[SOC-AI-AGENT]

Automated Investigation Report

Alert ID: ff8a9ed6-71f2-4155-a423-8ca9053df90c | Generated: 2026-02-13 04:30:33 UTC

Executive Summary

Verdict: FALSE_POSITIVE (82.5% confidence) — benign activity (false positive). Key factors: No IOCs flagged as malicious by enrichment sources. IOCs appeared in 6 previously confirmed true positive(s). Strong correlation with known malicious activity.

Verdict

Confidence: 82.5%

Alert Details

Field	Value
Alert Type	sysmon
Timestamp	2024-01-13T07:30:14.218000+00:00
Classification	c2_communication
Initial Severity	LOW
Source Host	WORKSTATION-PC08.corp.acme.local

Investigation Timeline

Triage — Complete

Classified as c2_communication. Severity: LOW.

Ioc Extraction — Complete

Extracted 24 IOCs: {'url': 1, 'domain': 1, 'file_path_windows': 22}

Enrichment — Complete

Enriched 24 IOCs across threat intel sources.

Correlation — Complete

Found 13 related investigation(s). Shared IOCs: http://schemas.microsoft.com/win/2004/08/events/event (seen 6x), C:\Windows\explorer.exe (seen 5x), C:\Windows\System32\svchost.exe (seen 2x). 6 related investigation(s) were previously confirmed as true positives. This significantly increases the likelihood of this alert being malicious.

Att&ck Mapping — Complete

Matched 0 techniques across 0 tactics.

Verdict — Complete

FALSE_POSITIVE (confidence: 82.5%)

IOC Enrichment Results

IOC	Type	Risk Score	Sources Flagged	Summary
http://schemas.microsoft.com/win/2004/08/events/event		0.0	0 / 3	VT: 0/94 engines flagged URL as malicious.
schemas.microsoft.com		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
C:\Windows\System32\		0.0	0 / 0	
D:\Shares\Finance		0.0	0 / 0	

D:\Shares\Finance\20[redacted]nual_Budget_Master.xlsx	0.0	0 / 0		
D:\Shares\Finance\Pa[redacted]ee_Salary_Schedule_2024.xlsx	0.0	0 / 0		
D:\Shares\Finance\Ba[redacted]ate_Bank_Account_Details.pdf	0.0	0 / 0		
D:\Shares\Finance\Re[redacted]3_Revenue_Confidential.xlsx	0.0	0 / 0		
D:\Shares\Finance\Ta[redacted]Tax_Returns_2023.pdf	0.0	0 / 0		
D:\Shares\HR_Data [redacted]	0.0	0 / 0		
D:\Shares\HR_Data\Em[redacted]ds\All_Employees_PII_2024.xlsx	0.0	0 / 0		
D:\Shares\HR_Data\Pe[redacted]views\Executive_Performance_2023.docx	0.0	0 / 0		
D:\Shares\HR_Data\Co[redacted]lanned_Layoffs_Q1_2024.xlsx	0.0	0 / 0		
D:\Shares\HR_Data\Be[redacted]yee_Benefits_Summary_2024.xlsx	0.0	0 / 0		
D:\Shares\HR_Data\Or[redacted]xec_Org_Chart_Restructuring.pptx	0.0	0 / 0		
D:\Shares\Finance\Ac[redacted]le\Vendor_Payment_Schedule_2024.xlsx	0.0	0 / 0		
D:\Shares\Finance\Me[redacted]itions\Project_Phoenix_Due_Diligence.pdf	0.0	0 / 0		
D:\Shares\HR_Data\Co[redacted]mployee_SSN_Directory.xlsx	0.0	0 / 0		
D:\Shares\Finance\Cr[redacted]orporate_Card_Statements_Dec2023.pdf	0.0	0 / 0		
D:\Shares\HR_Data\Be[redacted]_Health_Insurance_Claims_2023.xlsx	0.0	0 / 0		
E:\Backup\Finance_Da[redacted]p	0.0	0 / 0		

C:\Windows\explorer.[redacted]	0.0	0 / 0	
E:\Backup\HR_Confide[redacted].zip	0.0	0 / 0	
E:\Backup\Project_Ph[redacted]als.zip	0.0	0 / 0	

Historical Correlation

Found 13 related investigation(s). Shared IOCs: http://schemas.microsoft.com/win/2004/08/events/event (seen 6x), C:\Windows\explorer.exe (seen 5x), C:\Windows\System32\svchost.exe (seen 2x). 6 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
b57401c7...	sysmon	FALSE_POSITIVE	C:\Windows\System32\[redacted]	2026-02-13T04:02:04.0466
c2b942a9...	sysmon	FALSE_POSITIVE	C:\Windows\System32\[redacted]	2026-02-13T04:18:27.4388
047f07d3...	sysmon	NEEDS_ESCALATION	C:\Windows\explorer.exe	2026-02-13T04:00:26.4622
a6461952...	sysmon	TRUE_POSITIVE	C:\Windows\explorer.exe	2026-02-13T04:02:10.1518
88d8bb87...	sysmon	NEEDS_ESCALATION	C:\Windows\explorer.exe	2026-02-13T04:17:16.7654
fcb003d9...	sysmon	TRUE_POSITIVE	C:\Windows\explorer.exe	2026-02-13T04:18:33.5441
f065cfda...	sysmon	NEEDS_ESCALATION	C:\Windows\explorer.exe	2026-02-13T04:29:14.8977
5023fdde...	sysmon	NEEDS_ESCALATION	http://schemas.microsoft.com/win/2004/08/events/event	2026-02-13T03:25:04.8897

0390d2d6...	sysmon	NEEDS_ESCALATION	http://schemas.micros	2026-02-13T04:21:06.3375
5ead2fc7...	sysmon	TRUE_POSITIVE	http://schemas.micros	2026-02-13T04:19:48.5803

Reasoning Chain

No IOCs flagged as malicious by enrichment sources.

No significant behavioral indicators detected.

IOCs appeared in 6 previously confirmed true positive(s). Strong correlation with known malicious activity.

IOCs correlated across 13 previous investigations.

No MITRE ATT&CK techniques identified.

Alert occurred on a weekend.

Score Breakdown

Component	Score	Weight	Weighted Score
Enrichment	15.0	35.0%	5.2
Behavioral	0.0	25.0%	0.0
Correlation	65.0	20.0%	13.0
Mitre	0.0	15.0%	0.0
Temporal	10.0	5.0%	0.5

Recommended Response Actions

1. No immediate action required.

2. Consider adding to allowlist/exception list if recurring.

3. Document the false positive for tuning detection rules.

Raw Evidence


```
<Events> <!-- Event 1: RDP Logon at 2:30 AM Saturday --> <Event
xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider
Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}"/>
<EventID>4624</EventID> <Version>2</Version> <Level>0</Level> <Task>12544</Task>
<Opcode>0</Opcode> <Keywords>0x8020000000000000</Keywords> <TimeCreated
SystemTime="2024-01-13T07:30:14.218Z"/> <EventRecordID>204851</EventRecordID> <Correlation
ActivityID="{A1B2C3D4-E5F6-7890-ABCD-EF1234567890}"/> <Execution ProcessID="648"
ThreadID="1204"/> <Channel>Security</Channel>
<Computer>WORKSTATION-PC08.corp.acme.local</Computer> <Security/> </System> <EventData> <Data
Name="SubjectUserSid">S-1-5-18</Data> <Data Name="SubjectUserName">WORKSTATION-PC08$</Data>
<Data Name="SubjectDomainName">ACME</Data> <Data Name="SubjectLogonId">0x3E7</Data> <Data
Name="TargetUserSid">S-1-5-21-3541430928-2051711210-1391384369-1156</Data> <Data
Name="TargetUserName">jsmith</Data> <Data Name="TargetDomainName">ACME</Data> <Data
Name="TargetLogonId">0x1A2B3C4</Data> <Data Name="LogonType">10</Data> <Data
Name="LogonProcessName">User32</Data> <Data Name="AuthenticationPackageName">Negotiate</Data>
<Data Name="WorkstationName">WORKSTATION-PC08</Data> <Data
Name="LogonGuid">{F1E2D3C4-B5A6-9780-1234-567890ABCDEF}</Data> <Data
Name="TransmittedServices">-</Data> <Data Name="LmPackageName">-</Data> <Data
Name="KeyLength">0</Data> <Data Name="ProcessId">0x2BC</Data> <Data
Name="ProcessName">C:\Windows\System32\svchost.exe</Data> <Data
Name="IpAddress">10.0.3.15</Data> <Data Name="IpPort">51842</Data> <Data
Name="ImpersonationLevel">%%1833</Data> <Data Name="RestrictedAdminMode">-</Data> <Data
Name="TargetOutboundUserName">-</Data> <Data Name="TargetOutboundDomainName">-</Data> <Data
Name="VirtualAccount">%%1843</Data> <Data Name="TargetLinkedLogonId">0x0</Data> <Data
Name="ElevatedToken">%%1842</Data> </EventData> </Event> <!-- Event 2: Network share access -
\\fileserver\finance --> <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System> <Provider Name="Microsoft-Windows-Security-Auditing"
Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}"/> <EventID>5140</EventID> <Version>1</Version>
<Level>0</Level> <Task>12808</Task> <Opcode>0</Opcode> <Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2024-01-13T07:32:41.502Z"/> <EventRecordID>204852</EventRecordID>
<Correlation/> <Execution ProcessID="4" ThreadID="1208"/> <Channel>Security</Channel>
<Computer>FILESERVER.corp.acme.local</Computer> <Security/> </System> <EventData> <Data
Name="SubjectUserSid">S-1-5-21-3541430928-2051711210-1391384369-1156</Data> <Data
Name="SubjectUserName">jsmith</Data> <Data Name="SubjectDomainName">ACME</Data> <Data
Name="SubjectLogonId">0x1A2B3C4</Data> <Data Name="ObjectType">File</Data> <Data
Name="IpAddress">10.0.3.15</Data> <Data Name="IpPort">49921</Data> <Data
Name="ShareName">\\*\finance</Data> <Data Name="ShareLocalPath">\??\D:\Shares\Finance</Data>
<Data Name="AccessMask">0x1</Data> <Data Name="AccessList">%%4416</Data> </EventData> </Event>
<!-- Event 3: File access in finance share --> <Event
xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider
Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}"/>
<EventID>4663</EventID> <Version>1</Version> <Level>0</Level> <Task>12800</Task>
<Opcode>0</Opcode> <Keywords>0x8020000000000000</Keywords> <TimeCreated
SystemTime="2024-01-13T07:33:02.108Z"/> <EventRecordID>204853</EventRecordID> <Correlation/>
```

```
<Execution ProcessID="4" ThreadID="1208"/> <Channel>Security</Channel>
<Computer>FILESERVER.corp.acme.local</Computer> <Security/> </System> <EventData> <Data
Name="SubjectUserSid">S-1-5-21-3541430928-2051711210-1391384369-1156</Data> <Data
Name="SubjectUserName">jsmith</Data> <Data Name="SubjectDomainName">ACME</Data> <Data
Name="SubjectLogonId">0x1A2B3C4</Data> <Data Name="ObjectServer">Security</Data> <Data
Name="ObjectType">File</Data> <Data
Name="ObjectName">D:\Shares\Finance\2024_Budget\Annual_Budget_Master.xlsx</Data> <Data
Name="HandleId">0x1240</Data> <Data Name="AccessList">%%4416 %%4417 %%4418</Data> <Data
Name="AccessMask">0x12019F</Data> <Data Name="ProcessId">0x4</Data> <Data Name="ProcessName"/>
<Data Name="ResourceAttributes">S:AI</Data> </EventData> </Event> <
```
