

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 15:18:17 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Babuk Locker

Tool: Babuk Locker

Names	Babuk Locker Babuk Babyk Vasa Locker
Category	Malware
Type	Ransomware , Big Game Hunting
Description	(Cyberint) Babuk, also known as 'Babuk Locker', 'Babyk' and initially 'Vasa Locker', is a ransomware threat utilizing big-game hunter tactics to 'steal, encrypt and leak' victim data in an attempt to extort payments of reportedly up to USD 85,000 in Bitcoin (BTC).
Information	< https://blog.cyberint.com/babuk-locker/ > < https://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/ > < https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/ > < https://www.mcafee.com/blogs/other-blogs/mcafee-labs/babuk-ransomware/ > < https://therecord.media/builder-for-babuk-locker-ransomware-leaked-online/ > < https://www.bleepingcomputer.com/news/security/leaked-babuk-locker-ransomware-builder-used-in-new-attacks/ > < https://www.bleepingcomputer.com/news/security/babuk-ransomware-is-back-uses-new-version-on-corporate-networks/ > < https://darkfeed.io/babukhak-13444/ > < https://www.mcafee.com/blogs/other-blogs/mcafee-labs/babuk-biting-off-more-than-they-could-chew-by-aiming-to-encrypt-vm-and-nix-systems/ > < https://medium.com/s2wlab/blackmatter-x-babuk-using-the-same-web-server-for-sharing-leaked-files-d01c20a74751 > < https://www.bleepingcomputer.com/news/security/babuk-ransoms-full-source-code-leaked-on-hacker-forum/ > < https://www.advintel.io/post/groove-vs-babuk-groove-ransom-manifesto-ramp-underground-platform-secret-inner-workings > < https://www.bleepingcomputer.com/news/security/babuk-ransomware-decryptor-released-to-

	recover-files-for-free/ < https://blog.morphisec.com/babuk-ransomware-variant-major-attack >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.babuk > < https://malpedia.caad.fkie.fraunhofer.de/details/elf.babuk >
Playbook	< https://www.nomoreransom.org/uploads/Avast_how-to-guide.pdf >

Last change to this tool card: 29 December 2022

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

All groups using tool Babuk Locker

Changed	Name	Country	Observed	
APT groups				
	Indrik Spider		2007-Oct 2024	
	Tortilla	[Unknown]	2021	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=ea976a65-102c-4b60-8ae7-d24e357473a8>