Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:00:25 UTC

Tool: XDMonitor

Names	XDMonitor
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(ESET) XDMonitor is intended to monitor the machine's activity. It monitors when removable drives are inserted by creating a new hidden window and registering it for device notification (using RegisterDeviceNotificationW and the GUID GUID_DEVINTERFACE_DISK). When a new drive is inserted, it crawls it recursively. When a file with an interesting extension (the same list as for XDList) is found, it encrypts it using RC4 (the hard-coded key is 1234123412341234) and uploads it to the C&C server. It also takes a screenshot every minute. Unlike the screenshots taken by XDList, the image is not encrypted and is stored in %TEMP%\tmp%YEAR%%MONTH%%DAY%_%TICK_COUNT%.s. The screenshot is uploaded to the C&C immediately after being taken. Finally, XDMonitor sends regular debug messages to the C&C server.
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 XDMonitor

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=87dcdd53-b099-4067-ae5e-2bf242977fa0