[SOC-AI-AGENT]

Automated Investigation Report

Alert ID: a6461952-68ee-4e08-a035-4e68a4b706e0 | Generated: 2026-02-13 04:02:41 UTC

Executive Summary

Verdict: TRUE_POSITIVE (82.475% confidence) — confirmed malicious activity. Key factors: IOC e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 flagged by 1 source(s) (risk score: 100.0). IOC 61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1 flagged by 2 source(s) (risk score: 100). IOC 8a2122e8162dbef04694b9c3e0b6cdee flagged by 1 source(s) (risk score: 40.0).

Verdict

Confidence: 82.5%

Alert Details

Field	Value
Alert Type	sysmon
Timestamp	2024-01-15T14:32:08.804000
Classification	credential_theft
Initial Severity	CRITICAL
Source Host	WORKSTATION-PC12.corp.acme.local

User	ACME\jdoe
Process	C:\Users\jdoe\Desktop\tools\mimikatz.exe
Command Line	`"C:\Users\jdoe\Desktop\tools\mimikatz.exe" "privilege::debug" "sekurlsa::logonpasswords" "exit"`
Parent Process	C:\Windows\System32\cmd.exe

Investigation Timeline

Triage — Complete

Classified as credential_theft. Severity: CRITICAL.

Ioc Extraction — Complete

Extracted 21 IOCs: {'sha256': 2, 'md5': 4, 'url': 1, 'domain': 1, 'file_path_windows': 13}

Enrichment — Complete

Enriched 21 IOCs across threat intel sources.

Correlation — Complete

Found 4 related investigation(s). Shared IOCs: C:\Windows\explorer.exe (seen 2x), 8a2122e8162dbef04694b9c3e0b6cdee (seen 1x), http://schemas.microsoft.com/win/2004/08/events/event (seen 1x). 1 related investigation(s) were previously classified as false positives.

Att&ck Mapping — Complete

Matched 6 techniques across 3 tactics.

Verdict — Complete

TRUE_POSITIVE (confidence: 82.5%)

IOC Enrichment Results

IOC	Type	Risk Score	Sources Flagged	Summary

e3b0c44298fc1c149afb	🟩96fb92427ae41e4649b934ca495991b7852b855	100.0	1 / 3	VT: 0/76 detections. Type: unknown, Names: A91lk7jqv_1v5ob28_1eo.tmp, A915d1gt8_33crhk_1ec.tmp, partner-custom-asset.png OTX: 50 pulses reference this IOC. Tags: delete, et, alerts, head meta, sensor-tagged
61c0810a23580cf492a6	🟩654566108331e7a4134c968c2d6a05261b2d8a1	100	2 / 3	VT: 66/76 detections. Type: Win32 EXE, Names: file.exe, mimikatz.exe, $RFBJXNS.exe OTX: 50 pulses reference this IOC. Tags: coinminer, cve-2020-1066, tesla, lazagne, byovd
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

a53a02b997935fd8eedc[redacted]7abab9b9f		40.0	1 / 3	OTX: 4 pulses reference this IOC. Tags: nowy, authentihash, compiler, e9 cd, b6 f8
a3b5de47052b4989d346[redacted]afcbe1a58		0.0	0 / 3	OTX: 0 pulses reference this IOC. Tags: none
d16ac0b23eeb9b04fe1d[redacted]5f4286f42		0.0	0 / 3	OTX: 0 pulses reference this IOC. Tags: none
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
C:\Windows\System32\[redacted]		0.0	0 / 0	
C:\Users\jdoe\Deskto[redacted]atz.exe		0.0	0 / 0	

C:\Users\jdoe\Deskto	🟩	0.0	0 / 0	
C:\Windows\explorer.	🟩	0.0	0 / 0	
C:\Windows\System32\	🟩	0.0	0 / 0	
C:\Windows\SYSTEM32\ 4C4	🟩	0.0	0 / 0	
C:\Windows\System32\ ll+2C13E	🟩	0.0	0 / 0	
C:\Users\jdoe\Deskto katz.exe+6DC5D	🟩	0.0	0 / 0	
C:\Users\jdoe\Deskto katz.exe+6DE12	🟩	0.0	0 / 0	
C:\Users\jdoe\Deskto katz.exe+73B89	🟩	0.0	0 / 0	
C:\Users\jdoe\Deskto katz.exe+75AE6	🟩	0.0	0 / 0	
C:\Users\jdoe\Deskto katz.exe+171A6	🟩	0.0	0 / 0	
C:\Users\jdoe\Deskto katz.exe+73C21	🟩	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`
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory	`mimikatz`

Credential Access	T1003	OS Credential Dumping	`mimikatz`
Command and Control	T1090	Proxy	`Enrichment tag: via-tor`
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	`Enrichment tag: mirai botnet`
Execution	T1204.002	User Execution: Malicious File	`Enrichment tag: malware url`

Attack chain analysis:
1. **Execution**: Command and Scripting Interpreter: Windows Command Shell (T1059.003), User Execution: Malicious File (T1204.002)
2. **Credential Access**: OS Credential Dumping: LSASS Memory (T1003.001), OS Credential Dumping (T1003)
3. **Command and Control**: Proxy (T1090), Application Layer Protocol: Web Protocols (T1071.001)

Historical Correlation

Found 4 related investigation(s). Shared IOCs: C:\Windows\explorer.exe (seen 2x), 8a2122e8162dbef04694b9c3e0b6cdee (seen 1x), http://schemas.microsoft.com/win/2004/08/events/event (seen 1x). 1 related investigation(s) were previously classified as false positives.

Alert ID	Type	Verdict	Matching IOC	Date
`0390d2d6...`	sysmon	NEEDS_ESCALATION	`8a2122e8162dbef04694b9c3e0b6cdee`	2026-02-13T04:01:06.3355
`047f07d3...`	sysmon	NEEDS_ESCALATION	`C:\Windows\explorer.exe`	2026-02-13T04:00:26.4622
`b57401c7...`	sysmon	FALSE_POSITIVE	`C:\Windows\explorer.exe`	2026-02-13T04:02:04.0466
`5023fdde...`	sysmon	NEEDS_ESCALATION	`http://schemas.microsoft.com/win/2004/08/`	2026-02-13T03:55:04.889

Reasoning Chain

IOC e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 flagged by 1 source(s) (risk score: 100.0).

IOC 61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1 flagged by 2 source(s) (risk score: 100).

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

IOC a53a02b997935fd8eedcb5f7abab9b9f flagged by 1 source(s) (risk score: 40.0).

Known malicious tool detected: mimikatz|mimi\.exe

Suspicious command pattern: lsass\.exe|sekurlsa|logonpasswords

IOCs correlated across 4 previous investigations.

IOCs appeared in 1 false positive(s). May reduce malicious confidence.

High-impact tactics detected: Credential Access

Matched 6 MITRE ATT&CK technique(s) across 3 tactic(s).

No temporal risk factors identified.

Score Breakdown

Component	Score	Weight	Weighted Score
Enrichment	100	35.0%	35.0
Behavioral	75.0	25.0%	18.8
Correlation	5.0	20.0%	1.0
Mitre	68	15.0%	10.2
Temporal	0.0	5.0%	0.0

Recommended Response Actions

1. Immediately isolate the affected host from the network.

2. Reset credentials for user 'ACME\jdoe'.

3. Review all recent activity for user 'ACME\jdoe'.

4. Search environment for file hash 61c0810a23580cf4...

5. Initiate organization-wide password reset for affected accounts.

6. Collect forensic evidence and preserve volatile data.

7. File incident report and notify security leadership.

Raw Evidence

```
<Events> <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="2024-01-15T14:32:07.891Z"/>
<EventRecordID>104832</EventRecordID> <Correlation/> <Execution ProcessID="2844"
ThreadID="3160"/> <Channel>Microsoft-Windows-Sysmon/Operational</Channel>
<Computer>WORKSTATION-PC12.corp.acme.local</Computer> <Security
UserID="S-1-5-21-3541430928-2051711210-1391384369-1104"/> </System> <EventData> <Data
Name="RuleName">technique_id=T1059.003,technique_name=Windows Command Shell</Data> <Data
Name="UtcTime">2024-01-15 14:32:07.882</Data> <Data
Name="ProcessGuid">{B3A285F2-7C1A-65A5-1F04-000000001A00}</Data> <Data
Name="ProcessId">6284</Data> <Data Name="Image">C:\Windows\System32\cmd.exe</Data> <Data
Name="FileVersion">10.0.19041.1 (WinBuild.160101.0800)</Data> <Data Name="Description">Windows
Command Processor</Data> <Data Name="Product">Microsoft Windows Operating System</Data> <Data
Name="Company">Microsoft Corporation</Data> <Data Name="OriginalFileName">Cmd.Exe</Data> <Data
Name="CommandLine">cmd.exe /c "C:\Users\jdoe\Desktop\tools\mimikatz.exe"</Data> <Data
Name="CurrentDirectory">C:\Users\jdoe\Desktop\tools\</Data> <Data Name="User">ACME\jdoe</Data>
<Data Name="LogonGuid">{B3A285F2-1B2C-65A5-A9B2-0D0000000000}</Data> <Data
Name="LogonId">0xDB2A9</Data> <Data Name="TerminalSessionId">1</Data> <Data
Name="IntegrityLevel">High</Data> <Data
Name="Hashes">SHA256=E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855,MD5=8A2122E8162DE
 <Data Name="ParentProcessGuid">{B3A285F2-1B45-65A5-0E01-000000001A00}</Data> <Data
Name="ParentProcessId">3920</Data> <Data Name="ParentImage">C:\Windows\explorer.exe</Data>
<Data Name="ParentCommandLine">C:\Windows\explorer.exe</Data> <Data
Name="ParentUser">ACME\jdoe</Data> </EventData> </Event> <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="2024-01-15T14:32:08.104Z"/>
<EventRecordID>104833</EventRecordID> <Correlation/> <Execution ProcessID="2844"
```

```
ThreadID="3160"/> <Channel>Microsoft-Windows-Sysmon/Operational</Channel>
<Computer>WORKSTATION-PC12.corp.acme.local</Computer> <Security
UserID="S-1-5-21-3541430928-2051711210-1391384369-1104"/> </System> <EventData> <Data
Name="RuleName">technique_id=T1003.001,technique_name=LSASS Memory</Data> <Data
Name="UtcTime">2024-01-15 14:32:08.097</Data> <Data
Name="ProcessGuid">{B3A285F2-7C1B-65A5-2004-000000001A00}</Data> <Data
Name="ProcessId">7812</Data> <Data Name="Image">C:\Users\jdoe\Desktop\tools\mimikatz.exe</Data>
<Data Name="FileVersion">2.2.0</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\jdoe\Desktop\tools\mimikatz.exe" "privilege::debug"
"sekurlsa::logonpasswords" "exit"</Data> <Data
Name="CurrentDirectory">C:\Users\jdoe\Desktop\tools\</Data> <Data Name="User">ACME\jdoe</Data>
<Data Name="LogonGuid">{B3A285F2-1B2C-65A5-A9B2-0D0000000000}</Data> <Data
Name="LogonId">0xDB2A9</Data> <Data Name="TerminalSessionId">1</Data> <Data
Name="IntegrityLevel">High</Data> <Data
Name="Hashes">SHA256=61C0810A23580CF492A6BA4F7654566108331E7A4134C968C2D6A05261B2D8A1,MD5=A3B5DE47052B4
<Data Name="ParentProcessGuid">{B3A285F2-7C1A-65A5-1F04-000000001A00}</Data> <Data
Name="ParentProcessId">6284</Data> <Data Name="ParentImage">C:\Windows\System32\cmd.exe</Data>
<Data Name="ParentCommandLine">cmd.exe /c "C:\Users\jdoe\Desktop\tools\mimikatz.exe"</Data>
<Data Name="ParentUser">ACME\jdoe</Data> </EventData> </Event> <Event
xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider
Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FFBD9}"/>
<EventID>10</EventID> <Version>3</Version> <Level>4</Level> <Task>10</Task> <Opcode>0</Opc
```

Generated by SOC-AI-Agent | Automated Security Investigation Platform
Report generated at 2026-02-13 04:02:41 UTC