MALWARE INTELLIGENCE DOSSIER

XWORM

Public-source history of a modular Windows RAT, from the 2022 MaaS to the 2025–26 plugin revival

Classification: UNCLASSIFIED // PUBLIC OSINT SYNTHESIS
Cut-off date: 6 October 2026
Prepared for: Crygma / Encrygma research file
Primary anchors: Trellix (Oct 2025), Netskope, The Hacker News, Gurucul (Feb 2026), NTT (Feb 2026), Zscaler ThreatLabz (Oct 2026)
Scope: lineage, maintainer break, plugin model, delivery, defence
Excluded: builder steps, the 5.6 flaw as a procedure, plugin loading recipe, command grammar, cracked-builder sources

Still observed in distribution as of 4–5 October 2026

0. Control note

This dossier is the public record on XWorm, a commodity Windows remote-access trojan sold as malware-as-a-service since 2022 and still in distribution on the cut-off date. It is a defensive synthesis. It does not include builder configuration, the remote-code flaw in version 5.6 as a procedure, a plugin-loading recipe, command syntax, or sources for cracked builders. Those cracked builders are themselves a common way operators get infected; pointing at them would be operationally useless and unsafe.

XWorm is not one build. After the original seller left in the second half of 2024, cracked copies, a June 2025 "6.0" sold by an account named XCoderTools, and later 6.4, 6.5, and 7.x samples all circulate under the same name. A detection written for one configuration will miss the next. Version strings found in memory, such as UD_XWormClient 6.5, are evidence of lineage, not proof of a single operator.

1. Executive assessment

XWorm is a modular Windows RAT, first sold on underground forums in 2022 by a developer known as XCoder. The last version confidently tied to that seller is 5.6. In the second half of 2024 XCoder deleted the Telegram accounts used for updates. Cracked builders filled the gap and were widely redistributed; researchers have repeatedly found those cracks themselves backdoored. On 4 June 2025 an account named XCoderTools offered XWorm 6.0 on crime forums at 500 dollars for lifetime access, described as fully re-coded and as a fix for a remote-code flaw in 5.6. Trellix, The Hacker News, and later writers all mark the authorship of 6.0 as unresolved. It may be the original seller. It may not.

What did not change is the product shape. A .NET client beacons to an operator-chosen TCP listener. A plugin command pulls DLLs by hash and loads them in memory. Trellix counted more than 35 plugins in the 6.0–6.5 set, covering remote desktop, a stealer for browsers, FileZilla, Discord, Telegram, MetaMask, Wi-Fi, and Windows product keys, a file manager, a shell, a rootkit module based on a modified r77, a reset-survival module, hidden VNC, and a ransomware DLL that shares code with NoCry. Version 6 moved the custom TCP protocol behind AES-256 with a key set at build time, which broke signatures that matched older cleartext beacons. Version 7 samples analyzed in February 2026 add process hollowing into a suspended legitimate process and a low-level keyboard hook. As of 4–5 October 2026, C2 trackers still list live XWorm infrastructure, and Zscaler described a new loader, 2CLoader, delivering XWorm alongside Vidar and Remus.

There is no single campaign and no measured global device count comparable to Group-IB's Millenium census. XWorm is a platform. Silver Fox has been tied to one lookalike chain at medium confidence. Most reporting treats it as a tool used by many crews, delivered by phishing, fake remote-support installers, JavaScript, and malicious Office add-ins.

2. Identity and the maintainer break

The stable facts are the name, the 2022 start, and the seller handle XCoder. One secondary write-up also says "EvilCoder"; that alias is not established in the Trellix or Netskope material used here and should not be merged into the attribution without a second source. XCoder's operational signature was a Telegram update channel. Its deletion in the second half of 2024 is the break point. After that, the family survived as leaked and cracked builders. Popularity on ANY.RUN's public malware tracker is repeatedly cited as evidence that XWorm became one of the most uploaded RATs, which fits a cracked commodity tool better than a closed licence.

The June 2025 XCoderTools post is the revival claim: 500 dollars lifetime, a fix for the 5.6 flaw, and a plugin expansion. Treating XCoderTools as XCoder is a hypothesis, not a finding. The defensive consequence is the same either way. Operators are not buying from one shop. They are running heterogeneous 5.x cracks, 6.x plugin builds, and 7.x loaders, often without knowing the builder itself is hostile.

3. Chronology

Date	Event	Grade
2022	XWorm offered on underground forums by XCoder. .NET RAT, operator-run TCP listener, early plugin model.	Established
Through 5.6	Last version confidently tied to the original seller. A remote-code flaw in this generation becomes public among criminals and researchers.	Established; flaw not reproduced here
H2 2024	XCoder deletes Telegram update accounts. Cracked builders proliferate, many themselves backdoored.	Trade press and vendor research
4 Jun 2025	XCoderTools offers 6.0 at 500 dollars lifetime, claims a full recode and a fix.	Trellix, via The Hacker News

Date	Event	Grade
Jul 2025	Netskope publishes on a 6.0 sample: hardcoded C2, AMSI-related delivery, anti-analysis including an ip-api hosting check and a Windows XP exit.	Netskope
Oct 2025	Trellix maps 6.0, 6.4, 6.5 and more than 35 plugins, including Ransomware.dll overlapping NoCry. Sample C2 94.159.113.64 port 4411.	Trellix
Sep 2025	Forcepoint: phishing Excel add-in (.xlam) leads to in-memory execution; string UD_XWormClient 6.5.	Forcepoint
Feb 2026	Gurucul analyzes a v7 chain: process hollowing, AES config, keyboard hook, plugin command set. NTT summarizes V6 C2 as AES-256.	Gurucul; NTT
2026	A V7.4-associated PyInstaller loader described in a Tata Communications advisory.	Secondary advisory
4–5 Oct 2026	Derp lists live XWorm C2 and distribution hosts. Zscaler reports 2CLoader delivering XWorm with Vidar and Remus.	Current

Table 1. Public chronology. Version labels overlap; a 2026 sample can still be a 5.x crack.

4. Architecture, as published

4.1 Client and listener

The operator runs the listener. The client is built with a host, a port, and a key. Older builds stored that configuration as Base64 and AES. Version 6 keeps a custom TCP protocol and wraps it in AES-256 with a build-time key, so a network signature for a cleartext banner no longer matches. Gurucul's v7 write-up describes the same idea: version, address, port, and a shared SETTINGS.KEY pulled from the embedded config at start. Some Netskope samples took the address from a command line passed by a PowerShell stager; others hardcoded it. Both patterns exist. Beacon ports in published cases include 4411 and 10992; they are operator-chosen and are not a family constant.

4.2 Plugins

The feature that defines the family after 6.0 is the plugin bus. Trellix describes a command that carries the SHA-256 of a DLL and the arguments. If the client has not cached that hash, it asks the listener for the plugin, receives it encoded, and loads it in memory. Plugins have been stored under a per-user registry key. Named modules in the 6.x set include RemoteDesktop.dll, FileManager.dll, WindowsUpdate.dll, Stealer.dll, Recovery.dll, Chromium.dll, SystemCheck.Merged.dll, Ransomware.dll, Rootkit.dll, and ResetSurvival.dll. Hidden VNC is described in the NTT summary. The ransomware plugin encrypts user files, sets a wallpaper, and writes a ransom note; Trellix reported code overlap with NoCry, including key and IV handling. Rootkit.dll is described as a modified r77. ResetSurvival.dll abuses registry configuration so a reset does not clear the foothold. This list is a capability inventory, not a loading guide.

4.3 Collection and control

Across versions, published capabilities are host profiling, a shell, PowerShell, keylogging, screen capture, webcam, clipboard monitoring, file management, USB propagation in some builds, and a clipper-style address swap. The stealer plugins target browser stores, with later builds attempting to deal with Chrome app-bound encryption, plus FileZilla, Discord, Telegram, MetaMask, Wi-Fi profiles, and the Windows product key. Gurucul's v7 sample installs a low-level keyboard hook and caches keystrokes for later exfiltration. DDoS participation is claimed in product descriptions and in the Gurucul summary; it is a plugin-level feature, not evidence that every infection is part of a botnet for hire.

4.4 Evasion

Published anti-analysis includes debugger checks, a virtual-machine and sandbox exit, an ip-api lookup used to leave if the address belongs to a hosting provider or a known analysis network, and a terminate-on-Windows-XP check that Netskope noted is also used by AsyncRAT. Delivery chains disable or bypass AMSI before reflective loading. Forcepoint and Gurucul both document in-memory execution, including hollowing into a suspended legitimate process such as RegSvcs.exe. A critical-process trick in one 6.0 sample is described by Netskope: stopping the process can bugcheck the host, after which the Run key starts it again. Persistence observed in the wild is a Run key, a startup shortcut, or a hidden scheduled task; some builds do not survive reboot. There is no single persistence artefact.

5. Delivery

Initial access is commodity. Phishing attachments and links, JavaScript that launches PowerShell, malicious Excel add-ins with an embedded OLE object, executables disguised as invoices or installers, and fake ScreenConnect packages are all published

paths. Forcepoint's September 2025 case used a fake-invoice email and an .xlam add-in whose OLE stream held shellcode; the in-memory result contained the 6.5 client string. A 2026 Gurucul chain used cloud-hosted bait and process hollowing. Zscaler's October 2026 2CLoader is a reminder that XWorm is now a second-stage payload for other loaders, next to Vidar and Remus, not only a phish that drops itself. Geofencing via ip-api and country settings appears in multiple analyses. One reported lure theme impersonated the Italian national health service. None of these is unique to the family.

6. Who uses it

The honest answer is many unattributed operators. A public tracker listed on the order of a dozen named actors in reporting that mentions XWorm; most of those are campaign labels, not owners of the tool. Seqrite-linked reporting has attributed one lookalike chain, a tax-themed executable loading a DLL that behaved as XWorm or DcRAT, to Silver Fox at medium-to-high confidence. That is a use, not authorship. Brazilian government-site abuse has been described in reporting that included XWorm as one backdoor among stealers. The economically important fact is the cracked-builder market: low-skill operators run a tool whose own supply chain is hostile, and the original licence relationship is broken.

7. Indicators and defence

Hashes and single IPs rot. Published seeds, for retro-hunt only, include the Trellix listener 94.159.113.64 on 4411, Gurucul's 158.94.209.180, and the Gurucul sample hashes beginning de7d74d374a4422c5084280ff71f7942d61f35c271df7d5af01bdd756d0f630b and 3f4c3c16f63fb90d1fd64b031d8a9803035f3cb18332e198850896881fb42fe5. A memory string UD_XWormClient is a high-quality family marker when a sample is dumped. It will not be present on disk in a hollowed process.

Detections that survive repacking: Office or a script host spawning PowerShell that then starts RegSvcs or another .NET framework binary in a suspended state; a non-browser process making a long-lived TCP session to a residential or VPS port immediately after an ip-api lookup; DLL content appearing in a Run key or under HKCU\Software without a matching file on disk; AMSI telemetry gaps followed by .NET load from memory. Application control on script hosts and macro-signed add-ins cuts the common lure path. Blocking ip-api is noisy and incomplete. Network detection must assume the beacon is AES-wrapped and matched on behavior, not on a banner.

8. Comparison

Dimension	XWorm	Millenium RAT	ZeroDayRAT
Platform	Windows	Windows	Android; iOS claimed
Since	2022	September 2023	February 2026
C2	Operator TCP listener, AES in v6+	Telegram Bot API	Buyer-hosted panel
Extension model	35+ in-memory DLL plugins	Feature flags in the build	Panel modules
Price, public	500 dollars lifetime for the 6.0 claim; cracks free and hostile	50–90 dollars	About 2,000 dollars, secondary
Maintainer	XCoder left in 2024; 6.0 author unresolved	ShinyEnigma, still selling	Unattributed Telegram seller
Measured scale	No device census; live C2 in Oct 2026	62,289 endpoints	No census
Distinctive risk	Ransomware and rootkit plugins; backdoored cracks	Cheap, Telegram-native	SMS and banking overlays

Table 2. Peer contrast with the two preceding dossiers. XWorm is the oldest and the most modular of the three.

9. Assessment

High confidence: XWorm is a Windows MaaS RAT from 2022; XCoder was the original seller and left Telegram in the second half of 2024; 6.x added an AES-wrapped TCP beacon and a large in-memory plugin set including stealer, remote-desktop, rootkit, reset-survival, and ransomware modules; cracked builders are widely circulated and often backdoored; the family was still being delivered in early October 2026. Medium confidence: XCoderTools is a new maintainer rather than the original seller; the NoCry code overlap is inheritance rather than a shared operator. Low confidence: any single crew as the dominant user; a global infection total. Not supported: a zero-day, a mobile build, or a government customer.

The open question is whether 7.x is a maintained product or another cracked fork. The February 2026 analyses and the October 2026 loader report show the name is operationally alive either way. Defence should key off the plugin-and-hollowing behavior,

not off a version string.

10. Sources

Trellix Advanced Research Center, XWorm V6 plugin analysis, reflected in The Hacker News, 7 October 2025, and BleepingComputer, 6 October 2025. Netskope Threat Labs, XWorm V6.0, 28 July 2025. Forcepoint, Excel add-in to in-memory XWorm 6.5, September 2025. Gurucul, XWorm v7 infection chain and C2, 11–12 February 2026. NTT Security, V6 technical note, 4 February 2026. Zscaler ThreatLabz, 2CLoader delivering Vidar, Remus, and XWorm, reported 5 October 2026. Derp public C2 view, activity through 4 October 2026.

End of dossier. Cut-off 6 October 2026. Public-source synthesis for defensive use. Nothing in this document is an instruction to build, buy, or operate intrusion software.