Raspberry Robin (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 02:58:40 UTC

win.raspberry_robin (Back to overview)

Raspberry Robin

aka: RaspberryRobin, QNAP-Worm, LINK_MSIEXEC

Worm spread by external drives that leverages Windows Installer to reach out to QNAP-associated domains and download a malicious DLL.

References

2025-08-06 · Silent Push · Silent Push
Unmasking SocGholish: Silent Push Untangles the Malware Web Behind the “Pioneer of Fake Updates” and Its Operator, TA569
FAKEUPDATES MintsLoader Parrot TDS Parrot TDS WebShell Raspberry Robin

2024-11-19 · Zscaler · Nikolaos Pantazopoulos
Unraveling Raspberry Robin's Layers: Analyzing Obfuscation Techniques and Core Mechanisms
Raspberry Robin Roshtyak

2024-04-03 · HarfangLab · Alice Climent-Pommeret
Raspberry Robin and its new anti-emulation trick
Raspberry Robin

2024-04-02 · Darktrace · Alexandra Sentenac, Trent Kessler, Victoria Baldie
The Early Bird Catches the Worm: Darktrace’s Hunt for Raspberry Robin
Raspberry Robin

2024-02-07 · Check Point Research · Check Point Research
Raspberry Robin Keeps Riding the Wave of Endless 1-Days
Raspberry Robin

2023-09-07 · Huntress Labs · Harlan Carvey
Evolution of USB-Borne Malware, Raspberry Robin
Raspberry Robin

2023-04-18 · Check Point Research · Shavit Yosef
Raspberry Robin: Anti-Evasion How-To & Exploit Analysis
Raspberry Robin

2023-04-18 · Checkpoint · Shavit Yosef
Raspberry Robin: Anti-Evasion How-To & Exploit Analysis
Raspberry Robin

2023-01-03 · Security Joes · SecurityJoes
Raspberry Robin Detected ITW Targeting Insurance & Financial Institutes In Europe
Raspberry Robin

2022-12-20 · Trend Micro · Christopher Daniel So
Raspberry Robin Malware Targets Telecom, Governments
Raspberry Robin Roshtyak

2022-12-08 · Cisco Talos · Tiago Pereira
Breaking the silence - Recent Truebot activity
Clop Cobalt Strike FlawedGrace Raspberry Robin Silence Teleport

2022-10-27 · Microsoft · Microsoft Security Threat Intelligence
Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity
FAKEUPDATES BumbleBee Fauppod PhotoLoader Raspberry Robin Roshtyak

2022-10-27 · Bleeping Computer · Sergiu Gatlan
Microsoft links Raspberry Robin worm to Clop ransomware attacks
Clop Raspberry Robin

2022-10-27 · Microsoft · Microsoft Threat Intelligence
Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity
FAKEUPDATES BumbleBee Clop Fauppod Raspberry Robin Roshtyak Silence DEV-0950 Mustard Tempest

2022-09-26 · Palo Alto Networks Unit 42 · Daniela Shalev, Itay Gamliel
Hunting for Unsigned DLLs to Find APTs
PlugX Raspberry Robin Roshtyak

2022-09-22 · Avast · Jan Vojtěšek
Raspberry Robin’s Roshtyak: A Little Lesson in Trickery
Raspberry Robin Roshtyak

2022-09-01 · IBM · Emmy Ebanks, Kevin Henson
Raspberry Robin and Dridex: Two Birds of a Feather
Dridex Raspberry Robin

2022-08-09 · Cisco · Onur Mustafa Erdogan
Raspberry Robin: Highly Evasive Worm Spreads over External Disks
Raspberry Robin

2022-07-30 · The Hacker News · Ravie Lakshmanan
Microsoft Links Raspberry Robin USB Worm to Russian Evil Corp Hackers
FAKEUPDATES Raspberry Robin

2022-07-07 · Cybereason · Loïc Castel
THREAT ALERT: Raspberry Robin Worm Abuses Windows Installer and QNAP Devices
Raspberry Robin

2022-05-05 · Red Canary · Lauren Podber, Stef Rand
Raspberry Robin gets the worm early
Raspberry Robin

There is no Yara-Signature yet.
