

Defray (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 01:06:31 UTC

Defray is ransomware that appeared in 2017, and is targeted ransomware, mainly on the healthcare vertical.

The distribution of Defray has several notable characteristics:

According to Proofpoint:

"

Defray is currently being spread via Microsoft Word document attachments in email

The campaigns are as small as several messages each

The lures are custom crafted to appeal to the intended set of potential victims

The recipients are individuals or distribution lists, e.g., group@ and websupport@

Geographic targeting is in the UK and US

Vertical targeting varies by campaign and is narrow and selective

"

► [TLP:WHITE] win_defray_auto (20251219 | Detects win.defray.)

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