

Unidentified 103 (FIN8) (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-02 12:04:12 UTC

A malware that uses .NET to load unmanaged (shell)code which has some resemblance to BADHATCH, the IP found in the sample was referred to in coverage on WHITERABBIT ransomware attacks.

► [TLP:WHITE] win_unidentified_103_auto (20251219 | Detects win.unidentified_103.)

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_103