

A fake “prove you are human” box is talking staff into opening your network

Microsoft has published research on an active campaign, nicknamed TerminalFix, that persuades ordinary users to paste an attacker’s command into Windows Terminal. The result is not a virus on one PC. It is a live tunnel into the network behind it.

ISSUED

3 September 2026

SEVERITY

High

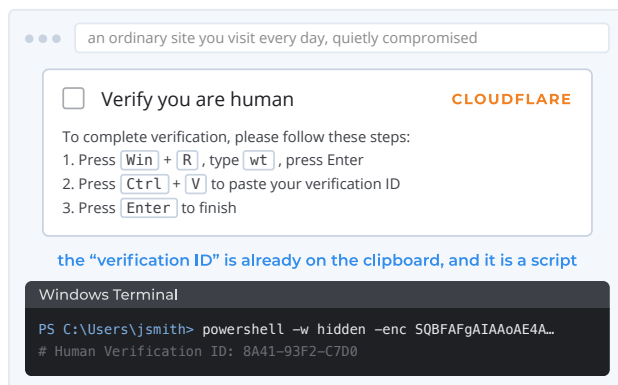
APPLIES TO

Windows workstations

ACTION

Share with all staff

WHAT IT LOOKS LIKE



Reconstruction by Netwolf Cyber of the technique described in Microsoft’s research. The wording, the styling and the fake identifier all change between campaigns. What never changes is the instruction to paste something into a terminal window.

No legitimate website will ever ask you to copy a command and run it in Windows Terminal, PowerShell or the Run box in order to prove you are human.

If a site asks for this, close the tab and tell us. If you have already done it, disconnect the machine from the network, leave it switched on, and call us before you try to clean anything up.

That single sentence is the control that stops this attack. Please put it in front of your whole team.

WHY IT MATTERS

There is no software flaw to patch here, and nothing to download and open. The attack works because a person voluntarily pastes a command into a terminal. Patching alone will not stop it.

Everything that follows runs from a legitimate Windows tool, launched by a legitimate user, on a legitimate workstation. To basic antivirus it looks unremarkable, which is the whole point of the technique.

For firms in legal, financial and healthcare work the exposure is specific. Once running, the malware hunts for domain controllers, databases, backup servers, mail systems and network gateways, and reads Active Directory. Those are the systems holding privileged and regulated material.

HOW IT UNFOLDS

- 1 A user visits a website that has been compromised. Usually it is an ordinary, reputable site.
- 2 A counterfeit Cloudflare check appears, claiming verification is required.
- 3 The page loads a command onto the clipboard and walks the user through opening Windows Terminal and pasting it.
- 4 The command retrieves an archive holding a legitimately signed program alongside a malicious library, which loads a hidden payload straight into memory. A second stage pulls further code concealed inside the pixel data of image files on the attacker's server.
- 5 Persistence is established through a scheduled task and a registry entry that re-run every hour, and the malware begins surveying the network and Active Directory.
- 6 It opens an outbound encrypted connection on port 443, handing the operator a proxy route to every internal system that machine can reach.

Microsoft found the campaign in the wild but saw no hands-on-keyboard activity. That pattern suggests access being banked for later use, or for sale.

OUR RESPONSE

On your behalf we have already:

- Added detection content to our monitoring platform for the reconnaissance, persistence and outbound tunnelling described in Microsoft's research.
- Searched your historical telemetry for indicators tied to this campaign.
- Reviewed PowerShell execution logging across your monitored endpoints.
- Recorded any gaps in script-block logging or endpoint protection for follow-up with your account contact.

If any of that surfaces something in your environment, you will hear from us directly and immediately.

WHAT TO DO

This week

- Put the statement above in front of every member of staff. Non-technical users are the target.
- Confirm with us that PowerShell script-block logging and endpoint protection are live everywhere.

Over the next month

- Narrow who can reach PowerShell and Windows Terminal at all. In most practices, very few people need either.
- Check that administrative credentials are not in routine use on ordinary workstations, and that privileged accounts require MFA.
- Confirm backups are isolated from the production network and have been test-restored recently.

If you think a machine is affected

- Disconnect it from the network and leave it powered on.
- Call us before running any cleanup tool.
- Treat every credential used on that machine as compromised, including any administrative credential reachable from it.

QUESTIONS

Reply to this note, email support@netwolfcyber.com, or contact your account lead. If it would help, we will run a short briefing for your staff. This is one of the few attacks that awareness alone genuinely prevents.

Netwolf Cyber support@netwolfcyber.com

Drawn from the Microsoft Security Blog, 28 August 2026, and reporting by BleepingComputer, 31 August 2026.