

FlawedGrace (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-02 11:01:18 UTC

According to ProofPoint, FlawedGrace is written in C++ and can be categorized as a Remote Access Trojan (RAT). It seems to have been developed in the second half of 2017 mainly.

FlawedGrace uses a series of commands:

FlawedGrace also uses a series of commands, provided below for reference:

- * desktop_stat
- * destroy_os
- * target_download
- * target_module_load
- * target_module_load_external
- * target_module_unload
- * target_passwords
- * target_rdp
- * target_reboot
- * target_remove
- * target_script
- * target_servers
- * target_update
- * target_upload

► [TLP:WHITE] win_flawedgrace_auto (20251219 | Detects win.flawedgrace.)

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