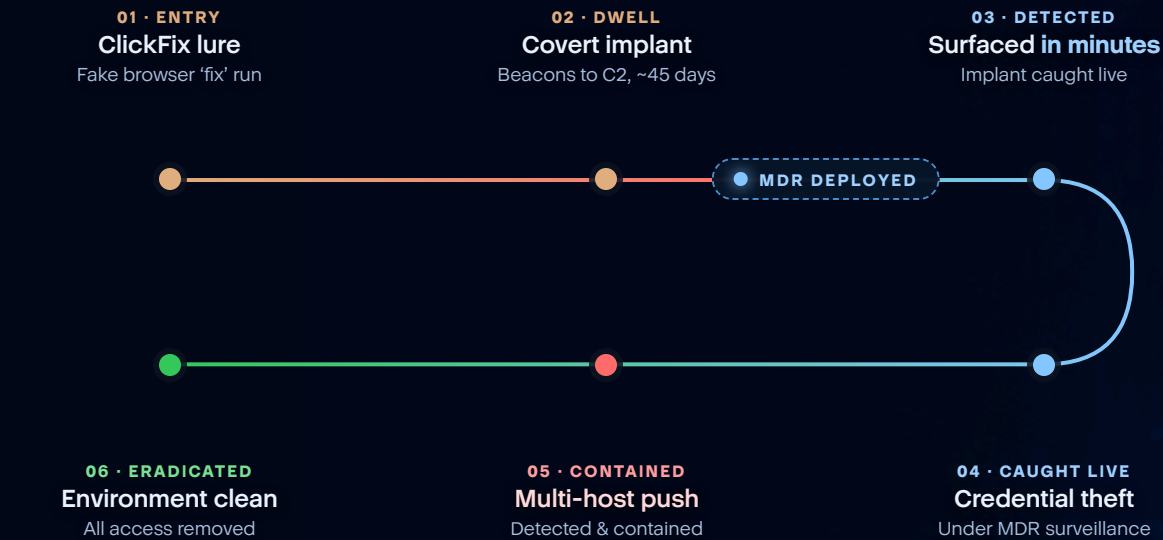


Dormant for weeks, dismantled in hours.

A ClickFix lure tricked an employee into running a malicious installer, planting a **covert implant** that beacons to command-and-control and stayed hidden for roughly six weeks — all **before Acronis MDR was deployed**. The moment coverage went live the implant was surfaced within minutes and as the attacker escalated to credential theft and a multi-host push, **MDR caught each move live** and drove containment in hours.

~45 DAYS ATTACKER DWELL PRE-MDR — a covert ClickFix implant beacons to command-and-control, hidden until Acronis MDR coverage went live.



Time is damage

Every hour an intruder stays hidden means more loss. MDR turns **weeks of exposure into minutes.**



Tools alone won't catch this

The implant hid inside a signed, trusted runtime and ordinary web traffic — it took **expert analysis to connect the signals** and expose the attack.



It could be any organization

ClickFix relies on social engineering rather than exploits. The difference is how quickly suspicious activity is detected and contained.

ClickFix social engineering to multi-host compromise

A ClickFix lure tricked a user into running a malicious installer, dropping a Node.js implant on Sliver C2 that harvested domain credentials and spread across the customer environment. The foothold sat dormant ~45 days before MDR coverage was live — the instant it went live, Acronis MDR surfaced the implant, kept it under surveillance and drove it to full scope and containment.

- #ClickFix T1566
- #SliverC2 T1071.001
- #LOLBin T1059.007
- #CredentialTheft T1003.002
- #Msiexec T1218.007

 DWELL TIME PRE-MDR

~45 days

Foothold persisted before MDR coverage; surfaced the moment it went live

 FULL SCOPE DELIVERED

<24 hrs

Full attack chain and IOC list documented within 24 hrs of escalation

 ATTACK SCOPE

Multi-host

Coordinated implant deployment across the customer environment, scoped and contained under MDR direction

 CREDENTIAL THEFT RESPONSE

Contained

Harvesting caught in real time; rotation and domain-trust remediation MDR-directed

 Threat actor profile

Consistent with a **financially motivated intrusion operator**: ClickFix for initial access, Sliver C2 for persistence, Impacket for credential harvesting and lateral movement and a rapid coordinated push across reachable hosts — tradecraft overlapping intrusion-for-hire and ransomware affiliates.

 Social Engineering

 Sliver C2 Framework

 45 Days Pre-MDR

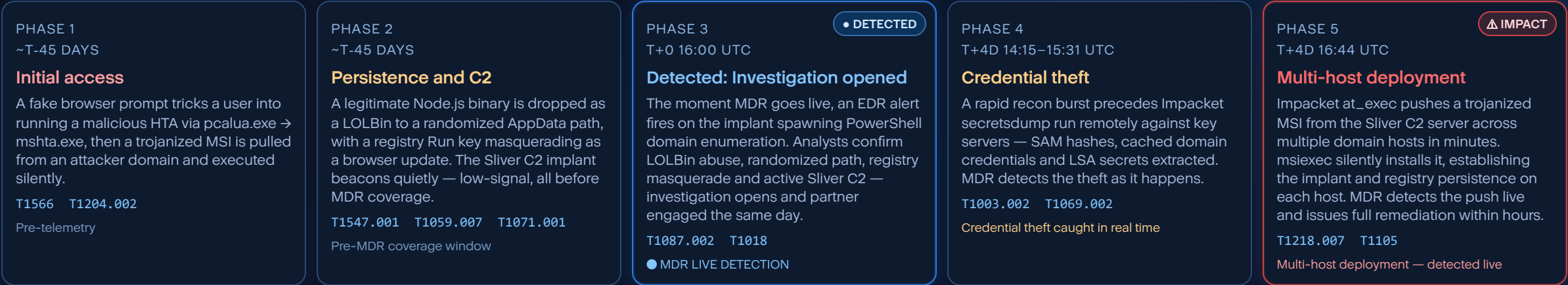
 Multi-Host Deployment

Outcome

- ✓ Implant and active C2 surfaced the moment MDR went live; investigation opened and partner engaged the same day
- ✓ Full scope reconstructed via MDR forensic correlation — coordinated deployment across the customer environment and credential theft identified, attack chain documented
- ✓ MDR-directed containment: C2 blocked, credentials rotated, software restriction policies deployed, affected systems rebuilt clean

From one click to multi-host implant: Caught and contained in hours

The ~45-day dwell all fell before MDR coverage was live (Phases 1–2). The instant it went live, MDR surfaced the implant and engaged the partner the same day (Phase 3) — then caught the credential theft and multi-host deployment (Phases 4–5) live and drove containment within hours.



! MDR DETECTION MOMENT — T+0 16:00 UTC — Investigation opened on a domain-enumeration anomaly, then continuous surveillance

Why standard controls miss this

ClickFix tricks users into executing attacker-provided commands under the guise of a legitimate fix. In this case, the attacker used a **signed Node.js runtime** from a user-writable AppData location, communicated over HTTPS and disguised persistence as a browser update. **Only behavioral correlation across process, file, registry and network telemetry exposed the attack.**

The detection needle

- Four signals, one process — all from the same node.exe instance:
- ① A signed runtime spawning domain-enumeration PowerShell
 - ② node.exe executing from a deeply nested, randomized AppData path
 - ③ A registry Run key posing as a browser update — a conhost.exe → node.exe chain
 - ④ node.exe beaconing to confirmed Sliver C2 infrastructure

Together: **a confirmed LOLBin implant with live command-and-control.**

Reconstructing the hidden LOLBin implant

Every indicator traced back to one node.exe instance. Rather than four scattered alerts, MDR reconstructed a single coherent chain — process tree, file system, registry and network telemetry read together — turning an ambiguous process into a confirmed implant with live C2.

PROCESS TREE

Signed Runtime Spawning Domain Enumeration

node.exe spawns powershell.exe running net group domain-enumeration commands — a parent-child relationship no legitimate Node.js application produces.

1

FILE SYSTEM

LOLBin Running from a Randomized AppData Path

The same binary runs from a deeply nested, randomized, user-writable AppData directory — not a standard install location, but a classic attacker staging pattern.

2

REGISTRY

Persistence Disguised as a Browser Update

An HKCU Run key with a browser-update-style name launches conhost --headless, which in turn runs node.exe against an attacker-supplied payload script.

3

NETWORK + THREAT INTELLIGENCE

Beaconing to Confirmed Sliver C2

That same node.exe makes periodic outbound HTTPS connections to a Sliver C2 server — corroborated by threat intelligence and confirmed malicious.

4

<> SANITIZED EDR ARTIFACT: RECONSTRUCTED NODE.EXE LINEAGE

Parent: node.exe [C:\Users\[USER]\AppData\Local\[RANDOM]\[RANDOM]\]
Child: powershell.exe -Command
"net group 'Domain Computers' /domain"

Registry: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
"[REDACTED]" = conhost --headless
"...\[RANDOM]\node.exe" "...\[PAYLOAD].ini"

Network: node.exe → TCP/443 → [ATTACKER-C2]
Periodic beacon | Confirmed Sliver C2 infrastructure

Q “The needle” — Analyst insight

Any one of these would warrant a look. All four belong to the same node.exe process instance — process tree, file system, registry and network telemetry lining up at once.

A signed runtime running domain recon from a randomized path, posing as a browser updater and beaconing to known attacker infrastructure — the cross-layer co-location made the verdict unambiguous. The analyst confirmed **CONFIRMED IMPLANT — ACTIVE C2** and opened full-scope review.

Response timeline: Detection to full eradication

Time	Action	Outcome / Status
T+0 16:00 UTC	EDR behavioral alert fires: node.exe spawning PowerShell domain enumeration from a randomized AppData path. MDR investigation opened automatically and picked up by an analyst for confirmation.	CRITICAL LOLBin implant with active C2 confirmed. Analyst-led investigation underway.
T+0 19:28 UTC	 Same-Day Partner Engagement — MDR notifies and engages the partner within hours of detection, requesting artifact collection and confirmation of activity on the initial-access host.	ENGAGED Partner engaged the same day — ~3.5 hours after first detection.
T+2d 20:28 UTC	Follow-up written report consolidating findings since the same-day engagement: confirmed domain enumeration, investigation status and recommended artifact collection.	REPORTED Written follow-up to the same-day engagement.
T+4d 14:15–15:31 UTC	MDR detects escalation live: a rapid recon burst then Impacket secretsdump harvesting credentials across key servers. All domain credentials on affected servers flagged compromised.	CRITICAL Active credential theft caught live. Immediate rotation advisory issued.
T+4d 16:44 UTC	MDR detects multi-host deployment via Impacket at _exec: a trojanized MSI pulled from the Sliver C2 server and run across multiple domain hosts in minutes, establishing the implant and registry persistence on each.	CRITICAL Coordinated multi-host compromise detected. Full remediation direction issued.
T+4d 20:02–21:51 UTC	MDR directs containment: C2 domain and IP blocks, software restriction policies for the implant runtime, domain-admin credential rotation, KRBTGT double-rotation and a full IOC list for the sweep.	CONTAINED Containment actioned under MDR direction — DA group restricted, C2 blocked, implant directories removed.
T+5d 08:07 UTC	MDR delivers full attack-chain documentation: complete IOC list covering file paths, network indicators, persistence commands and initial-access artifacts. Full scope confirmed across all hosts.	SCOPED Complete incident timeline delivered. All implant artifacts cataloged.
T+11d	All affected systems reloaded, implant artifacts removed and a residual IOC sweep run under MDR direction. Incident closed at T+12d after clean-telemetry verification.	ERADICATED Environment clean. No subsequent compromise observed.

 **TIME TO DETECT**

Minutes

EDR alert fired and the MDR investigation opened within minutes of the implant's domain recon, once coverage was live

 **PARTNER ENGAGED**

3.5 hrs

Partner engaged the same day for confirmation and artifact collection, within 3.5 hours of first detection

 **FULL SCOPE DELIVERED**

<24 hrs

Full multi-host attack chain and IOC list documented within 24 hrs of escalation

Priority hardening recommendations

Broadly applicable to any organization with a domain-joined Windows environment. Each recommendation addresses a specific failure point in the attack chain observed during this incident.

**CRITICAL**

User security awareness: ClickFix and social engineering defense

Initial access was a ClickFix lure that tricked a user into running a malicious HTA via a fake browser help prompt. Targeted awareness training — recognizing fake "fix this" prompts, unsolicited script-execution requests and the risk of running downloaded files from unverified sources — directly cuts the odds of this attack class succeeding.

**CRITICAL**

Application execution controls: Block execution from user-writable directories

The implant used a signed Node.js binary in a randomized AppData subdirectory to run attacker payload scripts. Denying execution from %AppData%, %LocalAppData%, %Temp% and equivalent user-writable directories by default — via Software Restriction Policies, AppLocker, or Windows Defender Application Control — would have stopped it running even after the installer executed.

**HIGH**

Privileged access management: Limit credential theft blast radius

Impacket secretsdump ran remotely against multiple servers, so the compromised account held privilege to harvest credentials across server tiers. Tiered administration (separating workstation from server admin credentials), LAPS for unique per-device local admin passwords and MFA on all administrative access would sharply limit the blast radius of a compromised workstation account.

**MEDIUM**

Network monitoring and egress controls: Visibility into C2 traffic and lateral movement

The implant talked to Sliver C2 over standard HTTPS, and the multi-host push relied on unrestricted workstation-to-server admin protocol access. DNS query logging and network-flow analysis alongside endpoint telemetry would flag beacon patterns during the dwell window, before credential theft or lateral movement. Proxying and filtering outbound traffic disrupts both payload delivery and active C2.



Acronis MDR context: Continuous MDR monitoring is what turns endpoint telemetry into analyst-actioned response. Had MDR coverage been active from the initial foothold, the implant's domain reconnaissance and Sliver C2 beacon traffic would have surfaced within hours — reducing the ~45-day dwell to **hours, not weeks**.

Is a fake browser 'fix' already hiding a dormant implant in your fleet?

If a user clicked a fake browser "fix" prompt today — ran a trojanized installer, dropped a persistent implant and spent 45 days quietly enumerating your domain — **would your team surface it within hours, or only after credential theft and multi-host deployment?**

ELEVATED RISK INDICATORS

- ⚠️ No application execution controls blocking process launch from user-writable directories (AppData, Temp, user profile paths)
- ⚠️ Workstation accounts with privilege to authenticate admin protocols (SMB/RPC/WMI) directly to server tiers
- ⚠️ Security monitoring limited to endpoint telemetry, with no network-layer (DNS / NetFlow / proxy) visibility into C2 beacon traffic

WHAT ACRONIS MDR DELIVERS

- ✓ **Behavioral detection across four telemetry layers** — process tree, file system, registry and network correlated at once to surface LOLBin abuse and implant activity that evades signature controls
- ✓ **24/7 analyst-led investigation** — credential-threat prioritization, full-scope forensic review and MDR-directed remediation delivered in hours, not days
- ✓ **Complete incident advisory** — from initial access to full lateral-movement scope, with actionable IOC lists, containment steps and environment-specific hardening recommendations

Schedule a live demo

Speak with an Acronis MDR specialist to **review your current detection coverage** against this attack chain: ClickFix social engineering, LOLBin persistence, credential harvesting and rapid multi-host lateral movement.

✉️ acronis.mdr@acronis.com

🌐 acronis.com/en/tru/

Partner note

This incident was identified and contained through the Acronis MDR service. For current threat landscape updates, ClickFix campaign indicators and sales enablement materials, contact your Acronis partner manager or visit the TRU threat intelligence portal.