Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

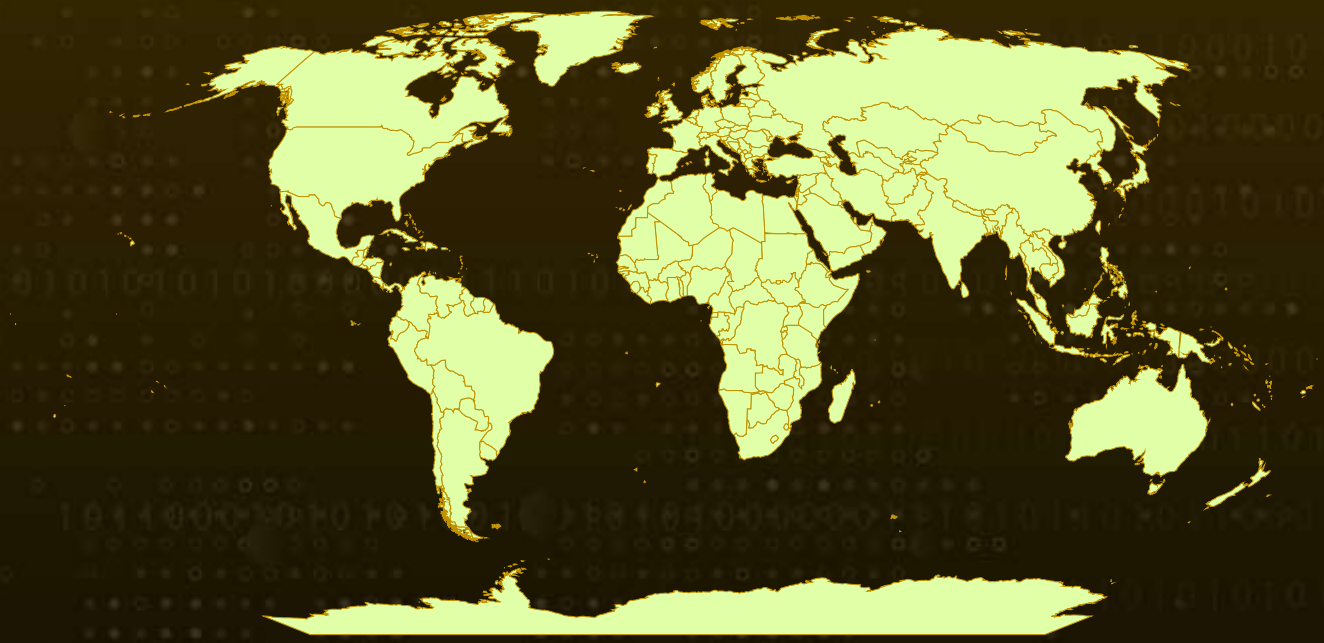
# C2Looper Builds Footholds for Ransomware

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| August 25, 2026 | A1 | TA2026244 |

# Summary

**First Seen:** July 2026
**Targeted Regions:** Worldwide
**Targeted Platforms:** Windows
**Malware:** C2Looper
**Attack:** C2Looper is a Rust-based Windows backdoor first seen in July 2026, likely delivered through ClickFix lures that trick users into running attacker-supplied commands themselves. It gives an operator remote command execution, host and domain reconnaissance, and the ability to drop follow-on payloads, while hiding through encrypted strings, runtime API resolution, and a malicious DLL loaded by the genuine OneDrive executable. Its newer version abandons its own C2 server and runs all tasking and data theft through a GitHub repository, so operator traffic looks like ordinary developer activity. The capability set fits an initial access broker preparing a foothold for ransomware deployment.

## Attack Regions



# Attack Details

**#1**

C2Looper is a Rust-based Windows backdoor first identified in July 2026. It likely reaches victims through a multi-stage ClickFix chain, where the user is talked into copying a command and running it themselves. The binary is built to resist analysis from the outset. It keeps its strings encrypted and decrypts them at runtime with a simple XOR operation. It declares almost none of its imports, instead resolving the Windows functions it needs on the fly through LoadLibrary and GetProcAddress. The practical effect is that a static look at the file reveals very little about what it actually does.

**#2**

Early builds talk to a hardcoded server over plain, unencrypted HTTP. On startup the backdoor collects the username, the machine's DNS hostname, and its own process ID, combines the hostname and username into a bot identifier, and beacons that data out once every second to request a task. The command set is small but enough to hold ground on a host, covering liveness checks, running commands through the Windows command shell either silently or with the output returned, and downloading further payloads. One of those downloads is planted in the folder used by OneDrive, after which the backdoor kills the running OneDrive process so the genuine executable loads the malicious library on restart. This serves as both an update mechanism and a hiding place, since the code now runs inside a trusted signed process.

**#3**

A later build, labelled version 2 in its own debug strings, adds the reconnaissance an operator needs before pushing deeper. A single command runs against the domain computers and domain admins groups, and wmic product get name, version, returning the network layout, the current user's privileges, the domain controllers, the privileged accounts, and the installed software in one response. Two further commands list a chosen directory and the drives attached to the host. Version 2 also gains an injection command that loads a legitimate Windows system module, writes downloaded shellcode into it, and runs that code on a new thread, letting follow-on payloads execute under the identity of a trusted module. The backdoor carries no credential theft capability of its own, so the enumeration is groundwork, mapping the domain and locating privileged accounts for whatever tooling arrives next.

#4

The largest change in version 2 is that it abandons its own C2 server and runs everything through GitHub. Each infected host gets its own folder in a repository holding three JSON files, one carrying tasking, one carrying command output, and one recording the bot identifier and the time of its last check in. Stolen data is written into the same repository. This matters most for defenders, because the traffic is ordinary HTTPS to a domain most organisations allow by default and few will block, so data theft is hard to separate from routine developer activity. Smaller refinements follow the same logic, with command output now captured through Windows pipes rather than written to disk, downloads landing in the temporary folder, and executed files deleted once they finish. Older builds have been observed downloading version 2, confirming the two are operated together. Taken as a whole, the capability set fits an initial access broker, providing quiet entry, reconnaissance, data theft, and a foothold ready to hand to a ransomware crew. Oyster, a family linked to the operators behind Latrodectus, uses closely similar API endpoints, a resemblance worth recording though not enough on its own to connect the two.

# Recommendations

- **Treat Paste-and-Run Prompts as an Attack Pattern:** ClickFix chains succeed only when a user copies attacker-supplied text into the Run dialog, a terminal, or PowerShell. Brief staff specifically on this pattern rather than on generic phishing awareness, and where policy allows, restrict interactive script execution for standard users so that a persuaded user still cannot complete the step.

- **Watch for DLL Sideloading in the OneDrive Folder:** Alert on the creation or modification of wtsapi32.dll under %LocalAppData%\Microsoft\OneDrive\, and on any process abruptly terminating OneDrive. The two events together are a strong signal, because legitimate OneDrive updates do not arrive this way.

- **Restrict Execution from User Writable Paths:** Payloads land in %LocalAppData% and the Windows temporary directory under names such as pld.exe. Application control policies that prevent execution from these locations break the second stage delivery step even after the backdoor is running.

- **Monitor Thread Creation in Trusted System Modules:** The injection command writes shellcode into the text section of a loaded winspool.drv and starts a thread there. Endpoint tooling should treat thread creation pointing into a modified section of a signed system module as a high-fidelity indicator.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Initial Access | T1566: Phishing | |
| Execution | T1204: User Execution | T1204.004: Malicious Copy and Paste |
| | T1059: Command and Scripting Interpreter | T1059.003: Windows Command Shell |
| | T1106: Native API | |
| Defense Evasion | T1027: Obfuscated Files or Information | |
| | T1140: Deobfuscate/Decode Files or Information | |
| | T1574: Hijack Execution Flow | T1574.001: DLL |
| | T1055: Process Injection | |
| | T1070: Indicator Removal | T1070.004: File Deletion |
| Discovery | T1033: System Owner/User Discovery | |
| | T1082: System Information Discovery | |
| | T1016: System Network Configuration Discovery | |
| | T1018: Remote System Discovery | |
| | T1069: Permission Groups Discovery | T1069.002: Domain Groups |
| | T1083: File and Directory Discovery | |
| | T1518: Software Discovery | |

| Tactic | Technique | Sub-technique |
|---|---|---|
| Discovery | T1120: Peripheral Device Discovery | |
| Collection | T1005: Data from Local System | |
| Command and Control | T1071: Application Layer Protocol | T1071.001: Web Protocols |
| | T1102: Web Service | T1102.002: Bidirectional Communication |
| | T1105: Ingress Tool Transfer | |
| | T1571: Non-Standard Port | |
| Exfiltration | T1567: Exfiltration Over Web Service | T1567.001: Exfiltration to Code Repository |
| Impact | T1486: Data Encrypted for Impact | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | f96ff2f3abbff7f382ace509b90e54853b4b61c402ecde27d82f1c17b414867b, 20675a659c338f7267fd09bacb431f4491f061d3acf42d07aca2dec3d25fa549, f59f32c9af4fa8a5dbd4668df8893593bc0c4324816cbf9b956acedcbfb8cdb6 |
| IPv4:Port | 45[.]158[.]196[.]23[:]8888, 45[.]158[.]196[.]184[:]8888 |

## References

https://www.zscaler.com/blogs/security-research/c2looper-new-backdoor-likely-tied-ransomware-github-c2

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

**August 25, 2026 • 04:00 AM**



More at www.hivepro.com