

NimbleMamba (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:58:57 UTC

NimbleMamba

Actor(s): [Molerats](#)

NimbleMamba is a new implant used by TA402/Molerats group as replacement of LastConn. It uses guardrails to ensure that victims are within the TA's target region. It is written in C# and delivered as an obfuscated .NET executable. One seen obfuscator is SmartAssembly.

References

Yara Rules

▶ [TLP:WHITE] win_nimblemamba_w0 (20220209 Detects .NET written NimbleMamba malware used by TA402/Molereats)	
--	--

[Download all Yara Rules](#)

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