Q-Dir and DesktopOK installers trojanized to deliver a Python remote access trojan



AhnLab reports that installers for Q-Dir and DesktopOK on the official SoftwareOK site were tampered with and signed, delivering a Python RAT. Anyone who recently installed or updated either tool should treat the device as potentially compromised.

- Official distribution channels for Q-Dir and DesktopOK delivered trojanized installers, affecting both new downloads and updates of existing installations.
- The tampered installers carry a valid digital signature issued to the legitimate developer.
- Affected releases listed: Q-Dir 12.83.0.0, 12.84.0.0, 12.85.0.0; DesktopOK 12.82.0.0 and 12.85.0.0. Not every listed build was infected.
- The RAT persists through a scheduled task, runs shell commands and Python code, transfers files, takes screenshots and reports installed security products.

> - ASEC could not determine how the installers were replaced or for how long they were distributed.

Researchers at AhnLab's Security Intelligence Center (ASEC) have confirmed that installers for two Windows utilities, Q-Dir and DesktopOK, distributed through the official SoftwareOK website were compromised. Both tools are developed by Nenad Hrg. They are not mainstream products, but they are used by IT professionals, power users and system administrators, which makes the audience relevant to enterprise environments.

What was found

The trojanized installers deliver a Python-based remote access trojan. They carry a digital signature from a certificate issued to the legitimate developer, so a valid signature alone is not proof of a clean file. Malicious files were produced both when users downloaded from the official page and when existing installations updated themselves.

ASEC lists Q-Dir 12.83.0.0, 12.84.0.0 and 12.85.0.0, and DesktopOK 12.82.0.0 and 12.85.0.0 as affected, while noting that not all of these builds were infected. It published SHA-256 hashes to help tell legitimate and malicious installers apart.

The RAT registers a scheduled task for persistence. It can run shell commands and Python code, transfer files and capture screenshots, and it gathers system details including active security products. It checks against a list of 1,206 process names tied to antivirus and EDR tools and sends the results to its command and control server.

What remains unknown

ASEC could not establish how the installers were replaced or during what period the malicious versions were available. BleepingComputer's request for comment from the developer had not been answered at publication.

ASEC advises treating any system that recently installed or updated either tool as potentially compromised. It also cautions that uninstalling the tools does not remove the RAT, so hosts should be checked for unexpected Python environments, scheduled tasks and external network connections.

What to do now

1. Inventory endpoints, especially administrator and IT workstations, for Q-Dir and DesktopOK and record installed versions and install or update dates.
2. Compare installer hashes against the SHA-256 values published by ASEC and on the official download page; do not rely on the digital signature alone.
3. Treat hosts that recently installed or updated either tool as potentially compromised: isolate them and start incident handling.

4. Hunt for unexpected Python environments, new scheduled tasks and unusual outbound connections, since removing the tools does not remove the RAT.
5. Review credentials and privileged sessions used on affected administrator machines and rotate them where exposure is possible.
6. Route third-party utility installs through an approved software process with hash verification.