

Initial Access Broker Landscape

 curatedintel.org/2021/10/initial-access-broker-landscape.html


Cypher


Version 1 of the **initial access broker (IAB) landscape** project helps clarify the economy of selling accesses by visualizing information flows. The project is curated by [Trevor Giffen](#) and reviewed by the broader Curated Intelligence community.

An "initial access broker" is an individual who compromises systems or user accounts with the intent of gaining privileged access, to later sell. Initial access sales happen both publicly and privately, across many contexts. KE-LA does a great job of [explaining initial access brokers](#) here; common examples include:

- Advertising access sales on underground forums
- Advertising access sales on underground marketplaces
- Advertising access sales privately to ransomware actors (ex. 5-30% cut for initial access alone)
- Advertising access sales privately to interested third-parties (ex. information theft)
- Gaining access to an internet-facing system, typically servers with an *RCE vulnerability* or *RDP*
- Gaining access using an *information stealer* campaign
- Gaining access using *information sold* on an underground marketplace
- Gaining access using *reused credentials* from third-party data breaches
- Gaining access using *password guessing*, typically bruteforcing or password spraying
- Gaining access using a *phishing* campaign
- Gaining access using an *insider threat*

High resolution files are available via GitHub:

 PNG: <https://github.com/curated-intel/Initial-Access-Broker-Landscape/blob/main/InitialAccessBrokers.png>

 SVG: <https://github.com/curated-intel/Initial-Access-Broker-Landscape/blob/main/InitialAccessBrokers.svg>

