Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:55:31 UTC

Tool: Remcom

Names	Remcom RemoteCommandExecution
Category	Tools
Type	Backdoor, Remote command
Description	RemCom is an open-source, redistributable utility providing the same remote management functions. It achieved a level of notoriety after adversaries used it to move laterally in their attack on the Democratic National Committee in 2016. However, it's also included in several legitimate software packages. By default, RemCom sends RemComSvc.exe to a remote computer, which then uses the named pipe \\.\pipe\remcom_comunication (misspelling and all) in the place of PsExec's named pipe. In addition, the process's internal name has a value of remcom.
Information	<https://redcanary.com/blog/threat-hunting-psexec-lateral-movement/> <https://doublepulsar.com/second-zerologon-attacker-seen-exploiting-internet-honeypot-c7fb074451ef>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.remcom>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Remcom

Changed	Name	Country	Observed	
APT groups				
	ALPHV, BlackCat Gang	[Unknown]	2021-Mar 2024	
	Chafer, APT 39		2014-Sep 2020	

	Dalbit		2022	

3 groups listed (3 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=36ef119d-9261-4c84-ade0-694c3c86428e