# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 15:38:51 UTC



## Tool: BlotchyQuasar

| | |
|---|---|
| Names | BlotchyQuasar |
| Category | Malware |
| Type | Banking trojan, Backdoor, Info stealer, Credential stealer |
| Description | (IBM) BlotchyQuasar, which X-Force describes as a banking trojan due to it containing a hardcoded list of banking applications, was developed on top of the QuasarRAT codebase, and is under active development and supports a wide range of different custom commands. Some of the most interesting features include the installation of root certificates and proxy auto-config URLs, which may be used in conjunction with Google Chrome Kiosk mode to impersonate financial institutions. |
| Information | <https://securityintelligence.com/posts/x-force-hive0129-targeting-financial-institutions-latam-banking-trojan/> |

Last change to this tool card: 05 September 2023

Download this tool card in JSON format

### All groups using tool BlotchyQuasar

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Blind Eagle | | 2018-Nov 2024 | |

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