sLoad (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:27:44 UTC

ps1.sload (Back to overview)

sLoad

aka: Starslord

URLhaus

---

sLoad is a PowerShell downloader that most frequently delivers Ramnit banker and includes noteworthy reconnaissance features. The malware gathers information about the infected system including a list of running processes, the presence of Outlook, and the presence of Citrix-related files. sLoad can also take screenshots and check the DNS cache for specific domains (e.g., targeted banks), as well as load external binaries.

References

2025-03-28 · Intrinsec · David Sardinha
From espionage to PsyOps: Tracking operations and bulletproof providers of UACs in 2025
sLoad NetSupportManager RAT Remcos SmokeLoader

2021-06-21 · Minerva Labs · Minerva Labs
Sload Targeting Europe Again
sLoad

2020-10-28 · Bitdefender · Ruben Andrei Condor
A Decade of WMI Abuse – an Overview of Techniques in Modern Malware
sLoad Emotet Maze

2020-07-13 · · Cert-AgID · Cert-AgID
Campagna sLoad v.2.9.3 veicolata via PEC
sLoad

2020-03-10 · · Cert-Pa · Cert-PA
Campagna sLoad “Star Wars Edition” veicolata via PEC
sLoad

2020-01-21 · Microsoft · Microsoft Defender ATP Research Team
sLoad launches version 2.0, Starslord

sLoad

2019-12-13 · Threatpost · Tara Seals

Elegant sLoad Carries Out Spying, Payload Delivery in BITS

sLoad

2019-01-03 · Cybereason · Eli Salem, Lior Rochberger, Niv Yona

LOLbins and trojans: How the Ramnit Trojan spreads via sLoad in a cyberattack

sLoad

2018-11-27 · Yoroi · Luca Mella, Luigi Martire

The SLoad Powershell Threat is Expanding to Italy

sLoad

2018-11-23 · Certego · Matteo Lodi

Sload hits Italy. Unveil the power of powershell as a downloader

sLoad

2018-10-25 · Sophia Brown

New sLoad malware downloader being leveraged by APT group TA554 to spread Ramnit

sLoad

2018-10-23 · Proofpoint · Proofpoint Staff

sLoad and Ramnit pairing in sustained campaigns against UK and Italy

sLoad

2018-08-05 · Vitali Kremez Blog · Vitali Kremez

Let's Learn: Diving into the Latest "Ramnit" Banker Malware via "sLoad" PowerShell

sLoad

2018-05-19 · Xavier Mertens

Malicious Powershell Targeting UK Bank Customers

sLoad

There is no Yara-Signature yet.
