

ROMULUS ClickFix platform used to deliver LegionLoader and other malware



Forescout's Vedere Labs describes ROMULUS, a ClickFix delivery platform that works like a malware-distribution service and is used to spread Legion Loader through fake landing pages.

- Forescout Research - Vedere Labs disclosed details of ROMULUS, a ClickFix delivery platform.
- It operates like a malware delivery service rather than a single campaign.
- Fake landing pages use ClickFix-style lures to persuade users to run malicious commands.
- Victims effectively infect their own machines, which bypasses some technical controls.
- Legion Loader is named as one of the malware families distributed.

Researchers at Forescout Research - Vedere Labs have published details of ROMULUS, a platform built to

deliver malware using ClickFix techniques. The report describes it as comparable to a malware delivery service, meaning the infrastructure can be used to distribute more than one kind of payload. Legion Loader is one of the named examples.

How the technique works

ROMULUS relies on bogus landing pages carrying ClickFix-style lures. Rather than exploiting a software flaw, the page persuades the visitor to run malicious commands themselves, so the user effectively carries out the infection. This makes the attack depend on user behaviour as much as on technical weaknesses.

Why it matters

Because the user initiates the action, standard download and attachment filtering may not stop it. Staff awareness and control over what commands users can execute are therefore central to defence. The source excerpt does not give details on targets, regions, victim numbers or indicators of compromise, so organisations should consult the full Forescout research for technical specifics.

Regulated institutions should treat this as a reminder to cover copy-and-paste command lures in awareness programmes and to review endpoint controls accordingly.

What to do now

1. Add ClickFix-style lures, where a page asks users to paste and run commands, to security awareness training.
2. Instruct staff never to run commands copied from a web page or a verification prompt.
3. Review endpoint policies that restrict script and command-line execution for standard users.
4. Ensure endpoint detection monitors suspicious command-line activity launched from user sessions.
5. Read the full Forescout Vedere Labs research and feed any published indicators into detection.