UAC - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:50:25 UTC

Tool: Bypass-UAC

Names	Bypass-UAC
Category	Tools
Type	Loader
Description	Bypass-UAC provides a framework to perform UAC bypasses based on auto elevating IFileOperation COM object method calls. This is not a new technique, traditionally, this is accomplished by injecting a DLL into 'explorer.exe'. This is not desirable because injecting into explorer may trigger security alerts and working with unmanaged DLL's makes for an inflexible work-flow.
Information	<https://github.com/FuzzySecurity/PowerShell-Suite/blob/master/Bypass-UAC/Bypass-UAC.ps1>

Last change to this tool card: 10 July 2020

Download this tool card in JSON format

All groups using tool Bypass-UAC

Changed	Name	Country	Observed	
APT groups				
	Evilnum	[Unknown]	2018-2022	

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