

Cardinal RAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:38:46 UTC

Cardinal RAT is a remote access Trojan capable of stealing username and credentials, cleaning out cookies from browsers, keylogging and capturing screenshots on targeted systems. It is delivered via a downloader dubbed “Carp” which uses malicious macros in Microsoft Excel documents to compile embedded source code into an executable, which then deploys the Cardinal RAT malware family.

► [TLP:WHITE] win_cardinal_rat_auto (20180607 | autogenerated rule brought to you by yara-signator)

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.cardinal_rat