

DILLJUICE (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:54:02 UTC

DILLJUICE

Actor(s): Stone Panda



APT10's fork of the (open-source) Quasar RAT.

References

Yara Rules

▶ [TLP:WHITE] win_dilljuice_w0 (20190708 Detection of DILLJUICE.A through its dropper)	
▶ [TLP:WHITE] win_dilljuice_w1 (20190708 Detection of DILLJUICE.B through its dropper)	

[Download all Yara Rules](#)

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