

Hamsa Wiper - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:45:10 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Hamsa Wiper

Tool: Hamsa Wiper

Names	Hamsa Wiper
Category	Malware
Type	Wiper
Description	<p>(Intezer) After masquerading as a routine update, the script strategically pauses for 30 minutes. This delay creates a deceptive appearance of typical system behavior during this period. In the meantime, the script accomplishes reconnaissance to identify the Linux distribution in use, whether it be Red Hat, Ubuntu, or Debian. Subsequently, it quietly installs necessary tools, such as xfsprogs, wipe, and parted, which are pivotal for later tasks involving disk partition manipulation and the secure erasure of data.</p> <p>Like its Windows variant, this wiper version transmits data to the same Telegram channel. The shared information aligns with what's sent by the Windows variant but adds specific details, such as the system directory's drive letter and prepared information on disk space. The data is organized with clear headers and separators to facilitate understanding, forming a structured log that allows the attackers to track and assess the impact of their infiltration.</p>
Information	< https://intezer.com/blog/research/stealth-wiper-israeli-infrastructure/ >

Last change to this tool card: 16 January 2024

Download this tool card in [JSON](#) format

All groups using tool Hamsa Wiper

Changed	Name	Country	Observed
Other groups			
	Handala Hack Team	[Unknown]	2023-Dec 2023

1 group listed (0 APT, 1 other, 0 unknown)

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=e1054c22-a722-4645-9807-b4212f86beb0>