

Crimson RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:04:29 UTC

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

Tool: Crimson RAT



Names	Crimson RAT Crimson SEEDOOR Scarimson MSIL MSIL/Crimson
Category	Malware
Type	Backdoor
Description	Crimson is malware used as part of a campaign known as Operation Transparent Tribe that targeted Indian diplomatic and military victims.
Information	< https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf > < https://s.tencent.com/research/report/669.html > < https://www.amnesty.org/download/Documents/ASA3383662018ENGLISH.PDF >
MITRE ATT&CK	< https://attack.mitre.org/software/S0115/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.crimson >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:CrimsonRAT >

Last change to this tool card: 30 December 2022

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

All groups using tool Crimson RAT

Changed	Name	Country	Observed
APT groups			

	Gorgon Group		2017-Jul 2020	
	Transparent Tribe, APT 36		2013-Mar 2025	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=12f48fde-94b3-4bae-a6cd-90b31e77c31f>