Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:38:11 UTC

Tool: Bookcode

Names	Bookcode
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration, Botnet
Description	(Kaspersky) We recently observed the Lazarus group attacking a software vendor in South Korea using Bookcode, malware that we evaluate to be a Volgmer variant, utilizing a watering-hole attack to deliver it. Manuscrypt is one of the Lazarus group's tools that is actively being updated and used. The group attacked the same victim twice. Almost a year prior to compromising this victim, Lazarus attempted to infect it by masquerading as a well-known security tool, but failed. We were able to construct the group's post-exploitation activity, identifying various freeware and red-teaming tools used. Although Lazarus has recently tended to focus more on targeting the financial industry, we believe that in this campaign they were seeking to exfiltrate intellectual property. We also observed that they previously spread Bookcode using a decoy document related to a company working in the defense sector. Based on our observations, we evaluate that the Bookcode malware is being used exclusively for cyber-espionage campaigns.
Information	<https://securelist.com/apt-trends-report-q2-2020/97937/>

Last change to this tool card: 30 July 2020

Download this tool card in JSON format

All groups using tool Bookcode

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

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