

CARROTBALL (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:17:48 UTC

CARROTBALL is a simple FTP downloader built to deploy SYSCON, a Remote Access Trojan used by the same threat actor. Discovered by Unit 42 in late 2019, the downloader was adopted for use in spear phishing attacks against US government agencies.

► [TLP:WHITE] win_carrotball_auto (20251219 | Detects win.carrotball.)

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.carrotball>