sRDI (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:54:40 UTC

sRDI

aka: DAVESHELL

Actor(s): APT29, Lazarus Group

---

sRDI allows for the conversion of DLL files to position independent shellcode. It attempts to be a fully functional PE loader supporting proper section permissions, TLS callbacks, and sanity checks. It can be thought of as a shellcode PE loader strapped to a packed DLL.

References

2024-07-29 · Mandiant · Ashley Pearson, Jake Nicastro, Joseph Pisano, Josh Murchie, Joshua Shilko, Raymond Leong
UNC4393 Goes Gently into the SILENTNIGHT
Black Basta QakBot sRDI SystemBC Zloader UNC3973 UNC4393

2023-09-29 · ESET Research ·
Lazarus luring employees with trojanized coding challenges: The case of a Spanish aerospace company
CLOUDBURST LightlessCan miniBlindingCan sRDI

2023-09-22 · Mandiant · Dan Black, Josh Atkins, Luke Jenkins
Backchannel Diplomacy: APT29’s Rapidly Evolving Diplomatic Phishing Operations
Brute Ratel C4 Cobalt Strike EnvyScout GraphDrop QUARTERRIG sRDI Unidentified 107 (APT29)

2022-09-14 · Mandiant · James Maclachlan, Mathew Potaczek, Matt Williams, Nino Isakovic, Yash Gupta
It's Time to PuTTY! DPRK Job Opportunity Phishing via WhatsApp
BLINDINGCAN miniBlindingCan sRDI

2022-06-17 · Github (monoxgas) · Nick Landers
sRDI - Shellcode Reflective DLL Injection
sRDI

There is no Yara-Signature yet.
