

[SOC-AI-AGENT]

Automated Investigation Report

Alert ID: 88d8bb87-84db-4da8-8dfe-32d8e5b2d37f | Generated: 2026-02-13 04:17:52 UTC

Executive Summary

Verdict: NEEDS_ESCALATION (37.075% confidence) — suspicious activity requiring human review. Key factors: IOC 1.0.0.0 flagged by 1 source(s) (risk score: 51.5). Suspicious command pattern: vssadmin.*delete|bcdedit.*recoveryenabled IOCs appeared in 2 previously confirmed true positive(s). Strong correlation with known malicious activity.

Verdict



Confidence: 37.1%

Alert Details

Field	Value
Alert Type	sysmon
Timestamp	2024-01-15T16:42:22.843000
Classification	ransomware
Initial Severity	CRITICAL
Source Host	ACCT-WS07.corp.acme.local
User	ACME\rjones

Process	C:\Users\rjones\AppData\Local\Temp\invoice_2024_final.exe
Command Line	bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
Parent Process	C:\Users\rjones\AppData\Local\Temp\invoice_2024_final.exe

Investigation Timeline

Triage — Complete

Classified as ransomware. Severity: CRITICAL.

Ioc Extraction — Complete

Extracted 22 IOCs: {'sha256': 1, 'md5': 6, 'url': 1, 'ipv4': 1, 'domain': 1, 'file_path_windows': 12}

Enrichment — Complete

Enriched 22 IOCs across threat intel sources.

Correlation — Complete

Found 6 related investigation(s). Shared IOCs: 1.0.0.0 (seen 2x), C:\Windows\explorer.exe (seen 2x), 0fd5c9a25aae055c1f8f5a8ae76c00c2 (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 2 techniques across 1 tactics.

Verdict — Complete

NEEDS_ESCALATION (confidence: 37.1%)

IOC Enrichment Results

IOC	Type	Risk Score	Sources Flagged	Summary
b6e66b47f7a236e1eabc[REDACTED]f9581ba7cd988db8a3b74eda3d1ac651ae60457		0.0	0 / 3	OTX: 0 pulses reference this IOC. Tags: none
9e8d7c6b5a4f3e2d1c0b[REDACTED]f7e6d5c4b		0.0	0 / 3	OTX: 0 pulses reference this IOC. Tags: none

2c41d8394a2a7de5ae4f[REDACTED]118360ff8	0.0	0 / 3	OTX: 0 pulses reference this IOC. Tags: none
2a40b2668ed9b73c8d0e[REDACTED]b0e1dfab0	0.0	0 / 3	OTX: 0 pulses reference this IOC. Tags: none
67f87b343f1e84c7f88b[REDACTED]f35c8e5ff	0.0	0 / 3	OTX: 0 pulses reference this IOC. Tags: none
0fd5c9a25aae055c1f8f[REDACTED]ae76c00c2	0.0	0 / 3	OTX: 0 pulses reference this IOC. Tags: none
12b3c4d5e6f7a8b9c0d1[REDACTED]3a4b5c6d7	0.0	0 / 3	OTX: 0 pulses reference this IOC. Tags: none
http://schemas.microsoft.com/win/2004/08/events/event	0.0	0 / 3	VT: 0/94 engines flagged URL as malicious.

1.0.0.0	<div></div>	51.5	1 / 5	<div>VT: 0/93 engines flagged as malicious. AS: CLOUDFLARENET, Country: N/A AbuseIPDB: Abuse confidence 3%, 1 reports. ISP: APNIC and Cloudflare DNS Resolver project, Usage: Content Delivery Network, Country: AU OTX: 50 pulses reference this IOC. Tags: archivesha1, archivesha256, powershell, desktop, look GreyNoise: IP not observed scanning the internet</div>
schemas.microsoft.co <div></div>	<div></div>	15.0	0 / 4	<div>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</div>
C:\Users\rjones\AppData <div></div> mp\invoice_2024_final.exe		0.0	0 / 0	

C:\Users\rjones\Down██████████	0.0	0 / 0	
C:\Windows\explorer.██████████	0.0	0 / 0	
C:\Windows\System32\██████████	0.0	0 / 0	
C:\Users\rjones\AppData██████████p	0.0	0 / 0	
C:\Windows\System32\██████████	0.0	0 / 0	
C:\Users\rjones\Docu██████████al_Report██████████Q4_2023.xlsx.locked	0.0	0 / 0	
C:\Users\rjones\Docu██████████_Projections_2024.docx.locked	0.0	0 / 0	
C:\Users\rjones\Docu██████████_Salary_S_S_Confidential.pdflocked	0.0	0 / 0	
C:\Users\rjones\Docu██████████_Contracts_2023.zip.locked	0.0	0 / 0	
C:\Users\rjones\Docu██████████_Logic_Plan██████████Presentation.pptx.locked	0.0	0 / 0	
C:\Users\rjones\Docu██████████_YOUR_FILES.txt	0.0	0 / 0	

MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name	Evidence
Impact	T1490	Inhibit System Recovery	Encrypted for Impact 2024-01-15 16:42:22.843 {A1F23B4C-9D2E-65A5-4A08-0 9412 C:\Users\rj

Impact	T1486	Data Encrypted for Impact	Encrypted for Impact 2024-01-15 16:42:22.843 {A1F23B4C-9D2E-65A5-4A08-09412 C:\Users\rj
--------	-------	---------------------------	---

Attack chain analysis:

1. **Impact**: Inhibit System Recovery (T1490), Data Encrypted for Impact (T1486)

Historical Correlation

Found 6 related investigation(s). Shared IOCs: 1.0.0.0 (seen 2x), C:\Windows\explorer.exe (seen 2x), 0fd5c9a25aae055c1f8f5a8ae76c00c2 (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
047f07d3...	sysmon	NEEDS_ESCALATION	0fd5c9a25aae055c1f8f5a8ae76c00c2	2026-02-13T04:00:26.462Z
5023fdde...	sysmon	NEEDS_ESCALATION	1.0.0.0	2026-02-13T03:55:04.889Z
5ead2fc7...	sysmon	TRUE_POSITIVE	1.0.0.0	2026-02-13T04:13:33.500Z
b57401c7...	sysmon	FALSE_POSITIVE	C:\Windows\explorer.exe	2026-02-13T04:02:04.046Z
a6461952...	sysmon	TRUE_POSITIVE	C:\Windows\explorer.exe	2026-02-13T04:02:10.151Z
0390d2d6...	sysmon	NEEDS_ESCALATION	http://schemas.microsoft.com/2003/11/...	2026-02-13T04:01:06.335Z

Reasoning Chain

IOC 1.0.0.0 flagged by 1 source(s) (risk score: 51.5).

Suspicious command pattern: vssadmin.*delete|bcdedit.*recoveryenabled

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

IOCs correlated across 6 previous investigations.

High-impact tactics detected: Impact

Matched 2 MITRE ATT&CK technique(s) across 1 tactic(s).

No temporal risk factors identified.

Score Breakdown

Component	Score	Weight	Weighted Score
Enrichment	51.5	35.0%	18.0
Behavioral	40.0	25.0%	10.0
Correlation	55.0	20.0%	11.0
Mitre	26	15.0%	3.9
Temporal	0.0	5.0%	0.0

Recommended Response Actions

- Escalate to senior analyst for manual review.
- Gather additional context from the host and user.
- Do not take destructive action until further analysis is complete.

Raw Evidence

```
<Events> <!-- Stage 1: Initial execution of ransomware dropper --> <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="2024-01-15T16:42:18.204Z"/>
```

```
<EventRecordID>112450</EventRecordID> <Correlation/> <Execution ProcessID="2844"
ThreadID="3160"/> <Channel>Microsoft-Windows-Sysmon/Operational</Channel>
<Computer>ACCT-WS07.corp.acme.local</Computer> <Security
UserID="S-1-5-21-3541430928-2051711210-1391384369-1189"/> </System> <EventData> <Data
Name="RuleName">technique_id=T1204,technique_name=Malicious File</Data> <Data
Name="UtcTime">2024-01-15 16:42:18.192</Data> <Data
Name="ProcessGuid">{A1F23B4C-9D2E-65A5-4A08-000000002200}</Data> <Data
Name="ProcessId">9412</Data> <Data
Name="Image">C:\Users\rjones\AppData\Local\Temp\invoice_2024_final.exe</Data> <Data
Name="FileVersion">1.0.0.0</Data> <Data Name="Description"/> <Data Name="Product"/> <Data
Name="Company"/> <Data Name="OriginalFileName">cryptolocker_v3.exe</Data> <Data
Name="CommandLine">"C:\Users\rjones\AppData\Local\Temp\invoice_2024_final.exe"</Data> <Data
Name="CurrentDirectory">C:\Users\rjones\Downloads\</Data> <Data Name="User">ACME\rjones</Data>
<Data Name="LogonGuid">{A1F23B4C-2D1A-65A5-E2A4-070000000000}</Data> <Data
Name="LogonId">0x7A4E2</Data> <Data Name="TerminalSessionId">1</Data> <Data
Name="IntegrityLevel">High</Data> <Data
Name="Hashes">SHA256=3F2B4A5C6D7E8F9A0B1C2D3E4F5A6B7C8D9E0F1A2B3C4D5E6F7A8B9C0D1E2F,MD5=9E8D7C6B5A4F3E2
<Data Name="ParentProcessGuid">{A1F23B4C-2D30-65A5-0F01-000000002200}</Data> <Data
Name="ParentProcessId">4120</Data> <Data Name="ParentImage">C:\Windows\explorer.exe</Data>
<Data Name="ParentCommandLine">C:\Windows\explorer.exe</Data> <Data
Name="ParentUser">ACME\rjones</Data> </EventData> </Event> <!-- Stage 2: Delete Volume Shadow
Copies --> <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="2024-01-15T16:42:19.871Z"/>
<EventRecordID>112451</EventRecordID> <Correlation/> <Execution ProcessID="2844"
ThreadID="3160"/> <Channel>Microsoft-Windows-Sysmon/Operational</Channel>
<Computer>ACCT-WS07.corp.acme.local</Computer> <Security
UserID="S-1-5-21-3541430928-2051711210-1391384369-1189"/> </System> <EventData> <Data
Name="RuleName">technique_id=T1490,technique_name=Inhibit System Recovery</Data> <Data
Name="UtcTime">2024-01-15 16:42:19.860</Data> <Data
Name="ProcessGuid">{A1F23B4C-9D30-65A5-4B08-000000002200}</Data> <Data
Name="ProcessId">9504</Data> <Data Name="Image">C:\Windows\System32\vssadmin.exe</Data> <Data
Name="FileVersion">10.0.19041.1 (WinBuild.160101.0800)</Data> <Data Name="Description">Command
Line Interface for Microsoft Volume Shadow Copy Service</Data> <Data Name="Product">Microsoft
Windows Operating System</Data> <Data Name="Company">Microsoft Corporation</Data> <Data
Name="OriginalFileName">VSSADMIN.EXE</Data> <Data Name="CommandLine">vssadmin.exe delete
shadows /all /quiet</Data> <Data
Name="CurrentDirectory">C:\Users\rjones\AppData\Local\Temp\</Data> <Data
Name="User">ACME\rjones</Data> <Data
Name="LogonGuid">{A1F23B4C-2D1A-65A5-E2A4-070000000000}</Data> <Data
Name="LogonId">0x7A4E2</Data> <Data Name="TerminalSessionId">1</Data> <Data
Name="IntegrityLevel">High</Data> <Data
Name="Hashes">SHA256=B6E66B47F7A236E1EABC25C5CF9581BA7CD988DB8A3B74EDA3D1AC651AE62E57,MD5=2A40B2668ED9E
<Data Name="ParentProcessGuid">{A1F23B4C-9D2E-65A5-4A08-000000002200}</Data> <Data
Name="ParentProcessId">9412</Data> <Data
Name="ParentImage">C:\Users\rjones\AppData\Local\Temp\invoice_2024_final.exe</Data> <Data
Name="ParentCommandLine">"C:\Users\rjones\AppData\Local\Temp\invoice_2024_final.exe"</Data>
<Data Name="ParentUser">ACME\rjones</Data> </EventData> </Event> <!-- Stage 3: Disable recovery
mode via bcdedit --> <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System> <Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-4
```


