

THREAT INTELLIGENCE

We see every online store.
Including the compromised ones.

OneRisk examines more than 22 million live merchant sites. Here is what that view reveals about card skimming on the open web, and about one network in particular.

THE VIEW

One view across 22 million+ online merchants

The same view that scores a merchant at onboarding recognizes known threats on any site, wherever they appear. Today it is tracking:

143k+

Counterfeit storefronts built from a single card-skimming kit

650+

Legitimate stores compromised with card skimmers or malicious loaders

62

Fake bank and login pages hidden behind a counterfeit security check

46

Storefronts with a checkout plugin that sends each card number to the fraudster as the shopper types it

CASE STUDY

GorgonAgora

Counterfeit storefronts for brands shoppers already know. At checkout, each presents a card payment form and sends the card details entered to the operator's servers.

Researchers at Sansec first documented the kit in June 2026. Across OneRisk's view, it runs on **143,926** storefronts.

sansec.io/research/gorgonagora-fake-storefront-skimming-network

BY THE NUMBERS

A network built for volume

95%

of the storefronts are registered under the .shop top-level domain

220 of 220

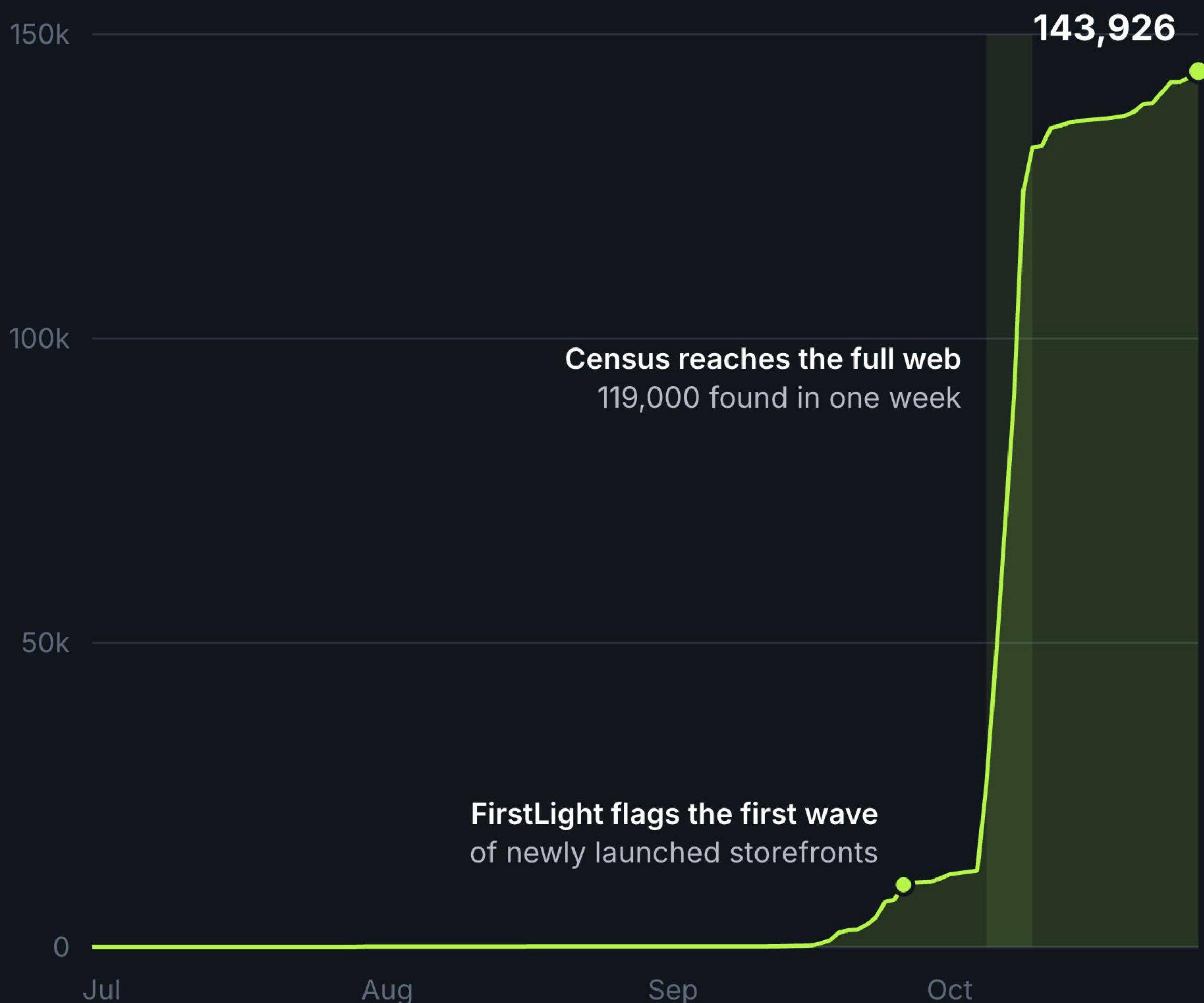
storefronts that received a full OneRisk merchant scan were rated high risk

5,708

new storefronts appeared between October 21 and 27, 2026

MAPPING THE NETWORK

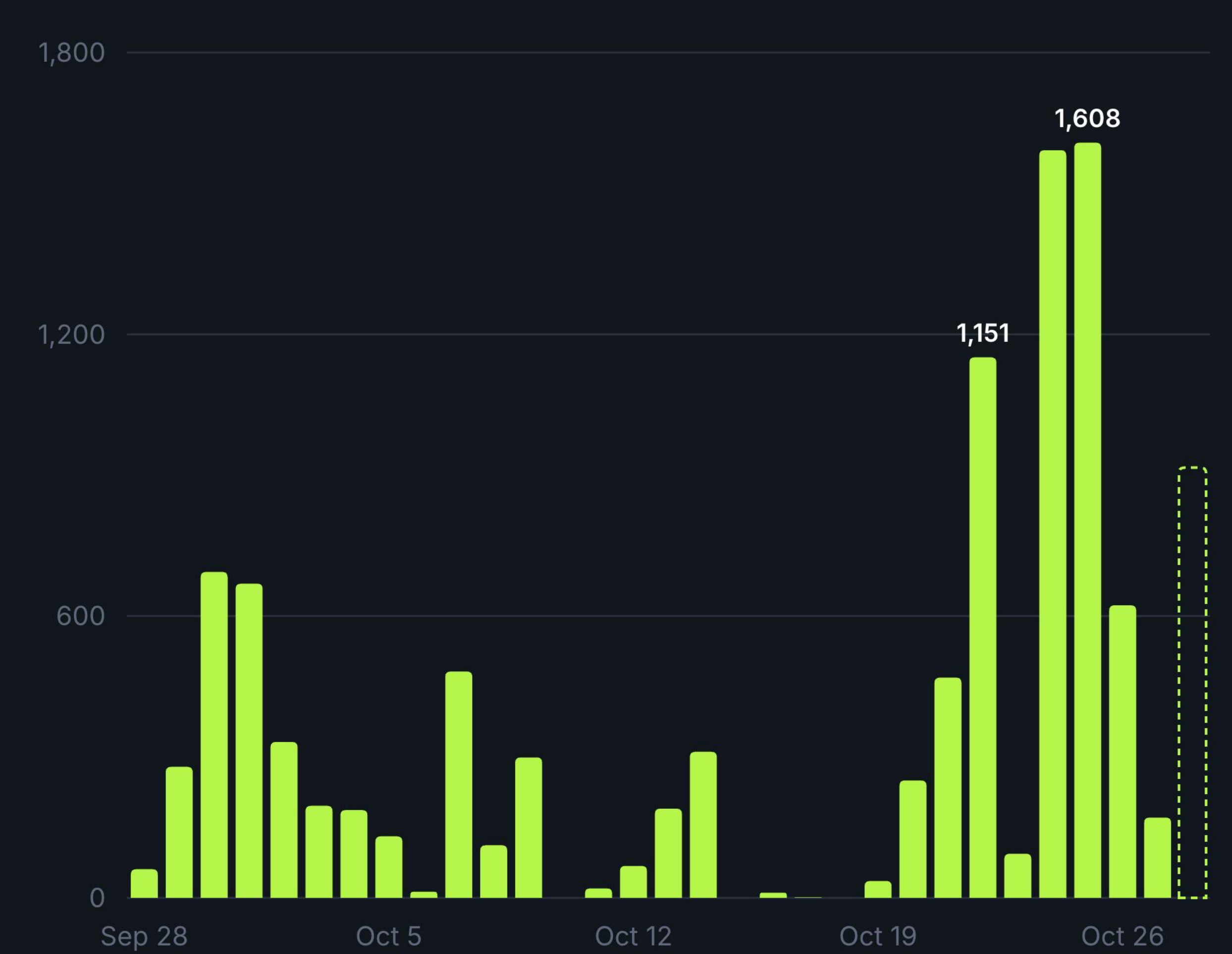
Every storefront running the kit, as OneRisk found it



Sites carrying the GorgonAgora storefront kit, by the date OneRisk first observed each one. June 30 to October 28, 2026.

STILL GROWING

New storefronts arrive in batches of over a thousand a day



New GorgonAgora storefronts by the day OneRisk first saw each one's domain, September 28 to October 28, 2026. Today is a partial day.

THE MERCHANT VIEW

The finding lands on the merchant's risk profile

A site carrying a known threat is rated high risk automatically, with the evidence stated in plain language.

luxecosme.....shop

Copy

Completed

Re-scan

More

Risk score

100

High risk

Scanned 10 days ago

100 — 100

The business appears to present itself as a brand or public service it is not, and public reviews and commentary raise concerns.

Its store, payment, advertising, and tracking accounts, contact details, and hosting setup are shared with merchants previously identified as fraudulent....

Show more

Dimensions

Risk

Fraud Analytics	+16.05
Commerce Infrastructure	+1.41
Public Reputation	+0.81
Geography	+0.19
Hosting Profile	+0.10
Social Media	No findings
Business Profile	No findings
Operator Profile	No findings

What stands out

- An account identifier on the merchant's website is used by another fraudulent merchant
- The merchant's website carries a known card skimmer
- The merchant's website is a visual copy of another brand's website

Site preview

Home | Luxe Cosmetics luxecosme.....shop

Captured 10 days ago

Luxe

Our Products Eyelashes Eyebrows Extras Nail Products Hair Products

Account Your Cart (0)

Radiate Beauty, Redefine Luxury

Experience premium skincare and makeup crafted with clean ingredients for a flawless, glowing complexion.

Shop Now

View full page

onerisk.com

7 / 10

THE NETWORK VIEW

One view of the whole operation

Every site linked to the threat, updated as new ones appear and rated as they are scanned.

Threat family

GorgonAgora

Counterfeit brand storefronts on .shop domains, built on Medusa.js, that present a fake card payment form and send the entered card details to the operator's servers over an encrypted WebSocket. Active since August 2025.

Card skimmerCritical Also known as PaymentVanilla 143,393 sites matched · last 36 seconds ago

References

GorgonAgora: fake storefront skimming network · Sansec, 2026-06-02

Matches

Merchant scans

Site	Risk rating	Seen on	Last seen
officialstack.....shop	100	Merchant homepage	23 hours ago
4xspower.....shop	100	Merchant homepage	24 hours ago
pureh.....shop	100	Merchant homepage	yesterday
madisoncen.....shop	100	Merchant homepage	yesterday
halvacol.....shop	100	Merchant homepage	yesterday
halva.....shop	100	Merchant homepage	yesterday
shopmadis.....shop	100	Merchant homepage	yesterday
buddhasto.....shop	100	Merchant homepage	yesterday

WHY IT MATTERS

What a complete view makes possible

1 Find compromised merchants already in your portfolio

A legitimate store carrying a skimmer puts its customers' cards, and its acquirer, at risk.

2 Stop counterfeit storefronts before they apply

Sites built from a known fraud kit are rated high risk the moment they appear.

3 See the entire fraud operation, not one site at a time

Every site linked to a threat is tracked together, and the list keeps itself current.

ABOUT ONERISK

Merchant risk intelligence at internet scale

OneRisk maintains intelligence on every active online merchant, links the storefronts that share supporting infrastructure, and scores merchants at onboarding and throughout the relationship.

Acquirers, ISOs, payment facilitators and issuers use it to see fraud and compromise across the web, not one storefront at a time.

onerisk.com