Threat Group Cards: A Threat Actor Encyclopedia

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)