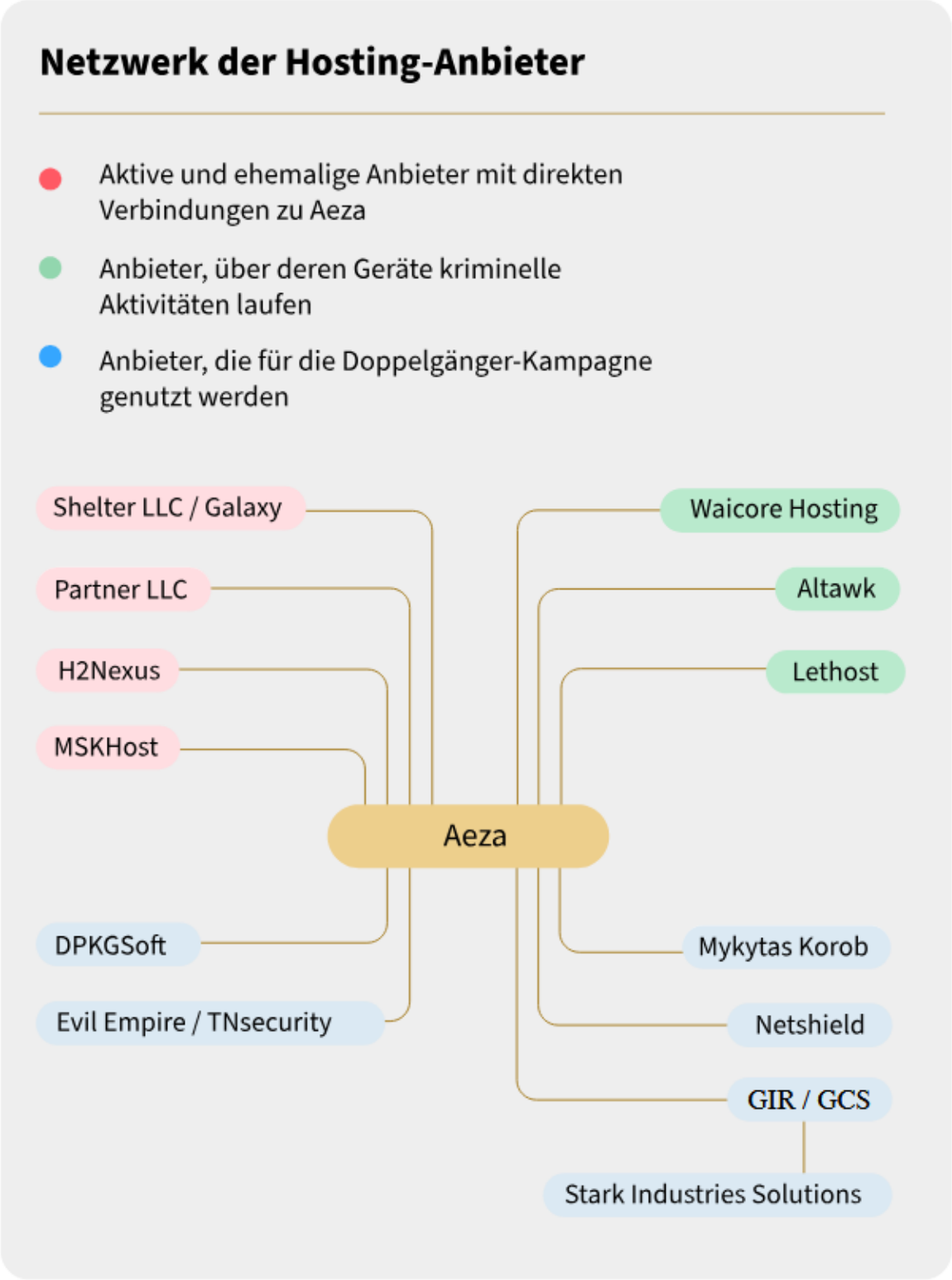
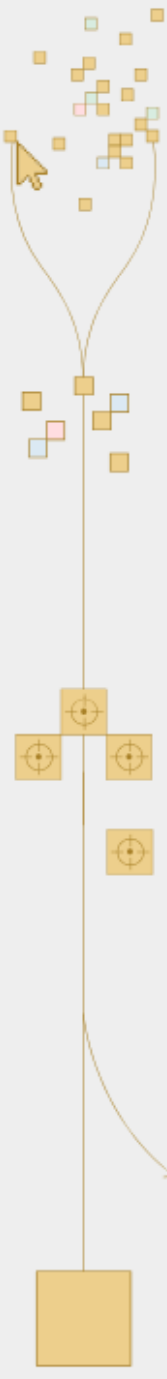
Russische Propaganda und Fakes – dank Technik aus Europa




Aeza steht laut der Analyse von Qurium im Zentrum eines Netzwerks an Hosting-Anbietern. Über deren Dienste laufen teils kriminelle Aktivitäten (grün markiert) und oder sie werden auch für die Desinformationskampagne „Doppelgänger“ genutzt (blau markiert).

## Die IT-Infrastruktur von Doppelgänger

So werden Nutzerinnen und Nutzer weitergeleitet, wenn sie auf einen Link der Doppelgänger-Kampagne klicken.



### Wegwerf-Domains

Künstliche Accounts teilen auf X und Facebook unzählige Links. Die Domains verschleiern ihr eigentliches Ziel und liegen bei Firmen wie TNSecurity oder Netshield in Großbritannien. Der Datenverkehr läuft auch über Hostinger in Litauen und Aurologic in Deutschland.

### Zwischen-Domains

Ein Code wartet auf diesen Domains und leitet Ihren Browser an die nächste Station weiter. Die Domains liegen bei BL Networks aus den USA und dem britischen Liber Systems.

### Keitaro-Domains

Der Werbetracker Keitaro der estnischen Firma Apliteni OU prüft den Standort des Browsers und leitet zur korrekten Propaganda-Webseite weiter, wenn zum Beispiel ein gefälschter Spiegel-Artikel von Deutschland aus aufgerufen wird. Dies geschieht über eine von nur vier Domains, die bei Hetzner in Finnland liegen.

Besucher vom falschen Standort werden weggeleitet.

### Doppelgänger-Domain

Sie sind am Ziel angekommen. Hier wartet eine gefälschte Medienwebseite oder ein Propaganda-Blog der Kampagne. Diese Seiten, wie der gefälschte Spiegel-Artikel, liegen bei Shinjiru in Malaysia und Hostinger in Litauen.