INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-20 06:53 UTC

ClickOnce Weaponized: Microsoft's Deployment Technology Becomes a Persistence and Initial Access Vector

SECURITY ANALYSIS | MEDIUM | CVSS 5.0

SCC Item ID	SCC-STY-2026-0228
Type	Security Analysis
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Microsoft ClickOnce (Windows enterprise environments)
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike researchers have documented, in detail, how Microsoft's ClickOnce deployment technology is being abused by threat actors to gain initial access and maintain persistence on Windows endpoints, without requiring administrative privileges. Because ClickOnce is a legitimate, built-in Windows capability, most enterprise security stacks do not monitor or restrict it, leaving a broadly deployed attack surface largely invisible to defenders. This research signals a maturing exploitation pattern against trusted deployment infrastructure and raises the operational bar for detection engineering teams who have not yet accounted for it.

Technical Analysis

CrowdStrike's two-part series (published June 18, 2026) is the first comprehensive public documentation of ClickOnce weaponization at this level of technical depth. ClickOnce is a Microsoft deployment technology that allows applications to be installed and auto-updated from a URL with minimal user interaction and, critically, without elevated privileges. Threat actors are abusing this in two distinct ways: as an initial access vector and as a persistence mechanism.

For initial access, the attack chain typically begins with a spearphishing link or attachment (MITRE T1566, T1566.002) that directs a target to an attacker-controlled URL hosting a malicious .application or .appref-ms file. The user executes the file (T1204.002), triggering ClickOnce's native deployment workflow. Because the process uses a signed Microsoft component and operates entirely in user space, it bypasses many endpoint controls that gate on administrative privilege elevation.

For persistence, ClickOnce's auto-update feature becomes a callback mechanism. Once a ClickOnce application is installed, it periodically checks an attacker-controlled deployment URL for updates (T1105, T1547). This creates a durable, low-noise channel for payload delivery or command-and-control that survives reboots and does not require registry run key manipulation or scheduled task creation, the artifacts defenders most commonly hunt.

The research also documents ClickOnce's use as a living-off-the-land technique (T1218), where the legitimate dfsvc.exe process is invoked as part of the deployment workflow, and where msiexec may be used as a secondary execution proxy, further blending malicious activity into normal Windows operations. CrowdStrike identified CWE-494 (Download of Code Without Integrity Check) and CWE-346 (Origin Validation Error) as the underlying weakness classes driving the abuse. No CVE has been assigned because the behavior represents a technique pattern, not a discrete patchable vulnerability.

The defensive gap this research exposes is primarily one of monitoring coverage, not missing patches. ClickOnce operates through dfsvc.exe and deploys applications to user-profile directories (typically %LOCALAPPDATA%\Apps\). Most EDR and SIEM deployments do not have explicit detection logic for malicious ClickOnce manifests, and many application control policies do not extend to user-space deployment workflows. The absence of a patch or CVE means organizations cannot rely on vulnerability management programs to drive remediation; this is a detection and configuration problem.

Action Checklist

1. Step 1: Assess exposure, audit your environment for ClickOnce usage: query endpoint telemetry for dfsvc.exe execution, .application and .appref-ms file opens, and application deployments under %LOCALAPPDATA%\Apps\ across Windows endpoints
2. Step 2: Review controls, verify EDR detection coverage for ClickOnce abuse patterns (dfsvc.exe spawning unexpected child processes, .appref-ms file execution from email client or browser process trees); confirm application control policies (NIST CM-7 Least Functionality) address user-space deployment mechanisms, not just system-level installs
3. Step 3: Update threat model, add T1547 (Boot/Logon Autostart Execution), T1204.002 (Malicious File), T1566.002 (Spearphishing Link), T1105 (Ingress Tool Transfer), and T1218 (System Binary Proxy Execution) to your threat register as a chained ClickOnce abuse scenario; flag CWE-494 and CWE-346 as relevant weakness classes for your application vetting program
4. Step 4: Implement detective controls, create SIEM/EDR rules alerting on: dfsvc.exe network connections to non-corporate URLs, .application or .appref-ms files opened from user Downloads or Temp directories, and ClickOnce application directories created in user profiles for unknown applications (NIST SI-4 System Monitoring, CIS 8.3 Collect Detailed Audit Logs)
5. Step 5: Enforce least privilege and URL controls, block or alert on .application and .appref-ms MIME types at the email gateway and web proxy where ClickOnce is not a business requirement; apply NIST AC-6 (Least Privilege) review to confirm no unnecessary ClickOnce deployment permissions exist; consider restricting dfsvc.exe network egress via host firewall policy (CIS 4.4, CIS 4.5)
6. Step 6: Communicate findings, brief application security and SOC leadership on the detection gap; frame this as a configuration and monitoring problem, not a patch cycle issue, and set a timeline for EDR rule deployment
7. Step 7: Monitor developments, track CrowdStrike's research series for part three or follow-on disclosures; monitor MITRE ATT&CK for technique updates to T1218 sub-techniques that may formalize

ClickOnce abuse

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent if Sysmon or EDR telemetry detects dfsvc.exe spawning cmd.exe, powershell.exe, or wscript.exe from an email client or browser parent process on any endpoint, or if a .appref-ms or .application file is found in a user Startup folder or Run registry key, indicating active ClickOnce-based persistence rather than theoretical exposure.
Recovery Notes	After containment controls are in place (MIME blocks, dfsvc.exe firewall egress restrictions, and Sysmon detection rules deployed), audit all %LOCALAPPDATA%\Apps\ directories across the endpoint fleet and remove any ClickOnce application installations that cannot be attributed to an approved business application. Verify that no .appref-ms files persist in user Startup folders (C:\Users*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\) or under HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry keys. Monitor dfsvc.exe network connection telemetry continuously for 30 days post-remediation to detect any reinfection attempts or previously undetected installations phoning home.
Forensic Artifacts	%LOCALAPPDATA%\Apps\ directory tree with full timestamps — ClickOnce installs user-space payloads here by design; unexpected application directories with recent creation timestamps are the primary host-side indicator of abuse | Sysmon Event ID 1 (Process Create) logs showing dfsvc.exe parent-child relationships — malicious ClickOnce abuse produces process chains such as outlook.exe → dfsvc.exe → cmd.exe or powershell.exe that do not appear in legitimate ClickOnce deployments | Sysmon Event ID 3 (Network Connection) logs for dfsvc.exe — legitimate ClickOnce deployments connect to known internal or vendor update URLs; connections to external, non-corporate hostnames by dfsvc.exe indicate a weaponized deployment manifest being fetched | HKCU\Software\Microsoft\Windows\CurrentVersion\Run and C:\Users*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ — ClickOnce persistence is achieved by writing .appref-ms shortcuts to user-accessible autostart locations that do not require administrative privilege to create or survive reboots | Email gateway and web proxy logs filtered for MIME type application/x-ms-application or file extensions .application and .appref-ms — the initial delivery vector for weaponized ClickOnce is a phishing link or email attachment; gateway logs record the delivery URL and sender identity that host-side forensics cannot recover after the file is opened

Per-Action IR Details

Step 1: Assess exposure — audit your environment for ClickOnce usage: query endpoint telemetry for dfsvc.exe execution, .application and .appref-ms file opens, and application deployments under %LOCALAPPDATA%\Apps\ across Windows endpoints

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing baseline visibility and understanding of the environment before an incident occurs

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), NIST AU-2 (Event Logging)

Compensating: On endpoints without EDR, deploy Sysmon with a configuration that logs Event ID 1 (Process Create) for dfsvc.exe and Event ID 11 (File Create) targeting *.application and *.appref-ms extensions. Use PowerShell:

`Get-ChildItem -Path "$env:LOCALAPPDATA\Apps" -Recurse -ErrorAction SilentlyContinue | Select FullName, CreationTime, LastWriteTime | Export-Csv clickonce_audit.csv`. Run across the fleet via scheduled task or GPO logon script.

Evidence: This is a pre-incident assessment step and does not alter live state. However, document baseline dfsvc.exe execution telemetry and the %LOCALAPPDATA%\Apps\ directory tree before any remediation actions are taken, as this establishes the pre-action state for comparison. Capture: Sysmon Event ID 1 logs for dfsvc.exe parent-child relationships, directory listings of %LOCALAPPDATA%\Apps\ with timestamps, and .application/.appref-ms file creation timestamps in user Download and Temp directories.

Step 2: Review controls — verify EDR detection coverage for ClickOnce abuse patterns (dfsvc.exe spawning unexpected child processes, .appref-ms file execution from email client or browser process trees); confirm application control policies (NIST CM-7 Least Functionality) address user-space deployment mechanisms, not just system-level installs

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: validating that tools, policies, and detection capabilities are in place prior to an incident

Controls: CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 2.2 (Ensure Authorized Software is Currently Supported), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Without EDR, use Sysmon Event ID 1 to audit dfsvc.exe child process creation: filter for dfsvc.exe as ParentImage and flag any child other than expected ClickOnce subprocess names (e.g., spawning cmd.exe, powershell.exe, wscript.exe). Use the Sigma rule community (SigmaHQ) to search for existing ClickOnce/dfsvc.exe detection rules and convert them to Windows Event Log queries runnable with Get-WinEvent. Review AppLocker or Software Restriction Policy rules to confirm they evaluate %LOCALAPPDATA%\Apps\ paths, not just %ProgramFiles%.

Evidence: This step reviews policy and tooling configuration and does not alter live host state. No volatile capture is required before this step. Document the current EDR rule inventory and AppLocker/SRP policy exports as a baseline artifact for post-incident review.

Step 3: Update threat model — add T1547 (Boot/Logon Autostart Execution), T1204.002 (Malicious File), T1566.002 (Spearphishing Link), T1105 (Ingress Tool Transfer), and T1218 (System Binary Proxy Execution) to your threat register as a chained ClickOnce abuse scenario; flag CWE-494 and CWE-346 as relevant weakness classes for your application vetting program

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: maintaining and updating threat intelligence, scenario planning, and incident handling procedures

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without a formal threat modeling platform, maintain a living markdown or spreadsheet threat register. Document the ClickOnce abuse chain as a scenario: phishing link or email attachment delivers a .application or .appref-ms file → dfsvc.exe fetches and installs a user-space payload → .appref-ms file written to the user's Startup folder or registry Run key for persistence — all without requiring administrative privileges. Reference CrowdStrike's published research as the intelligence source in the register entry.

Evidence: This is a threat-modeling and documentation step; it does not alter live host state and requires no volatile evidence capture. Retain the CrowdStrike research publication and any associated IOC lists as supporting documentation for the threat register entry.

Step 4: Implement detective controls — create SIEM/EDR rules alerting on: dfsvc.exe network connections to non-corporate URLs, .application or .appref-ms files opened from user Downloads or Temp directories, and ClickOnce application directories created in user profiles for unknown applications (NIST SI-4 System Monitoring, CIS 8.2 Collect Audit Logs)

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: establishing and tuning detection mechanisms to identify ClickOnce abuse indicators

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

Compensating: Deploy Sysmon with Event ID 3 (Network Connection) logging enabled for dfsvc.exe; alert on connections where DestinationHostname does not match an internal domain allowlist. Use Sysmon Event ID 11 (File Create) to detect .application or .appref-ms files written to %USERPROFILE%\Downloads or %TEMP%. Write a Sigma rule targeting Sysmon Event ID 1 where ParentImage matches outlook.exe, chrome.exe, firefox.exe, or msedge.exe and Image matches dfsvc.exe. Forward Sysmon events to a centralized syslog server (e.g., Graylog Community or the free tier of Elastic) for correlation.

Evidence: Detection rule deployment does not alter live host state. Before deploying new rules, export and archive the existing Sysmon configuration and any current EDR detection policy as a baseline. After rule activation, retain initial alert output for false-positive tuning documentation.

Step 5: Enforce least privilege and URL controls — block or alert on .application and .appref-ms MIME types at the email gateway and web proxy where ClickOnce is not a business requirement; apply NIST AC-6 (Least Privilege) review to confirm no unnecessary ClickOnce deployment permissions exist; consider restricting dfsvc.exe network egress via host firewall policy (CIS 4.4, CIS 4.5)

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: applying network and host controls to reduce the attack surface and limit ClickOnce abuse propagation

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Use Windows Defender Firewall with Advanced Security via GPO to create an outbound block rule for dfsvc.exe (path: %SystemRoot%\System32\dfshim.dll is the loader; target the dfsvc.exe binary at %SystemRoot%\Microsoft.NET\Framework*\dfsvc.exe) on endpoints where ClickOnce is not required. At the email gateway, add MIME-type blocks for application/x-ms-application and the .appref-ms extension. For web proxy, block or sandbox downloads of Content-Type: application/x-ms-application. Document business justifications for any exemptions before applying blocks.

Evidence: Before applying firewall policy changes or MIME blocks on active endpoints, capture: active dfsvc.exe network connections via `netstat -ano | findstr dfsvc` correlated with PID, current running processes showing dfsvc.exe instances via `tasklist /v`, and any existing %LOCALAPPDATA%\Apps\ directory state with `dir /s /tc "%LOCALAPPDATA%\Apps"`. These preserve evidence of any ClickOnce activity already in progress before controls alter network reachability.

Step 6: Communicate findings — brief application security and SOC leadership on the detection gap; frame this as a configuration and monitoring problem, not a patch cycle issue, and set a timeline for EDR rule deployment

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned, communication of findings, and process improvement to address identified gaps

Controls: NIST AC-1 (Policy And Procedures)

Compensating: For teams without a formal incident communication process, prepare a one-page brief using the following structure: (1) threat summary citing the CrowdStrike ClickOnce research, (2) current detection gap (dfsvc.exe not monitored, ClickOnce excluded from application control scope), (3) proposed Sysmon/firewall compensating controls with owner and deadline, (4) success metric (alert fired on dfsvc.exe spawning cmd.exe within 48 hours of rule deployment in test environment). Distribute via email with read-receipt to create an accountability record.

Evidence: No volatile evidence capture is required for this communication step. Attach the ClickOnce audit CSV from Step 1, the Sysmon rule export from Step 4, and the firewall policy change record from Step 5 as supporting documentation for the leadership brief.

Step 7: Monitor developments — track CrowdStrike's research series for part three or follow-on disclosures; monitor MITRE ATT&CK for technique updates to T1218 sub-techniques that may formalize ClickOnce abuse

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: integrating updated threat intelligence into detection and response processes to prevent recurrence

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Subscribe to CrowdStrike's Adversary Intelligence blog via RSS and configure a free Google Alert for the query: `ClickOnce dfsvc.exe malware`. Set a calendar-driven 30-day review cycle to check the MITRE ATT&CK T1218 technique page for sub-technique additions referencing ClickOnce. Maintain a change log in the threat register from Step 3 to record each update, the date reviewed, and any resulting detection rule modifications.

Evidence: This is a monitoring and intelligence-tracking step and does not alter live host state. No volatile evidence capture is required. Retain all research publications, ATT&CK changelog entries, and detection rule version history as institutional knowledge artifacts.

Detection Guidance

Primary hunting targets:

1. Process telemetry: Hunt for dfsvc.exe (the ClickOnce host process) spawning child processes, making outbound network connections to non-internal URLs, or writing executables to disk. Baseline legitimate dfsvc.exe behavior in your environment before deploying alerts to reduce false positives.

2. File system: Alert on .application and .appref-ms files written to user Download, Temp, or Desktop directories. Monitor for new application directories created under %LOCALAPPDATA%\Apps\ for applications not in your approved software inventory (CIS 2.1 Software Inventory).

3. Parent-child process chains: Flag .application or .appref-ms file opens where the parent process is a mail client (Outlook, Thunderbird), browser, or Teams, as this indicates the spearphishing delivery chain (T1566, T1566.002, T1204.002).

4. Network: Monitor for periodic, low-frequency outbound HTTP/HTTPS requests from dfsvc.exe to external hosts, which may indicate the auto-update callback (T1105, T1547). Compare destination URLs against known-good ClickOnce deployment infrastructure in your environment.

5. Log sources to enable: Windows Security Event Log (process creation with command-line logging enabled), Sysmon Event ID 1 (Process Create) and Event ID 3 (Network Connection), EDR process tree visibility, and proxy/firewall logs filtered for dfsvc.exe User-Agent strings.

6. D3FEND countermeasures: Apply D3-SFA (System File Analysis) to monitor ClickOnce manifest files and application directories for unauthorized modifications. Use D3-LAM (Local Account Monitoring) to detect ClickOnce applications deployed under service or shared accounts. D3-UAP (User Account Permissions) review can identify accounts with unnecessary ClickOnce deployment rights.

Audit gaps: Confirm your application allowlisting or control policy explicitly addresses user-space deployments via dfsvc.exe, not only MSI or EXE installs requiring elevation. Most AppLocker and WDAC policies focus on system-level paths and may miss user-profile deployment directories.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`dfsvc.exe`	dfsvc.exe (Microsoft ClickOnce host process) leveraged via malicious .application or .appref-ms files to deploy attacker-controlled payloads in user-profile directories without administrative privileges, establishing persistence via auto-update callbacks to attacker-controlled URLs	HIGH
TOOL	`Pending — refer to CrowdStrike blog series (Part 1 and Part 2) for published indicators`	CrowdStrike's two-part technical series may contain specific payload hashes, C2 URLs, or ClickOnce manifest samples; the provided source material does not include discrete indicator values	LOW

Framework Mappings

MITRE-ATTACK

- **T1547** — Boot or Logon Autostart Execution
- **T1204.002** — Malicious File
- **T1566.002** — Spearphishing Link
- **T1105** — Ingress Tool Transfer
- **T1218** — System Binary Proxy Execution
- **T1566** — Phishing

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

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

ISO-27001-2022

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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1547	Boot or Logon Autostart Execution	Persistence
T1204.002	Malicious File	Execution
T1566.002	Spearphishing Link	Initial-Access
T1105	Ingress Tool Transfer	Command-And-Control
T1218	System Binary Proxy Execution	Defense-Evasion
T1566	Phishing	Initial-Access

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/new-abuse-of-the-clickonce-t...	T3
	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
How CrowdStrike Falcon® Protects Against Follina (CVE-2022-30190)	https://www.crowdstrike.com/en-us/blog/how-crowdstrike-falcon-prote...	T3

Generated 2026-06-20 06:53 UTC by TJS Security Command Center