Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:15:02 UTC

Tool: USBCulprit

Names	USBCulprit
Category	Malware
Type	Info stealer, Worm
Description	(Kaspersky) One of the most notable examples in Cycldek's toolset that demonstrates both data stealing and lateral movement capabilities is a malware we discovered and dubbed USBCulrpit. This tool, which we saw downloaded by RedCore implants in several instances, is capable of scanning various paths in victim machines, collecting documents with particular extensions and passing them on to USB drives when they are connected to the system. It can also selectively copy itself to a removable drive in the presence of a particular file, suggesting it can be spread laterally by having designated drives infected and the executable in them opened manually.
Information	<https://securelist.com/cycldek-bridging-the-air-gap/97157/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.usbculprit>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:usbculprit>

Last change to this tool card: 15 May 2021

Download this tool card in JSON format

All groups using tool USBCulprit

Changed	Name	Country	Observed	
APT groups				
	Goblin Panda, Cycldek, Conimes		2013-Jun 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2efd7c09-c2d3-4e8c-b48b-5cda7a3a80e8