Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:50:30 UTC

APT group: XDSpy

Names	XDSpy *(ESET)*	
Country	[Unknown]	
Motivation	Information theft and espionage	
First seen	2011	
Description	(ESET) Rare is the APT group that goes largely undetected for nine years, but XDSpy is just that; a previously undocumented espionage group that has been active since 2011. It has attracted very little public attention, with the exception of an advisory from the Belarusian CERT in February 2020. In the interim, the group compromised many government agencies and private companies in Eastern Europe and the Balkans. In this paper, we present our analysis of this nine-year-long espionage campaign, active since 2011, but which apparently went dark in February 2020. With its primary purpose seemingly being cyber espionage, this group stole documents and other sensitive files, such as victims' mailboxes. These outcomes were achieved through the use of the XDSpy malware ecosystem, composed of at least seven components: XDDown, XDRecon, XDList, XDMonitor, XDUpload, XDLoc and XDPass. As our research has not uncovered links with any previously known APT groups, we have attributed this malware toolset to a previously unknown group.	
Observed	Sectors: Government. Countries: Belarus, Moldova, Russia, Serbia, Ukraine.	
Tools used	ChromePass, IE PassView, MailPassView, Network Password Recovery, OperaPassView, PasswordFox, Protected Storage PassView, XDDown, XDList, XDLoc, XDMonitor, XDPass, XDRecon, XDUpload.	
Operations performed	Jul 2024	Russia, Moldova targeted by obscure hacking group in new cyberespionage campaign <https://therecord.media/russia-moldova-cyberespionage-campaign>

Information	<https://vblocalhost.com/uploads/VB2020-Faou-Labelle.pdf> <https://www.welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011/> <https://therecord.media/xdspy-hackers-target-russian-military-industrial-companies>

Last change to this card: 27 August 2024

Download this actor card in PDF or JSON format
