Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:33:40 UTC

Tool: BIRDWATCH

Names	BIRDWATCH
Category	Malware
Type	Loader
Description	(Mandiant) Our deep dive also revealed usage of BIRDWATCH and its' similar variants used by FIN7 and suspected FIN7 groups such as UNC3381. BIRDWATCH is a .NET-based downloader which retrieves payloads over HTTP, writing them to disk and then executing them. BIRDWATCH uploads reconnaissance information from targeted systems as well, which includes running processes, software installed, network configuration, web browser information and active directory data. BIRDWATCH is often referred to collectively as "JSSLoader"; however, multiple variations of BIRDWATCH exist which we track as separate code families. One variant of BIRDWATCH is CROWVIEW, which is also .NET-based, but has enough code differences from prototypical BIRDWATCH that we cluster it separately. Unlike BIRDWATCH, CROWVIEW can house an embedded payload, can self-delete, supports additional arguments and stores a slightly different configuration.
Information	<https://www.mandiant.com/resources/evolution-of-fin7>

Last change to this tool card: 05 April 2022

Download this tool card in JSON format

All groups using tool BIRDWATCH

Changed	Name	Country	Observed	
APT groups				
	FIN7		2013-Jul 2024	

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