Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:25:05 UTC

Tool: CryptoMix

Names	CryptoMix CryptFile2 Zeta CryptoShield Azer
Category	Malware
Type	Ransomware
Description	(ZDNet) First spotted in early 2016, CryptoMix is a combination of CryptXXX and CryptoWall ransomware. While it has caused issues for users over the years, it's a relatively low-profile form of file-locking malware that until recently appeared to have fallen off the radar.
Information	<https://www.zdnet.com/article/this-old-ransomware-is-using-an-unpleasant-new-trick-to-try-and-make-you-pay-up/> <https://www.bleepingcomputer.com/news/security/work-cryptomix-ransomware-variant-released/> <https://www.cert.pl/en/news/single/technical-analysis-of-cryptomixcryptfile2-ransomware/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptomix>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:cryptomix>
Playbook	<https://blog.avast.com/cryptomix-avast-adds-a-new-free-decryption-tool-to-its-collection> <https://www.nomoreransom.org/uploads/Avast_how-to-guide.pdf>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool CryptoMix

Changed	Name	Country	Observed

APT groups

	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	

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

↑

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=363e38d6-848a-4356-a22e-736dbd211a07