Ukraine: a fake recruiter, a fake interview, a poisoned VPN

Someone reads your CV, offers you a role, interviews you over video, then sends a technical test that needs a network connection. The connection fails, so they offer their own software instead. The targets are system administrators.

INCIDENT DETAILS · 5WH

Who A cluster Ukraine's CERT-UA tracks as UAC-0145, identified as part of Sandworm (APT44, Seashell Blizzard) and attributed to Russia's GRU. Targets are Ukraine-based system administrators and IT specialists.
What A recruitment fraud ending in the victim installing a modified VPN client built from genuine open-source code, with a hidden addition that runs commands on the machine.
Where Ukraine. Infrastructure impersonates real organisations - a look-alike domain themed on an IT firm's Bulgarian office, and projects hosted on SourceForge.
When Running since at least May 2026; CERT-UA advisory 9 Aug 2026, reported 11 Aug.
Why Access. The administrator is not the objective; the networks they manage are.
How Real job site, real messenger, real video service, real company name, real distribution platform, real VPN protocol - none of them compromised.

IMPACT

- Access: a compromised system administrator is a compromised organisation - elevated rights across servers, accounts and backups by definition.
- Reach: running since May. CERT-UA has not said how many were approached or what the operators were ultimately after.
- Labour market: Ukrainian technical workers must now treat routine recruitment as an attack surface.
- Detection: the malicious instructions sit in the configuration file rather than the program, and the download comes from a trusted platform.

SEQUENCE OF EVENTS

A Built on WireGuard, so it behaves like the real thing because most of it is
B Commands hidden in the settings file, not the program - inspection finds a VPN client
C Jul 2026: the same cluster used fake security check-boxes on compromised sites

1 They read your CV on a legitimate job site and contact you
2 The conversation moves to Telegram, off the platform
3 A video interview in English discusses the role
4 A technical test arrives with configuration files built to fail
5 The helpful fix is their own client, hosted on SourceForge

ASSESSMENT, LESSONS, AND RECOMMENDATIONS

- The target is the administrator because the objective is everyone they administer.
- A multi-day process defeats a single-moment defence - the malicious step arrives after days of ordinary interaction.
- The deliberate failure is the cleverest part: the victim ends up wanting the malicious client.
- It is highly likely that recruitment-themed social engineering against technical staff continues.