Saudi Arabia CNA report

Archived: 2026-04-05 21:28:56 UTC

Destructive Attack “DUSTMAN”

3

Technical Report

1.

Overview

Destructive attacks are quite extraordinary as threat actors employ their malware to disrupt or disable availability of the victim’s resources by wiping contents on storage devices of the targeted systems. In these attacks, threat actors have already compromised the victim’s network and gained privilege access to the internal infrastructure prior to the destruction activities. 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” has different characteristics when compared to the multiple wiper malwares that have been observed through the years, especially the “Shamoon” variants although they all use the same third-party driver “Eldos RawDisk”. Furthermore, “DUSTMAN” varies in terms of techniques and capability when compared to “Shamoon” and from the observed behavior and capabilities, “DUSTMAN” can be considered as a new variant of “ZeroCleare” malware, published in December 2019

(1)

. This report will shed the light on the attack life cycle, technical analysis of the malware, and the preventive recommendation with the Yara rules. It is worth mentioning that NCSC is still coordinating all efforts in understanding the extent of the attack, malware and attribution.

(1): New Destructive Wiper “ZeroCleare” Targets Energy Sector in the Middle East, December 2019, IBM X-Force.

Source: https://www.scribd.com/document/442225568/Saudi-Arabia-CNA-report