

## Orcus RAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-02 10:48:58 UTC

Orcus has been advertised as a Remote Administration Tool (RAT) since early 2016. It has all the features that would be expected from a RAT and probably more. The long list of the commands is documented on their website. But what separates Orcus from the others is its capability to load custom plugins developed by users, as well as plugins that are readily available from the Orcus repository. In addition to that, users can also execute C# and VB.net code on the remote machine in real-time.

► [TLP:WHITE] win\_orcus\_rat\_auto (20200421 | autogenerated rule brought to you by yara-signator)

---

Source: [https://malpedia.caad.fkie.fraunhofer.de/details/win.orcus\\_rat](https://malpedia.caad.fkie.fraunhofer.de/details/win.orcus_rat)