INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-21 13:20 UTC

ClickOnce as a Persistence Platform: Why a Decades-Old Deployment Tech Is Getting Fresh Attention from Attackers

SECURITY ANALYSIS | MEDIUM | CVSS 5.0

SCC Item ID	SCC-STY-2026-0236
Type	Security Analysis
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Microsoft Windows, ClickOnce framework (.appref-ms manifests, dfsvc.exe, rundll32.exe); all Windows versions supporting ClickOnce deployment
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike has published a two-part research series revealing how Microsoft's ClickOnce deployment technology, a framework present on virtually every modern Windows system, can be weaponized for initial access, payload delivery, and persistent footholds without requiring administrator privileges. Because execution runs inside legitimate Microsoft process trees (dfsvc.exe, rundll32.exe), most signature-based endpoint tools will not flag the activity. This research signals a broader attacker trend toward living off the land (LOTL) techniques that abuse trusted deployment infrastructure, where the attack surface is not a flaw to patch but a design feature to detect around.

Technical Analysis

CrowdStrike's two-part series maps a previously underexamined attack surface: Microsoft's ClickOnce deployment framework, which has shipped with Windows since the early 2000s and remains active across all current Windows versions. The research documents how threat actors can weaponize three specific components: the .appref-ms manifest file format (used to reference and launch ClickOnce applications), the dfsvc.exe deployment service host (the legitimate Microsoft process that fetches and installs ClickOnce packages), and rundll32.exe invocation paths that can be chained into the deployment flow.

Part One of the series establishes the initial access and payload delivery mechanics. A malicious .appref-ms file, delivered via spearphishing link (T1566.002) or social engineering to induce user execution (T1204.002), triggers dfsvc.exe to fetch and install a remote payload (T1105). Because dfsvc.exe is a signed Microsoft binary performing its designed function, the process tree appears benign to tools that rely on process parentage or

binary signature checks. The technique maps to T1218.011 (Rundll32 abuse) where rundll32.exe is used as an invocation path alongside the deployment chain. Masquerading techniques (T1036.005) are relevant because the .appref-ms extension is unfamiliar to most users and security teams, reducing suspicion on delivery.

Part Two introduces a persistence technique detailed in this research. The research maps this to T1547 and T1547.001 (Boot or Logon Autostart Execution, Registry Run Keys/Startup Folder), T1053.005 (Scheduled Task/Job: Scheduled Task), and T1197 (BITS Jobs), indicating the researchers identified multiple persistence vectors achievable through ClickOnce's update and re-execution mechanisms. T1071.001 (Application Layer Protocol: Web Protocols) covers the C2 or update-channel communication that ClickOnce's design natively supports, providing a built-in, low-friction exfiltration or command channel.

The core defensive gap this research exposes is the blind spot created when legitimate, trusted deployment infrastructure becomes the delivery mechanism. ClickOnce was designed to install and update applications silently and without elevated privileges, properties that are features in a developer context and liabilities in a threat context. No CVE is assigned because no discrete vulnerability exists; the framework behaves as intended. CWE-494 (Download of Code Without Integrity Check) and CWE-693 (Protection Mechanism Failure) characterize the underlying weakness classes, pointing to the absence of enforced integrity verification on fetched manifests and the failure of downstream protection mechanisms to distinguish malicious from legitimate ClickOnce activity.

The industry implication is significant. This research joins a growing body of work documenting how attackers are shifting from exploiting broken code to exploiting trusted infrastructure: Windows Management Instrumentation, Microsoft Build Engine, and now ClickOnce. Detection engineering must account for behavioral context, not binary reputation. CrowdStrike provides Falcon-specific hunting guidance in the source series, and the MITRE ATT&CK mappings offer a framework-agnostic starting point for teams on other platforms.

Action Checklist

1. Step 1: Assess ClickOnce exposure, audit whether your Windows environment has ClickOnce deployment enabled or in active use (check for .appref-ms file associations and dfsvc.exe execution history in EDR telemetry); if ClickOnce is not required by any business application, evaluate disabling or restricting it via Group Policy
2. Step 2: Review detection coverage for T1218.011 and T1204.002, verify that your EDR and SIEM have behavioral rules covering rundll32.exe abuse and user-executed file types beyond Office macros; .appref-ms should be treated as an executable-class extension in email gateway and endpoint policies (CIS 2.3: Address Unauthorized Software; NIST SI-4: System Monitoring)
3. Step 3: Audit persistence detection coverage, review detection rules for T1547.001 (Registry Run Key modifications), T1053.005 (Scheduled Task creation by non-admin processes), and T1197 (BITS Job creation); ensure low-privilege persistence mechanisms are logged and alerted (NIST AU-2: Event Logging; CIS 8.2: Collect Audit Logs)
4. Step 4: Harden execution controls, block or alert on dfsvc.exe making outbound connections to non-approved hosts using application-layer firewall rules or DNS filtering; apply NIST AC-6 (Least Privilege) and AC-4 (Information Flow Enforcement) principles to restrict what ClickOnce's service host can reach
5. Step 5: Update threat model and hunting backlog, incorporate T1566.002 (spearphishing link via .appref-ms), T1105 (remote payload delivery via dfsvc.exe), and T1547/T1053.005 persistence chains into your threat register; assign a hunting hypothesis to review historical dfsvc.exe network connections and

.appref-ms execution events in EDR logs

6. Step 6: Communicate to leadership, brief security leadership that this is a technique-class risk with no patch available; mitigation is detection engineering and configuration hardening, and the organization's exposure depends on ClickOnce usage and current behavioral detection maturity

7. Step 7: Monitor for threat actor adoption and community reproductions, the CrowdStrike two-part series establishes the technique; track for independent confirmations, detection tool updates, or threat actor adoption reports that would elevate urgency

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent if threat hunting (Step 5) surfaces any confirmed dfsvc.exe process with outbound connections to non-approved external hosts, .appref-ms execution originating from email client or browser download paths, or Registry Run Key / Scheduled Task creation by a dfsvc.exe child process — any of these indicators suggest active exploitation rather than latent exposure, warranting immediate containment and incident declaration per NIST 800-61r3 §3.2.
Recovery Notes	Because ClickOnce can establish low-privilege persistence via Registry Run Keys, Scheduled Tasks, or BITS jobs without leaving obvious high-privilege artifacts, recovery validation must explicitly enumerate all three persistence vectors on any host where dfsvc.exe showed anomalous network activity: query `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, export the Task Scheduler operational log for tasks created within the suspicious timeframe, and audit the BITS client log for unexpected jobs. After clearing identified persistence mechanisms, maintain elevated Sysmon and network logging on affected hosts for a minimum of 30 days, specifically watching for dfsvc.exe re-execution or rundll32.exe invoking dfshim.dll, as ClickOnce's auto-update mechanism could re-pull a malicious manifest if the original delivery URL remains accessible.
Forensic Artifacts	Sysmon Event ID 1 (Process Create) records for dfsvc.exe and rundll32.exe with command lines containing 'dfshim' — captures the ClickOnce execution chain from initial .appref-ms invocation through payload staging | Sysmon Event ID 3 (Network Connection) records for dfsvc.exe — captures outbound connections to attacker-controlled ClickOnce distribution servers used for remote payload delivery via the auto-update mechanism | Windows Prefetch files at C:\Windows\Prefetch\DFSVC.EXE-*.pf and RUNDLL32.EXE-*.pf — timestamps and referenced file paths establish when ClickOnce was invoked and which DLLs (including dfshim.dll) were loaded, surviving after process termination | ClickOnce application cache directory at %LOCALAPPDATA%\Apps\2.0\ — contains downloaded manifests, staged payloads, and application files written by dfsvc.exe during deployment; preserves attacker-controlled content and delivery URLs from the .appref-ms manifest | Windows Task Scheduler operational log (Microsoft-Windows-TaskScheduler/Operational) and registry keys HKCU\Software\Microsoft\Windows\CurrentVersion\Run filtered for entries created within the dfsvc.exe execution timeframe — captures low-privilege persistence mechanisms a ClickOnce-delivered payload would establish without requiring administrator rights

Per-Action IR Details

Step 1: Assess ClickOnce exposure — audit whether your Windows environment has ClickOnce deployment enabled or in active use (check for .appref-ms file associations and dfsvc.exe execution history in EDR telemetry); if ClickOnce is not required by any business application, evaluate disabling or restricting it via

Group Policy

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing the capability to respond by inventorying attack surface and hardening before exploitation occurs

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), NIST AC-6 (Least Privilege)

Compensating: Run the following PowerShell one-liner across endpoints (via PSRemoting or a scheduled task deployed by GPO) to enumerate dfsvc.exe execution history from Windows Security Event Log: `Get-WinEvent -LogName Security | Where-Object {$_.Message -match 'dfsvc.exe'} | Select-Object TimeCreated, Message | Export-Csv dfsvc_audit.csv`. Separately, query the registry for .appref-ms file association: `Get-ItemProperty 'HKLM:\SOFTWARE\Classes\.appref-ms'`. On endpoints running Sysmon (Event ID 1), filter for Image path containing dfsvc.exe to get a historical execution baseline without EDR.

Evidence: This step is an audit/assessment action and does not alter live system state; no volatile capture is required before execution. However, before making any GPO change to disable ClickOnce, document current .appref-ms handler registrations (`HKLM\SOFTWARE\Classes\.appref-ms` and `HKCU\SOFTWARE\Classes\.appref-ms`) and capture the current dfsvc.exe execution history from Sysmon Event ID 1 logs as a pre-change baseline.

Step 2: Review detection coverage for T1218.011 and T1204.002 — verify that your EDR and SIEM have behavioral rules covering rundll32.exe abuse and user-executed file types beyond Office macros; .appref-ms should be treated as an executable-class extension in email gateway and endpoint policies (CIS 2.3: Address Unauthorized Software; NIST SI-4: System Monitoring)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: building detection capability and tooling before an incident occurs, including tuning sensors for known attacker techniques

Controls: CIS 2.3 (Address Unauthorized Software), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation)

Compensating: Deploy the following Sysmon configuration additions if no EDR is present: ensure Event ID 1 (Process Create) captures full command lines for rundll32.exe and dfsvc.exe parents; add Sysmon Event ID 11 (File Create) filtering for *.appref-ms drops in user-writable paths (%TEMP%, %APPDATA%, Downloads). For email gateway, add .appref-ms to the blocked attachment extension list alongside .exe, .js, and .hta — most mail gateways (including free tiers of Exchange transport rules) support extension-based blocking. Reference the community Sigma rule `proc_creation_win_rundll32_parent_dfsvc` if available in your Sigma rule set.

Evidence: This step modifies detection rules and gateway policies, not live host state; no volatile evidence capture is required before execution. Before tuning, export the current SIEM/EDR rule set for rundll32.exe and .appref-ms as a versioned baseline so rule gaps are documented for the post-incident review record.

Step 3: Audit persistence detection coverage — review detection rules for T1547.001 (Registry Run Key modifications), T1053.005 (Scheduled Task creation by non-admin processes), and T1197 (BITS Job creation); ensure low-privilege persistence mechanisms are logged and alerted (NIST AU-2: Event Logging; CIS 8.2: Collect Audit Logs)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: ensuring logging and alerting infrastructure can surface the specific low-privilege persistence mechanisms ClickOnce-delivered payloads would use after initial access

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

Compensating: Enable Windows audit policy for Object Access (registry) and Task Scheduler operational log (`Microsoft-Windows-TaskScheduler/Operational`) on all endpoints via GPO — both are free and natively available. For Registry Run Key monitoring without EDR, use Sysmon Event ID 13 (Registry Value Set) filtered to `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\...\Run` — these are the specific keys a low-privilege ClickOnce payload would write to. For BITS job monitoring, enable Sysmon Event ID 22 (DNS Query) and cross-correlate with Windows BITS client operational log (`Microsoft-Windows-Bits-Client/Operational`) for unexpected

job creation by dfsvc.exe or its child processes.

Evidence: This step modifies detection and logging configuration, not live host state; no volatile capture is required before execution. Document the current state of Task Scheduler operational log retention settings and registry audit policy before changes so coverage gaps are formally recorded.

Step 4: Harden execution controls — block or alert on dfsvc.exe making outbound connections to non-approved hosts using application-layer firewall rules or DNS filtering; apply NIST AC-6 (Least Privilege) and AC-4 (Information Flow Enforcement) principles to restrict what ClickOnce's service host can reach

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: restricting attacker capabilities and limiting blast radius by controlling network reachability of the abused process before confirmed exploitation is identified

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: Create a Windows Defender Firewall outbound rule via GPO blocking dfsvc.exe (`%WinDir%\system32\dfshim.dll` is loaded by rundll32.exe; target the rundll32.exe process when invoked with dfshim.dll argument) from connecting to any destination except explicitly approved ClickOnce distribution servers. Command: `netsh advfirewall firewall add rule name='Block dfsvc Outbound' dir=out action=block program='%SystemRoot%\System32\dfsvc.exe'`. For DNS filtering, if Pi-hole or a similar free DNS sink is in use, create a blocklist entry for any domains not in the approved ClickOnce manifest allowlist. Alert-mode (log but allow) is preferred over hard block until the approved server list is confirmed to avoid breaking legitimate deployments.

Evidence: Before applying firewall rules that alter network flow for dfsvc.exe, capture current active network connections from any host where dfsvc.exe execution has been observed: run `netstat -ano | findstr ` and `Get-NetTCPConnection | Where-Object {$_.OwningProcess -eq }` to document existing outbound destinations. If a host shows dfsvc.exe with active or recent connections to non-approved infrastructure, treat it as potentially compromised and acquire a full memory image (via WinPmem or Magnet RAM Capture) and prefetch artifacts (`C:\Windows\Prefetch\DFSVC.EXE-*.pf`) before applying the block rule.

Step 5: Update threat model and hunting backlog — incorporate T1566.002 (spearphishing link via .appref-ms), T1105 (remote payload delivery via dfsvc.exe), and T1547/T1053.005 persistence chains into your threat register; assign a hunting hypothesis to review historical dfsvc.exe network connections and .appref-ms execution events in EDR logs

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: proactively analyzing telemetry for indicators of the ClickOnce abuse chain before a confirmed incident is declared, using threat-informed hunting hypotheses

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

Compensating: For teams without a SIEM, conduct structured manual hunting using the following targeted queries. In Windows Security Event Log (Event ID 4688 with command-line auditing enabled), filter for: (1) rundll32.exe with command line containing 'dfshim' or 'dfsvc'; (2) process creation where Parent Image is dfsvc.exe and Child is not a known-good ClickOnce subprocess. In Sysmon logs (Event ID 3 — Network Connection), filter for dfsvc.exe initiating connections to external IPs. Export results with: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 3 -and $_.Message -match 'dfsvc.exe'} | Export-Csv dfsvc_netconn.csv`. Hunting timeframe should cover at least 90 days of available telemetry given ClickOnce's use as a persistence platform.

Evidence: This step is analytical and does not alter live host state; no volatile capture is required before execution. Preserve all raw EDR query results, Sysmon exports, and Event Log extracts as timestamped evidence files before analysis modifies or filters the data set — these become the hunting artifact record if a confirmed incident is subsequently declared per NIST 800-61r3 §3.2.

Step 6: Communicate to leadership — brief security leadership that this is a technique-class risk with no patch available; mitigation is detection engineering and configuration hardening, and the organization's exposure depends on ClickOnce usage and current behavioral detection maturity

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: communicating findings, risk posture, and remediation strategy to stakeholders; applicable here as a proactive risk communication prior to confirmed exploitation

Controls: NIST AC-1 (Policy and Procedures)

Compensating: Prepare a one-page risk brief using the following structure: (1) Threat summary — ClickOnce abuse executes via legitimate Microsoft processes (dfsvc.exe, rundll32.exe) with no patch available; (2) Exposure assessment — list business applications currently using ClickOnce (output from Step 1 audit); (3) Current detection gap — confirm whether .appref-ms is blocked at email gateway and whether behavioral rules for dfsvc.exe outbound connections exist; (4) Recommended actions with owner and timeline drawn from Steps 1-5. No special tooling required; a structured Word or PDF document is sufficient for the communication artifact.

Evidence: This step does not alter live system state; no volatile capture is required. Attach the dfsvc.exe execution audit output from Step 1, the detection coverage gap analysis from Step 2, and the threat hunting results from Step 5 as supporting appendices to the leadership brief so that risk assertions are evidence-backed.

Step 7: Monitor CrowdStrike research channel for follow-on disclosures — the published series is two parts; track for additional parts, community reproductions, or threat actor adoption reports that would elevate urgency

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: integrating external threat intelligence updates into organizational risk posture and updating detection and response capabilities as the threat evolves

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

Compensating: Subscribe to the CrowdStrike Adversary Intelligence blog RSS feed and configure a free RSS-to-email alert (e.g., via RSS.app free tier or a self-hosted RSS reader) filtered for terms: 'ClickOnce', 'dfsvc', 'appref-ms', 'dfshim'. Additionally, monitor the MITRE ATT&CK T1218.011 and T1204.002 technique pages for new procedure examples referencing ClickOnce, and set a Google Alert for 'ClickOnce malware' and 'dfsvc.exe threat actor'. Assign a recurring 2-week calendar review to the threat hunting backlog item created in Step 5 so new IOCs from community reproductions are incorporated promptly.

Evidence: This step does not alter live system state; no volatile capture is required. Maintain a dated intelligence log entry each time this monitoring cadence is executed, recording the sources checked, any new findings, and whether the triage priority assigned in this analysis requires re-evaluation — this log constitutes the threat intelligence maintenance record for audit purposes.

Detection Guidance

Detection for ClickOnce abuse is behavioral, not signature-based. The following hunting priorities are derived from the MITRE ATT&CK techniques mapped in the CrowdStrike research.

Process execution: Hunt for dfsvc.exe making outbound HTTP/HTTPS connections to external or non-internal-update-server hosts. In most enterprise environments, dfsvc.exe should connect only to known internal deployment servers or approved vendor URLs; any deviation is suspicious. Correlate dfsvc.exe parent-child relationships: if dfsvc.exe is spawning cmd.exe, powershell.exe, or any interpreter, that is a high-fidelity signal.

File execution: Alert on .appref-ms file execution, particularly when the source is email delivery, browser download, or a user temp directory. Most enterprises have no legitimate user-initiated .appref-ms execution outside of managed software deployment workflows. Treat .appref-ms as an executable-class extension in DLP and email gateway rules (aligns with CIS 2.3).

Rundll32.exe chains: Monitor for rundll32.exe invocations that reference dfshim.dll (ClickOnce's legitimate DLL shim) in contexts outside expected software deployment workflows - unusual parent processes, external URLs, or non-admin user contexts are high-fidelity signals. Review rundll32.exe command-line arguments for unusual paths or remote URLs (T1218.011).

Persistence artifacts: Query for new scheduled tasks (T1053.005) and Registry Run Key writes (T1547.001) created by dfsvc.exe, rundll32.exe, or any process descending from a ClickOnce invocation. BITS job creation (T1197) by non-system, non-admin accounts in proximity to dfsvc.exe execution is a secondary persistence indicator.

Network: Flag outbound web protocol traffic (T1071.001) originating from dfsvc.exe to newly registered or low-reputation domains. ClickOnce's update mechanism can be repurposed as a C2 channel, so recurring beaconing from dfsvc.exe to external hosts is a high-priority hunt.

Log sources to enable: Windows Security Event Log (process creation with command-line logging, Event ID 4688), Sysmon (Events 1, 3, 7, 11, 12, 13), EDR process telemetry, DNS query logs filtered on dfsvc.exe process context, and BITS job logs (Microsoft-Windows-Bits-Client/Operational). Aligns with NIST AU-2 (Event Logging), AU-3 (Content of Audit Records), and CIS 8.2 (Collect Audit Logs).

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`dfsvc.exe`	dfsvc.exe (Microsoft ClickOnce deployment service host) leveraged via user-executed .appref-ms manifest to fetch and install remote payloads from attacker-controlled infrastructure without elevated privileges	HIGH
TOOL	`rundll32.exe`	rundll32.exe leveraged via ClickOnce deployment chain (dfshim.dll) to execute and persist malicious payloads while evading process-parentage detection mechanisms.	HIGH
TOOL	`.appref-ms`	.appref-ms manifest files delivered via spearphishing link (T1566.002) or social engineering; user execution triggers dfsvc.exe to initiate remote payload retrieval (T1204.002, T1105)	HIGH
TOOL	`dfshim.dll`	dfshim.dll (ClickOnce DLL shim) invoked via rundll32.exe as part of the ClickOnce execution chain; presence in rundll32.exe command-line arguments outside managed deployment context is a detection signal	HIGH

Type	Value	Context	Confidence
URL	`Pending — refer to CrowdStrike blog (Part One and Part Two) for published behavioral indicators and Falcon hunting queries`	CrowdStrike's two-part series includes Falcon-specific hunting guidance and additional indicators; specific IOC values (hashes, C2 domains) are not reproduced in the available source text	LOW

Framework Mappings

MITRE-ATTACK

- **T1204.002** — Malicious File
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1218.011** — Rundll32
- **T1053.005** — Scheduled Task
- **T1197** — BITS Jobs
- **T1547** — Boot or Logon Autostart Execution
- **T1566.002** — Spearphishing Link
- **T1105** — Ingress Tool Transfer
- **T1071.001** — Web Protocols
- **T1547.001** — Registry Run Keys / Startup Folder

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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1204.002	Malicious File	Execution
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1218.011	Rundll32	Defense-Evasion
T1053.005	Scheduled Task	Execution
T1197	BITS Jobs	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1566.002	Spearphishing Link	Initial-Access
T1105	Ingress Tool Transfer	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1547.001	Registry Run Keys / Startup Folder	Persistence

Sources

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

Generated 2026-06-21 13:20 UTC by TJS Security Command Center