Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:30:40 UTC

Tool: XtremeRAT

Names	XtremeRAT Xtreme RAT ExtRat
Category	Tools
Type	Backdoor, Keylogger, Info stealer, Exfiltration
Description	A publicly available RAT. (FireEye) XtremeRAT allows an attacker to: • Interact with the victim via a remote shell • Upload/download files • Interact with the registry • Manipulate running processes and services • Capture images of the desktop • Record from connected devices, such as a webcam or microphone Moreover, during the build process, the attacker can specify whether to include keylogging and USB infection functions.
Information	<https://www.fireeye.com/blog/threat-research/2014/02/xtremerat-nuisance-or-threat.html> <https://community.rsa.com/community/products/netwitness/blog/2017/08/02/malspam-delivers-xtreme-rat-8-1-2017> <https://www.symantec.com/connect/blogs/colombians-major-target-email-campaigns-delivering-xtreme-rat> <https://malware.lu/articles/2012/07/22/xtreme-rat-analysis.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.extreme_rat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:xtremerat>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool XtremeRAT

Changed	Name	Country	Observed	
APT groups				
	Molerats, Extreme Jackal, Gaza Cybergang	[Gaza]	2012-Jul 2023	
	Packrat	[Latin America]	2008	
	TA558	[Unknown]	2018-Jun 2023	

3 groups listed (3 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7886a052-0559-45f4-92ac-44366fe0791f