Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:37:42 UTC

Tool: Topinambour

Names	Topinambour
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Kaspersky) The purpose of all this infrastructure and modules in JavaScript, .NET and PowerShell is to build a “fileless” module chain on the victim’s computer consisting of an initial small runner and several Windows system registry values containing the encrypted remote administration tool. The tool does all that a typical Trojan needs to accomplish: upload, download and execute files, fingerprint target systems. The PowerShell version of the Trojan also has the ability to get screenshots.
Information	<https://securelist.com/turla-renews-its-arsenal-with-topinambour/91687/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.topinambour>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool Topinambour

Changed	Name	Country	Observed	
APT groups				
	Tomiris	[Unknown]	2020	
	Turla, Waterbug, Venomous Bear		1996-2024	

2 groups listed (2 APT, 0 other, 0 unknown)