[SOC-AI-AGENT]

Automated Investigation Report

Alert ID: 4baa5d0f-ebd5-4f96-b1ca-1b5e8066a3a8 | Generated: 2026-02-13 04:18:17 UTC

Executive Summary

Verdict: TRUE_POSITIVE (81.625% confidence) — confirmed malicious activity. Key factors: IOC 27304b246c7d5b4e149124d5f93c5b01 flagged by 1 source(s) (risk score: 50.7). IOC e96a73c7bf33a464c510ede582318bf2 flagged by 1 source(s) (risk score: 40.0). IOC 8a2122e8162dbef04694b9c3e0b6cdee flagged by 1 source(s) (risk score: 40.0).

Verdict

Confidence: 81.6%

Alert Details

Field	Value
Alert Type	sysmon
Timestamp	2024-01-15T11:28:06.500000
Classification	c2_communication
Initial Severity	HIGH
Source IP	10.0.2.100
Destination IP	10.0.1.25

Source Host	IT-ADMIN-WS01.corp.acme.local
User	NT AUTHORITY\SYSTEM
Process	C:\Windows\PSEXESVC.exe
Command Line	`cmd.exe /c "net user backdoor P@ssw0rd123 /add && net localgroup administrators backdoor /add"`
Parent Process	C:\Windows\PSEXESVC.exe

Investigation Timeline

Triage — Complete

Classified as c2_communication. Severity: HIGH.

Ioc Extraction — Complete

Extracted 16 IOCs: {'sha256': 2, 'md5': 4, 'url': 1, 'domain': 2, 'file_path_windows': 7}

Enrichment — Complete

Enriched 16 IOCs across threat intel sources.

Correlation — Complete

Found 7 related investigation(s). Shared IOCs: http://schemas.microsoft.com/win/2004/08/events/event (seen 5x), 272245e2988e1e430500b852c4fb5e18 (seen 1x), 8a2122e8162dbef04694b9c3e0b6cdee (seen 1x). 2 related investigation(s) were previously confirmed as true positives. This significantly increases the likelihood of this alert being malicious.

Att&ck Mapping — Complete

Matched 8 techniques across 4 tactics.

Verdict — Complete

TRUE_POSITIVE (confidence: 81.6%)

IOC Enrichment Results

IOC	Type	Risk Score	Sources Flagged	Summary
`ad6b98c01dc3a1c96e96[redacted]7b2f05ccae1673d8[redacted]2a4e2d8f91f5e97c6c[redacted]1`		80	7 / 41	OTX: 0 pulses reference this IOC. Tags: none

b99d61d874728edc0918 10eab93d381e7367 78377406e65963366c870		70.0	1 / 4	OTX: 0 pulses reference this IOC. Tags: none
27304b246c7d5b4e1491 5f93c5b01		50.7	1 / 3	VT: 1/76 detections. Type: Win32 EXE, Names: PsExec, psexec.c, PsExec.exe OTX: 24 pulses reference this IOC. Tags: nanocore rat, maze download, zoom, tools, cobalt strike
e96a73c7bf33a464c510 582318bf2		40.0	1 / 3	OTX: 4 pulses reference this IOC. Tags: nowy, authentihash, compiler, e9 cd, b6 f8
8a2122e8162dbef04694 3e0b6cdee		40.0	1 / 3	VT: 0/76 detections. Type: Win32 EXE, Names: cmd.exe, alpha.exe, cmd OTX: 4 pulses reference this IOC. Tags: iocs, powershell, ip address, mirai botnet, mimikatz
272245e2988e1e430500 2c4fb5e18		60.0	1 / 3	OTX: 6 pulses reference this IOC. Tags: looks, desc, imagesize, Telus, malware file

http://schemas.micro[redacted]ft.com/win/2004/08/events/event		0.0	0 / 3	VT: 0/94 engines flagged URL as malicious.
schemas.microsoft.co[redacted]		15.0	0 / 4	VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=MarkMonitor, Inc., Created=1991-05-02 04:00:00, Expires=2027-05-03 04:00:00, Country=N/A
www.sysinternals.com[redacted]		5.0	0 / 4	VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=CSC Corporate Domains, Inc., Created=1998-04-12 04:00:00, Expires=2026-04-11 04:00:00, Country=N/A
C:\Tools\Sysinternal[redacted]c64.exe		0.0	0 / 0	
C:\Tools\Sysinternal[redacted]		0.0	0 / 0	
C:\Windows\System32\[redacted]		0.0	0 / 0	

C:\Windows\system32\	0.0	0 / 0	
C:\Windows\PSEXESVC.	0.0	0 / 0	
C:\Windows\system32	0.0	0 / 0	
C:\Windows\System32\	0.0	0 / 0	

MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name	Evidence
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	`cmd.exe /c`
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares	`SMB/Windows Admin Shares 2024-01-15 11:28:06.500 {E7F8A9B0-4B1E-65A5-0B01-00 8844 C:\Wind`
Lateral Movement	T1570	Lateral Tool Transfer	`SMB/Windows Admin Shares 2024-01-15 11:28:06.500 {E7F8A9B0-4B1E-65A5-0B01-00 8844 C:\Wind`
Discovery	T1087	Account Discovery	`net user`
Discovery	T1069	Permission Groups Discovery	`net user`
Command and Control	T1090	Proxy	`Enrichment tag: via-tor`

Execution	T1204.002	User Execution: Malicious File	`Enrichment tag: malware url`
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	`Enrichment tag: mirai botnet`

Attack chain analysis:
1. **Execution**: Command and Scripting Interpreter: Windows Command Shell (T1059.003), User Execution: Malicious File (T1204.002)
2. **Discovery**: Account Discovery (T1087), Permission Groups Discovery (T1069)
3. **Lateral Movement**: Remote Services: SMB/Windows Admin Shares (T1021.002), Lateral Tool Transfer (T1570)
4. **Command and Control**: Proxy (T1090), Application Layer Protocol: Web Protocols (T1071.001)

Historical Correlation

Found 7 related investigation(s). Shared IOCs: http://schemas.microsoft.com/win/2004/08/events/event (seen 5x), 272245e2988e1e430500b852c4fb5e18 (seen 1x), 8a2122e8162dbef04694b9c3e0b6cdee (seen 1x). 2 related investigation(s) were previously confirmed as true positives. This significantly increases the likelihood of this alert being malicious.

Alert ID	Type	Verdict	Matching IOC	Date
`0390d2d6...`	sysmon	NEEDS_ESCALATION	`272245e2988e1e430500b852c4fb5e18`	2026-02-13T04:01:06.3355
`a6461952...`	sysmon	TRUE_POSITIVE	`8a2122e8162dbef04694b9c3e0b6cdee`	2026-02-13T04:02:10.1518
`5023fdde...`	sysmon	NEEDS_ESCALATION	`http://schemas.microsoft.com/win/2004/08/events/event`	2026-02-13T03:25:04.8897
`047f07d3...`	sysmon	NEEDS_ESCALATION	`http://schemas.microsoft.com/win/2004/08/events/event`	2026-02-13T04:20:24.4621
`b57401c7...`	sysmon	FALSE_POSITIVE	`http://schemas.microsoft.com/win/2004/08/events/event`	2026-02-13T04:22:04.0460
`5ead2fc7...`	sysmon	TRUE_POSITIVE	`http://schemas.microsoft.com/win/2004/08/events/event`	2026-02-13T04:23:48.5803

88d8bb87...	sysmon	NEEDS_ESCALATION	http://schemas.micros	2026-02-13T04:27:16.785

Reasoning Chain

IOC 27304b246c7d5b4e149124d5f93c5b01 flagged by 1 source(s) (risk score: 50.7).

IOC e96a73c7bf33a464c510ede582318bf2 flagged by 1 source(s) (risk score: 40.0).

IOC 8a2122e8162dbef04694b9c3e0b6cdee flagged by 1 source(s) (risk score: 40.0).

IOC 272245e2988e1e430500b852c4fb5e18 flagged by 1 source(s) (risk score: 60.0).

Known malicious tool detected: psexec|PsExe[cs]

Suspicious command pattern: net\s+user.*\/add|net\s+localgroup.*admin

IOCs appeared in 2 previously confirmed true positive(s). Strong correlation with known malicious activity.

IOCs correlated across 7 previous investigations.

Attack chain spans 4 MITRE ATT&CK tactics, indicating a sophisticated multi-stage attack.

High-impact tactics detected: Lateral Movement

Matched 8 MITRE ATT&CK technique(s) across 4 tactic(s).

No temporal risk factors identified.

Score Breakdown

Component	Score	Weight	Weighted Score
Enrichment	70.0	35.0%	24.5
Behavioral	60.0	25.0%	15.0
Correlation	55.0	20.0%	11.0

Mitre	85	15.0%	12.8
Temporal	0.0	5.0%	0.0

Recommended Response Actions

1. Immediately isolate the affected host from the network.
2. Block source IP 10.0.2.100 at the firewall.
3. Reset credentials for user 'NT AUTHORITY\SYSTEM'.
4. Review all recent activity for user 'NT AUTHORITY\SYSTEM'.
5. Scan adjacent hosts for indicators of compromise.
6. Collect forensic evidence and preserve volatile data.
7. File incident report and notify security leadership.

Raw Evidence


```
<Events> <!-- Event 1: PsExec copied to remote host via SMB (source machine) --> <Event
xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider
Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FFBD9}"/>
<EventID>3</EventID> <Version>5</Version> <Level>4</Level> <Task>3</Task> <Opcode>0</Opcode>
<Keywords>0x8000000000000000</Keywords> <TimeCreated SystemTime="2024-01-15T11:28:04.512Z"/>
<EventRecordID>87201</EventRecordID> <Correlation/> <Execution ProcessID="2844"
ThreadID="3160"/> <Channel>Microsoft-Windows-Sysmon/Operational</Channel>
<Computer>IT-ADMIN-WS01.corp.acme.local</Computer> <Security
UserID="S-1-5-21-3541430928-2051711210-1391384369-1105"/> </System> <EventData> <Data
Name="RuleName">technique_id=T1021.002,technique_name=SMB/Windows Admin Shares</Data> <Data
Name="UtcTime">2024-01-15 11:28:04.498</Data> <Data
Name="ProcessGuid">{D5E6F7A8-4B1C-65A5-0912-000000001800}</Data> <Data
Name="ProcessId">3248</Data> <Data Name="Image">C:\Tools\SysinternalsSuite\PsExec64.exe</Data>
<Data Name="User">ACME\svc-admin</Data> <Data Name="Protocol">tcp</Data> <Data
Name="Initiated">true</Data> <Data Name="SourceIsIpv6">false</Data> <Data
Name="SourceIp">10.0.1.25</Data> <Data
Name="SourceHostname">IT-ADMIN-WS01.corp.acme.local</Data> <Data Name="SourcePort">49842</Data>
<Data Name="SourcePortName"/> <Data Name="DestinationIsIpv6">false</Data> <Data
Name="DestinationIp">10.0.2.100</Data> <Data
Name="DestinationHostname">FILE-SRV01.corp.acme.local</Data> <Data
Name="DestinationPort">445</Data> <Data Name="DestinationPortName">microsoft-ds</Data>
</EventData> </Event> <!-- Event 2: PsExec process creation on source (initiating connection)
```

```
--> <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="2024-01-15T11:28:03.201Z"/>
<EventRecordID>87200</EventRecordID> <Correlation/> <Execution ProcessID="2844"
ThreadID="3160"/> <Channel>Microsoft-Windows-Sysmon/Operational</Channel>
<Computer>IT-ADMIN-WS01.corp.acme.local</Computer> <Security
UserID="S-1-5-21-3541430928-2051711210-1391384369-1105"/> </System> <EventData> <Data
Name="RuleName">technique_id=T1570,technique_name=Lateral Tool Transfer</Data> <Data
Name="UtcTime">2024-01-15 11:28:03.188</Data> <Data
Name="ProcessGuid">{D5E6F7A8-4B1C-65A5-0912-000000001800}</Data> <Data
Name="ProcessId">3248</Data> <Data Name="Image">C:\Tools\SysinternalsSuite\PsExec64.exe</Data>
<Data Name="FileVersion">2.43</Data> <Data Name="Description">Execute processes remotely</Data>
<Data Name="Product">Sysinternals PsExec</Data> <Data Name="Company">Sysinternals -
www.sysinternals.com</Data> <Data Name="OriginalFileName">psexec.c</Data> <Data
Name="CommandLine">PsExec64.exe \\10.0.2.100 -u ACME\svc-admin -p ******* -s cmd.exe /c "net
user backdoor P@ssw0rd123 /add &amp;amp;&amp;amp; net localgroup administrators backdoor /add"</Data>
<Data Name="CurrentDirectory">C:\Tools\SysinternalsSuite\</Data> <Data
Name="User">ACME\svc-admin</Data> <Data
Name="LogonGuid">{D5E6F7A8-1A2B-65A5-F1D2-030000000000}</Data> <Data
Name="LogonId">0x3D2F1</Data> <Data Name="TerminalSessionId">1</Data> <Data
Name="IntegrityLevel">High</Data> <Data
Name="Hashes">SHA256=AD6B98C01DC3A1C96E9652DFC7B2F05CCAE1673D8D2A4E2D8F91F5E97C6C7E41,MD5=27304B246C7D5
<Data Name="ParentProcessGuid">{D5E6F7A8-1A40-65A5-0201-000000001800}</Data> <Data
Name="ParentProcessId">5640</Data> <Data Name="ParentImage">C:\Windows\System32\cmd.exe</Data>
<Data Name="ParentCommandLine">"C:\Windows\System32\cmd.exe"</Data> <Data
Name="ParentUser">ACME\svc-admin</Data> </EventData> </Event> <!-- Event 3: PSEXESVC service
installed on target (observed on target host) --> <Event
xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider
Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FFBD9}"/>
<EventID>13</EventID> <Version>2</Version> <Level>4</Level> <Task>13</Task> <Opcode>0</Opcode>
<Keywords>0x8000000000000000</Keywords> <TimeCreated SystemTime="2024-01-15T11:28:05.710Z"/>
<EventRecordID>45302</EventRecordID> <Correlation/> <Execution ProcessID="1892"
ThreadID="2108"/> <Channel>Microsoft-Window
```
