INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-17 14:04 UTC

Dragon Boss Adware Evolves Into AV Killer: Scheduled Task Persistence and Defender Exclusions Signal Intent Shift

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0183
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows (Scheduled Task Subsystem), Windows Defender
Published	2026-04-16T15:07:26
Discovery Source	Rss

Executive Summary

The Dragon Boss adware family, previously limited to ad fraud, gained two significant new capabilities in March 2025: scheduled task persistence and programmatic Windows Defender exclusions. These additions reposition Dragon Boss as a likely loader or dropper platform capable of delivering follow-on malware while evading standard endpoint detection. Organizations relying on Windows Defender as a primary endpoint detection control face materially higher risk of undetected compromise and subsequent payload deployment.

Technical Analysis

In March 2025, Dragon Boss adware was updated to include two capability additions that signal an operational shift beyond ad fraud. First, the malware registers scheduled tasks (MITRE T1053.005) to survive reboots and user-level remediation attempts, consistent with techniques documented in the Tarrask campaign (Microsoft Security Blog, April 2022). Second, it programmatically adds exclusions to Windows Defender (MITRE T1562.001), neutralizing endpoint detection for subsequently dropped payloads. Additional mapped techniques include T1547 (Boot/Logon Autostart Execution), T1105 (Ingress Tool Transfer, consistent with loader staging), and T1036 (Masquerading). CWE classifications: CWE-693 (Protection Mechanism Failure) and CWE-284 (Improper Access Control). No CVE has been assigned; this is a malware capability evolution, not a software vulnerability. No patch exists. Affected components are the Windows Scheduled Task Subsystem and Windows Defender exclusion policy. Dragon Boss attribution is based on security vendor reporting and threat intelligence community consensus; independent confirmation of campaign continuity and actor identity is limited. Validation

of capability evolution details from primary threat intelligence sources is recommended as additional reporting emerges.

Action Checklist

1. Step 1: Containment, Identify Windows endpoints where Windows Defender is the primary endpoint detection control, particularly those without supplementary EDR solutions. Isolate any host exhibiting unauthorized scheduled task creation or Defender exclusion additions pending investigation. Prioritize internet-facing and high-value asset segments first.
2. Step 2: Detection, Query Windows Event Log for Scheduled Task creation events (Event ID 4698) and Defender exclusion modifications (Event ID 5007 in Microsoft-Windows-Windows Defender/Operational log). Hunt for tasks with randomized or non-standard names in HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache and for PowerShell or cmd.exe invocations of 'Add-MpPreference -ExclusionPath'. Cross-reference against MITRE T1053.005 and T1562.001 behavioral patterns.
3. Step 3: Eradication, Remove unauthorized scheduled tasks via Task Scheduler or schtasks.exe. Audit and remove unauthorized Windows Defender exclusions via 'Get-MpPreference | Select-Object ExclusionPath' and 'Remove-MpPreference -ExclusionPath'. Deploy or verify a secondary EDR solution on Defender-only endpoints to close the detection gap Dragon Boss is designed to exploit.
4. Step 4: Recovery, After task and exclusion removal, run a full Windows Defender scan with exclusions cleared. Validate no follow-on payloads were staged or executed by reviewing process creation logs (Event ID 4688) for unusual child processes spawned by the scheduled task. Monitor for task re-creation attempts for at least 72 hours post-remediation.
5. Step 5: Post-Incident, This campaign exposes a systemic control gap: single-layer endpoint defense. Evaluate deployment of a complementary EDR product alongside Defender. Establish alerting on Defender exclusion modifications as a standing detection rule. Review scheduled task baselines and implement allowlisting for approved tasks where feasible. Document the gap for the next risk assessment cycle.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to senior IR leadership and legal/compliance if Event ID 4688 analysis confirms a follow-on payload executed under the Dragon Boss scheduled task context on any host processing PII, PHI, or financial data, as this elevates the incident from adware persistence to potential data breach requiring regulatory notification assessment.
Recovery Notes	After removing Dragon Boss scheduled tasks and Defender exclusions, run a full Defender scan with clean exclusion configuration and verify zero detections in the previously excluded paths before returning hosts to production. Monitor Security Event Log Event ID 4698 and Defender Operational Event ID 5007 continuously for at least 72 hours post-remediation to detect Dragon Boss re-persistence attempts, which may indicate a deeper dropper or a second-stage component not yet identified. Validate process creation logs (Event ID 4688) for the full window between Dragon Boss's first observed activity and eradication to confirm no follow-on payload achieved execution before containment.

Forensic Artifacts	Microsoft-Windows-Windows Defender/Operational EVTX — Event ID 5007 entries recording the specific ExclusionPath values Dragon Boss programmatically added via Add-MpPreference, including timestamps and the process context that made the change. | Windows Security EVTX — Event ID 4698 (Scheduled Task Created) XML bodies containing Dragon Boss task names (typically randomized or masquerading as legitimate software), trigger definitions, action executable paths, and the registering account context. | Registry hive export of HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks and TaskCache\Tree — preserves Dragon Boss task GUIDs, action binaries, and trigger configuration verbatim before eradication disturbs the keys. | File system contents and hash inventory of directories Dragon Boss added to Defender exclusions — these paths are the designated staging areas for follow-on payloads and are the most likely locations for delivered loader or dropper binaries. | PowerShell Operational EVTX — Event ID 4104 (Script Block Logging) capturing the full Add-MpPreference -ExclusionPath command as executed by Dragon Boss, including the exact exclusion path argument, enabling IOC extraction and scope confirmation across the environment.

Per-Action IR Details

Step 1: Containment — Identify Windows endpoints where Windows Defender is the primary or sole endpoint detection control. Isolate any host exhibiting unauthorized scheduled task creation or Defender exclusion additions pending investigation. Prioritize internet-facing and high-value asset segments first.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'Get-MpComputerStatus | Select-Object AMProductVersion,RealTimeProtectionEnabled,AMServiceEnabled' via PowerShell remoting across the environment to enumerate Defender-only hosts. For isolation without an EDR quarantine function, use Windows Firewall to block all outbound traffic except necessary ports: 'netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound' — stage this as a pre-approved script for rapid deployment by one analyst while the second handles triage.

Evidence: Before isolating, snapshot the current Defender exclusion list via 'Get-MpPreference | Select-Object ExclusionPath,ExclusionProcess,ExclusionExtension' and export to a timestamped file. Capture the live scheduled task registry hive at 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks' and 'TaskCache\Tree' using 'reg export' to preserve task GUIDs and action metadata before any remediation disturbs them. Record Windows Security Event Log Event ID 4698 (Scheduled Task Created) and Microsoft-Windows-Windows Defender/Operational Event ID 5007 (Configuration Changed) timestamps to establish a Dragon Boss activity timeline.

Step 2: Detection — Query Windows Event Log for Scheduled Task creation events (Event ID 4698) and Defender exclusion modifications (Event ID 5007 in Microsoft-Windows-Windows Defender/Operational log). Hunt for tasks with randomized or non-standard names in HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache and for PowerShell or cmd.exe invocations of 'Add-MpPreference -ExclusionPath'. Cross-reference against MITRE T1053.005 and T1562.001 behavioral patterns.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy Sysmon with a config capturing Event ID 1 (Process Create) to detect 'powershell.exe' or 'cmd.exe' spawning with 'Add-MpPreference' or 'schtasks /create' arguments — use the SwiftOnSecurity or Olaf Hartong Sysmon config as a baseline. For scheduled task hunting without a SIEM, run: 'Get-ScheduledTask |

Where-Object {$_.TaskPath -notlike "\Microsoft*"} | Select-Object TaskName,TaskPath,@{N="Actions";E={$_.Actions.Execute}}' to surface non-Microsoft tasks with executable actions. Apply the public Sigma rule 'win_scheduled_task_creation_via_at.yml' and community rules targeting T1562.001 (Add-MpPreference exclusion) using Chainsaw or Hayabusa against collected EVTX files.

Evidence: Collect and preserve: (1) Microsoft-Windows-Windows Defender/Operational EVTX log — Event ID 5007 entries will contain the specific ExclusionPath value Dragon Boss added, appearing as 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\ = 0x0'. (2) Windows Security EVTX — Event ID 4698 XML body contains the full task XML including trigger type, action executable path, and the account context under which the task was registered. (3) PowerShell Script Block Logging (Event ID 4104 in Microsoft-Windows-PowerShell/Operational) for the 'Add-MpPreference' invocation, which will capture the full command including the exclusion path argument passed by Dragon Boss.

Step 3: Eradication — Remove unauthorized scheduled tasks via Task Scheduler or schtasks.exe. Audit and remove unauthorized Windows Defender exclusions via 'Get-MpPreference | Select-Object ExclusionPath' and 'Remove-MpPreference -ExclusionPath'. Deploy or verify a secondary EDR solution on Defender-only endpoints to close the detection gap Dragon Boss is designed to exploit.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST CM-6 (Configuration Settings), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Remove each Dragon Boss scheduled task with: 'schtasks /delete /tn "" /f' — capture the task name from the TaskCache registry export taken pre-containment. Enumerate and remove each Defender exclusion added by Dragon Boss: 'Get-MpPreference | Select-Object -ExpandProperty ExclusionPath | ForEach-Object { Remove-MpPreference -ExclusionPath $_ }' — execute only after confirming exclusion list against your known-good baseline. For secondary detection layer without budget, deploy Malwarebytes Free or ClamAV with a manual scan triggered immediately after exclusion removal to catch any follow-on payload Dragon Boss may have staged in the now-excluded directory.

Evidence: Before removing the scheduled task, export its full XML definition: 'schtasks /query /tn "" /xml > task_evidence_.xml' — this preserves the Dragon Boss persistence mechanism verbatim for threat intel and legal hold. Before removing Defender exclusions, document the exact exclusion paths Dragon Boss added (from Event ID 5007 and Get-MpPreference output) as these paths are the staging locations where follow-on payloads were likely written and may contain active malware samples for analysis.

Step 4: Recovery — After task and exclusion removal, run a full Windows Defender scan with exclusions cleared. Validate no follow-on payloads were staged or executed by reviewing process creation logs (Event ID 4688) for unusual child processes spawned by the scheduled task. Monitor for task re-creation attempts for at least 72 hours post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Run the full Defender scan via: 'Start-MpScan -ScanType FullScan' and monitor completion with 'Get-MpThreatDetection'. For process lineage analysis without EDR, query Security Event Log Event ID 4688 (requires 'Audit Process Creation' policy enabled) filtering for parent processes matching the Dragon Boss task's action executable — use PowerShell: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688} | Where-Object {$_.Message -like "**"}'. Set a 72-hour Sysmon-based watchdog: monitor Event ID 12/13 (Registry value set) on 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache' and Sysmon Event ID 1 for 'schtasks.exe /create' to catch Dragon Boss re-dropping its persistence mechanism.

Evidence: During recovery validation, preserve: (1) The Defender scan report showing any detections in the previously excluded path — this confirms whether a follow-on payload was successfully staged before remediation. (2) Event ID 4688 process creation log filtered on the task's action executable as the parent process, covering the period from

Dragon Boss's first observed activity to the point of eradication — any child processes here represent potential payload execution. (3) File system artifacts in the directories Dragon Boss excluded from Defender — these paths are the high-probability staging locations; use 'Get-ChildItem -Path -Recurse | Select-Object FullName,CreationTime,LastWriteTime' to enumerate and hash all files for malware analysis.

Step 5: Post-Incident — This campaign exposes a systemic control gap: single-layer endpoint defense. Evaluate deployment of a complementary EDR product alongside Defender. Establish alerting on Defender exclusion modifications as a standing detection rule. Review scheduled task baselines and implement allowlisting for approved tasks where feasible. Document the gap for the next risk assessment cycle.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-4 (System Monitoring), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: Implement a standing detection for Dragon Boss re-emergence or similar AV-killer adware using a Sigma rule targeting Event ID 5007 with keyword 'ExclusionPath' in the Defender Operational log — publish to Hayabusa or Chainsaw for periodic log sweeps if no SIEM exists. Establish a scheduled task baseline by exporting all current approved tasks: 'Get-ScheduledTask | Export-Clixml -Path .\task_baseline_.xml' and diff against this file weekly using 'Compare-Object'. For the risk register entry, document the Dragon Boss capability shift — adware-to-loader — as a threat intelligence finding referencing MITRE T1053.005 and T1562.001, with the single-layer Defender dependency flagged as an accepted risk requiring executive sign-off.

Evidence: Post-incident, collect and retain: (1) The full incident timeline reconstructed from Event IDs 4698 and 5007, correlating Dragon Boss task creation to exclusion addition to any subsequent payload staging — this establishes dwell time and blast radius for the lessons-learned report. (2) The pre- and post-remediation Defender exclusion lists as documented evidence of the control gap. (3) Any Dragon Boss binary or dropper samples recovered from the staging path for submission to VirusTotal or an internal threat intel platform to track hash-based IOCs and monitor for variant evolution.

Detection Guidance

Primary detection targets: (1) Windows Security Event ID 4698 (scheduled task created), filter for tasks created outside standard provisioning windows or by unexpected processes. (2) Microsoft-Windows-Windows Defender/Operational Event ID 5007, log entries indicating exclusion path additions, particularly those added programmatically via PowerShell (Add-MpPreference). (3) PowerShell ScriptBlock logging (Event ID 4104), hunt for 'Add-MpPreference -ExclusionPath' or 'Set-MpPreference' with exclusion parameters. (4) Process creation logs (Event ID 4688 or Sysmon Event ID 1), look for schtasks.exe or at.exe spawned by non-administrative, unexpected parent processes. Behavioral indicator: a process that creates a scheduled task AND modifies Defender exclusions in close temporal proximity is a high-confidence signal. No confirmed IOC hashes, domains, or IPs are available in current sources; IOC list is empty pending higher-confidence reporting. This guidance emphasizes behavioral detection because file-based IOCs are unavailable. Organizations without behavioral detection capabilities (e.g., scheduled task alerting, Defender exclusion monitoring) cannot currently detect Dragon Boss activity.

Framework Mappings

MITRE-ATTACK

- **T1053.005** — Scheduled Task

- **T1547** — Boot or Logon Autostart Execution
- **T1562.001** — Disable or Modify Tools
- **T1105** — Ingress Tool Transfer
- **T1036** — Masquerading

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1053.005	Scheduled Task	Execution
T1547	Boot or Logon Autostart Execution	Persistence
T1562.001	Disable or Modify Tools	Defense-Evasion

Technique ID	Technique Name	Tactic
T1105	Ingress Tool Transfer	Command-And-Control
T1036	Masquerading	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/harmless-glo...	T3
Antivirus, taskscheduler malware : r/WindowsHelp - Reddit	https://www.reddit.com/r/WindowsHelp/comments/1pxtd7n/antivirus_tas...	T3
Tarrask malware uses scheduled tasks for defense evasion - Microsoft	https://www.microsoft.com/en-us/security/blog/2022/04/12/tarrask-ma...	T1
Defender recognizes my scheduled task as malicious - Super User	https://superuser.com/questions/1859965/defender-recognizes-my-sche...	T3
New Windows Task Scheduler Bugs Let Attackers Bypass UAC and ...	https://thehackernews.com/2025/04/experts-uncover-four-new-privileg...	T3

Generated 2026-04-17 14:04 UTC by TJS Security Command Center