Threat Group Cards: A Threat Actor Encyclopedia

Tool: BTC Changer

Names	BTC Changer
Category	Malware
Type	Info stealer, Credential stealer
Description	(Group-IB) The threat actor went back to the old habit of stealing crypto using a never-before-seen tool. Lazarus attacked online stores which accept cryptocurrency payments through crypto skimmers: JS-sniffers modified for the purpose of stealing crypto currency. Some victims, identified by Sansec, in fact, didn't fell prey to the clientToken= campaign, but to a different, previously undocumented Lazarus campaign, codenamed BTC Changer by Group-IB researchers.
Information	<https://www.group-ib.com/blog/btc_changer>

Last change to this tool card: 21 April 2021

Download this tool card in JSON format

All groups using tool BTC Changer

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

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