

# Loda (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:36:25 UTC

win.loda ([Back to overview](#))

## Loda

aka: LodaRAT, Nymeria

URLhaus

---

Loda is a previously undocumented AutoIT malware with a variety of capabilities for spying on victims. Proofpoint first observed Loda in September of 2016 and it has since grown in popularity. The name Loda is derived from a directory to which the malware author chose to write keylogger logs. It should be noted that some antivirus products currently detect Loda as “Trojan.Nymeria”, although the connection is not well-documented.

### References

2023-10-25 · [Cisco Talos](#) · [Asheer Malhotra](#), [Vitor Ventura](#)

Kazakhstan-associated YoroTrooper disguises origin of attacks as Azerbaijan  
[Ave Maria Loda YoroTrooper](#)

2023-03-14 · [Cisco Talos](#) · [Asheer Malhotra](#), [Vitor Ventura](#)

Talos uncovers espionage campaigns targeting CIS countries, embassies and EU health care agency  
[Poet RAT Loda Kasablanka YoroTrooper](#)

2023-01-17 · [Qianxin](#) · [Red Raindrop Team](#)

Kasablanka Group Probably Conducted Campaigns Targeting Russia  
[Ave Maria Loda](#)

2022-11-17 · [Cisco Talos](#) · [Chris Neal](#)

Get a Loda This: LodaRAT meets new friends  
[Loda Kasablanka](#)

2022-08-18 · [Proofpoint](#) · [Joe Wise](#), [Proofpoint Threat Research Team](#), [Selena Larson](#)

Reservations Requested: TA558 Targets Hospitality and Travel  
[AsyncRAT Loda NjRAT Ozone RAT Revenge RAT Vjw0rm](#)

2022-08-17 · [360](#) · [360 Threat Intelligence Center](#)

Kasablanka organizes attacks against political groups and non-profit organizations in the Middle East

[SpyNote Loda Nanocore RAT NjRAT](#)

2021-02-15 · [Silent Push](#) · [Martijn Grooten](#)

More LodaRAT infrastructure targeting Bangladesh uncovered

[Loda](#)

2021-02-09 · [Talos](#) · [Chris Neal](#), [Vitor Ventura](#), [Warren Mercer](#)

Kasablanka Group's LodaRAT improves espionage capabilities on Android and Windows

[Loda](#)

2020-09-29 · [Cisco Talos](#) · [Chris Neal](#)

LodaRAT Update: Alive and Well

[Loda](#)

2020-02-12 · [Cisco Talos](#) · [Chris Neal](#)

Loda RAT Grows Up

[Loda](#)

2018-01-23 · [Zerophage](#)

Maldoc (RTF) drops Loda Logger

[Loda](#)

2017-05-10 · [Proofpoint](#) · [Proofpoint Staff](#)

Introducing Loda Malware

[Loda](#)

There is no Yara-Signature yet.

---

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.loda>