

Dacls RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:08:15 UTC

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

Tool: Dacls RAT

Names	Dacls RAT Dacls
Category	Malware
Type	Backdoor
Description	(Qihoo 360) Dacls is a new type of remote-control software targeting both Windows and Linux environment. Its functions are modular, the C2 protocol uses TLS and RC4 double-layer encryption, the configuration file uses AES encryption and supports C2 instruction dynamic update. The Win32.Dacls plug-in module is dynamically loaded through a remote URL, and the Linux version of the plug-in is compiled directly in the Bot program.
Information	< https://blog.netlab.360.com/dacls-the-dual-platform-rat-en/ > < https://blog.malwarebytes.com/threat-analysis/2020/05/new-mac-variant-of-lazarus-dacls-rat-distributed-via-trojanized-2fa-app/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/elf.dacls > < https://malpedia.caad.fkie.fraunhofer.de/details/win.dacls > < https://malpedia.caad.fkie.fraunhofer.de/details/osx.dacls >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:Dacls >

Last change to this tool card: 29 December 2022

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

All groups using tool Dacls RAT

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.eta.or.th/cgi-bin/listgroups.cgi?u=ece6a72a-df67-40cb-8f1a-17bb6fee43cc>