Raspberry Robin - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:13:50 UTC

Tool: Raspberry Robin

Names	Raspberry Robin RaspberryRobin LINK_MSIEXEC QNAP-Worm
Category	Malware
Type	Backdoor, Worm
Description	(Red Canary) “Raspberry Robin” is Red Canary’s name for a cluster of activity we first observed in September 2021 involving a worm that is often installed via USB drive. This activity cluster relies on msiexec.exe to call out to its infrastructure, often compromised QNAP devices, using HTTP requests that contain a victim’s user and device names. We also observed Raspberry Robin use TOR exit nodes as additional command and control (C2) infrastructure.
Information	<https://redcanary.com/blog/raspberry-robin/> <https://blogs.cisco.com/security/raspberry-robin-highly-evasive-worm-spreads-over-external-disks> <https://securityintelligence.com/posts/raspberry-robin-worm-dridex-malware/> <https://www.bleepingcomputer.com/news/security/microsoft-links-raspberry-robin-malware-to-evil-corp-attacks/> <https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/> <https://www.trendmicro.com/en_us/research/22/l/raspberry-robin-malware-targets-telecom-governments.html> <https://blog.checkpoint.com/security/raspberry-robin-evolving-cyber-threat-with-advanced-exploits-and-stealth-tactics/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1130>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.raspberry_robin>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool Raspberry Robin

Changed	Name	Country	Observed	
APT groups				
	Indrik Spider		2007-Oct 2024	

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

↑

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=aa33ee5c-7411-475f-a356-21664c8411e1