

xmrig (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:24:27 UTC

xmrig



According to PCrisk, XMRIG is a completely legitimate open-source application that utilizes system CPUs to mine Monero cryptocurrency. Unfortunately, criminals generate revenue by infiltrating this app into systems without users' consent. This deceptive marketing method is called "bundling".

In most cases, "bundling" is used to infiltrate several potentially unwanted programs (PUAs) at once. So, there is a high probability that XMRIG Virus came with a number of adware-type applications that deliver intrusive ads and gather sensitive information.

References

There is no Yara-Signature yet.

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