

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:15:12 UTC

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

Tool: XDRecon

Names	XDRecon
Category	Malware
Type	Reconnaissance , Info stealer
Description	(ESET) This is the most basic type of stealer plug-in. It gathers basic information about the victim machines (computer name, username, volume serial number) and writes it in %APPDATA%\Temp.NET\hdir.dat. It uploads this file to the C&C server and finally deletes it before exiting.
Information	< https://vblocalhost.com/uploads/VB2020-Faou-Labelle.pdf >

Last change to this tool card: 19 October 2020

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

All groups using tool XDRecon

Changed	Name	Country	Observed
APT groups			
	XDSpY	[Unknown]	2011-Jul 2024

1 group listed (1 APT, 0 other, 0 unknown)

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a859dde1-21f4-48da-bdfa-d493185035e2>