INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-20 18:47 UTC

ClickOnce Weaponized: How Attackers Use Microsoft's Deployment Framework for Fileless Persistence Without Admin Rights

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0230
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Windows, ClickOnce deployment technology (.application, .appref-ms), dfsvc.exe, rundll32.exe
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike researchers have documented a multi-technique attack campaign exploiting Microsoft's ClickOnce deployment framework, a built-in Windows mechanism, to deliver malware, achieve fileless persistence, and update payloads without requiring administrator privileges. The attack chain executes entirely within trusted Microsoft process trees, allowing it to evade email filters and endpoint controls tuned to detect traditional executable formats. This research signals a broader adversarial shift toward abusing legitimate, low-scrutiny Windows components, meaning organizations cannot rely on perimeter or signature-based controls alone to detect or block this class of threat.

Technical Analysis

ClickOnce is a Microsoft deployment technology designed to let users install and run Windows applications directly from a web page or network share, with automatic update capabilities and no elevation requirement. CrowdStrike's two-part research series documents how attackers have repurposed these legitimate mechanics into a delivery and persistence chain that sidesteps conventional defenses.

The attack surface centers on two file types: .application manifests and .appref-ms shortcut references. When a user clicks a malicious link, Windows invokes dfsvc.exe, the ClickOnce deployment service, which downloads and installs the payload into the user's AppData directory without triggering a UAC prompt. Subsequent execution and persistence can occur through rundll32.exe, a trusted Windows binary, keeping the process tree within Microsoft-signed parent processes. This is a living-off-the-land technique that leverages signed Windows binaries to evade detection, mapped to MITRE T1218.011 (Signed Binary Proxy Execution: Rundll32) and

T1036.005 (Masquerading: Match Legitimate Name or Location).

Persistence is established through mechanisms including Scheduled Tasks (T1053.005), Boot or Logon Autostart Execution (T1547 and T1547.001 specifically, targeting the Registry Run Keys path), and BITS Jobs (T1197), which can also serve as a covert payload update channel, satisfying T1105 (Ingress Tool Transfer). The update-without-interaction capability is particularly consequential: an attacker can silently push new payload versions through the same ClickOnce channel used for initial installation, effectively turning Microsoft's patching logic against defenders.

Initial access relies on spearphishing links (T1566.002) and user execution (T1204.001), consistent with a low-barrier delivery model. Obfuscation techniques (T1027) are applied to the manifest or payload to reduce static detection coverage. The two CWEs assigned, CWE-494 (Download of Code Without Integrity Check) and CWE-693 (Protection Mechanism Failure), identify the root technical conditions that make this exploitation path viable: ClickOnce's trust in remotely hosted manifests and the absence of consistent security tooling scrutiny on .application and .appref-ms file types.

Part 2 of the CrowdStrike series, covering newly identified techniques beyond the initial disclosure, indicates active research and likely adversarial iteration. The defensive gap this exploits is primarily a coverage gap: most organizations have tuned EDR and email gateway rules around .exe, .msi, and Office macro delivery. The .application and .appref-ms extensions pass through many filters unexamined. Security teams that have not explicitly addressed ClickOnce in their threat models are likely blind to this execution path in their telemetry.

Action Checklist

1. Step 1: Assess exposure, determine whether ClickOnce is enabled in your environment; check Group Policy under Computer Configuration > Administrative Templates > Windows Components > Application Deployment for ClickOnce controls, and inventory whether any internal or vendor applications deploy via .application or .appref-ms files (NIST AC-20, CIS 2.1)
2. Step 2: Review email and web gateway rules, add .application and .appref-ms to blocked or quarantined attachment types in your mail gateway; configure web proxies to flag or block downloads of these file types from uncategorized or external URLs (CIS 4.4, CIS 4.5, NIST SC controls)
3. Step 3: Audit EDR detection coverage for dfsvc.exe and rundll32.exe, verify that your endpoint telemetry captures process creation events under dfsvc.exe and flags rundll32.exe invocations that originate from AppData paths or that have no associated signed parent; tune detection rules to alert on these patterns (NIST SI-4, NIST AU-2, CIS 8.2)
4. Step 4: Hunt for existing persistence via Scheduled Tasks and Registry Run Keys, query endpoint telemetry for Scheduled Tasks created by dfsvc.exe or entries written to HKCU\Software\Microsoft\Windows\CurrentVersion\Run by non-standard processes; review BITS job queues for unexpected download tasks (MITRE T1053.005, T1547.001, T1197)
5. Step 5: Update your threat model and detection rules, map the full TTP chain from the CrowdStrike Part 1 and Part 2 disclosures into your SIEM detection logic and threat register; assign ownership for ongoing monitoring of the CrowdStrike ClickOnce research series for additional technique disclosures (NIST IR-4, CIS 7.1)
6. Step 6: Communicate findings to leadership, brief stakeholders on the specific risk that a single webpage click can install persistent malware on any standard user workstation without admin rights, and explain that existing email filters likely do not block the delivery mechanism (NIST IR-1, CIS 7.2)

7. Step 7: Monitor for follow-up research and threat actor adoption, track the CrowdStrike blog for additional parts in this series and watch threat intelligence feeds for adoption of these techniques by named threat actors or ransomware affiliates

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to incident response immediately if dfsvc.exe child processes, rundll32.exe invocations from %LOCALAPPDATA%\Apps\2.0\, or Scheduled Tasks/BITS jobs created by ClickOnce processes are confirmed on any endpoint, or if threat intelligence feeds report active ransomware affiliate adoption of the documented ClickOnce TTP chain, as this would indicate imminent mass exploitation risk requiring breach notification assessment for environments holding PII or PHI.
Recovery Notes	After confirming eradication, verify the complete removal of all ClickOnce-installed payloads by recursively hashing and reviewing %LOCALAPPDATA%\Apps\2.0\ against the pre-compromise baseline, deleting any Scheduled Tasks or Registry Run Keys created by dfsvc.exe, and canceling all suspicious BITS jobs. Reimage affected workstations where forensic analysis cannot conclusively rule out fileless secondary payloads written to memory-mapped regions or injected into legitimate processes. Monitor all recovered workstations for a minimum of 30 days using Sysmon Event ID 1 alerts on dfsvc.exe process creation and outbound connections from dfsvc.exe or rundll32.exe to external IPs, given that ClickOnce's native auto-update mechanism could re-pull a payload if the manifest URL remains reachable and the application registration persists.
Forensic Artifacts	%LOCALAPPDATA%\Apps\2.0\ directory tree — ClickOnce installs all application files here under uniquely hashed subdirectories; forensic review should hash all executables and DLLs within this path and compare against known-good ClickOnce application manifests to identify malicious payloads staged as legitimate-looking assemblies | Windows Security Event Log Event ID 4688 (Process Creation) or Sysmon Event ID 1 — filter for processes with ParentImage of dfsvc.exe or for rundll32.exe with CommandLine paths referencing %LOCALAPPDATA%\Apps\2.0\, which are the specific execution chain artifacts left by this ClickOnce campaign | Scheduled Task XML definitions in C:\Windows\System32\Tasks\ — export and review all task definitions for Action elements pointing to %LOCALAPPDATA%\Apps\2.0\ paths or invoking rundll32.exe with AppData arguments, as ClickOnce-based persistence is achieved via per-user Scheduled Tasks that do not require admin privileges and survive reboots | HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry key — export and review for values written by non-standard processes referencing dfsvc.exe, .application files, or AppData paths, capturing the user-level auto-run persistence mechanism used in this campaign without requiring HKLM write access | BITS job queue (bitsadmin /list /allusers /verbose output) — ClickOnce leverages BITS for background payload retrieval and update delivery; preserve the full BITS job list including remote URL, local destination path, and job owner before any remediation, as BITS jobs writing to %LOCALAPPDATA%\Apps\2.0\ from external domains are direct indicators of active C2-driven update activity

Per-Action IR Details

Step 1: Assess exposure — determine whether ClickOnce is enabled in your environment; check Group Policy under Computer Configuration > Administrative Templates > Windows Components > Internet Explorer for ClickOnce controls, and inventory whether any internal or vendor applications deploy via .application or

.appref-ms files (NIST AC-20, CIS 2.1)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and understanding the attack surface before an incident occurs

Controls: NIST AC-20 (Use Of External Systems) — governs authorization of externally-sourced deployment mechanisms such as ClickOnce .application files retrieved from vendor or internet URLs, CIS 2.1 (Establish and Maintain a Software Inventory) — requires inventorying all licensed software including ClickOnce-deployed applications distributed via .application or .appref-ms manifests

Compensating: Run `Get-AppLockerPolicy -Effective | Select-Object -ExpandProperty RuleCollections` to identify whether AppLocker rules restrict .application execution. Use `reg query HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Security` to surface Group Policy restrictions on ClickOnce. Search %LOCALAPPDATA%\Apps\2.0\ on sampled workstations with `dir /s /b *.application` to discover previously installed ClickOnce apps without an EDR.

Evidence: This step is an assessment and does not alter live state. Before acting on findings, document the current state of %LOCALAPPDATA%\Apps\2.0\ directory trees (ClickOnce application cache), existing Scheduled Task XML exports via `schtasks /query /fo XML /v > tasks_baseline.xml`, and HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry exports as a clean baseline for later comparison during hunting.

Step 2: Review email and web gateway rules — add .application and .appref-ms to blocked or quarantined attachment types in your mail gateway; configure web proxies to flag or block downloads of these file types from external URLs (CIS 4.4, CIS 4.5, NIST SC controls, MITRE D3-PBWSAM)

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Preventing further delivery of the ClickOnce payload via email and web channels before compromise spreads

Controls: NIST AC-4 (Information Flow Enforcement) — directly governs blocking the flow of .application and .appref-ms file types from external sources through mail and web gateways based on information flow policy, CIS 4.4 (Implement and Manage a Firewall on Servers) — covers server-side gateway enforcement to block delivery of malicious ClickOnce manifest file types, CIS 4.5 (Implement and Manage a Firewall on End-User Devices) — covers host-based filtering on workstations to prevent execution of .application files downloaded from uncategorized external URLs

Compensating: On mail gateways without MIME-type blocking, add a Postfix header_checks or Exchange transport rule matching filename extensions `\.application$` and `\.appref-ms$` to quarantine. For web proxies, add a Squid ACL: `acl clickonce urlpath_regex -i \.application$ \.appref-ms$` with `http_access deny clickonce`. Use Windows Firewall with `netsh advfirewall` to block outbound port 80/443 from dfsvc.exe specifically using AppID rules where supported.

Evidence: Before applying gateway blocks, capture proxy and mail gateway logs for the prior 30 days and filter for any downloads or attachments matching `*.application` or `*.appref-ms` from external domains. Export these records as immutable evidence of prior delivery attempts. Also capture current dfsvc.exe network connections via `Get-NetTCPConnection -OwningProcess (Get-Process dfsvc -ErrorAction SilentlyContinue).Id` before any firewall changes disrupt active sessions.

Step 3: Audit EDR detection coverage for dfsvc.exe and rundll32.exe — verify that your endpoint telemetry captures process creation events under dfsvc.exe and flags rundll32.exe invocations that originate from AppData paths or that have no associated signed parent; tune detection rules to alert on these patterns (NIST SI-4 equivalent monitoring posture, NIST AU-2, CIS 8.2, MITRE D3-SFA)

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Verifying that telemetry coverage exists for the specific dfsvc.exe and rundll32.exe process tree patterns used in this ClickOnce campaign

Controls: NIST AU-2 (Event Logging) — requires identifying and enabling logging of process creation events for dfsvc.exe child processes and rundll32.exe invocations from AppData, which are the specific execution artifacts of this campaign, CIS 8.2 (Collect Audit Logs) — requires that audit logging is enabled and collecting process telemetry

across enterprise assets sufficient to surface dfsvc.exe and rundll32.exe execution chains

Compensating: Deploy Sysmon with a configuration that captures Event ID 1 (Process Create) with `ParentImage` containing `dfsvc.exe` and Event ID 1 where `Image` contains `rundll32.exe` and `CommandLine` contains `AppData`. Use the following Sigma rule pattern: `detection: selection: ParentImage|endswith: '\dfsvc.exe'` combined with `Image|endswith: '\rundll32.exe'`. Without EDR, enable Windows Security Audit Policy for Process Creation (Event ID 4688) via `auditpol /set /subcategory:'Process Creation' /success:enable`.

Evidence: Before tuning detection rules (which may flush alert queues or alter logging behavior), export current Sysmon or Security Event Log entries for Event ID 1/4688 filtered on `dfsvc.exe` and `rundll32.exe` from the past 90 days. Preserve raw log exports as evidence prior to any rule changes. Also snapshot the current contents of %LOCALAPPDATA%\Apps\2.0\ and note any recently modified .dll or .exe files within ClickOnce application subdirectories, as these are the fileless payload staging locations.

Step 4: Hunt for existing persistence via Scheduled Tasks and Registry Run Keys — query endpoint telemetry for Scheduled Tasks created by dfsvc.exe or entries written to HKCU\Software\Microsoft\Windows\CurrentVersion\Run by non-standard processes; review BITS job queues for unexpected download tasks (MITRE T1053.005, T1547.001, T1197)

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Actively hunting for evidence that ClickOnce-delivered payloads have already established persistence via Scheduled Tasks, Registry Run Keys, or BITS jobs on endpoints

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting) — governs the active review and analysis of audit records (Scheduled Task creation logs, registry modification events) to identify indicators of ClickOnce-based persistence already present in the environment

Compensating: Run `schtasks /query /fo LIST /v | findstr /i "dfsvc appdata .application"` on each workstation to surface Scheduled Tasks pointing to ClickOnce AppData paths. Query the registry with `reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and cross-reference values against known-good baselines. Enumerate BITS jobs with `bitsadmin /list /allusers /verbose` and flag any jobs with download URLs resolving to external domains or AppData destinations. Use osquery: `SELECT * FROM scheduled_tasks WHERE action LIKE '%AppData%';`

Evidence: This step queries live state and must capture volatile artifacts BEFORE any remediation of discovered persistence. Acquire a full memory image using WinPmem or DumpIt before terminating any suspicious processes. Run `netstat -ano` and `Get-NetTCPConnection` to capture active outbound connections from BITS or dfsvc.exe. Export all Scheduled Task XML definitions via `schtasks /query /fo XML /v > tasks_hunt.xml` and take a registry export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` with `reg export` before any keys are deleted. Preserve BITS job details via `bitsadmin /list /allusers /verbose > bits_jobs.txt`.

Step 5: Update your threat model and detection rules — map the full TTP chain from the CrowdStrike Part 1 and Part 2 disclosures into your SIEM detection logic and threat register; assign ownership for ongoing monitoring of the CrowdStrike ClickOnce research series for additional technique disclosures (NIST IR-4, CIS 7.1)

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Updating detection logic and the threat register with the ClickOnce TTP chain to improve future detection before threat actor adoption broadens

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting) — governs integrating new threat intelligence from the CrowdStrike ClickOnce disclosure into ongoing audit record review processes and SIEM detection logic, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — requires updating the vulnerability and threat management process to incorporate the newly documented ClickOnce TTP chain and assign remediation ownership

Compensating: Without a SIEM, create file-based Sigma rules for the dfsvc.exe → rundll32.exe execution chain and load them into Chainsaw or Hayabusa for periodic log scanning: `chainsaw hunt /path/to/logs --sigma sigma_rules/ --mapping mappings/sigma-event-logs-all.yml`. Maintain a plain-text threat register in a shared document tracking the CrowdStrike ClickOnce series URL, assigned analyst, and review cadence. Set a monthly calendar reminder to check the CrowdStrike Adversary Intelligence blog for Part 3 and beyond.

Evidence: This step modifies detection logic rather than live system state and does not require volatile capture prior to execution. However, preserve a snapshot of your current SIEM detection rule set (exported as versioned files with timestamps) before making changes, so you can demonstrate the detection gap window if a breach notification or audit is later required.

Step 6: Communicate findings to leadership — brief stakeholders on the specific risk that a single webpage click can install persistent malware on any standard user workstation without admin rights, and explain that existing email filters likely do not block the delivery mechanism (NIST IR-1, CIS 7.2)

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Ensuring leadership understands the capability gap exposed by the ClickOnce research so that resourcing and risk acceptance decisions are informed and documented

Controls: NIST AC-1 (Policy And Procedures) — governs the development and dissemination of access control policies; leadership communication should result in updated policy decisions regarding ClickOnce authorization and acceptable use of .application file delivery, CIS 7.2 (Establish and Maintain a Remediation Process) — requires documenting a risk-based remediation strategy; the leadership brief should produce a documented risk acceptance or remediation priority decision for the ClickOnce exposure

Compensating: Prepare a one-page risk brief using concrete, non-technical language: a standard user visiting a website or opening an email link triggers dfsvc.exe (a signed Microsoft binary), which installs and persists a payload entirely within %LOCALAPPDATA% without UAC prompts, evading controls that look for admin-level installation events. Attach a screenshot of the %LOCALAPPDATA%\Apps\2.0\ directory structure from a test workstation to make the file-based persistence tangible. Document leadership's risk decision in writing for audit purposes.

Evidence: No live system state is altered by this step; no volatile capture is required. Retain all supporting evidence compiled during Steps 1–5 (gateway log exports, Scheduled Task XML snapshots, registry exports, Sysmon logs) as the evidentiary basis for the leadership brief, ensuring traceability between observed artifacts and the risk statements being communicated.

Step 7: Monitor for follow-up research and threat actor adoption — track the CrowdStrike blog for additional parts in this series and watch threat intelligence feeds for adoption of these techniques by named threat actors or ransomware affiliates

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Integrating ongoing threat intelligence monitoring to detect escalation of ClickOnce technique adoption by named threat actors before it manifests in your environment

Controls: NIST AU-13 (Monitoring For Information Disclosure) — governs monitoring of open-source information sites at a defined frequency to detect new disclosures related to the ClickOnce attack chain and emerging threat actor adoption

Compensating: Set up an RSS feed or email alert for the CrowdStrike blog filtered on 'ClickOnce' and 'dfsvc'. Subscribe to free threat intelligence feeds (OTX AlienVault, abuse.ch, Feodo Tracker) and create a YARA rule monitoring for .application manifest files referencing external C2 infrastructure. Use osquery scheduled queries to alert on new entries in %LOCALAPPDATA%\Apps\2.0\ created after your baseline snapshot: `SELECT * FROM file WHERE path LIKE 'C:\Users\%\AppData\Local\Apps\2.0\%' AND ctime > ;`

Evidence: This step does not alter live system state. Maintain a dated log of all threat intelligence sources reviewed, including CrowdStrike blog post URLs, MITRE ATT&CK technique updates, and any named threat actor reporting that references ClickOnce or dfsvc.exe as a delivery mechanism. This log serves as documentation of due diligence if a future incident involves this technique chain.

Detection Guidance

Focus detection on process behavior rather than file signatures, as the attack chain deliberately uses trusted Microsoft binaries.

Process tree anomalies: Alert on dfsvc.exe spawning child processes other than expected ClickOnce update checks. Alert on rundll32.exe executing from AppData\Local\Apps or AppData\Roaming paths, particularly when the parent is dfsvc.exe or explorer.exe with no corresponding legitimate application install on record.

File system events: Monitor for .application and .appref-ms file writes to temp or download directories (NIST AU-2, AU-3). Alert on new executable content appearing in AppData\Local\Apps, the default ClickOnce installation target, for accounts that are not known to use ClickOnce-deployed software (NIST SI-4).

Scheduled Task creation: Query Windows Security event ID 4698 (Scheduled Task Created) for tasks created under user context with actions pointing to AppData paths or invoking rundll32.exe (MITRE T1053.005, NIST AU-6).

Registry persistence: Monitor HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce for entries added by processes other than known software installers (MITRE T1547.001, NIST AU-12).

BITS jobs: Use Get-BitsTransfer PowerShell cmdlet output or Windows event logs (Microsoft-Windows-Bits-Client/Operational) to identify BITS jobs downloading from external or uncategorized URLs; correlate with dfsvc.exe activity windows (MITRE T1197).

Network: Log and review outbound HTTP/HTTPS connections from dfsvc.exe to external hosts. ClickOnce manifests reference remote update URLs; connections to non-corporate domains from dfsvc.exe should be treated as suspicious (NIST SC-7, NIST AU-13).

Email gateway: Review quarantine and delivery logs for .application and .appref-ms attachments or URLs ending in these extensions. Most organizations will find no legitimate business use for inbound delivery of these file types from external senders (CIS 8.2).

Refer to the CrowdStrike ClickOnce Part 1 and Part 2 blog posts for any specific IOC hashes, manifest signatures, or C2 patterns published alongside the research.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`dfsvc.exe`	dfsvc.exe (Windows ClickOnce deployment service) leveraged via malicious .application manifest delivered through spearphishing link to silently install malware payloads into AppData without UAC elevation	HIGH
TOOL	`rundll32.exe`	rundll32.exe leveraged via ClickOnce application deployment (dfsvc.exe) to execute malicious payloads from AppData directories and establish fileless persistence without requiring administrative privileges.	HIGH

Type	Value	Context	Confidence
TOOL	`BITS (Background Intelligent Transfer Service)`	BITS jobs leveraged via ClickOnce update mechanism to silently download updated malicious payloads from attacker-controlled URLs without user interaction (T1197)	HIGH
URL	`Pending — refer to CrowdStrike ClickOnce Part 1 and Part 2 blog posts for published indicators`	CrowdStrike research series may include specific malicious manifest URLs, C2 domains, or payload hashes; values not available in the provided source text	LOW

Framework Mappings

MITRE-ATTACK

- **T1053.005** — Scheduled Task
- **T1547** — Boot or Logon Autostart Execution
- **T1197** — BITS Jobs
- **T1105** — Ingress Tool Transfer
- **T1566.002** — Spearphishing Link
- **T1027** — Obfuscated Files or Information
- **T1204.001** — Malicious Link
- **T1218.011** — Rundll32
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1547.001** — Registry Run Keys / Startup Folder

NIST-800-53R5

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1053.005	Scheduled Task	Execution
T1547	Boot or Logon Autostart Execution	Persistence
T1197	BITS Jobs	Defense-Evasion
T1105	Ingress Tool Transfer	Command-And-Control
T1566.002	Spearphishing Link	Initial-Access
T1027	Obfuscated Files or Information	Defense-Evasion
T1204.001	Malicious Link	Execution
T1218.011	Rundll32	Defense-Evasion
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
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/av-comparatives-awards-for-e...	T3
	https://www.crowdstrike.com/en-us/blog/why-small-businesses-choose-...	T3
	https://www.crowdstrike.com/en-us/blog/reasons-why-nonprofits-are-t...	T3
New Abuse of the ClickOnce Technology: Part 1 - CrowdStrike	https://www.crowdstrike.com/content/crowdstrike-www/locale-sites/us...	T3

Generated 2026-06-20 18:47 UTC by TJS Security Command Center