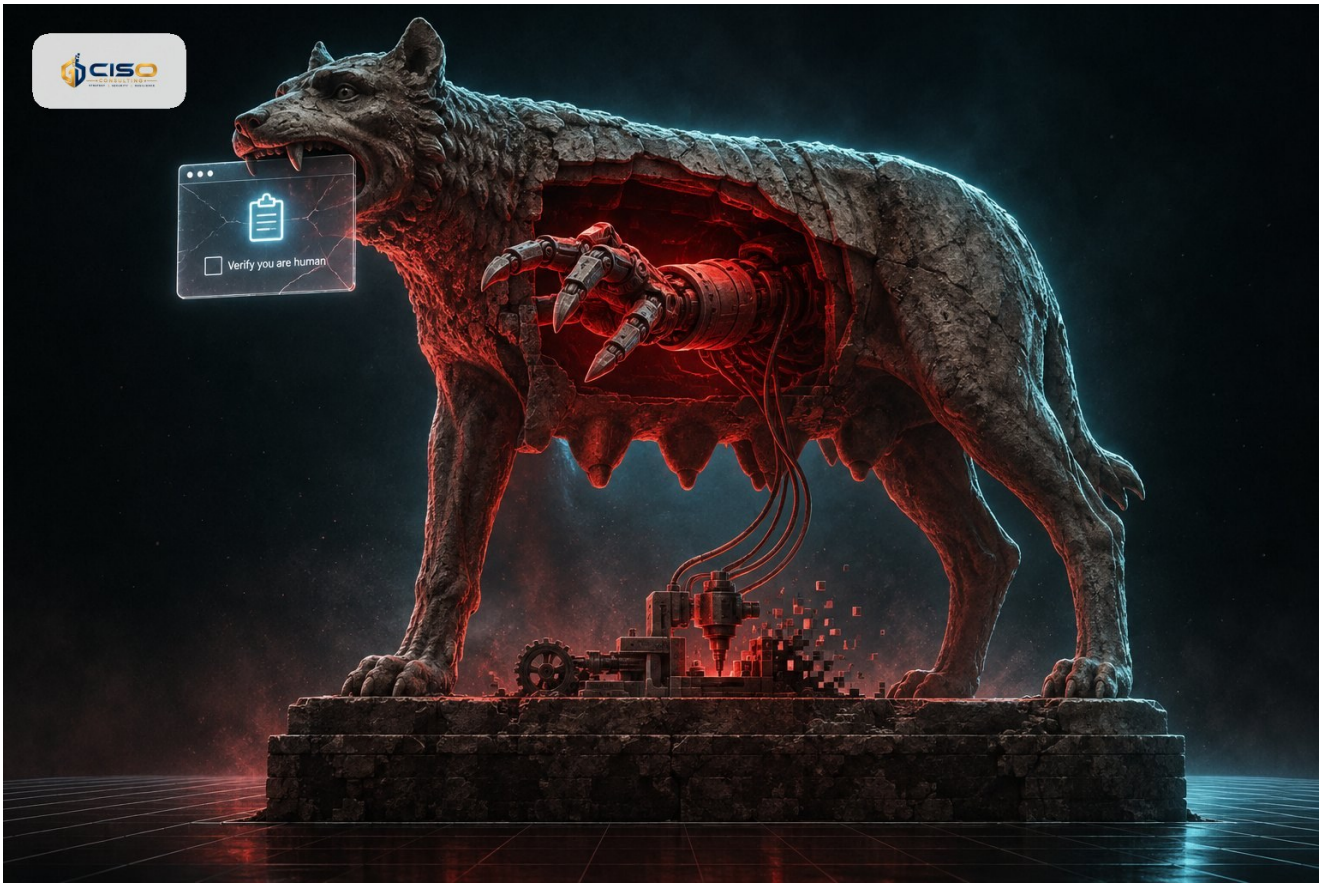
ROMULUS ClickFix Campaign Delivers a New Remote Access Trojan



Threat actors are using the ROMULUS ClickFix delivery platform to distribute a previously undocumented RAT that resembles CNCMachineRMS. Blackpoint assesses ROMULUS likely works as a delivery service.

- ROMULUS is a ClickFix-based malware delivery platform now linked to a previously undocumented RAT.
- The RAT shares similarities with CNCMachineRMS.
- Blackpoint assesses ROMULUS likely acts as a delivery service.
- It distributes CNCMachineRMS and Legion Loader through separate chains.
- The chains keep ClickFix and signed binary sideloading techniques.

What was observed

Threat actors have been seen using the ROMULUS ClickFix malware delivery platform to deploy a previously undocumented remote access trojan (RAT). According to the report, the RAT shares similarities with CNCMachineRMS. The headline describes it as capable of spying on users and controlling PCs.

How the platform operates

Blackpoint's assessment is that ROMULUS likely operates as a delivery service rather than a single-purpose tool. It distributes CNCMachineRMS and Legion Loader through separate chains, while keeping two techniques in common: ClickFix, which relies on persuading the user to take an action themselves, and sideloading of signed binaries, which abuses legitimately signed files.

Why it matters

Because the platform serves more than one payload, defending against a single malware family is not enough. Controls need to address the delivery techniques: user-initiated execution and the abuse of trusted, signed software. The source excerpt does not give details on targets, victim numbers, regions or indicators of compromise, so organisations should avoid assuming exposure or safety without checking their own telemetry.

The practical response is to review awareness content, endpoint controls and detection coverage for these two techniques, and to follow the original vendor research for technical indicators as they are published.

What to do now

1. Add ClickFix-style lures, where users are told to paste or run commands, to security awareness training.
2. Restrict or alert on users launching command interpreters from browser or dialog prompts.
3. Review detections for sideloading of signed binaries from unusual folders.
4. Hunt for CNCMachineRMS and Legion Loader indicators once published by vendors.
5. Confirm incident response playbooks cover remote access trojan containment and credential reset.