INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-21 18:40 UTC

ClickOnce Weaponized: How Threat Actors Exploit Microsoft's Deployment Technology for Stealthy Persistence

THREAT CAMPAIGN | **MEDIUM** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0530
Type	Threat Campaign
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Microsoft Windows, ClickOnce deployment framework (.application files, .appref-ms files, dfsvc.exe, rundll32.exe); applicable across Windows enterprise environments
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike researchers have documented new abuse techniques targeting Microsoft's ClickOnce deployment framework, including a privilege-escalation-free persistence method that is newly documented. Any Windows enterprise environment using ClickOnce is exposed; threat actors can deliver malicious payloads via .application or .appref-ms files that commonly bypass email security gateways. The business risk is unauthorized persistent access to enterprise endpoints without triggering standard executable-based controls.

Technical Analysis

CrowdStrike's Part 2 research on ClickOnce abuse documents multiple attack vectors against Microsoft's application deployment technology across Windows enterprise environments. The attack chain abuses .application and .appref-ms file types as initial delivery vehicles (T1566.001, T1204.002), leveraging dfsvc.exe (ClickOnce deployment service host) and dfshim.dll (ClickOnce shim library) and rundll32.exe (T1218.011) as execution intermediaries to blend into legitimate Windows process trees. A newly documented persistence technique plants ClickOnce artifacts in Startup folders (T1547.001) and scheduled tasks (T1053.005) without requiring elevated privileges. Obfuscation techniques (T1027) and masquerading (T1036.005) are used to reduce detection probability. Relevant weakness classes are CWE-494 (Download of Code Without Integrity Check) and CWE-693 (Protection Mechanism Failure). No CVE is assigned; this is a technique-level abuse of legitimate Windows functionality. No vendor patch is available; mitigations are detection- and configuration-based. Source: CrowdStrike blog (T3), https://www.crowdstrike.com/en-us/blog/new-abuse-of-the-clickonce-technology-part-two/

Action Checklist

1. Step 1: Containment, Identify all hosts where dfsvc.exe has spawned child processes outside normal ClickOnce application update workflows; isolate any host showing dfsvc.exe or rundll32.exe launching unsigned or unexpected binaries. Block inbound delivery of .application and .appref-ms file types at email gateways and web proxies where ClickOnce deployment is not a business requirement (NIST AC-4, Information Flow Enforcement; CIS 4.4, Implement and Manage a Firewall on Servers).
2. Step 2: Detection, Query EDR telemetry for process trees rooted in dfsvc.exe with child processes that are not dfshim.dll or standard ClickOnce update components. Audit Startup folder locations (%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup and %ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup) for .appref-ms artifacts not tied to known-good deployments. Review scheduled tasks created by non-administrative users referencing ClickOnce paths. Enable audit logging on ClickOnce-related registry keys under HKCU\Software\Classes\clickonce and HKCU\Software\Apps (NIST AU-2, Event Logging; NIST AU-12, Audit Record Generation; CIS 8.2, Collect Audit Logs).
3. Step 3: Eradication, Remove unauthorized .appref-ms and .application artifacts from Startup folders on all affected endpoints. Delete scheduled tasks created by the attack chain referencing dfsvc.exe or ClickOnce deployment paths. If ClickOnce is not used in your environment, disable dfsvc.exe execution via application control policy and restrict .application and .appref-ms file associations (NIST AC-6, Least Privilege; CIS 2.3, Address Unauthorized Software).
4. Step 4: Recovery, Re-image or perform verified clean restoration on any host where dfsvc.exe-rooted persistence was confirmed. Validate Startup folder contents and scheduled task inventories against a known-good baseline post-remediation. Monitor dfsvc.exe process activity for 30 days post-remediation using EDR behavioral rules scoped to this technique cluster (T1547.001, T1053.005, T1218.011) (NIST SI-4, Information System Monitoring; CIS 8.2, Collect Audit Logs; NIST AU-6, Audit Record Review, Analysis, And Reporting).
5. Step 5: Post-Incident, Conduct a gap assessment against email gateway controls for .application and .appref-ms attachment handling; document exceptions where ClickOnce delivery is a legitimate business requirement and apply compensating controls. Formalize a detection rule for dfsvc.exe anomalous child process spawning in your SIEM or EDR platform. Review user account privilege boundaries to ensure no general-purpose accounts hold unnecessary scheduled task creation rights (NIST AC-5, Separation Of Duties; NIST AC-6, Least Privilege; CIS 5.4, Restrict Administrator Privileges to Dedicated Administrator Accounts; D3-UAP, User Account Permissions; D3-SFA, System File Analysis).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to senior IR leadership and legal/compliance if any confirmed-compromised host is found to have processed, stored, or transmitted PII, PHI, or payment card data during the dfsvc.exe persistence window, or if the attack chain is identified on hosts with privileged access to production systems, Active Directory, or OT/ICS networks, triggering breach notification assessment under applicable regulatory frameworks.

Recovery Notes	Before returning any remediated host to production, validate that the ClickOnce application store at %LOCALAPPDATA%\Apps\2.0 contains only signed, known-good application manifests matching your approved ClickOnce deployment inventory, and that no .appref-ms files exist in either per-user or system-wide Startup folders outside of documented business exceptions. Maintain Sysmon-based behavioral monitoring on dfsvc.exe child process spawning for a minimum of 30 days post-remediation, as ClickOnce persistence mechanisms (Startup folder .appref-ms entries and scheduled tasks referencing ClickOnce paths) may survive partial remediation if the %LOCALAPPDATA%\Apps\2.0 store is not fully purged. If threat actor infrastructure (deployment server URLs extracted from .application manifests) is identified, submit indicators to your threat intelligence platform and monitor proxy and DNS logs for re-contact attempts from any enterprise host.
Forensic Artifacts	ClickOnce application store directory (%LOCALAPPDATA%\Apps\2.0): contains attacker-delivered payload binaries, deployment manifests (.application, .manifest files), and publisher certificate data — the manifest's deploymentProvider URL directly identifies attacker-controlled staging infrastructure. | Windows Startup folder .appref-ms files (%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup and %ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup): malicious .appref-ms shortcuts planted by the ClickOnce persistence technique; MACB timestamps establish when the persistence mechanism was installed relative to dfsvc.exe execution. | Sysmon Event ID 1 (Process Create) logs with ParentImage = dfsvc.exe: captures the full command-line arguments of any child process spawned by the ClickOnce deployment engine, directly evidencing payload execution and any LOLBin abuse (e.g., rundll32.exe loading an attacker DLL via ClickOnce). | Windows Security Event ID 4698 and 4702 (Scheduled Task Created/Updated) in the Security event log: records scheduled tasks created by the attack chain referencing dfsvc.exe or ClickOnce paths, including the creating user's SID and the full task XML with trigger and action definitions. | Registry keys HKCU\Software\Classes\clickonce\Shell\open\command and HKCU\Software\Apps: attacker modifications to these per-user keys establish file-handler hijacking for ClickOnce-associated file types and may contain direct references to the malicious payload path, surviving even after binary removal.

Per-Action IR Details

Step 1: Containment — Identify all hosts where dfsvc.exe has spawned child processes outside normal ClickOnce application update workflows; isolate any host showing dfsvc.exe or rundll32.exe launching unsigned or unexpected binaries. Block inbound delivery of .application and .appref-ms file types at email gateways and web proxies where ClickOnce deployment is not a business requirement (NIST AC-4 — Information Flow Enforcement; CIS 4.4 — Implement and Manage a Firewall on Servers).

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)

Compensating: Use Sysmon Event ID 1 (Process Create) filtered on ParentImage containing 'dfsvc.exe' to enumerate anomalous child processes: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Message -match 'dfsvc.exe'}`. At the email gateway, add MIME-type and extension-based block rules for application/x-ms-application (.application) and .appref-ms; at the proxy, block downloads with those extensions via URL-filtering policy. Network isolation can be enforced with a host-based firewall rule via: `netsh advfirewall firewall add rule name='Block dfsvc outbound' program='%SystemRoot%\System32\dfshim.dll' action=block dir=out`.

Evidence: Before isolating any host, capture: (1) full RAM image using WinPmem or DumpIt to preserve in-memory ClickOnce deployment state and any injected payloads loaded by dfsvc.exe or rundll32.exe; (2) live process tree snapshot via `Get-CimInstance Win32_Process | Select-Object ProcessId, ParentProcessId, Name, CommandLine |

Export-Csv`; (3) active network connections via `Get-NetTCPConnection | Where-Object {$_.OwningProcess -in (Get-Process dfsvc,rundll32).Id}` to capture C2 callback endpoints before network cut; (4) Prefetch files for dfsvc.exe and rundll32.exe at `%SystemRoot%\Prefetch\DFSVC.EXE-*.pf` to establish execution timeline.

Step 2: Detection — Query EDR telemetry for process trees rooted in dfsvc.exe with child processes that are not dfshim.dll or standard ClickOnce update components. Audit Startup folder locations (%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup and %ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup) for .appref-ms artifacts not tied to known-good deployments. Review scheduled tasks created by non-administrative users referencing ClickOnce paths. Enable audit logging on ClickOnce-related registry keys under HKCU\Software\Classes\clickonce and HKCU\Software\Apps (NIST AU-2 — Event Logging; NIST AU-12 — Audit Record Generation; CIS 8.2 — Collect Audit Logs).

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without EDR, deploy Sysmon with a configuration that logs Event ID 1 (Process Create), Event ID 11 (File Create), and Event ID 13 (Registry Value Set) targeting `HKCU\Software\Classes\clickonce` and `HKCU\Software\Apps`. Query Startup folder artifacts via: `Get-ChildItem -Path "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup","C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup" -Filter '*.appref-ms'`. Enumerate scheduled tasks created by standard users referencing ClickOnce paths: `Get-ScheduledTask | Where-Object {$_.Actions.Execute -match 'dfsvc|appref-ms|clickonce'} | Select-Object TaskName, TaskPath, @{n='Author';e={$_.Principal.UserId}}`. Enable Windows Security Event ID 4698 (Scheduled Task Created) and 4702 (Scheduled Task Updated) via Group Policy audit settings.

Evidence: This step is analytical and does not alter live state; however, before enabling any new registry auditing policy that may alter HKCU keys, capture a registry export of `HKCU\Software\Classes\clickonce` and `HKCU\Software\Apps` via `reg export HKCU\Software\Classes\clickonce clickonce_classes_baseline.reg`. Key forensic indicators specific to this campaign: .appref-ms files in Startup folders with creation timestamps correlating to dfsvc.exe execution events; Windows Security Event ID 4698/4702 entries authored by standard user SIDs referencing `%LOCALAPPDATA%\Apps` paths; Sysmon Event ID 13 showing writes to `HKCU\Software\Classes\clickonce\Shell\open\command` from dfsvc.exe.

Step 3: Eradication — Remove unauthorized .appref-ms and .application artifacts from Startup folders on all affected endpoints. Delete scheduled tasks created by the attack chain referencing dfsvc.exe or ClickOnce deployment paths. If ClickOnce is not used in your environment, disable dfsvc.exe execution via application control policy and restrict .application and .appref-ms file associations (NIST AC-6 — Least Privilege; CIS 2.3 — Address Unauthorized Software).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), CIS 2.3 (Address Unauthorized Software)

Compensating: Remove malicious .appref-ms Startup artifacts: `Remove-Item -Path "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\*.appref-ms" -Confirm`. Delete attacker-created scheduled tasks: `Get-ScheduledTask | Where-Object {$_.Actions.Execute -match 'dfsvc|appref-ms'} | Unregister-ScheduledTask -Confirm:$false`. Disable dfsvc.exe via Windows Defender Application Control (WDAC) or Software Restriction Policy if ClickOnce is not in use: `New-SRPPolicy -Path '%SystemRoot%\System32\dfshim.dll' -SecurityLevel Disallowed`. Reset .application and .appref-ms file associations to break the execution chain: `cmd /c assoc .application=` and `cmd /c assoc .appref-ms=`.

Evidence: Before removing any artifact or deleting scheduled tasks, capture: (1) forensic copy of all .appref-ms and .application files from Startup folders using `robocopy` to a write-protected evidence share, preserving MACB timestamps; (2) full scheduled task XML export via `Export-ScheduledTask` for all tasks referencing ClickOnce paths, as these contain the attacker's command-line arguments and trigger configurations; (3) registry snapshot of

`HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store` to capture any additional persistence mechanisms seeded alongside the ClickOnce abuse chain; (4) ClickOnce application store directory listing at `%LOCALAPPDATA%\Apps\2.0` before deletion, as this directory contains installed ClickOnce application binaries and manifests that may evidence the payload delivered.

Step 4: Recovery — Re-image or perform verified clean restoration on any host where dfsvc.exe-rooted persistence was confirmed. Validate Startup folder contents and scheduled task inventories against a known-good baseline post-remediation. Monitor dfsvc.exe process activity for 30 days post-remediation using EDR behavioral rules scoped to this technique cluster (T1547.001, T1053.005, T1218.011) (NIST SI-4 referenced as no mapped control from knowledge base — SI-4 not present in provided control set; CIS 8.2 — Collect Audit Logs; NIST AU-6 — Audit Record Review, Analysis, And Reporting).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 8.2 (Collect Audit Logs), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: For teams without EDR, implement a Sysmon-based 30-day watch using Event ID 1 filtered on `dfsvc.exe` as ParentImage, forwarded to Windows Event Forwarding (WEF) to a central collector. Post-reimage, validate Startup folders and scheduled tasks against a scripted baseline check run daily via scheduled task: `Get-ChildItem "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup" | Export-Csv startup_audit_$(Get-Date -f yyyyMMdd).csv`. Deploy a YARA rule scanning `%LOCALAPPDATA%\Apps\2.0` for ClickOnce manifests with unsigned or mismatched publisher fields as a recurring integrity check.

Evidence: Before reimaging, ensure the following volatile and persistent evidence has been collected from confirmed-compromised hosts: (1) full disk image using dd or FTK Imager to preserve the ClickOnce application store at `%LOCALAPPDATA%\Apps\2.0` and all payload binaries; (2) ClickOnce deployment manifest files (.application, .manifest) from the store directory, which contain publisher certificate hashes, deployment URLs, and payload hashes usable for threat-actor infrastructure attribution; (3) Windows Event Log exports (Security, System, Application, and Microsoft-Windows-AppModel-Runtime/Admin) covering the full suspected compromise window; (4) browser history and download records if the .application file was delivered via web vector, to identify the initial delivery URL for blocking and intelligence reporting.

Step 5: Post-Incident — Conduct a gap assessment against email gateway controls for .application and .appref-ms attachment handling; document exceptions where ClickOnce delivery is a legitimate business requirement and apply compensating controls. Formalize a detection rule for dfsvc.exe anomalous child process spawning in your SIEM or EDR platform. Review user account privilege boundaries to ensure no general-purpose accounts hold unnecessary scheduled task creation rights (NIST AC-5 — Separation Of Duties; NIST AC-6 — Least Privilege; CIS 5.4 — Restrict Administrator Privileges to Dedicated Administrator Accounts; D3-UAP — User Account Permissions; D3-SFA — System File Analysis).

NIST Phase: Post Incident

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

Controls: NIST AC-5 (Separation Of Duties), NIST AC-6 (Least Privilege), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without a SIEM, publish a Sigma rule targeting Sysmon Event ID 1 where ParentImage ends with 'dfsvc.exe' and Image does not match known ClickOnce components (dfshim.dll loader, dfsvc.exe self-updates) — convert to a WEF subscription for ongoing collection. Document ClickOnce business exceptions in a signed waiver with a compensating control: mandatory code-signing certificate pinning for all permitted .application deployments, enforced via AppLocker publisher rule. Audit scheduled task creation rights by running: `Get-LocalGroupMember -Group 'Administrators' | Compare-Object -ReferenceObject (Import-Csv approved_admins_baseline.csv)` to identify privilege creep since the incident.

Evidence: No live-state-altering actions occur in this phase; evidence collection focus shifts to lessons-learned inputs: (1) email gateway logs showing delivery attempts of .application and .appref-ms files during the campaign window,

including sender domains and IP addresses for threat-intel reporting; (2) proxy logs showing ClickOnce deployment manifest fetch requests to attacker-controlled URLs (ClickOnce manifests must be fetched from a deployment server — the URL in the .application file is a direct C2/staging indicator); (3) final reconciled timeline of dfsvc.exe execution events across all affected hosts, constructed from Sysmon Event ID 1 and Windows Security Event ID 4688, to scope the full blast radius for any required breach notification assessment.

Detection Guidance

Primary detection surface is the dfsvc.exe process tree. Alert on dfsvc.exe spawning any child process other than dfshim.dll-based update operations, particularly cmd.exe, powershell.exe, wscript.exe, mshta.exe, or unsigned binaries. Secondary surface is rundll32.exe (T1218.011) launched from ClickOnce application directories under %LOCALAPPDATA%\Apps\2.0\. For persistence, diff Startup folder contents (%APPDATA% and %ProgramData% paths) against baseline and flag any .appref-ms files not in your approved ClickOnce application inventory. For scheduled tasks, query for tasks created under non-SYSTEM, non-administrative user contexts referencing dfsvc.exe or ClickOnce application paths. Registry monitoring: flag writes to HKCU\Software\Classes\clickonce and HKCU\Software\Apps from processes other than known ClickOnce updaters. CrowdStrike Falcon telemetry is confirmed as a viable data source per source material. D3FEND countermeasures applicable: D3-SFA (System File Analysis) for Startup folder and scheduled task artifact monitoring; D3-LAM (Local Account Monitoring) for non-privileged persistence creation; D3-FMBV (File Magic Byte Verification) for .application and .appref-ms payload inspection at gateway.

Framework Mappings

MITRE-ATTACK

- **T1566.001** — Spearphishing Attachment
- **T1218** — System Binary Proxy Execution
- **T1204.002** — Malicious File
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1195.002** — Compromise Software Supply Chain
- **T1053.005** — Scheduled Task
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1218.011** — Rundll32
- **T1027** — Obfuscated Files or Information
- **T1059** — Command and Scripting Interpreter

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CM-7** — Least Functionality

- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **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
- **8.2** — Collect Audit Logs

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566.001	Spearphishing Attachment	Initial-Access
T1218	System Binary Proxy Execution	Defense-Evasion
T1204.002	Malicious File	Execution
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1195.002	Compromise Software Supply Chain	Initial-Access
T1053.005	Scheduled Task	Execution
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1218.011	Rundll32	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution

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

Source	URL	Tier
	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 2 - CrowdStrike	https://www.crowdstrike.com/content/crowdstrike-www/locale-sites/us...	T3

Generated 2026-06-21 18:40 UTC by TJS Security Command Center