INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-22 06:23 UTC

ClickOnce Weaponization: Microsoft's App Deployment Framework Abused for No-Privilege Persistence

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0532
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Windows (ClickOnce / .NET deployment framework); processes: rundll32.exe, dfsvc.exe; any standard-user enterprise endpoint
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike researchers have documented a campaign abusing Microsoft's ClickOnce application deployment framework to establish persistence and deliver malicious payloads on Windows endpoints without requiring administrator privileges. Any enterprise endpoint running standard user accounts is in scope, making this a broad, stealthy threat that bypasses traditional executable-focused detection controls by leveraging trusted, Microsoft-signed infrastructure. The primary business risk is undetected persistence across the enterprise estate, enabling follow-on data theft, ransomware staging, or lateral movement with minimal forensic footprint.

Technical Analysis

Threat actors are weaponizing Microsoft's ClickOnce deployment framework, specifically abusing dfsvc.exe and rundll32.exe process chains alongside .application and .appref-ms file artifacts, to achieve persistence and payload delivery without elevated privileges. The attack exploits the trusted, signed Microsoft deployment infrastructure (T1553.002) to evade executable-focused detection. Delivery vectors include spearphishing links (T1566.002) and user-executed malicious files (T1204.002). Attackers leverage scheduled tasks (T1053.005) and registry run keys (T1547.001) for persistence, use rundll32.exe as a signed binary proxy (T1218.011), and may communicate over non-standard ports (T1571) or use ingress tool transfer (T1105). Relevant weaknesses: CWE-346 (origin validation error), CWE-494 (download of code without integrity check), CWE-693 (protection mechanism failure). No CVE has been assigned; this is a technique-based abuse of legitimate functionality, not a discrete software vulnerability. No vendor patch exists; mitigation requires detection and policy controls.

(CrowdStrike blog, 'New Abuse of the ClickOnce Technology: Part 1' and 'Part 2'; see sources section for URLs.)

Action Checklist

1. Step 1: Containment. Identify all endpoints where dfsvc.exe or rundll32.exe has spawned unexpected child processes. Isolate any endpoint showing anomalous ClickOnce process trees pending investigation. Block .application and .appref-ms file delivery at email gateways and web proxies where these file types are not operationally required.
2. Step 2: Detection. Query EDR and SIEM telemetry for dfsvc.exe spawning processes other than expected ClickOnce update flows; alert on rundll32.exe executing with ClickOnce-related parent processes (AU-6, CIS 8.2). Search endpoint logs for creation of .application or .appref-ms files in user-writable directories. Review scheduled task creation events (Event ID 4698) and registry run key modifications (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) for ClickOnce-sourced entries (T1053.005, T1547.001).
3. Step 3: Eradication. No vendor patch exists because this is a technique-based abuse of legitimate functionality, not a discrete software vulnerability. Mitigation is control-based. Remove unauthorized scheduled tasks and registry persistence entries tied to ClickOnce abuse. Delete malicious .application and .appref-ms artifacts from affected endpoints. Where ClickOnce is not operationally required, disable dfsvc.exe via application control policy (CIS 4.6, NIST AC-6). Restrict or block .application and .appref-ms file associations at the OS level on standard-user endpoints.
4. Step 4: Recovery. After removing persistence mechanisms, verify no residual scheduled tasks or run key entries remain. Monitor dfsvc.exe and rundll32.exe process trees continuously for 30 days post-remediation (NIST SI-4 equivalent monitoring posture). Confirm application control policies are enforced and telemetry confirms expected process behavior. Review ClickOnce application whitelists and remove any unauthorized application entries.
5. Step 5: Post-Incident. This technique exposed gaps in process-tree-based detection coverage for signed Microsoft binaries used as proxy executables. Implement detection rules specifically for dfsvc.exe and rundll32.exe anomalous child process spawning (NIST AU-2, AU-12). Review and update application allowlisting policies to cover ClickOnce file types (CIS 2.3). Conduct a broader living-off-the-land binary (LOLBin) detection coverage review using MITRE ATT&CK T1218 sub-techniques as a baseline. Brief security awareness audiences on spearphishing links delivering .application files (T1566.002).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to senior IR leadership and legal/compliance immediately if any compromised endpoint is confirmed to have accessed, stored, or transmitted PII, PHI, or PCI-scoped data during the window of ClickOnce-established persistence, or if dfsvc.exe child process artifacts indicate lateral movement or C2 communication to external infrastructure.

Recovery Notes	After eradicating ClickOnce persistence entries and payload artifacts, verify recovery completeness by re-baselining all scheduled tasks and HKCU run keys on affected endpoints and comparing against pre-incident inventory snapshots. Monitor dfsvc.exe and rundll32.exe process trees via Sysmon for a minimum of 30 days, as ClickOnce manifests can be re-triggered by cached .appref-ms shortcuts that survive eradication if the `%LOCALAPPDATA%\Apps\2.0\` cache and Start Menu shortcuts are not fully purged. Confirm application control policies blocking .application and .appref-ms file associations remain enforced through the monitoring period by periodically re-querying AppLocker or equivalent policy enforcement logs.
Forensic Artifacts	ClickOnce deployment cache directory at %LOCALAPPDATA%\Apps\2.0\ — contains staged malicious application manifests (.application XML files) and downloaded payload binaries, preserving the full attacker-controlled ApplicationIdentity, publisher certificate thumbprint, and payload download URL | Sysmon Event ID 1 (Process Create) logs showing dfsvc.exe parent-child process trees with unexpected child ImagePaths and full command-line arguments — primary evidence of ClickOnce weaponization and payload execution chain | Windows Security Event Log Event ID 4698 (Scheduled Task Created) and Event ID 4657 (Registry Value Modified) entries for HKCU\Software\Microsoft\Windows\CurrentVersion\Run — documents attacker persistence mechanism established without administrator privileges | Network proxy or DNS query logs recording the HTTP GET request to the attacker-controlled URL serving the .application manifest, including the full URI, response Content-Type header (application/x-ms-application), and any subsequent payload download URLs embedded in the manifest | Windows Prefetch files in C:\Windows\Prefetch\ for any payload binary executed as a child of dfsvc.exe — provides executable name, run count, last execution timestamp, and up to 10 seconds of file system activity associated with the malicious payload at first launch

Per-Action IR Details

Step 1: Containment — Identify all endpoints where dfsvc.exe or rundll32.exe has spawned unexpected child processes. Isolate any endpoint showing anomalous ClickOnce process trees pending investigation. Block .application and .appref-ms file delivery at email gateways and web proxies where these file types are not operationally required.

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: Without EDR, deploy Sysmon with a configuration that logs Event ID 1 (Process Create) and Event ID 10 (ProcessAccess) for dfsvc.exe and rundll32.exe. Run: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Message -match 'dfsvc.exe'}` to identify parent-child anomalies. At the gateway, use free mail filter or proxy ACL rules to block MIME types application/x-ms-application and file extensions .application and .appref-ms.

Evidence: Before isolating any endpoint, capture volatile state: run `Get-Process | Where-Object {$_.Name -match 'dfsvc|rundll32'} | Select-Object Id,Name,Path,StartTime` and `Get-NetTCPConnection -State Established | Where-Object {$_.OwningProcess -in (Get-Process dfsvc,rundll32).Id}` to record active network connections. Capture full RAM image using WinPmem or DumpIt prior to network isolation, as dfsvc.exe child process arguments and injected payloads reside only in live memory. Also export `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and list all scheduled tasks via `schtasks /query /fo LIST /v` before any host isolation action.

Step 2: Detection — Query EDR and SIEM telemetry for dfsvc.exe spawning processes other than expected ClickOnce update flows; alert on rundll32.exe executing with ClickOnce-related parent processes (AU-6, CIS 8.2). Search endpoint logs for creation of .application or .appref-ms files in user-writable directories. Review

scheduled task creation events (Event ID 4698) and registry run key modifications (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) for ClickOnce-sourced entries (T1053.005, T1547.001).

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, deploy Sysmon and collect Event ID 1 (Process Create) filtering on ParentImage containing dfsvc.exe. Use this PowerShell query against Windows Security event log: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4698} | Select-Object TimeCreated,Message` to surface scheduled task creation. For file creation in user-writable paths, Sysmon Event ID 11 (FileCreate) filtered on TargetFilename ending in .application or .appref-ms under `%APPDATA%`, `%LOCALAPPDATA%`, and `%TEMP%` will surface delivery artifacts. Publish the corresponding Sigma rule for dfsvc.exe anomalous child process spawning to a local Hayabusa instance for offline log hunting.

Evidence: This step is analytical and does not alter live state, so no volatile pre-capture is required before running queries. Key artifacts to collect during analysis: Windows Security Event Log entries for Event ID 4698 (Scheduled Task Created) and Event ID 4657 (Registry Value Modified) targeting HKCU run keys; Sysmon Event ID 1 logs showing dfsvc.exe process trees with unexpected child ImagePaths; file system evidence of .application or .appref-ms files written to `%APPDATA%\Local\Apps\` or `%TEMP%` (the default ClickOnce deployment cache path); and Windows Prefetch files for any payload binary spawned by dfsvc.exe, located in `C:\Windows\Prefetch\`.

Step 3: Eradication — No vendor patch exists; mitigation is control-based. Remove unauthorized scheduled tasks and registry persistence entries tied to ClickOnce abuse. Delete malicious .application and .appref-ms artifacts from affected endpoints. Where ClickOnce is not operationally required, disable dfsvc.exe via application control policy (CIS 4.6, NIST AC-6). Restrict or block .application and .appref-ms file associations at the OS level on standard-user endpoints.

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), CIS 2.3 (Address Unauthorized Software)

Compensating: Without enterprise application control, use AppLocker (available in Windows 10/11 Pro and above at no cost) with a deny rule for `%SystemRoot%\System32\dfshim.dll` and `%SystemRoot%\SysWOW64\dfshim.dll` to prevent dfsvc.exe from loading the ClickOnce host shim. To remove scheduled tasks: `schtasks /delete /tn "" /f`. To remove registry persistence: `Remove-ItemProperty -Path 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Run' -Name "`. Delete ClickOnce deployment cache artifacts under `%LOCALAPPDATA%\Apps\2.0\` using: `Remove-Item -Recurse -Force "$env:LOCALAPPDATA\Apps\2.0\*"`.

Evidence: Before deleting any persistence entry or artifact, preserve forensic copies: export the full `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` hive with `reg export HKCU\Software\Microsoft\Windows\CurrentVersion\Run C:\IR\run_keys_backup.reg`; export all scheduled tasks to XML with `schtasks /query /xml > C:\IR\scheduled_tasks_pre_eradication.xml`; and copy all files from `%LOCALAPPDATA%\Apps\2.0\` to an evidence directory before deletion, as these directories contain the staged malicious .application manifests and any downloaded payload binaries that constitute the primary forensic record of the ClickOnce abuse chain.

Step 4: Recovery — After removing persistence mechanisms, verify no residual scheduled tasks or run key entries remain. Monitor dfsvc.exe and rundll32.exe process trees continuously for 30 days post-remediation (NIST SI-4 equivalent monitoring posture). Confirm application control policies are enforced and telemetry confirms expected process behavior. Review ClickOnce application whitelists and remove any unauthorized application entries.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-12 (Audit Record Generation), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: Without EDR for continuous monitoring, configure a Sysmon-based osquery scheduled query to run every 15 minutes checking for new entries under `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and newly created scheduled tasks. Use: `osquery> SELECT * FROM scheduled_tasks WHERE enabled = 1;` and `SELECT * FROM registry WHERE path LIKE 'HKEY_USERS\%\Software\Microsoft\Windows\CurrentVersion\Run\%';` to baseline and alert on drift. Compare output against the pre-eradication snapshot saved during Step 3 to detect re-infection within the 30-day watch window.

Evidence: Recovery verification does not directly alter live state, but confirm residual-check completeness by documenting: a post-eradication export of scheduled tasks and HKCU run keys (compare SHA-256 hashes of registry exports against pre-eradication baseline); a Sysmon Event ID 1 log confirming dfsvc.exe has not spawned any child processes since eradication; and confirmation that `%LOCALAPPDATA%\Apps\2.0\` directories have not been recreated, verified via `Get-ChildItem -Recurse "$env:LOCALAPPDATA\Apps\2.0"` returning empty or only known-good entries.

Step 5: Post-Incident — This technique exposed gaps in process-tree-based detection coverage for signed Microsoft binaries used as proxy executables. Implement detection rules specifically for dfsvc.exe and rundll32.exe anomalous child process spawning (NIST AU-2, AU-12). Review and update application allowlisting policies to cover ClickOnce file types (CIS 2.3). Conduct a broader living-off-the-land binary (LOLBin) detection coverage review using MITRE ATT&CK T1218 sub-techniques as a baseline. Brief security awareness audiences on spearphishing links delivering .application files (T1566.002).

NIST Phase: Post Incident

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

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 2.3 (Address Unauthorized Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Publish a Sigma rule targeting Sysmon Event ID 1 where ParentImage ends in `dfsvc.exe` and Image does NOT match known-good ClickOnce update binaries (e.g., `dfsvc.exe` self-update). For the LOLBin coverage gap review, map current Sysmon/Event Log detection rules against the LOLBAS project (lolbas-project.github.io) entries for dfshim.dll and dfsvc.exe to identify uncovered execution paths. Deliver a one-page awareness brief to end users illustrating how a spearphishing link to a malicious .application URL installs malware without any UAC prompt — use this campaign's mechanism as the concrete example.

Evidence: No live-state-altering action occurs in this phase; evidence focus shifts to documentation. Preserve the full incident record: the dfsvc.exe process tree logs from Sysmon, the scheduled task and registry export artifacts collected in Steps 3–4, network proxy or DNS logs showing the source URL from which the .application manifest was fetched (typically an HTTP GET to an attacker-controlled host returning Content-Type: application/x-ms-application), and any .application manifest XML files recovered from the ClickOnce deployment cache, which contain the attacker's ApplicationIdentity, publisher certificate details, and payload download URL — critical intelligence for threat actor attribution and future detection tuning.

Detection Guidance

Primary behavioral indicators: dfsvc.exe spawning unexpected child processes (cmd.exe, powershell.exe, wscript.exe, or any non-ClickOnce binary); rundll32.exe invoked with ClickOnce-related parent processes or with unusual command-line arguments referencing .application or .appref-ms files. File-based indicators: creation of .application or .appref-ms files in user-writable paths (APPDATA, TEMP, Downloads). Persistence indicators: scheduled task creation (Windows Event ID 4698) or registry run key writes (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) where the originating process is dfsvc.exe or a ClickOnce-spawned binary. Network indicators: outbound connections from dfsvc.exe to non-Microsoft

infrastructure, or connections over non-standard ports (T1571) originating from ClickOnce process trees. SIEM query approach: join process creation logs on ParentProcessName = 'dfsvc.exe' OR (ParentProcessName = 'rundll32.exe' AND CommandLine contains '.application'); alert on any result where ChildProcessName is a shell interpreter or scripting host. Map to NIST AU-2 (Audit Events) and AU-12 (Audit Generation) for process and file creation logging. Confirm logging is enabled per CIS 8.2 (Collect Audit Logs) before relying on absence of events as a clean indicator.

Framework Mappings

MITRE-ATTACK

- **T1218.011** — Rundll32
- **T1204.002** — Malicious File
- **T1105** — Ingress Tool Transfer
- **T1571** — Non-Standard Port
- **T1053.005** — Scheduled Task
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1553.002** — Code Signing
- **T1566.002** — Spearphishing Link
- **T1072** — Software Deployment Tools
- **T1547** — Boot or Logon Autostart Execution

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
- **CM-7** — Least Functionality
- **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
T1218.011	Rundll32	Defense-Evasion
T1204.002	Malicious File	Execution
T1105	Ingress Tool Transfer	Command-And-Control
T1571	Non-Standard Port	Command-And-Control
T1053.005	Scheduled Task	Execution
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1553.002	Code Signing	Defense-Evasion
T1566.002	Spearphishing Link	Initial-Access
T1072	Software Deployment Tools	Execution
T1547	Boot or Logon Autostart Execution	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/en-us/blog/new-abuse-of-the-clickonce-t...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-22 06:23 UTC by TJS Security Command Center