AI-Assisted Investigation Report

Analyst

MalwareLab User

Analysis Time

2026-07-16 19:55:42 (EDT - America/New_York) | 2026-07-16 23:55:42 UTC

Model

gpt-4.1-mini

Version

beta-v2.0

Report Metrics

Input Size: 106.51 KB
IOCs Found: 41
ATT&CK Techniques: 10

Severity

Critical

Confidence

95% - High Confidence

Confidence Factors

• Multiple critical events detected including credential dumping (Mimikatz-like LSASS access)
• Detected shadow copy deletion indicating ransomware activity
• Large outbound data transfer (~700MB) to known-bad external IP 185.220.101.47
• Multiple file encryption events consistent with ransomware behavior (.blackcat extension)
• High severity events showing lateral movement using harvested admin credentials
• Repeated PowerShell executions across multiple hosts indicating possible automated malicious activity

Reducing Factors

• Most PowerShell executions are labeled as baseline or allowed by policy with informational or low severity
• No known malware hashes found in MalwareBazaar or VirusTotal for the uploaded file
• Internal IP addresses involved are reserved/private, reducing confidence in external attacker infrastructure

Threat Type

Ransomware with Credential Dumping and Data Exfiltration

Executive Summary

The log data indicates a sophisticated multi-stage attack involving credential dumping, lateral movement using harvested credentials, ransomware file encryption with .blackcat extension, shadow copy deletion to inhibit recovery, and large data exfiltration to a known malicious external IP. The activity spans multiple hosts and users, with evidence of PowerShell usage for execution and tool staging. This represents a confirmed domain compromise with active ransomware deployment and data theft.

Event Timeline

Initial failed logon attempts and suspicious PowerShell executions precede credential dumping on WKS-FIN-014. Subsequently, lateral movement occurs using harvested admin credentials to remote hosts. Shadow copy deletion and ransomware file encryption follow, accompanied by large data exfiltration to an external IP. The timeline shows a coordinated attack progressing through multiple stages.

2024-06-10T00:06:16.655Z — Multiple failed logon attempts
Several users including schen, kobrien, and helpdesk experience failed logons indicating possible brute force or credential guessing.
Why it matters: Potential initial reconnaissance or credential harvesting activity
Confidence: High

2024-06-11T08:07:33.226Z — Suspicious PowerShell execution from Excel
excel.exe spawns powershell.exe with encoded command indicating download cradle, suggesting initial execution of malicious payload.
Why it matters: Initial execution stage of attack
Confidence: High

2024-06-11T08:36:04.360Z — Credential dumping detected
Suspicious access to lsass.exe memory on WKS-FIN-014 by jsmith, consistent with Mimikatz-like credential dumping.
Why it matters: Credential access stage enabling lateral movement
Confidence: High

2024-06-11T08:44:55.829Z — Privileged admin logon and lateral movement

Event Timeline — continued

Admin user logs on to multiple hosts remotely using harvested credentials, including SRV-DC-01, SRV-FILE-01, SRV-APP-02, SRV-SQL-01, and WKS-EXEC-003.
Why it matters: Lateral movement and privilege escalation
Confidence: High

2024-06-11T09:08:05.733Z — Shadow copy deletion commands executed
Commands to delete shadow copies executed on SRV-FILE-01, indicating ransomware defense evasion.
Why it matters: Defense evasion stage
Confidence: High

2024-06-11T09:13:59.810Z — Large data exfiltration to known-bad IP
Approximately 700MB of archived data uploaded from SRV-FILE-01 to external IP 185.220.101.47.
Why it matters: Data exfiltration stage
Confidence: High

2024-06-11T09:18:15.654Z — Mass file encryption detected
Multiple files encrypted with .blackcat extension across various hosts, consistent with ransomware impact.
Why it matters: Impact stage with ransomware activity
Confidence: High

Timeline Gaps:
• No explicit initial access event such as phishing or exploit observed
• No detailed command line or script content for PowerShell executions to confirm payloads
• No persistence mechanism events such as scheduled tasks or registry modifications detected

Evidence Supporting Assessment

• Event EVT-0011686: Credential dumping detected via suspicious LSASS memory access by user jsmith on WKS-FIN-014
• Event EVT-0011896: Shadow copy deletion commands executed on SRV-FILE-01 by admin user
• Event EVT-0011946: Large outbound upload (~700MB) to IP 185.220.101.47 from SRV-FILE-01 by jsmith
• Multiple critical file encryption events (EVT-0011984 to EVT-0012014) encrypting various files with .blackcat extension
• High severity lateral movement events (EVT-0011740, EVT-0011769, EVT-0011800, EVT-0011861) showing remote logons using harvested admin credentials
• Numerous process_execution events showing powershell.exe started across many hosts and users, some associated with detections such as 'Office spawning PowerShell' and 'Signed binary'

Ambiguity Notes

• No direct evidence of initial access vector is present in the logs
• Some PowerShell executions are marked as baseline or allowed, making it difficult to distinguish benign from

Ambiguity Notes — continued

malicious without command line details
• Internal IP addresses are reserved/private, so external attacker infrastructure is inferred primarily from outbound connections
• No malware hashes or known malicious URLs were found in threat intelligence sources for the uploaded file
• Lack of explicit scheduled task or registry persistence indicators in the provided data

Alternative Hypotheses

• Red team simulation or penetration test involving credential dumping and ransomware simulation
• Controlled lab environment capturing multi-stage ransomware attack behavior
• Malware collection sample used for research or detection tuning

Alternative Explanations

None

Indicators of Compromise

IP Addresses
- 185.220.101.47

Domains
- cdn-sync-update.net

URLs
- https://teams.microsoft.com/
- https://github.com/
- https://slack.com/
- https://intranet.acme.corp/
- https://outlook.office365.com/
- https://sharepoint.acme.corp/
- https://aws.amazon.com/

Hashes
- d895ca8a0ca9442c8009b55129a1ea333be8d159
- d596972fbe90bf7c6d4de8b877775c42a139273cc0ee9cbaddc2158f84c2b13e

Ports
- 443
- 8443
- 53
- 123

Indicators of Compromise — continued

- 46143
- 34258
- 32315
- 37409
- 44521
- 46336

Processes
- powershell.exe
- excel.exe
- locker.exe
- outlook.exe
- svchost.exe
- chrome.exe

Users
- admin
- jsmith
- tturner
- lnguyen
- dlee
- svc_sql
- svc_backup
- kobrien
- bwilson
- helpdesk
- schen
- akhan
- ewright
- rpatel

MITRE ATT&CK Mapping

• T1003.001 - LSASS Memory
• T1490 - Inhibit System Recovery
• T1567.002 - Exfiltration to Cloud
• T1486 - Data Encrypted for Impact
• T1059.001 - PowerShell
• T1071.001 - Web Protocols (C2)
• T1078 - Valid Accounts
• T1021 - Remote Services

MITRE ATT&CK Mapping — continued

• T1570 - Lateral Tool Transfer
• T1489 - Service Stop

Recommended Actions

• Investigate and contain host WKS-FIN-014 for credential dumping and C2 beaconing activity
• Review and isolate SRV-FILE-01 due to shadow copy deletion and data exfiltration events
• Perform forensic analysis on affected hosts WKS-EXEC-003, WKS-HR-007, SRV-APP-02, and SRV-SQL-01 for ransomware impact
• Hunt for presence and execution of locker.exe on remote hosts and remove any persistence mechanisms
• Reset credentials for compromised admin and user accounts including jsmith, admin, tturner, and others involved in lateral movement
• Monitor network traffic for further connections to IP 185.220.101.47 and domain cdn-sync-update.net
• Implement enhanced logging and alerting for PowerShell execution and suspicious remote logons
• Restore affected systems from clean backups after ensuring ransomware eradication

Analyst Notes

None

AI-Assisted Analysis Disclaimer

This report was generated using AI-assisted analysis and is intended to support security investigations. Findings, conclusions, and recommendations should be reviewed and validated by a qualified analyst before operational, legal, or business decisions are made.