# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:44:17 UTC



## Tool: DILLJUICE

| | |
|---|---|
| Names | DILLJUICE<br>FYAnti |
| Category | Malware |
| Type | Reconnaissance, Backdoor, Info stealer, Credential stealer, Exfiltration |
| Description | (Cylance) QuasarRAT is a lightweight remote administration tool written in C#. It can collect system information, download and execute applications, upload files, log keystrokes, grab screenshots/camera captures, retrieve system passwords and run shell commands. The remote access Trojan (RAT) is loaded by a bespoke loader (a.k.a. DILLWEED). The encrypted QuasarRAT payload is stored in the Microsoft.NET directory, decrypted into memory, and instantiated using a CLR host application. In later variants an additional component is also used to install the RAT as a service (a.k.a DILLJUICE).<br><br>The following technical analysis focuses on the bespoke QuasarRAT loader developed by MenuPass and modifications made to the QuasarRAT backdoor. |
| Information | <https://threatvector.cylance.com/en_us/home/threat-spotlight-menupass-quasarrat-backdoor.html> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.dilljuice> |

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

### All groups using tool DILLJUICE

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Stone Panda, APT 10, menuPass | | 2006-Mar 2025 | |

*1 group listed (1 APT, 0 other, 0 unknown)*

---