BOOSTWRITE (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:42:44 UTC

BOOSTWRITE

Actor(s): Anunak

FireEye describes BOOSTWRITE as a loader crafted to be launched via abuse of the DLL search order of applications which load the legitimate ‘Dwrite.dll’ provided by the Microsoft DirectX Typography Services. The application loads the ‘gdi’ library, which loads the ‘gdiplus’ library, which ultimately loads ‘Dwrite’. Mandiant identified instances where BOOSTWRITE was placed on the file system alongside the RDFClient binary to force the application to import DWriteCreateFactory from it rather than the legitimate DWrite.dll.

References

Yara Rules

▶ [TLP:WHITE] win_boostwrite_w0 (20191012 | No description)

Download all Yara Rules

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