

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:58:24 UTC

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

Tool: Koredos

Names	Koredos
Category	Malware
Type	DDoS , Wiper
Description	(Symantec) In 2011, organizations in South Korea were yet again targeted by DDoS attacks. Similar to 2009, a number of government and private websites were targeted, this time using a tool called Trojan.Koredos. This attack was unusual for a DDoS attack because it did not use a command and control (C&C) server; the commands were hidden inside the threat itself. The use of a tactic like this indicated a growth in sophistication from the group compared to the 2009 attacks. Symantec research into this threat also found that, as well as carrying out a DDoS attack, if the infected computers were not cleared of this Trojan the master boot record (MBR) of some of them would be destroyed within 10 days.
Information	< https://medium.com/threat-intel/lazarus-attacks-wannacry-5fdeddee476c >

Last change to this tool card: 20 April 2020

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

All groups using tool Koredos

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=cfb71534-8ca8-4c87-b2b9-9cbe59f98585>