Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:26:30 UTC

Tool: Lazarus

Names	Lazarus HIDDEN COBRA RAT/Worm
Category	Malware
Type	Backdoor, Worm, Downloader, Info stealer, Exfiltration
Description	(US-CERT) This submission includes four unique files. The first is an installer for additional malware: a Remote Access Trojan (RAT) and a malicious Dynamic Link Library (DLL) that functions as a Server Message Block (SMB) Worm. The fourth file is another SMB worm in the form of a Windows 32-bit executable. Both SMB worms attempt to spread locally and to random IP addresses on the public Internet by attempting to brute force vulnerable systems using a built-in list of common passwords. The RAT included with the SMB worm provides the attacker with the ability to deliver additional malware, run local commands, and exfiltrate data.
Information	<https://www.us-cert.gov/ncas/analysis-reports/AR18-149A>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Lazarus

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a9a4e1b1-d1fd-446f-9ea9-fa4a62f9a48a