Alreay (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:09:46 UTC

Alreay is a remote access trojan that uses HTTP(S) or TCP for communication with its C&C server.

It uses either RC4 or DES for encryption of its configuration, which is stored in the registry.

It sends detailed information about the victim's environment, like computer name, Windows version, system locale, and network configuration.

It supports almost 25 commands that include operations on the victim’s filesystem, basic process management, file exfiltration, command line execution, and process injection of an executable downloaded from the attacker’s C&C server. As in many RATs from Lazarus arsenal, the commands are indexed by 32-bit integers, starting with values like 0x21A8B293, 0x23FAE29C or 0x91B93485.

It comes either as an EXE or as a DLL with the internal DLL name t_client_dll.dll. It may contain statically linked code from open-source libraries like Mbed TLS or zLib (version 1.0.1).

Alreay RAT was observed in 2016-2017, running on networks of banks operating SWIFT Alliance software.

▶ [TLP:WHITE] win_alreay_auto (20251219 | Detects win.alreay.)
