Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:10:13 UTC

Tool: Derusbi

Names	Derusbi PHOTO
Category	Malware
Type	Backdoor
Description	(Palo Alto) Derusbi is a backdoor Trojan believed to be used among a small group of attackers, which includes the Rancor group. This particular sample is a loader that loads an encrypted payload for its functionality. This DLL requires the loading executable to include a 32-byte key on the command line to be able to decrypt the embedded payload, which unfortunately we do not have. Even though we don't have the decryption key or loader, we have uncovered some interesting artifacts.
Information	<https://unit42.paloaltonetworks.com/rancor-cyber-espionage-group-uses-new-custom-malware-to-attack-southeast-asia/> <http://www.novetta.com/wp-content/uploads/2014/11/Derusbi.pdf> <https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0021/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.derusbi>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Derusbi>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool Derusbi

Changed	Name	Country	Observed
APT groups			

	APT 19, Deep Panda, C0d0so0		2013-Mar 2022	●
	APT 41		2012-Jul 2025	●
	Axiom, Group 72		2008-2008/2014	
	Leviathan, APT 40, TEMP.Periscope		2013-Jul 2021	●
	Rancor		2017	
	Stone Panda, APT 10, menuPass		2006-Mar 2025	●
	Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens		2010-Oct 2018	●

7 groups listed (7 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=70e712fe-753d-4fdb-9da3-4b760cab51ee