INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-21 06:13 UTC

ClickOnce as a Persistence Platform: Why .appref-ms Files Deserve the Same Scrutiny as Macros

THREAT CAMPAIGN | MEDIUM | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0527
Type	Threat Campaign
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Microsoft Windows (ClickOnce deployment framework, dfsvc.exe, rundll32.exe); all Windows versions supporting ClickOnce
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike researchers have documented active threat actor abuse of Microsoft's ClickOnce deployment framework, a legitimate Windows application delivery mechanism, to install malware, maintain persistent access, and receive covert updates, all without elevated privileges or triggering most endpoint security tools. Attackers exploit the trusted process trees of dfsvc.exe and rundll32.exe alongside file types (.application, .appref-ms) that most security tools treat as benign, creating a detection gap that persists even in well-defended environments. Organizations running Windows across any version are exposed; the primary business risk is undetected, long-term attacker presence on corporate endpoints.

Technical Analysis

CrowdStrike Part 2 research (published June 18, 2026) details how adversaries weaponize Microsoft's ClickOnce deployment stack to achieve persistence and command-and-control without spawning suspicious process trees. The attack chain abuses dfsvc.exe (the ClickOnce deployment service) and rundll32.exe (T1218.011) to execute malicious payloads delivered via .application manifests or .appref-ms shortcut files. Persistence is established through Run key modifications (T1547.001) and event-triggered execution (T1546), with scheduled tasks (T1053.005) also in scope per the mapped technique set. Malware updates are pulled via ingress tool transfer (T1105) over standard HTTP/S (T1071.001), blending with legitimate ClickOnce update traffic. Initial access relies on spearphishing links (T1566.002) and user execution of malicious files (T1204.002), with masquerading (T1036.005) facilitated by the inherently trusted appearance of ClickOnce manifests. No CVE is assigned; the weakness is architectural, mapped to CWE-693 (Protection Mechanism Failure,

ClickOnce's trust model grants execution without adequate verification) and CWE-494 (Download of Code Without Integrity Check, ClickOnce update mechanisms do not enforce signing validation in all configurations). Microsoft has released Group Policy controls and manifest signing enforcement options in recent Windows versions; however, legacy deployments and permissive configurations remain vulnerable. Affected scope: all Windows versions with ClickOnce support enabled.

Action Checklist

1. Step 1: Containment, Audit all endpoints for .appref-ms files and unsigned .application manifests in user-writable paths (AppData, Temp, Downloads). Identify any dfsvc.exe process trees spawning unusual child processes and isolate affected hosts. Block delivery of .application and .appref-ms attachments at email gateway and web proxy immediately. Reference: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices).
2. Step 2: Detection, Query endpoint telemetry for dfsvc.exe spawning cmd.exe, powershell.exe, wscript.exe, or any non-Microsoft executable. Monitor rundll32.exe (T1218.011) invocations with unusual command-line arguments loading network-retrieved DLLs. Search Windows Event Logs for new Run key entries (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) created by dfsvc.exe or its children. Alert on outbound HTTP/S from dfsvc.exe to non-Microsoft domains. Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs). D3FEND countermeasure: D3-SFA (System File Analysis) for manifest and .appref-ms file monitoring; D3-LAM (Local Account Monitoring) for Run key persistence artifacts.
3. Step 3: Eradication, Remove all identified malicious .appref-ms and .application files. Purge associated Run key entries and scheduled tasks created by the attack chain. Revoke and rotate any credentials accessed by identified malicious processes (D3-CRO: Credential Rotation). Disable ClickOnce for user accounts that do not require it via Group Policy (Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Security Zones, restrict ClickOnce execution from internet zone). Reference: NIST CM (Configuration Management family), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 2.3 (Address Unauthorized Software).
4. Step 4: Recovery, Validate that dfsvc.exe no longer spawns anomalous child processes across the environment. Confirm Run key and scheduled task artifacts are cleared via endpoint inventory. Re-scan affected hosts with updated detection rules tuned to ClickOnce abuse patterns. Monitor outbound traffic from ClickOnce process trees for 30 days post-remediation. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting).
5. Step 5: Post-Incident, Add .application and .appref-ms file types to email attachment block lists and web proxy deny lists as a permanent policy change. Implement application allowlisting to prevent unsigned ClickOnce manifests from executing (D3-SICA: System Init Config Analysis). Tune EDR rules to alert on dfsvc.exe and rundll32.exe anomalous behavior patterns documented in the CrowdStrike research series. Conduct a control gap review against NIST AC-3 (Access Enforcement) and NIST AC-6 (Least Privilege) to assess whether users have broader execution rights than necessary. Reference: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process).

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance if any identified dfsvc.exe child process accessed credential stores (LSASS memory, Windows Credential Manager, browser credential databases), if the ClickOnce payload contacted external C2 infrastructure indicating active data exfiltration, or if affected hosts store PII/PHI/PCI-scoped data triggering regulatory breach notification obligations.
Recovery Notes	Post-containment, verify that the ClickOnce application cache directory (`%LOCALAPPDATA%\Apps\2.0\`) is fully purged on all remediated hosts and that GPO or AppLocker policy blocking unsigned ClickOnce manifests from internet-zone sources has propagated and is confirmed via `gpresult /r`. Monitor Sysmon Event ID 1 for dfsvc.exe parent-child process relationships and Windows Security Event IDs 5156/5158 for outbound connections from dfsvc.exe for a minimum of 30 days, given that ClickOnce's built-in update mechanism could re-download and re-execute a payload from a still-active deployment server if the original .appref-ms shortcut or Run key entry was not fully eradicated. Pay particular attention to re-emergence of .appref-ms files in user profile startup paths, which would indicate a surviving update schedule or a missed delivery vector.
Forensic Artifacts	ClickOnce application cache directory at `%LOCALAPPDATA%\Apps\2.0\` — contains installed ClickOnce application directories with XML deployment manifests naming the deployment URL, publisher certificate (or unsigned state), and update endpoint; primary artifact for identifying the malicious application source and C2 infrastructure | Windows Security Event Log Event ID 4688 (Process Creation with command-line auditing enabled) — captures the full dfsvc.exe → cmd.exe/powershell.exe/wscript.exe process lineage with command-line arguments, directly evidencing the ClickOnce abuse execution chain | Registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `RunOnce` hive exports — documents persistence entries created by dfsvc.exe children using the user-writable HKCU hive, which ClickOnce payloads exploit specifically because write access does not require elevation | Zone.Identifier alternate data stream on .appref-ms and .application files (readable via `Get-Content -Stream Zone.Identifier`) — confirms internet-zone origin (ZoneId=3) of the ClickOnce delivery file, establishing the delivery vector and distinguishing attacker-planted files from legitimate internal ClickOnce deployments | Sysmon Event ID 13 (Registry Value Set) logs filtered on TargetObject matching `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` with Image path under `%LOCALAPPDATA%\Apps\2.0\` — directly ties the Run key persistence write event to the specific ClickOnce-installed malicious application process, providing timestamped forensic evidence of the persistence establishment action

Per-Action IR Details

Step 1: Containment — Audit all endpoints for .appref-ms files and unsigned .application manifests in user-writable paths (AppData, Temp, Downloads). Identify any dfsvc.exe process trees spawning unusual child processes and isolate affected hosts. Block delivery of .application and .appref-ms attachments at email gateway and web proxy immediately. Reference: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices).

NIST Phase: Containment

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

Controls: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run `Get-ChildItem -Path $env:APPDATA,$env:TEMP,$env:USERPROFILE\Downloads -Recurse -Include *.appref-ms,*.application -ErrorAction SilentlyContinue` across endpoints via PSRemoting or a startup script to enumerate ClickOnce files. Deploy Sysmon Event ID 1 (Process Create) filtered on ParentImage=dfsvc.exe to a central log share; review for cmd.exe, powershell.exe, or wscript.exe children. Block .application and .appref-ms MIME

types (application/x-ms-application) at the email gateway via transport rule or content-type filter; add URL pattern `//*.application` and `//*.appref-ms` to web proxy deny list.

Evidence: Before isolating any host, acquire: (1) full RAM image using WinPmem or DumpIt to capture dfsvc.exe in-memory decoded manifest content and any injected DLL artifacts; (2) live process tree snapshot via `Get-Process | Select-Object Id,Name,Path,StartTime` and `Get-WmiObject Win32_Process | Select-Object ProcessId,Name,CommandLine,ParentProcessId`; (3) live network connections via `Get-NetTCPConnection | Where-Object {$_.OwningProcess -eq (Get-Process dfsvc).Id}` to identify active C2 channels from the ClickOnce process tree; (4) on-disk snapshot of `%LOCALAPPDATA%\Apps\2.0\` (ClickOnce application cache directory) and `%APPDATA%\Microsoft\Windows\Start Menu\Programs\` for .appref-ms shortcuts before any file removal.

Step 2: Detection — Query endpoint telemetry for dfsvc.exe spawning cmd.exe, powershell.exe, wscript.exe, or any non-Microsoft executable. Monitor rundll32.exe (T1218.011) invocations with unusual command-line arguments loading network-retrieved DLLs. Search Windows Event Logs for new Run key entries (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) created by dfsvc.exe or its children. Alert on outbound HTTP/S from dfsvc.exe to non-Microsoft domains. Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs). D3FEND countermeasure: D3-SFA (System File Analysis) for manifest and .appref-ms file monitoring; D3-LAM (Local Account Monitoring) for Run key persistence artifacts.

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), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config; Event ID 1 (Process Create) with ParentImage containing dfsvc.exe surfaces anomalous child spawns. Use Sysmon Event ID 13 (Registry Value Set) filtering on TargetObject containing `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and Image=dfsvc.exe or its known children to catch Run key persistence. Query Windows Security Event Log Event ID 4688 (Process Creation, with command-line auditing enabled via `auditpol /set /subcategory:'Process Creation' /success:enable`) for the same parent-child chain. For network detection, run Wireshark or tcpdump on the host capturing traffic from dfsvc.exe PID; filter on `http.host not contains 'microsoft.com' and http.host not contains 'windows.net'` as a heuristic for non-Microsoft C2 callbacks.

Evidence: This is a detection/analysis step that does not itself alter live state; however, capture before any downstream containment action: (1) Windows Security Event Log Event ID 4688 entries showing dfsvc.exe process creation lineage; (2) Sysmon Event ID 1 and 13 XML exports for the incident timeframe; (3) Registry export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce` for all affected user profiles; (4) ClickOnce deployment manifest files at `%LOCALAPPDATA%\Apps\2.0\` — these XML manifests contain the publisher signature (or absence thereof), deployment URL, and update endpoint, which are primary indicators of malicious ClickOnce abuse; (5) Windows DNS client cache via `ipconfig /displaydns` to surface domains contacted by dfsvc.exe before cache flush.

Step 3: Eradication — Remove all identified malicious .appref-ms and .application files. Purge associated Run key entries and scheduled tasks created by the attack chain. Revoke and rotate any credentials accessed by identified malicious processes (D3-CRO: Credential Rotation). Disable ClickOnce for user accounts that do not require it via Group Policy (Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Security Zones — restrict ClickOnce execution from internet zone). Reference: NIST CM (Configuration Management family), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 2.3 (Address Unauthorized Software).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 2.3 (Address Unauthorized Software)

Compensating: Delete malicious .appref-ms files and purge the full ClickOnce application cache under `%LOCALAPPDATA%\Apps\2.0\` for affected user profiles using `Remove-Item -Recurse -Force`. Remove Run key persistence entries via `reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v /f`. Enumerate and remove scheduled tasks created in the attack window via `Get-ScheduledTask | Where-Object {$_.Date -ge ''}` and remove with `Unregister-ScheduledTask`. Rotate credentials for all accounts whose LSASS process memory was accessible to dfsvc.exe children (any process running in the same user session). Apply GPO to set `HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Security\Internet` zone ClickOnce restriction, or set the URLAction DWORD for zone 3 (Internet) to disable ClickOnce execution.

Evidence: BEFORE revoking credentials or removing files, capture: (1) full volatile memory image (WinPmem) to preserve any in-memory credential material or decoded payload staged by dfsvc.exe children; (2) export the full scheduled task XML corpus via `Get-ScheduledTask | Export-ScheduledTask` for all tasks modified or created during the attack window; (3) registry hive export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `RunOnce`, and `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run` before deletion; (4) file system metadata (creation/modification timestamps, zone identifier alternate data streams) of all identified .appref-ms and .application files using `Get-Item | Select-Object FullName,CreationTime,LastWriteTime` and `Get-Content -Stream Zone.Identifier` to confirm internet-sourced delivery.

Step 4: Recovery — Validate that dfsvc.exe no longer spawns anomalous child processes across the environment. Confirm Run key and scheduled task artifacts are cleared via endpoint inventory. Re-scan affected hosts with updated detection rules tuned to ClickOnce abuse patterns. Monitor outbound traffic from ClickOnce process trees for 30 days post-remediation. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 — note: SI-4 is referenced in the NIST 800-53r5 knowledge base family list but the specific control text was not included in the loaded reference set; omit this citation and flag as no mapped control from loaded data.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Validate dfsvc.exe behavior continuously using a Sysmon Event ID 1 filter scheduled via Task Scheduler to run `Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Sysmon/Operational';Id=1} | Where-Object {$_.Message -match 'dfsvc.exe'}` daily and output to a CSV for manual review by the 2-person team. Confirm Run key and scheduled task clearance by re-running the registry export and scheduled task enumeration commands from the eradication step and diffing against a known-clean baseline. For network monitoring, configure Windows Firewall auditing (`auditpol /set /subcategory:'Filtering Platform Connection' /success:enable`) and review Security Event Log Event IDs 5156/5158 for dfsvc.exe outbound connections to non-Microsoft IP ranges for 30 days.

Evidence: Capture before and after recovery validation to confirm clean state: (1) re-run `Get-ChildItem -Path $env:LOCALAPPDATA\Apps\2.0\ -Recurse` to verify ClickOnce cache is cleared of malicious application directories; (2) collect a fresh Sysmon Event ID 1 process tree export post-remediation as a clean baseline for comparison against the pre-remediation export; (3) DNS query logs from the local resolver or Windows Event ID 5156 network connection logs confirming absence of known malicious domains contacted during the ClickOnce abuse campaign; (4) re-export registry Run keys for all remediated user profiles to confirm persistence artifacts are not re-established (indicating potential missed .appref-ms file or surviving scheduled update mechanism).

Step 5: Post-Incident — Add .application and .appref-ms file types to email attachment block lists and web proxy deny lists as a permanent policy change. Implement application allowlisting to prevent unsigned ClickOnce manifests from executing (D3-UAP: User Account Permissions). Tune EDR rules to alert on dfsvc.exe and rundll32.exe anomalous behavior patterns documented in the CrowdStrike research series. Conduct a control gap review against NIST AC-3 (Access Enforcement) and NIST AC-6 (Least Privilege) to assess whether users have broader execution rights than necessary. Reference: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process).

NIST Phase: Post Incident

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Implement application allowlisting via Windows Software Restriction Policies or AppLocker (available without EDR) with a rule explicitly blocking execution of unsigned .application manifests and .appref-ms files from user-writable paths: `New-AppLockerPolicy -RuleType Publisher -FilePath '%LOCALAPPDATA%\Apps\' -Action Deny` scoped to unsigned publishers. Write a YARA rule targeting .appref-ms files with no Authenticode signature block and deploy via scheduled scan with ClamAV or Windows Defender CLI (`MpCmdRun.exe -Scan -ScanType 3`). Add a Sigma rule detecting `ParentImage: *\dfsvc.exe` with `Image` matching `*\cmd.exe`, `*\powershell.exe`, or `*\wscript.exe` to Windows Event Log-based alerting. For the control gap review, enumerate user token privileges via `whoami /priv` on representative workstations and identify accounts with SeDebugPrivilege or other unnecessary privileges that would amplify ClickOnce payload reach.

Evidence: No live volatile state is altered in this phase; evidence focus shifts to documentation: (1) lessons-learned record documenting the initial .appref-ms delivery vector, dfsvc.exe process chain observed, and Run key persistence mechanism for threat intel sharing; (2) final artifact inventory of all identified malicious .application manifest URLs and associated ClickOnce deployment endpoints extracted from `%LOCALAPPDATA%\Apps\2.0\` manifests, suitable for IOC distribution; (3) before-and-after policy export confirming email gateway and proxy block rules for .application/.appref-ms MIME types are active; (4) AppLocker or SRP policy export confirming unsigned ClickOnce manifest execution is blocked as a permanent control.

Detection Guidance

Primary detection focus: anomalous process trees rooted at dfsvc.exe or rundll32.exe. Key behavioral indicators from the CrowdStrike research: (1) dfsvc.exe spawning cmd.exe, powershell.exe, wscript.exe, mshta.exe, or any third-party executable, this process relationship is not expected in legitimate ClickOnce deployments; (2) rundll32.exe (T1218.011) loading DLLs from AppData or Temp directories, particularly following dfsvc.exe execution; (3) new entries written to HKCU\Software\Microsoft\Windows\CurrentVersion\Run by dfsvc.exe or child processes (T1547.001); (4) outbound HTTP/S connections from dfsvc.exe to non-Microsoft, non-CDN infrastructure, legitimate ClickOnce updates target vendor-controlled endpoints; (5) .appref-ms files created in user-writable directories (Downloads, Desktop, Temp) shortly after email link clicks or browser downloads (T1566.002, T1204.002); (6) scheduled tasks (T1053.005) created with actions referencing AppData paths or ClickOnce deployment directories. Log sources to prioritize: Windows Security Event Log (process creation events 4688 with command-line auditing enabled), Sysmon Event ID 1 (process creation) and Event ID 11 (file creation) filtered to .appref-ms and .application extensions, EDR telemetry with parent-child process chain analysis, proxy logs filtered for dfsvc.exe user-agent strings connecting to non-Microsoft hosts. D3FEND countermeasures: D3-SFA (System File Analysis) applied to ClickOnce manifest directories; D3-LAM (Local Account Monitoring) for persistence artifact discovery; D3-SICA (System Init Config Analysis) for Run key and scheduled task monitoring.

Framework Mappings

MITRE-ATTACK

- **T1053.005** — Scheduled Task
- **T1204.002** — Malicious File
- **T1036.005** — Match Legitimate Resource Name or Location

- **T1546** — Event Triggered Execution
- **T1071.001** — Web Protocols
- **T1218.011** — Rundll32
- **T1105** — Ingress Tool Transfer
- **T1566.002** — Spearphishing Link
- **T1547.001** — Registry Run Keys / Startup Folder

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1053.005	Scheduled Task	Execution
T1204.002	Malicious File	Execution
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1546	Event Triggered Execution	Privilege-Escalation
T1071.001	Web Protocols	Command-And-Control
T1218.011	Rundll32	Defense-Evasion
T1105	Ingress Tool Transfer	Command-And-Control
T1566.002	Spearphishing Link	Initial-Access
T1547.001	Registry Run Keys / Startup Folder	Persistence

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/new-abuse-of-the-clickonce-t...	T3
	https://www.crowdstrike.com/en-us/blog/crowdstrike-signal-transform...	T3
	https://www.crowdstrike.com/en-us/blog/av-comparatives-awards-for-e...	T3
	https://www.crowdstrike.com/en-us/blog/why-small-businesses-choose-...	T3
New Abuse of the ClickOnce Technology: Part 1 - CrowdStrike	https://www.crowdstrike.com/content/crowdstrike-www/locale-sites/us...	T3

Generated 2026-06-21 06:13 UTC by TJS Security Command Center