Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:59:57 UTC

Tool: VHD

Names	VHD VHD Ransomware
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(Kaspersky) The ransomware itself is nothing special: it's written in C++ and crawls all connected disks to encrypt files and delete any folder called "System Volume Information" (which are linked to Windows' restore point feature). The program also stops processes that could be locking important files, such as Microsoft Exchange and SQL Server. Files are encrypted with a combination of AES-256 in ECB mode and RSA-2048. In our initial report published at the time we noted two peculiarities with this program's implementation: • The ransomware uses Mersenne Twister as a source of randomness, but unfortunately for the victims the RNG is reseeded every time new data is consumed. Still, this is unorthodox cryptography, as is the decision to use the "electronic codebook" (ECB) mode for the AES algorithm. The combination of ECB and AES is not semantically secure, which means the patterns of the original clear data are preserved upon encryption. This was reiterated by cybersecurity researchers who analyzed Zoom security in April 2020. • VHD implements a mechanism to resume operations if the encryption process is interrupted. For files larger than 16MB, the ransomware stores the current cryptographic materials on the hard drive, in clear text. This information is not deleted securely afterwards, which implies there may be a chance to recover some of the files.
Information	<https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/> <https://id-ransomware.blogspot.com/2020/03/vhd-ransomware.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.vhd_ransomware>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:VHD>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool VHD

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=151136f7-8f9b-47de-8edc-b2e38a63bde0