua dữ liệu vết

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: be2ff71127ea3b6c183bc81f34c4ac0d log: Application source: EventSystem index: 10744 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-10-23T00:59:23 writeTime: 2020-10-23T00:59:23 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:20
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16

	Properties
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 5e211fb9d6b841fb9f9a6118099a2ab log: Application source: EventSystem index: 8477 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-10-03T13:16:53 writeTime: 2020-10-03T13:16:53 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:21
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx

	Properties
Summary	@uid: 819616ff40134e8428687915b778f8 log: Application source: EventSystem index: 8101 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-10-02T08:13:05 writeTime: 2020-10-02T08:13:05 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:22
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: d62d37935a0984a50f05a971fb0ecda6 log: Application source: EventSystem index: 7918 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-30T12:10:52 writeTime: 2020-09-30T12:10:52 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:22

	Properties
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: f8d86d373ee2c72c0d7ec8d9013de783 log: Application source: EventSystem index: 7753 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-28T01:34:34 writeTime: 2020-09-28T01:34:34 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:22
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625

	Properties
Type	Logevtx
Summary	@uid: ee79acdd35cbd4e47f263920c1fe68c1 log: Application source: EventSystem index: 6623 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-15T10:47:36 writeTime: 2020-09-15T10:47:36 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:22
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 1d12a8d092697d77155241b4f103b543 log: Application source: EventSystem index: 6500 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-14T21:59:10 writeTime: 2020-09-14T21:59:10 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0

	Properties
CreationTime	2021-02-22T11:10:22
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: b03016ddbac6986b1ba034bfc66469bf log: Application source: EventSystem index: 6425 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-14T21:54:06 writeTime: 2020-09-14T21:54:06 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:22
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16

	Properties
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 1a571fc891ae8b2ec0d35bd3ab25a39c log: Application source: EventSystem index: 2007 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-08-18T17:40:20 writeTime: 2020-08-18T17:40:20 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:26
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx

	Properties
Summary	@uid: 82a6559258b57eade85b9a7b6f49d265 log: Application source: EventSystem index: 1882 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-08-18T10:17:30 writeTime: 2020-08-18T10:17:30 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:26
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: ab2f6746a5c499c6aea36a6b3e76a6c3 log: Application source: EventSystem index: 1719 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-08-18T09:57:40 writeTime: 2020-08-18T09:57:40 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:26

	Properties
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: f74f003ff8a81cb322106f5b37b725f2 log: Application source: EventSystem index: 1577 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-07-25T13:53:15 writeTime: 2020-07-25T13:53:15 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:26
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625

	Properties
Type	Logevtx
Summary	@uid: 190190b92e7fd8c21555f6e17aa02e12 log: Application source: EventSystem index: 25332 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2021-02-18T02:03:37 writeTime: 2021-02-18T02:03:37 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:12
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 6db0e2f5ed5df6f5f844ce79603ea76b log: Application source: EventSystem index: 21292 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2021-01-16T01:02:17 writeTime: 2021-01-16T01:02:17 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0

	Properties
CreationTime	2021-02-22T11:10:14
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 1816562e934287e99eeeb82835192cde log: Application source: EventSystem index: 15949 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-12-07T09:15:42 writeTime: 2020-12-07T09:15:42 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:17
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16

	Properties
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 5cbf8e85b015ef6310bf557d2859ef8b log: Application source: EventSystem index: 15356 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-12-04T11:36:41 writeTime: 2020-12-04T11:36:41 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:17
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx

	Properties
Summary	@uid: fc6dbf558d5e07d805dde10344898174 log: Application source: EventSystem index: 5729 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-14T21:50:49 writeTime: 2020-09-14T21:50:49 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:23
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 49d63bc9e4b04964bf39adf2cbe4e680 log: Application source: EventSystem index: 5640 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-14T21:45:04 writeTime: 2020-09-14T21:45:04 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:23

	Properties
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 5e46a4e09a7fb51f8772797b6665c7dc log: Application source: EventSystem index: 5569 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-14T21:37:34 writeTime: 2020-09-14T21:37:34 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:23
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625

	Properties
Type	Logevtx
Summary	@uid: 47dd0fd7635b07f1802f12ba9ff307c9 log: Application source: EventSystem index: 5488 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-14T21:34:32 writeTime: 2020-09-14T21:34:32 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:23
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: b3eac6ae07755ac49e5b38241629d420 log: Application source: EventSystem index: 5379 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-14T08:53:54 writeTime: 2020-09-14T08:53:54 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0

	Properties
CreationTime	2021-02-22T11:10:23
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 5e2fbbce20631ecfa68c00b1cb89a1b7 log: Application source: EventSystem index: 5250 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-14T03:45:29 writeTime: 2020-09-14T03:45:29 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:23
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16

	Properties
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 17d1c24cdcc743fa66802c46e4a50c2b log: Application source: EventSystem index: 5166 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-13T03:22:58 writeTime: 2020-09-13T03:22:58 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:23
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx

	Properties
Summary	@uid: 8e0a47a5f156282b0dd472a313337334 log: Application source: EventSystem index: 4983 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-12T02:15:40 writeTime: 2020-09-12T02:15:40 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:23
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: d82cc3fb6b1f5a2ff52e45ccf5ae3368 log: Application source: EventSystem index: 4720 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-07T14:59:15 writeTime: 2020-09-07T14:59:15 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:24

	Properties
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: c13e99db474f8fd7541d6b50740418a3 log: Application source: EventSystem index: 4578 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-06T09:09:26 writeTime: 2020-09-06T09:09:26 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:24
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625

	Properties
Type	Logevtx
Summary	@uid: fe858edc27d37c7d691a9a2578d37ea1 log: Application source: EventSystem index: 4436 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-09-05T00:54:39 writeTime: 2020-09-05T00:54:39 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:24
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 8cff5195ed7fbf4d90beb3a97202dcbd log: Application source: EventSystem index: 4214 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-08-31T12:40:31 writeTime: 2020-08-31T12:40:31 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0

	Properties
CreationTime	2021-02-22T11:10:24
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: aa40f4122d386927943569e52124ed81 log: Application source: EventSystem index: 4097 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-08-31T02:10:55 writeTime: 2020-08-31T02:10:55 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:24
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16

	Properties
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 9ee8de47a044130cc7bffc128fcb42b5 log: Application source: EventSystem index: 3968 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-08-30T03:58:19 writeTime: 2020-08-30T03:58:19 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:24
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx

	Properties
Summary	@uid: 7d08e7faf6d35ac1c3f58f8ce4db9806 log: Application source: EventSystem index: 3785 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-08-28T08:56:38 writeTime: 2020-08-28T08:56:38 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:24
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 8c56c010a2ffc1d37bb8ec441c0d81d log: Application source: EventSystem index: 1651 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-07-26T17:41:18 writeTime: 2020-07-26T17:41:18 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:26

	Properties
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: b61a701192ee389ff4a393c8da99549f log: Application source: EventSystem index: 1480 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-07-25T13:16:38 writeTime: 2020-07-25T13:16:38 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:26
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625

	Properties
Type	Logevtx
Summary	@uid: adfd669ea01c4b1909bef086b21c8d3 log: Application source: EventSystem index: 1350 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-07-26T01:24:17 writeTime: 2020-07-26T01:24:17 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:26
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: 8b0f874d9f8fb23b2b87ba98795e8a53 log: Application source: EventSystem index: 1272 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-07-26T01:18:28 writeTime: 2020-07-26T01:18:28 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0

	Properties
CreationTime	2021-02-22T11:10:26
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: a23d1ae3b8dd2b342bf1770a395e72c9 log: Application source: EventSystem index: 1162 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-07-26T01:12:20 writeTime: 2020-07-26T01:12:20 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:26
Handler	admin
Status	Success

	Properties
Risk	Medium
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16

	Properties
Suggesion	Gợi ý: Kiểm tra dữ liệu đăng nhập hệ thống, nguồn đăng nhập, user đăng nhập, số lần thực hiện từ một nguồn trong một khoảng thời gian nhất định và các event ID trong blacklist khác. Lý do: Đăng nhập hệ thống thất bại Nguồn: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625
Type	Logevtx
Summary	@uid: deb6cc58823acff1bb97651beb1713db log: Application source: EventSystem index: 1040 EID: 4625 type: EVENTLOG_INFORMATION_TYPE genTime: 2020-07-25T17:42:26 writeTime: 2020-07-25T17:42:26 machine: DESKTOP-4ER81B7 ActivityID: null ExecutionProcessId: 0 ExecutionThreadId: 0 message: " SuppressDuplicateDuration Software\\\\Microsoft\\\\EventSystem\\\\EventLog.>" category: 0
CreationTime	2021-02-22T11:10:26
Handler	admin
Status	Success

2.4. phân tích, xác định nguyên nhân sự cố ATTT qua file mã độc

	Properties
Risk	Critical
Endpoint	DESKTOP-4ER81B7
Case	Case0001
CollectedDate	2021-02-22T10:57:16
Suggesion	Gợi ý: xóa file: index.php Lí do: File: //illusion_bot/WebAdmin/index.php - Avg:Virus identified Citem_c.GIZ - Comodo:Backdoor Nguồn: http://112.137.129.233:8088/api/v1/sample/210
Type	Malware
Summary	file malware
CreationTime	2021-02-22T10:57:16
Handler	admin
Status	Success