Raindrop (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:16:45 UTC

win.raindrop (Back to overview)

Raindrop

Actor(s): UNC2452

Raindrop is a loader for Cobalt Strike that was observed in the SolarWinds attack.

References

2022-07-31 · BushidoToken Blog · BushidoToken
Space Invaders: Cyber Threats That Are Out Of This World
Poison Ivy Raindrop SUNBURST TEARDROP WastedLocker

2022-04-27 · Mandiant · Mandiant
Assembling the Russian Nesting Doll: UNC2452 Merged into APT29
Cobalt Strike Raindrop SUNBURST TEARDROP

2021-10-26 · Kaspersky · Kaspersky Lab ICS CERT
APT attacks on industrial organizations in H1 2021
8.t Dropper AllaKore AsyncRAT GoldMax LimeRAT NjRAT NoxPlayer Raindrop ReverseRAT ShadowPad Zebrocy

2021-07-13 · Symantec · Threat Hunter Team
Attacks Against the Government Sector
Raindrop TEARDROP

2021-07-13 · YouTube (Matt Soseman) · Matt Soseman
Solarwinds and SUNBURST attacks compromised my lab!
Cobalt Strike Raindrop SUNBURST TEARDROP

2021-06-01 · SANS · Jake Williams, Kevin Haley
A Contrarian View on SolarWinds
Cobalt Strike Raindrop SUNBURST TEARDROP

2021-01-18 · Symantec · Threat Hunter Team
Raindrop: New Malware Discovered in SolarWinds Investigation

Cobalt Strike Raindrop SUNBURST TEARDROP

2021-01-01 · Symantec · Symantec Threat Hunter Team

Supply Chain Attacks:Cyber Criminals Target the Weakest Link

Cobalt Strike Raindrop SUNBURST TEARDROP

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.raindrop