AI-Assisted Investigation Report

Analyst

MalwareLab User

Analysis Time

2026-07-16 19:19:53 (EDT - America/New_York) | 2026-07-16 23:19:53 UTC

Model

gpt-4.1-mini

Version

beta-v2.0

Report Metrics

Input Size: 1.20 KB
IOCs Found: 0
ATT&CK Techniques: 0

Severity

Low

Confidence

20% - Very Low Confidence

Confidence Factors

None

Reducing Factors

• PowerShell script is a standard Windows Update automation script using PSWindowsUpdate module
• No suspicious commands or obfuscation detected
• AbuseIPDB reports zero abuse for IP 2.8.5.201
• VirusTotal shows only 1 malicious detection out of 91 total scans for IP 2.8.5.201, majority are harmless or

Reducing Factors — continued

undetected

Threat Type

Insufficient Evidence

Executive Summary

The provided PowerShell script automates Windows Update installation using a legitimate module and standard commands. The IP address 2.8.5.201 referenced in the script is associated with a known ISP and has minimal malicious detections, insufficient to indicate malicious activity.

Evidence Supporting Assessment

• Script sets TLS 1.2 for secure PowerShell Gallery access
• Script installs and imports PSWindowsUpdate module if not present
• Script adds Microsoft Update service to include Office and other products
• Script creates a log directory and file for update logs
• Script runs Windows Update with parameters to accept all, install, and auto reboot
• IP 2.8.5.201 is referenced as a version number in Install-PackageProvider command, not as a network indicator

Ambiguity Notes

• IP 2.8.5.201 appears in the script as a version number argument, not as an IP address for network communication
• VirusTotal shows one vendor flagged the IP as malicious but majority did not, indicating low confidence in maliciousness
• No dynamic execution, obfuscation, or download-and-execute behavior observed
• No file or process artifacts provided to correlate with malicious activity

Alternative Hypotheses

• Routine administrative script for patch management
• Automated system maintenance task
• Script used in a controlled lab or testing environment

Alternative Explanations

None

Indicators of Compromise

None

MITRE ATT&CK Mapping

None

Recommended Actions

• Verify the source and intent of the PowerShell script within the environment
• Confirm that the PSWindowsUpdate module is obtained from a trusted repository
• Monitor execution of scripts modifying Windows Update settings for unexpected changes

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.

