Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:24:33 UTC

Tool: BanSwift

Names	BanSwift
Category	Malware
Type	SWIFT malware
Description	The money was stolen through fraudulent SWIFT transactions, though the SWIFT system itself was not compromised, and malware (Trojan.BanSwift) was used to cover the attackers' tracks.
Information	<https://medium.com/threat-intel/lazarus-attacks-wannacry-5fdeddee476c> <https://www.anomali.com/blog/evidence-of-stronger-ties-between-north-korea-and-swift-banking-attacks> <https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool BanSwift

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

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