AI-Assisted Investigation Report

Analyst

MalwareLab User

Analysis Time

2026-07-16 19:59:13 (EDT - America/New_York) | 2026-07-16 23:59:13 UTC

Model

gpt-4.1-mini

Version

beta-v2.0

Report Metrics

Input Size: 92.07 KB
IOCs Found: 14
ATT&CK Techniques: 10

Severity

Critical

Confidence

95% - High Confidence

Confidence Factors

• Repeated execution of encoded PowerShell commands with -nop -w hidden -enc flags launched by winword.exe indicating likely macro-based execution
• Multiple network connections from powershell.exe to suspicious external IPs including 185.220.101.42 (Tor exit node with 100% abuse confidence) and other data center IPs with some malicious detections
• Numerous Process Access events involving mimikatz.exe accessing lsass.exe with sekurlsa::logonpasswords command indicating credential dumping
• Execution of commands querying local and domain admin groups and domain controllers via cmd.exe spawned from powershell.exe indicating privilege escalation and reconnaissance

Confidence Factors — continued

• Audit Log Cleared events present (event_id 1102) indicating defense evasion
• Suspicious command lines invoking rundll32.exe to load update.dll from public user directory, a common malware persistence or execution technique

Reducing Factors

• No ransomware indicators or critical events explicitly detected in logs
• No known malware hashes found in VirusTotal or MalwareBazaar for uploaded file
• Internal IP addresses involved in some events are reserved/private reducing confidence in external attacker infrastructure for those endpoints

Threat Type

Domain Compromise / Credential Dumping / Privilege Escalation

Executive Summary

The logs show strong evidence of a domain compromise involving macro-enabled document execution leading to PowerShell-based payload execution, credential dumping using mimikatz, and active reconnaissance for privilege escalation. Multiple suspicious network connections to known malicious or Tor exit IPs support ongoing attacker command and control activity. Audit log clearing and use of rundll32 to load DLLs from public user folders indicate defense evasion and persistence attempts.

Event Timeline

Initial macro execution via winword.exe launches encoded PowerShell commands. Powershell.exe then makes multiple network connections to suspicious external IPs including a Tor exit node. Concurrently, mimikatz.exe is executed to dump credentials from lsass.exe. Subsequent cmd.exe processes run domain enumeration commands. Audit logs are cleared, indicating defense evasion. This sequence strongly suggests an active domain compromise with credential theft and privilege escalation.

2024-08-06T00:00:00 — Audit Log Cleared
Event ID 1102 indicates audit log clearing to evade detection
Why it matters: Defense evasion
Confidence: High

2024-08-06T14:15:23 — Suspicious Network Connections from PowerShell
powershell.exe connects to multiple suspicious external IPs including 185.220.101.42 (Tor exit node)
Why it matters: Possible command and control communication
Confidence: High

2024-08-06T15:27:31 — Encoded PowerShell Execution from Word

Event Timeline — continued

powershell.exe launched with encoded command by winword.exe indicating macro-based execution
Why it matters: Initial code execution and payload delivery
Confidence: High

2024-08-06T21:43:11 — Domain Enumeration Commands Executed
cmd.exe spawned by powershell.exe runs net group and nltest commands for domain reconnaissance
Why it matters: Privilege escalation and lateral movement preparation
Confidence: High

2024-08-07T17:27:06 — Credential Dumping with Mimikatz
mimikatz.exe accesses lsass.exe to extract credentials using sekurlsa::logonpasswords
Why it matters: Credential theft and privilege escalation
Confidence: High

Timeline Gaps:
• No direct evidence of lateral movement or persistence mechanisms beyond DLL execution
• No file hashes or artifacts for the update.dll payload
• No scheduled task or registry run key data provided

Evidence Supporting Assessment

• Multiple Process Create events of powershell.exe with encoded commands launched by winword.exe
• Repeated network connections from powershell.exe to IP 185.220.101.42 with 100% abuse confidence and other suspicious IPs
• Numerous Process Access events of mimikatz.exe targeting lsass.exe with sekurlsa::logonpasswords
• Process Create events of cmd.exe executing net localgroup administrators, net group "Enterprise Admins" /domain, nltest /dclist:corp.local, and net user /domain
• Audit Log Cleared events (event_id 1102) observed
• Use of rundll32.exe to execute C:\Users\Public\update.dll repeatedly

Ambiguity Notes

• No direct file artifacts or malware samples provided to confirm payload identity
• Some external IPs have mixed reputation with low to moderate abuse confidence scores
• Absence of explicit ATT&CK technique mappings due to lack of direct telemetry on lateral movement or persistence mechanisms beyond DLL execution
• No explicit scheduled tasks or registry run keys observed in provided data

Alternative Hypotheses

• Red team or penetration testing activity simulating credential dumping and reconnaissance
• Security research or malware analysis environment generating similar telemetry

Alternative Hypotheses — continued

• Compromised user executing legitimate administrative scripts with poor operational security

Alternative Explanations

None

Indicators of Compromise

IP Addresses
- 193.32.162.157
- 45.137.21.9
- 185.220.101.42

Hashes
- 5248a7ddfec96f072af043924c319b7fef2fe369
- 0ffc74f654c944fd1a50958ebea1281fcd0412b40b3fbfe1cc300133ab22a397

Ports
- 53
- 443
- 8443

Processes
- powershell.exe
- winword.exe
- cmd.exe
- mimikatz.exe
- rundll32.exe

Users
- CORP\jtoilolo

MITRE ATT&CK Mapping

• T1059.001 - PowerShell
• T1086 - PowerShell
• T1003.001 - LSASS Memory
• T1057 - Process Discovery
• T1087 - Account Discovery
• T1110 - Brute Force (possible/contextual)
• T1070.001 - Clear Windows Event Logs
• T1204.002 - User Execution: Malicious File

MITRE ATT&CK Mapping — continued

• T1547.001 - Registry Run Keys / Startup Folder (possible/contextual)
• T1105 - Ingress Tool Transfer (possible/contextual)

Recommended Actions

• Investigate all powershell.exe processes launched by winword.exe with encoded commands for malicious payloads
• Review network connections to IPs 185.220.101.42, 193.32.162.157, and 45.137.21.9 for C2 activity and block if confirmed malicious
• Search endpoints for presence of C:\Users\Public\update.dll and analyze for malware
• Audit and monitor use of mimikatz.exe and access to lsass.exe memory on endpoints
• Review and restore cleared audit logs; implement enhanced logging and alerting for event ID 1102
• Conduct thorough domain privilege enumeration and review recent changes to local and domain admin groups
• Perform endpoint forensic analysis on hosts WKS-0016 and WKS-0041 for persistence mechanisms and lateral movement
• Implement network segmentation and restrict PowerShell execution policies to reduce attack surface
• Educate users on risks of enabling macros and implement macro-blocking policies where feasible

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.

