AI-Assisted Investigation Report

Analyst

MalwareLab User

Analysis Time

2026-07-16 19:22:02 (EDT - America/New_York) | 2026-07-16 23:22:02 UTC

Model

gpt-4.1-mini

Version

beta-v2.0

Report Metrics

Input Size: 916 bytes
IOCs Found: 2
ATT&CK Techniques: 3

Severity

High

Confidence

90% - High Confidence

Confidence Factors

• PowerShell script decodes and executes Base64-encoded commands
• Script flushes DNS cache and clears clipboard, common in malware to evade detection
• PowerShell invokes a web request to a URL with 13 malicious detections on VirusTotal
• Downloaded content is executed dynamically in memory via Invoke-Expression
• User-Agent string mimics a legitimate browser to evade detection

Reducing Factors

None

Threat Type

Downloader / Remote Code Execution

Executive Summary

The analyzed PowerShell script performs DNS cache flushing, clears the clipboard, and downloads remote content from a URL with multiple malicious detections on VirusTotal. The downloaded content is executed dynamically in memory, indicating downloader behavior with remote code execution capabilities.

Evidence Supporting Assessment

• Base64-encoded commands decoded and executed via Invoke-Expression
• Command 'ipconfig /flushdns' executed to flush DNS cache
• Clipboard cleared with Set-Clipboard -Value " "
• Invoke-WebRequest used to download content from https://rtattack.baqebei1.online/KB/CODD
• VirusTotal reports 13 malicious detections for the URL https://rtattack.baqebei1.online/KB/CODD
• Downloaded content executed dynamically using IEX ([System.Text.Encoding]::UTF8.GetString($z04Q.Content))

Ambiguity Notes

• URL not found in URLHaus but found with multiple malicious detections on VirusTotal
• No direct visibility into the downloaded payload content to confirm full behavior
• No digital signature or file metadata available for further context

Alternative Hypotheses

• Red team or penetration testing activity using obfuscated PowerShell downloader
• Security research or malware analysis sample
• Controlled laboratory sample for malware behavior study

Alternative Explanations

None

Indicators of Compromise

Domains
- rtattack.baqebei1.online

Indicators of Compromise — continued

URLs
- https://rtattack.baqebei1.online/KB/CODD

MITRE ATT&CK Mapping

• T1059.001 - PowerShell
• T1105 - Ingress Tool Transfer
• T1204.002 - User Execution: Malicious File

Recommended Actions

• Investigate any execution of PowerShell scripts containing Base64 decoding and Invoke-Expression
• Monitor and block network connections to rtattack.baqebei1.online and related domains
• Search for processes or scheduled tasks invoking PowerShell with encoded commands
• Review DNS cache flush events and clipboard clearing activity for suspicious patterns
• Perform endpoint detection and response (EDR) hunting for similar downloader behavior

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.

