

# SUGARLOADER (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:39:32 UTC

osx.sugarloader ([Back to overview](#))

## SUGARLOADER

Actor(s): [Lazarus Group](#)

---

There is no description at this point.

### References

2026-02-09 · [Mandiant](#) · [Adrian Hernandez](#), [Ross Inman](#)

UNC1069 Targets Cryptocurrency Sector with New Tooling and AI-Enabled Social Engineering  
[SUGARLOADER WAVESHAPER](#)

2024-10-03 · [Virus Bulletin](#) · [Salim Bitam](#)

Sugarcoating KANDYKORN: a sweet dive into a sophisticated MacOS backdoor  
[HLOADER KANDYKORN SUGARLOADER](#)

2023-11-27 · [SentinelOne](#) · [Phil Stokes](#)

DPRK Crypto Theft | macOS RustBucket Droppers Pivot to Deliver KandyKorn Payloads  
[HLOADER KANDYKORN RustBucket SUGARLOADER](#)

2023-10-31 · [Elastic](#) · [Andrew Pease](#), [Colson Wilhoit](#), [Ricardo Ungureanu](#), [Seth Goodwin](#)

Elastic catches DPRK passing out KANDYKORN  
[HLOADER KANDYKORN SUGARLOADER](#)

There is no Yara-Signature yet.

---

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/osx.sugarloader>