Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:51:23 UTC

Tool: XDUpload

Names	XDUpload
Category	Malware
Type	Info stealer, Exfiltration
Description	(ESET) Like XDMonitor, XDUpload monitors removable drives and takes regular screenshots. The additional feature is that it will collect a list of files that are hard coded in the binary, as shown in Figure 11, and then upload the list to the C&C server. It uses %TEMP%\fl637136486220077590.data to keep track of how many files from the static list have been uploaded. We believe that the operators are checking the list of files from the C: drive, sent by XDList, and then selecting the ones that seem most interesting to them for exfiltration. What is surprising is that the paths are directly hard coded in the samples and not retrieved dynamically by a request to the C&C server. Thus, to collect additional files, the operators need to modify their source code, recompile and drop a new version of the plug-in on the victim's machine.
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 XDUpload

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=03db88bb-8a3b-467d-940d-0ad5f126b562