INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-20 13:35 UTC

ClickOnce Weaponized: How Attackers Turn Microsoft's Deployment Tool Into a Persistent Backdoor

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0524
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Windows (ClickOnce framework, .application files, .appref-ms shortcuts, dfsvc.exe, rundll32.exe); CrowdStrike Falcon (detection gap context)
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike researchers have documented a novel attack technique that weaponizes Microsoft's ClickOnce application deployment framework to install persistent backdoors on Windows systems without requiring administrator privileges. Attackers deliver malicious .appref-ms shortcut files, typically via spearphishing links, that execute through legitimate Microsoft system processes, bypassing email filters and endpoint controls tuned for traditional executable file types. Any organization running Windows with ClickOnce enabled and without explicit email gateway or endpoint controls for .appref-ms and .application files is exposed to this attack vector if users receive spearphishing links; the primary business risks are unauthorized persistent access, data exfiltration, and a detection gap that may allow attackers to operate undetected for extended periods.

Technical Analysis

CrowdStrike's two-part research series documents abuse of Microsoft's ClickOnce deployment framework (dfsvc.exe, rundll32.exe process chain) to achieve persistence and code execution without elevated privileges. The attack chain centers on .appref-ms shortcut files and .application manifests delivered via spearphishing links (T1566.002). These file types are not classified as executables by most mail gateways or EDR policies, creating a filter bypass (CWE-693: Protection Mechanism Failure). Once a user opens the file, ClickOnce fetches and installs a payload from an attacker-controlled server with no integrity verification requirement (CWE-494: Download of Code Without Integrity Check). The user interface presents minimal friction during execution (CWE-356: Product UI Does Not Warn User of Unsafe Actions). Execution is laundered through

legitimate Microsoft process trees, specifically dfsvc.exe and rundll32.exe (T1218, T1218.011), making behavioral detection difficult. Persistence is established via registry run keys or scheduled tasks (T1547, T1547.001, T1053.005). The technique also maps to masquerading (T1036), defense evasion via impair defenses (T1562.001), ingress tool transfer (T1105), non-standard port usage (T1571), and software deployment tool abuse (T1072). No CVE has been assigned; this is a documented abuse of legitimate framework functionality. CVSS base score: 7.5 (HIGH), assigned editorially based on high attack impact (persistence, code execution), broad scope (any Windows system with ClickOnce enabled), and requirement for user interaction. No patch is available; mitigation is configuration- and detection-based.

Action Checklist

1. Step 1: Containment. Audit email gateway and web proxy rules to block or quarantine inbound .appref-ms and .application file types. Confirm these extensions are explicitly listed alongside .exe and .msi in mail filtering policies. If ClickOnce is not required for business operations, disable the dfsvc.exe handler via Group Policy or AppLocker to prevent execution. Reference: NIST AC-6 (Least Privilege), CIS 8.5 (Implement and Manage Email Security Filters).
2. Step 2: Detection. Query EDR and SIEM for process chains where dfsvc.exe or rundll32.exe spawns child processes not consistent with normal application deployment. Specifically, hunt for: dfsvc.exe launching PowerShell, cmd.exe, mshta.exe, or network-connecting binaries; .appref-ms files executed from user download directories, temp folders, or email client staging paths; rundll32.exe with dfshim.dll arguments contacting external IPs. Review scheduled task creation events (Windows Event ID 4698) and registry run key modifications (Event ID 13 via Sysmon) following dfsvc.exe execution. Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs). MITRE techniques: T1547.001, T1053.005, T1218.011. MITRE D3FEND: System File Analysis (D3-SFA), Local Account Monitoring (D3-LAM).
3. Step 3: Eradication. No vendor patch exists; this is framework abuse, not a patched vulnerability. Apply the following configuration mitigations: (a) Use AppLocker or Windows Defender Application Control (WDAC) policies to block execution of .appref-ms and .application files by unauthorized users or from unauthorized paths; (b) Restrict dfsvc.exe execution via software restriction policies if ClickOnce is not required; (c) Enumerate and audit all scheduled tasks and HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry keys on affected endpoints for persistence artifacts. Reference: NIST AC-6 (Least Privilege), NIST CM controls (configuration management), CIS 2.1 (Establish and Maintain a Software Inventory).
4. Step 4: Recovery. Validate that AppLocker or WDAC policies are enforced and logging confirms blocked .appref-ms execution attempts. Confirm dfsvc.exe is not spawning unexpected child processes in post-remediation monitoring. Review all endpoints where ClickOnce-delivered applications are legitimately installed; verify manifests and source URLs are from authorized internal or vendor sources. Monitor for re-establishment of persistence via scheduled tasks and run keys for 30 days post-remediation. Reference: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting).
5. Step 5: Post-Incident. Conduct a gap analysis of email gateway extension block lists; .appref-ms and .application should have been blocked alongside .exe, .msi, and .bat. Evaluate EDR behavioral rules for coverage of process-chain execution originating from dfsvc.exe and rundll32.exe. Add hunting hypothesis for ClickOnce abuse to the threat hunting program. Review user security awareness training to include recognition of social-engineering lures that do not use traditional executable attachments. Reference: NIST IR controls (Incident Response), CIS 7.1 (Establish and Maintain a Vulnerability Management

Process), MITRE D3FEND: System File Analysis (D3-SFA), MITRE D3FEND: Local Account Monitoring (D3-LAM).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance if evidence shows successful persistence establishment (scheduled task or HKCU run key created post-dfsvc.exe execution), lateral movement from a compromised host, or exfiltration of data from endpoints where the ClickOnce payload executed — any of these conditions may trigger breach notification obligations under applicable data protection regulations if PII or PHI was accessible on affected systems.
Recovery Notes	After confirming AppLocker or WDAC policies are enforced and the ClickOnce cache has been purged on affected endpoints, maintain 30-day continuous monitoring of scheduled task creation (Event ID 4698) and HKCU\Software\Microsoft\Windows\CurrentVersion\Run modifications (Sysmon Event ID 13) across all endpoints that executed a .appref-ms file, as ClickOnce-delivered implants may attempt to re-register persistence through alternate user-writable run key locations such as HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce or through COM hijacking within the user profile. Verify that all legitimately authorized ClickOnce applications still function correctly from approved deployment URLs before closing the incident, to confirm that framework restrictions did not break sanctioned business workflows. Retain all forensic artifacts and event logs for a minimum of 90 days to support any downstream regulatory inquiry or threat intelligence sharing.
Forensic Artifacts	ClickOnce application cache at %LOCALAPPDATA%\Apps\2.0\ — contains the deployed manifest (.application file with DeploymentProvider URL pointing to attacker infrastructure), the payload binary, and installation metadata that directly ties the artifact to the malicious delivery chain | Windows Security Event Log Event ID 4698 (Scheduled Task Created) entries timestamped within minutes of dfsvc.exe execution — the task XML body will contain the attacker-controlled executable path or PowerShell command used to establish persistence | Sysmon Event ID 1 (Process Create) records showing dfsvc.exe or rundll32.exe with dfshim.dll command-line arguments as the ParentImage, with child processes such as powershell.exe, cmd.exe, or mshta.exe — this process chain is the primary behavioral indicator distinguishing malicious ClickOnce abuse from legitimate deployment | Email gateway quarantine logs and web proxy access logs containing the originating URL or attachment metadata for the .appref-ms delivery, including the sender address, delivery timestamp, and the external deployment server URL encoded within the file — essential for attributing the spearphishing campaign and identifying other potential recipients | Full memory image (acquired via WinPmem or Magnet RAM Capture) from any host where dfsvc.exe spawned a suspicious child process — memory analysis via Volatility will surface the in-memory implant, injected shellcode, and C2 beaconing artifacts (resolved DNS names, open sockets) that are absent from disk after a fileless or reflective-load delivery stage

Per-Action IR Details

Step 1: Containment — Audit email gateway and web proxy rules to block or quarantine inbound .appref-ms and .application file types. Confirm these extensions are explicitly listed alongside .exe and .msi in mail filtering policies. If ClickOnce is not required for business operations, disable the dfsvc.exe handler via Group Policy or AppLocker to prevent execution. 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: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On mail servers without enterprise gateway filtering, use PowerShell to enumerate Exchange transport rules: Get-TransportRule | Where {$_.AttachmentExtensionMatchesWords -ne $null}. Manually add .appref-ms and .application to blocked extensions via New-TransportRule with -AttachmentExtensionMatchesWords. For web proxy, if running Squid, add 'acl badext urlpath_regex \.appref-ms$ \.application$' with 'http_access deny badext'. To disable dfsvc.exe without AppLocker, remove or deny execute permission on C:\Windows\System32\dfsvc.exe for non-admin users via icacls: icacls C:\Windows\System32\dfsvc.exe /deny Users:(RX).

Evidence: Before modifying gateway rules or disabling dfsvc.exe, capture volatile state from any host that may have already received a .appref-ms payload: run 'netstat -ano' or 'Get-NetTCPConnection' to document active outbound connections from dfsvc.exe or rundll32.exe (PID-correlated), capture the running process list with 'Get-Process | Select-Object Name,Id,Path,StartTime' to identify any ClickOnce-deployed payloads already resident in %LOCALAPPDATA%\Apps\, and export currently scheduled tasks via 'schtasks /query /fo CSV /v > tasks_baseline.csv' before any policy change alters task visibility.

Step 2: Detection — Query EDR and SIEM for process chains where dfsvc.exe or rundll32.exe spawns child processes not consistent with normal application deployment. Specifically, hunt for: dfsvc.exe launching PowerShell, cmd.exe, mshta.exe, or network-connecting binaries; .appref-ms files executed from user download directories, temp folders, or email client staging paths; rundll32.exe with dfshim.dll arguments contacting external IPs. Review scheduled task creation events (Windows Event ID 4698) and registry run key modifications (Event ID 13 via Sysmon) following dfsvc.exe execution. Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs). MITRE techniques: T1547.001, T1053.005, T1218.011.

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 a configuration that enables Event ID 1 (Process Create) with ParentImage filtering on dfsvc.exe and rundll32.exe, Event ID 3 (Network Connection) for outbound connections initiated by dfsvc.exe or rundll32.exe, Event ID 11 (File Create) for .appref-ms files written to %USERPROFILE%\Downloads\ or %TEMP%\, Event ID 12/13 (Registry Create/Set) under HKCU\Software\Microsoft\Windows\CurrentVersion\Run. Use the Sigma rule 'proc_creation_win_dfsvc_susp_child_process' (community Sigma repo) as a detection template. Parse Sysmon logs with 'Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational | Where-Object {$_.Id -eq 1 -and $_.Message -match "dfsvc.exe"}' for immediate triage without a SIEM.

Evidence: This is a read-only analysis phase and does not alter live state; however, before any downstream containment action, preserve: Windows Security Event Log entries for Event ID 4688 (Process Creation with command-line auditing enabled) filtering on dfsvc.exe and rundll32.exe parent-child chains; Sysmon Event ID 1 logs from %SystemRoot%\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx; the ClickOnce application cache at %LOCALAPPDATA%\Apps\2.0\ (contains deployed manifests and binaries); browser download history and email client attachment staging directories (e.g., Outlook's SecureTemp at %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Outlook\) for the originating .appref-ms file; and web proxy logs filtered on requests to external hosts initiated by dfsvc.exe or rundll32.exe with dfshim.dll arguments.

Step 3: Eradication — No vendor patch exists; this is framework abuse, not a patched vulnerability. Apply the following configuration mitigations: (a) Use AppLocker or Windows Defender Application Control (WDAC) policies to block execution of .appref-ms and .application files by unauthorized users or from unauthorized

paths; (b) Restrict dfsvc.exe execution via software restriction policies if ClickOnce is not required; (c) Enumerate and audit all scheduled tasks and HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry keys on affected endpoints for persistence artifacts. Reference: NIST AC-6 (Least Privilege), NIST CM controls (configuration management), CIS 4.6 (Securely Manage Enterprise Assets and Software).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Without AppLocker (requires Enterprise/Education SKU), use Software Restriction Policies (SRP) via gpedit.msc: Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies > Additional Rules — create a Deny rule for path %USERPROFILE%* with file type .appref-ms. To enumerate persistence without EDR, run: 'schtasks /query /fo LIST /v | findstr /i "Task To Run\|Status\|Run As User"' and 'reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run' on each affected host. Remove identified malicious scheduled tasks with 'schtasks /delete /tn "" /f' and malicious run keys with 'reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v "" /f'. Purge the ClickOnce cache for affected users: 'rundll32 dfshim CleanOnlineAppCache' or manually delete %LOCALAPPDATA%\Apps\2.0\.

Evidence: CRITICAL — capture volatile evidence before removing persistence or purging the ClickOnce cache: acquire a full memory image of any confirmed-compromised host using WinPmem or Magnet RAM Capture before killing any implant process; export the complete scheduled task XML definitions ('schtasks /query /xml > tasks_full.xml') before deletion; export HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry hive ('reg export HKCU\Software\Microsoft\Windows\CurrentVersion\Run run_keys_evidence.reg') before removal; copy the entire %LOCALAPPDATA%\Apps\2.0\ directory to an evidence share before purging — this cache contains the ClickOnce manifest (.application file), deployment descriptor, and the actual delivered payload binary; document active network connections from implant processes ('Get-NetTCPConnection -State Established | Where-Object {$_.OwningProcess -in (Get-Process dfsvc,rundll32).Id}') before process termination.

Step 4: Recovery — Validate that AppLocker or WDAC policies are enforced and logging confirms blocked .appref-ms execution attempts. Confirm dfsvc.exe is not spawning unexpected child processes in post-remediation monitoring. Review all endpoints where ClickOnce-delivered applications are legitimately installed; verify manifests and source URLs are from authorized internal or vendor sources. Monitor for re-establishment of persistence via scheduled tasks and run keys for 30 days post-remediation. Reference: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting).

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: Without enterprise monitoring, create a scheduled PowerShell script (run daily via Task Scheduler as SYSTEM) that checks for new entries under HKCU\Software\Microsoft\Windows\CurrentVersion\Run and new scheduled tasks created after the remediation date, writing results to a log file: 'schtasks /query /fo CSV /v | ConvertFrom-Csv | Where-Object {$_["Next Run Time"] -ne "N/A"} | Export-Csv -Append -Path C:\IR\task_monitor.csv'. For AppLocker validation without SIEM, query the AppLocker event log directly: 'Get-WinEvent -LogName "Microsoft-Windows-AppLocker/EXE and DLL" | Where-Object {$_.Message -match "\.appref-ms|\.application"}'. Validate legitimate ClickOnce manifests by checking the DeploymentProvider URL in each .application file against an approved-source allowlist.

Evidence: Recovery validation does not alter previously compromised live state, but before returning hosts to production, confirm that: the %LOCALAPPDATA%\Apps\2.0\ cache contains only manifests referencing authorized deployment URLs (inspect with 'Get-ChildItem -Recurse %LOCALAPPDATA%\Apps\2.0\ -Filter *.application | Select-String -Pattern "deploymentProvider"'); AppLocker EXE/DLL and MSI/Script logs (Microsoft-Windows-AppLocker/EXE and DLL, Microsoft-Windows-AppLocker/MSI and Script) show block events for .appref-ms attempts with no corresponding allow events from unauthorized paths; and Sysmon Event ID 1 shows no new dfsvc.exe child process creation events since policy enforcement began.

Step 5: Post-Incident — Conduct a gap analysis of email gateway extension block lists; .appref-ms and .application should have been blocked alongside .exe, .msi, and .bat. Evaluate EDR behavioral rules for coverage of process-chain execution originating from dfsvc.exe and rundll32.exe. Add hunting hypothesis for ClickOnce abuse to the threat hunting program. Review user security awareness training to include recognition of social-engineering lures that do not use traditional executable attachments. Reference: NIST IR controls (Incident Response), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), D3-SFA (System File Analysis), D3-LAM (Local Account Monitoring).

NIST Phase: Post Incident

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

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), NIST AU-6 (Audit Record Review, Analysis, and Reporting)

Compensating: For teams without commercial threat hunting platforms, formalize the ClickOnce hunting hypothesis as a Sigma rule targeting dfsvc.exe parent-child process chains and submit to the community Sigma repository for peer validation. Conduct a manual extension audit of the email gateway block list by exporting current policies to CSV and diffing against a reference list that includes .appref-ms, .application, .appx, .appinstaller, .xbap, and .vsto — all ClickOnce-adjacent deployment formats. For user awareness, add a concrete phishing simulation scenario using a non-executable lure (e.g., a fake software update notification with a .appref-ms link) to the next security awareness campaign cycle.

Evidence: Post-incident analysis relies on preserved artifacts from earlier phases; ensure the following are available for the lessons-learned review: the original spearphishing delivery artifact (the .appref-ms or .application file recovered from email gateway quarantine or the user's download directory); the full ClickOnce manifest from the attacker-controlled deployment server URL (if retrievable safely via sandbox); Sysmon and Windows Security event logs from the initial compromise window covering dfsvc.exe execution, child process creation, scheduled task creation (Event ID 4698), and HKCU run key modifications (Sysmon Event ID 13); and the memory image acquired during eradication, which may contain the in-memory implant payload and C2 network indicators not present in disk artifacts.

Detection Guidance

Primary hunt targets: process chain dfsvc.exe (or rundll32.exe loading dfshim.dll) spawning cmd.exe, PowerShell, mshta.exe, wscript.exe, cscript.exe, or any process making outbound network connections to non-Microsoft infrastructure. Secondary hunt targets: .appref-ms or .application files present in user download directories, %TEMP%, %APPDATA%, or email client attachment staging folders. Persistence artifacts: Windows Event ID 4698 (scheduled task created) and Sysmon Event ID 13 (registry value set) under HKCU\Software\Microsoft\Windows\CurrentVersion\Run, correlated temporally with dfsvc.exe execution. Network indicators: outbound HTTP/HTTPS requests from dfsvc.exe to external hosts, particularly on non-standard ports (T1571). Log sources required: Windows Security event log, Sysmon (Events 1, 3, 11, 13), EDR process tree telemetry, proxy/web gateway logs filtered for .application and .appref-ms MIME types or extensions. No confirmed public IOCs (IPs, domains, hashes) were provided in the source material; behavioral detection is the primary detection approach for this technique. Reference: NIST AU-2, AU-6, AU-12; CIS 8.2; MITRE D3FEND: System File Analysis (D3-SFA), MITRE D3FEND: Local Account Monitoring (D3-LAM).

Framework Mappings

MITRE-ATTACK

- **T1204.002** — Malicious File
- **T1562.001** — Disable or Modify Tools

- **T1547** — Boot or Logon Autostart Execution
- **T1566.002** — Spearphishing Link
- **T1036** — Masquerading
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1218.011** — Rundll32
- **T1571** — Non-Standard Port
- **T1072** — Software Deployment Tools
- **T1218** — System Binary Proxy Execution
- **T1053.005** — Scheduled Task
- **T1105** — Ingress Tool Transfer

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **CA-7** — Continuous Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control
- **AC-6** — Least Privilege

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

NIST-CSF-2

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

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1204.002	Malicious File	Execution
T1562.001	Disable or Modify Tools	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1566.002	Spearphishing Link	Initial-Access
T1036	Masquerading	Defense-Evasion
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1218.011	Rundll32	Defense-Evasion
T1571	Non-Standard Port	Command-And-Control
T1072	Software Deployment Tools	Execution
T1218	System Binary Proxy Execution	Defense-Evasion
T1053.005	Scheduled Task	Execution
T1105	Ingress Tool Transfer	Command-And-Control

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/av-comparatives-awards-for-e...	T3
	https://www.crowdstrike.com/en-us/blog/reasons-why-nonprofits-are-t...	T3
	https://www.crowdstrike.com/en-us/blog/how-the-infrastructure-inves...	T3
New Abuse of the ClickOnce Technology: Part 1 - CrowdStrike	https://www.crowdstrike.com/content/crowdstrike-www/locale-sites/us...	T3

Generated 2026-06-20 13:35 UTC by TJS Security Command Center