DUSTMAN (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:30:59 UTC

In 2019, multiple destructive attacks were observed targeting entities within the Middle East. The National Cyber Security Centre (NCSC), a part of the National Cybersecurity Authority (NCA), detected a new malware named "DUSTMAN" that was detonated on December 29, 2019. Based on analyzed evidence and artifacts found on machines in a victim’s network that were not wiped by the malware. NCSC assess that the threat actor behind the attack had some kind of urgency on executing the files on the date of the attack due to multiple OPSEC failures observed on the infected network. NCSC is calling the malware used in this attack "DUSTMAN" after the filename and string embedded in the malware. "DUSTMAN" can be considered as a new variant of "ZeroCleare" malware,
published in December 2019.

▶ [TLP:WHITE] win_dustman_auto (20251219 | Detects win.dustman.)
