Q-Dir and DesktopOK installers from the official SoftwareOK site found trojanized



Researchers report a supply chain attack in which Q-Dir and DesktopOK installation files from the official SoftwareOK site were tampered with to deliver remote access malware, including through updates.

- Installation files for Q-Dir and DesktopOK distributed via the official SoftwareOK website were tampered with.
- The headline describes the payload as remote access malware.
- Malicious files appeared both on direct downloads from the official page and during updates of already installed copies.
- The source excerpt does not give dates, malware names or affected versions.

Researchers have disclosed a software supply chain attack affecting two Windows utilities, Q-Dir and DesktopOK. Installation files distributed through the official SoftwareOK website were tampered with, and the reported goal was to deliver remote access malware.

What is known

According to the report, the malicious files were not limited to fresh downloads from the official download page. They also appeared during the update process of copies that users had already installed. This means that trusting the official source, or relying on built-in updating, was not enough to avoid the problem.

The excerpt available to us does not state when the activity occurred, which versions were affected, or which malware family was used. Readers should wait for the full technical details before drawing conclusions about specific indicators.

Why it matters

Small utilities are often installed by administrators and staff outside formal procurement, so they may not appear in software inventories. A trojanized installer from a legitimate vendor can bypass the usual caution applied to unknown sources, and remote access malware gives an attacker a foothold inside the network.

What to do next

Treat this as a prompt to check whether either tool is present in your environment, to review how such utilities are approved and updated, and to confirm that endpoint monitoring would detect unexpected remote access behaviour.

What to do now

1. Search endpoints and software inventories for Q-Dir and DesktopOK, including copies installed by individual users.
2. Pause installing or updating these tools until the vendor or researchers publish clear guidance, and confirm installers against the full technical report.
3. Review any host where either tool was installed or updated recently for unexpected remote access sessions or outbound connections.
4. Route utility software through an approval and allow-listing process, even when it comes from an official vendor site.
5. Check that endpoint detection and logging cover remote access tooling, and brief the SOC on this report.