PointyPhish & TollShark

REPORT 2025

Rise in Rewards and Toll Scams

Analysis by CTM360

CTM360®

INDUSTRY Global | **COUNTRY** Global | **REGION** Global

OVERVIEW :

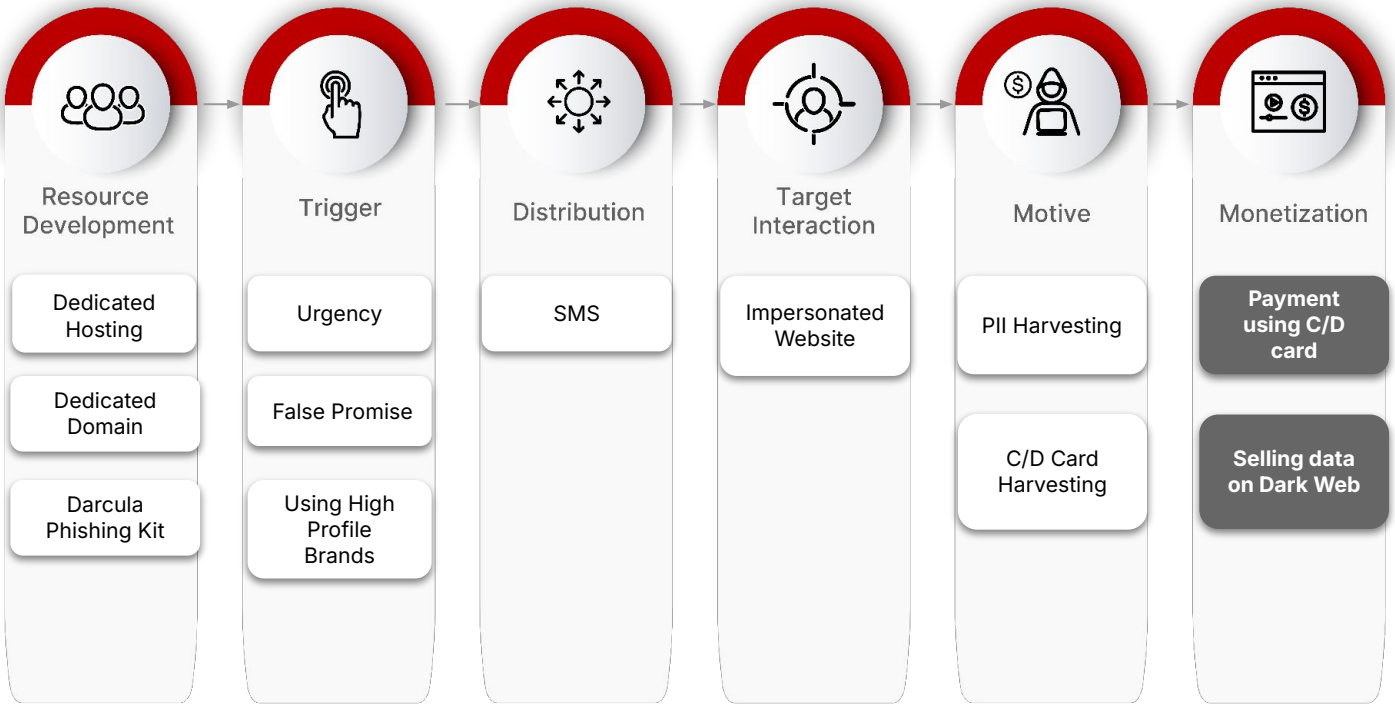
CTM360 has observed a sharp increase in two major scam campaigns, Reward Points Scam (**PointyPhish**) and Toll Scam (**TollShark**), where cybercriminals use advanced phishing tactics to deceive victims. These scams have seen a significant surge across **Asia Pacific**, **North America**, the **Middle East**, and **Europe**, indicating a coordinated global effort to exploit users.

Both campaigns leverage the **Darcula Phishing Kit**, a tool created by cybercriminals to enhance phishing attempts. The latest version, **Darcula-Suite,** allows easy frontend customization, making phishing sites more convincing and deployable within **10 minutes.**

The **Darcula phishing-as-a-service platform** enables large-scale attacks using technologies like **JavaScript, React, Docker, and Harbor**, delivering scam messages via **iMessage, RCS, and traditional SMS** to bypass firewalls blocking suspicious texts.

SCAM STAGES:

CTM360 Scam Navigator

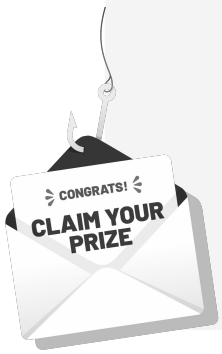


PointyPhish & TollShark scam stages

CTM360 Observations

REWARDS POINTS SCAM (POINTYPHISH)

A Rewards Points Scam campaign dubbed by CTM360 as 'PointyPhish' is targeting victims through fraudulent SMS messages, urging them to click on phishing links to claim rewards or redeem points. The scammers are focusing on Banking, Airlines and other Retail businesses that offer Rewards programs to their customers. The scammers objective is to gain the Credit/Debit card details including the Expiry date & CVV.



Key data:

- CTM360's research team, using their WebHunt platform has identified and discovered over **3,000+ domains and phishing sites targeting entities globally.**
- Scammers have utilized typo-squatted domains, registered on abused TLDs such as .top, .xin, .vip, .cc, and .ink.

TOLL SCAM (TOLLSHARK)

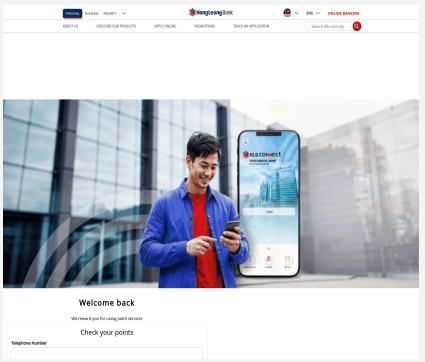
Toll scams dubbed by CTM360 as 'TollShark' are targeting users through fraudulent SMS messages that pose as unpaid toll payments. Scammers send consumers threatening texts pressuring them to click on fraudulent websites. These fraudulent messages create a sense of urgency to deceive recipients into disclosing their personal data and Credit/Debit card information on those phishing websites. Primary targets here are toll companies worldwide, exploiting their brand name to deceive customers.

Key data:

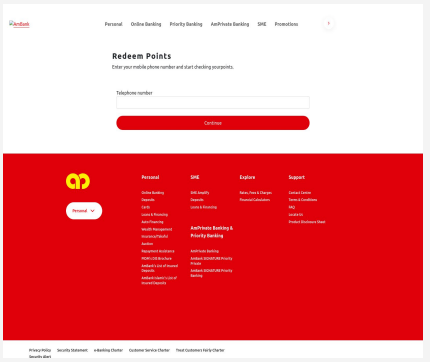
- CTM360's Webhunt platform has detected and tracked over **2000+ domains and phishing sites targeting entities globally.**
- Scammer often exploit typo-squatted domains registered under commonly misused top-level domains (TLDs), including .xyz, .top, .xin, .vip, .live, .sbs, and .world.
- Toll scams primarily target the transportation and infrastructure sectors, specifically exploiting electronic toll collection systems and related payment services.

REWARDS POINTS SCAM (POINTYPHISH)

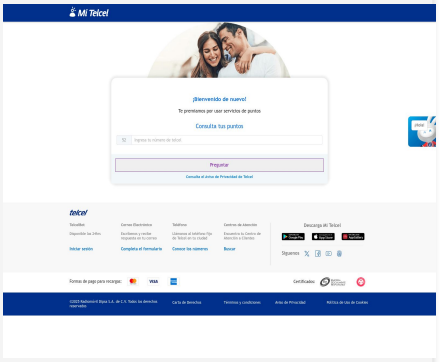
Rewards Brand in Hong Kong



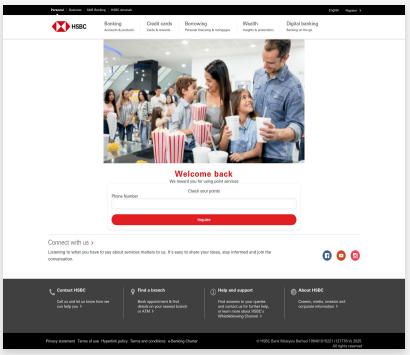
Bank in Malaysia



Bank in Malaysia

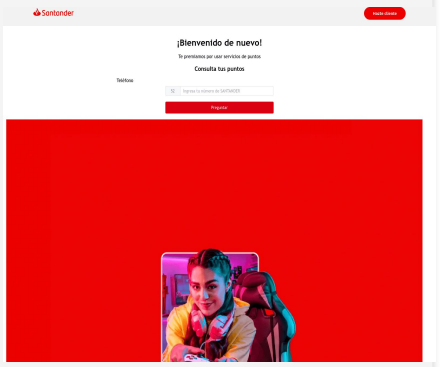


Telecom provider in Mexico

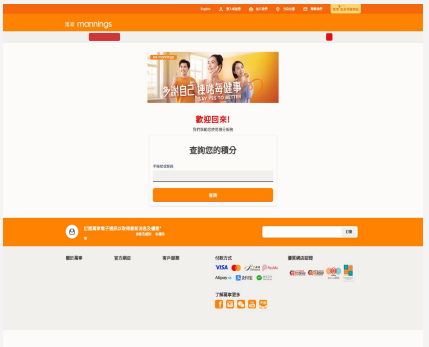


Bank in UK

Bank in India



Bank in Spain



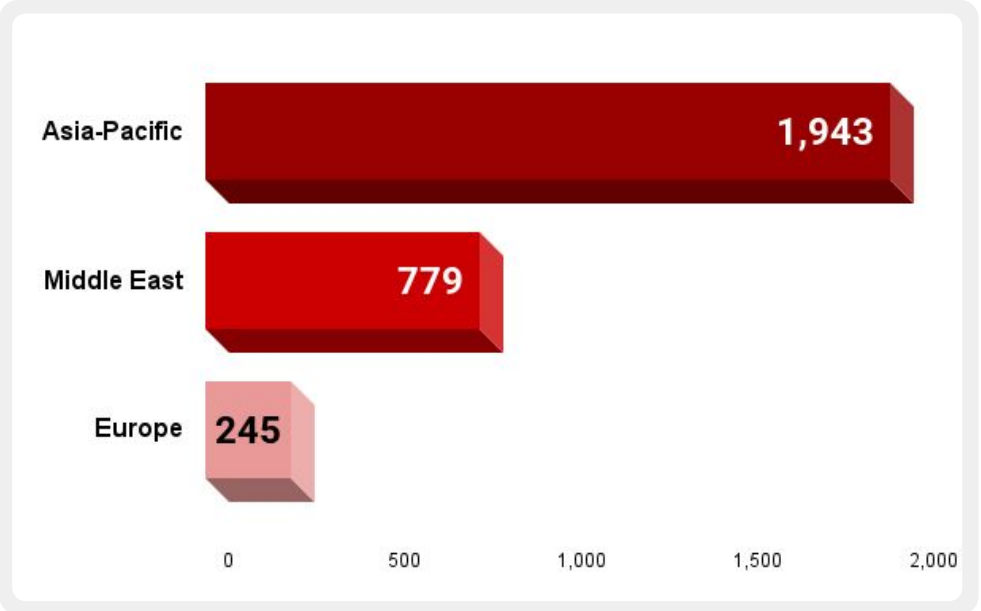
Personal Care Brand in China

Plus more brands across 10+ countries

TARGETED REGIONS DISTRIBUTION

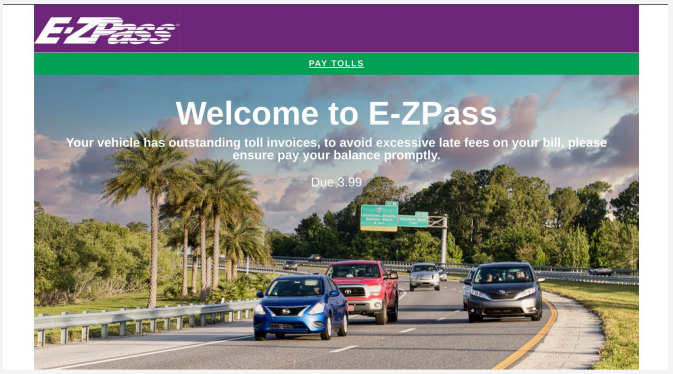
*The graphs below illustrate the number of detected incidents for **Rewards scams** across different regions, highlighting the geographic distribution and scale of these scam campaigns.*

Rewards Scam (PointyPhish)

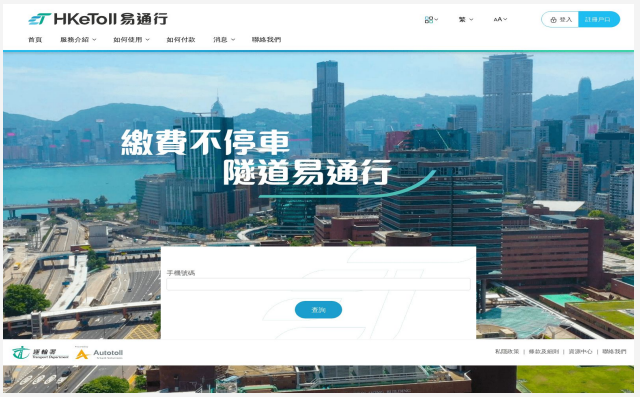


Rewards Scam incidents across different regions

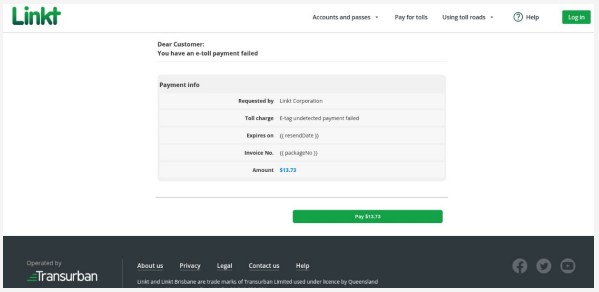
TOLL SCAM (TOLLSHARK)



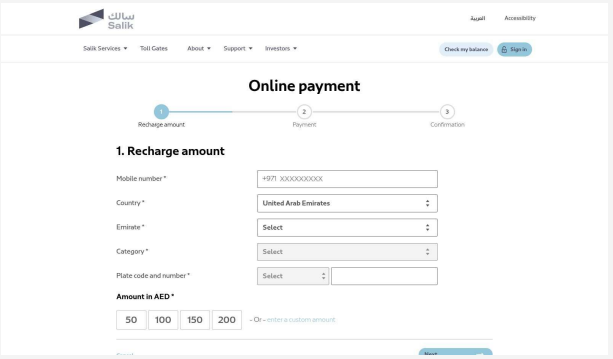
Toll Services in United States Of America



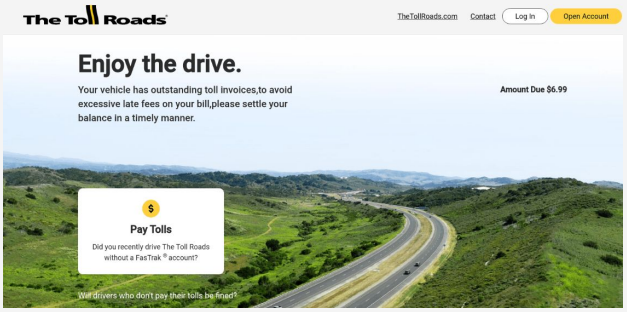
Toll Services in China



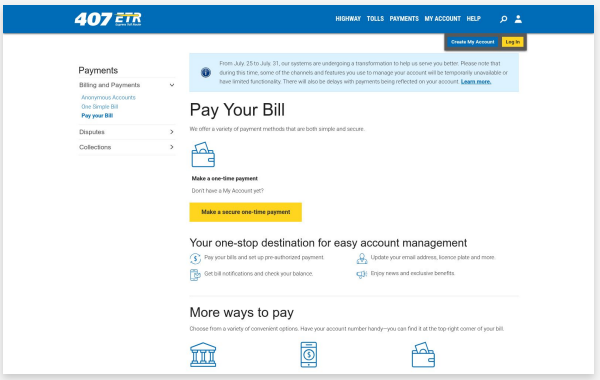
Toll Services in Australia



Toll Services in United Arab Emirates



Toll Services in United states of America

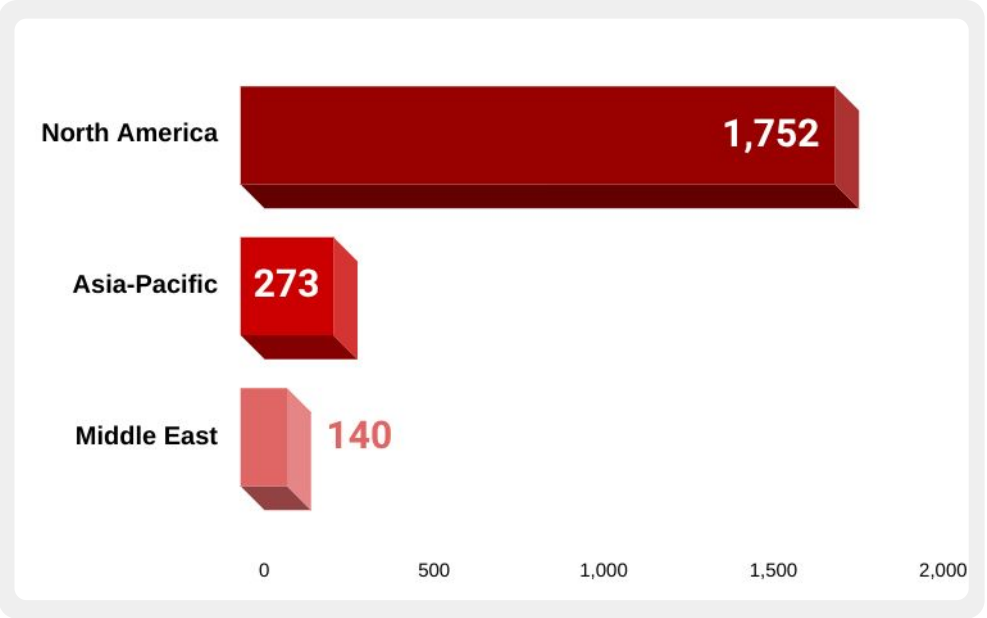


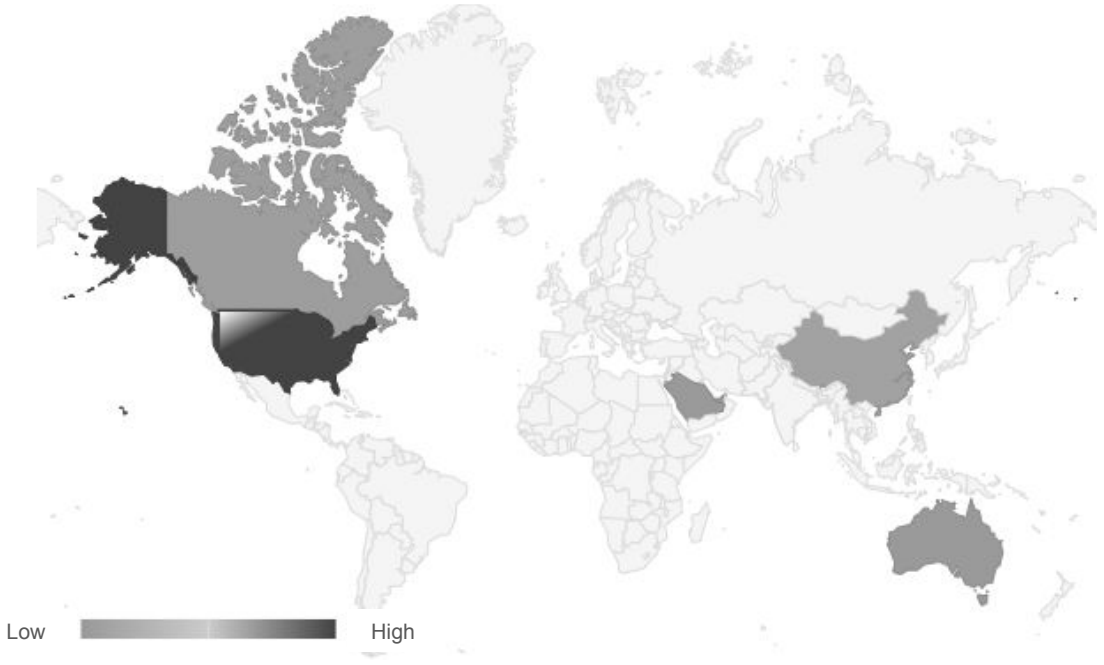
Toll Services in Canada

TARGETED REGIONS DISTRIBUTION

*The graphs below illustrate the number of detected incidents for **Toll scams** across different regions, highlighting the geographic distribution and scale of these scam campaigns.*

Toll Scam (TollShark)



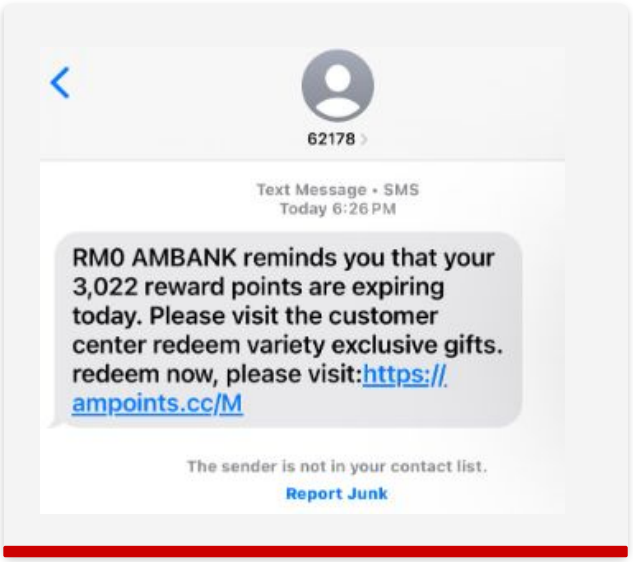


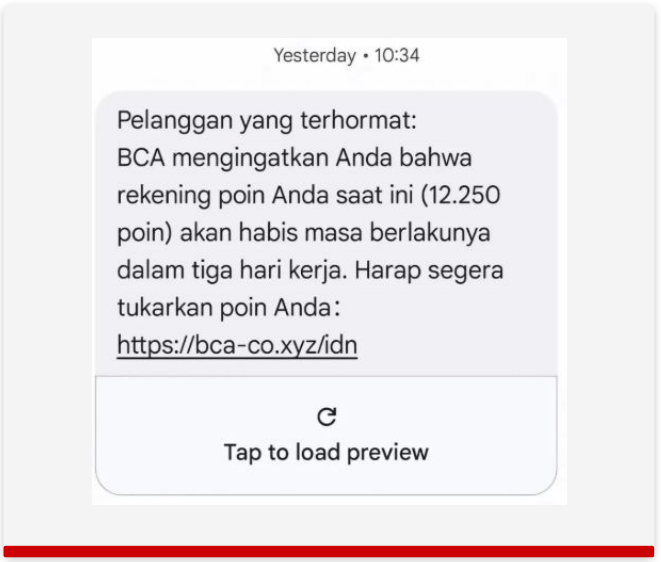
Toll Scam incidents across different regions

CTM360 OBSERVATIONS

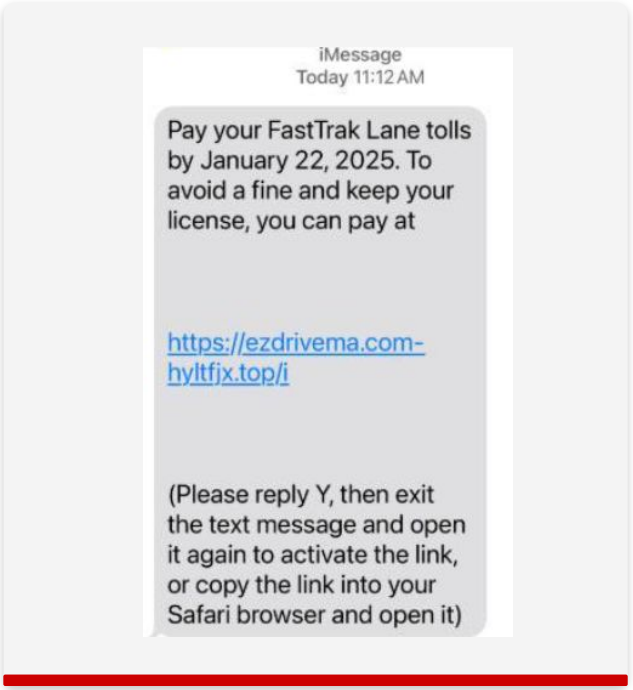
Step 1: Distribution via SMS – Fake Toll Bills & Reward Expiry Scams

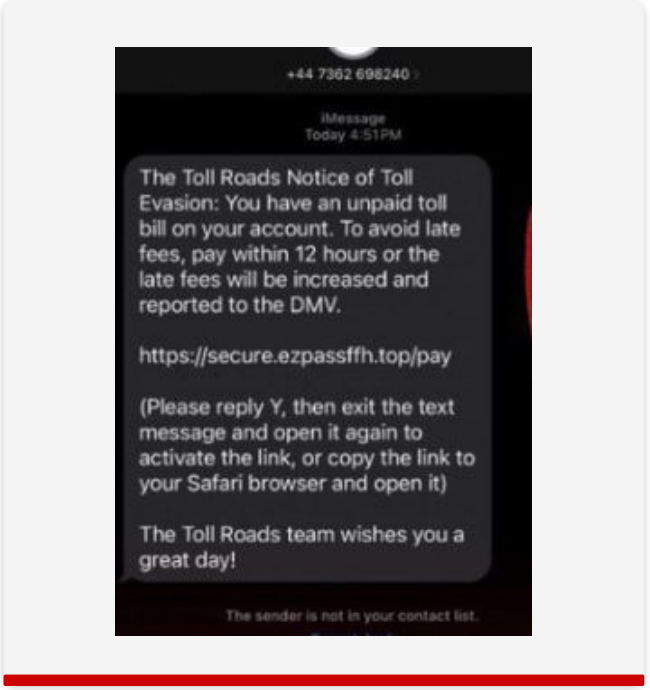
Both scams begin with attackers sending SMS messages that create a sense of urgency. Some messages claim the recipient has an unpaid toll bill that needs immediate payment, while others warn that their reward points are about to expire. In both campaign, victims are urged to click a link, leading them to a fraudulent website designed to steal their personal and financial information.





Rewards Points Scam (PointyPhish)



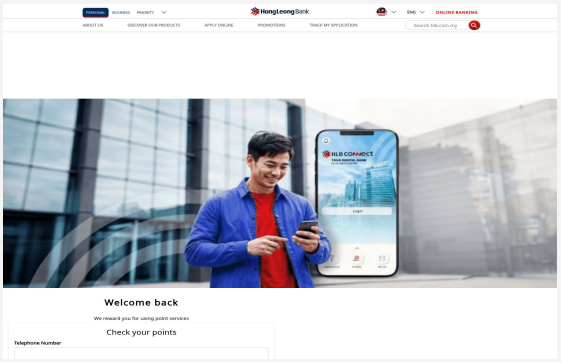


Toll Scam (TollShark)

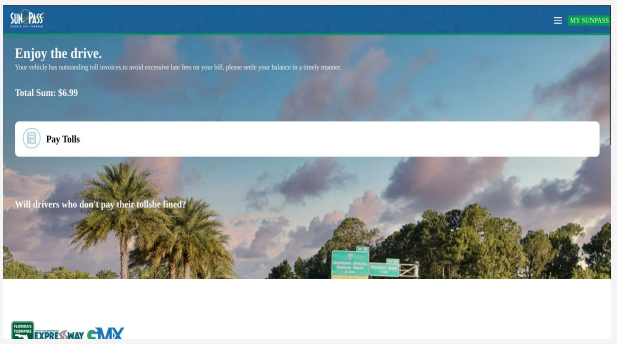
CTM360 OBSERVATIONS

Step 2: Deception via Fake Website

Clicking the link leads to a fake website mimicking top brands to deceive victims into trusting it as authentic.



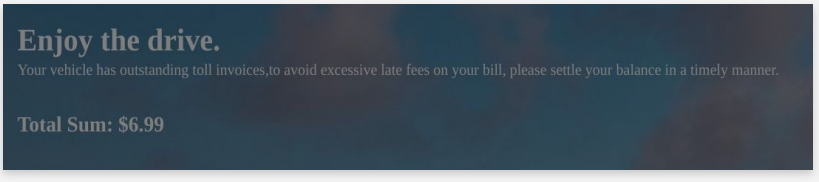
Rewards Points Scam (PointyPhish)



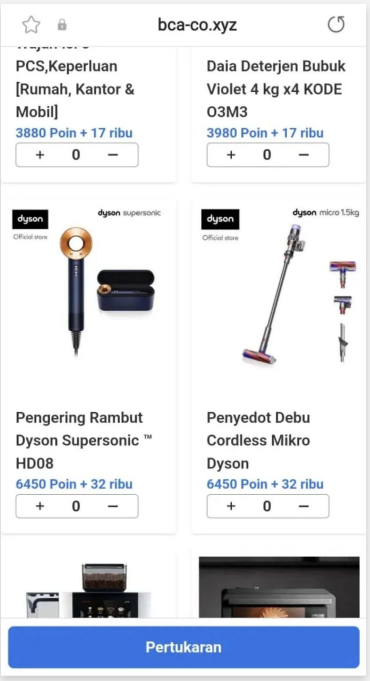
Toll Scam (TollShark)

Step 3: Fake Toll Bill Payment & Reward Redemption

Upon opening the fake website, victims are presented with an urgent message instructing them to settle their outstanding toll bill immediately to avoid additional charges. This sense of urgency pressures them into making a quick payment through a provided online link. Simultaneously, the website may also display items that victims can supposedly purchase using their reward points. Believing they are redeeming genuine rewards, victims add items to their cart and proceed to checkout—unknowingly falling for the scam.



Toll Scam (TollShark)

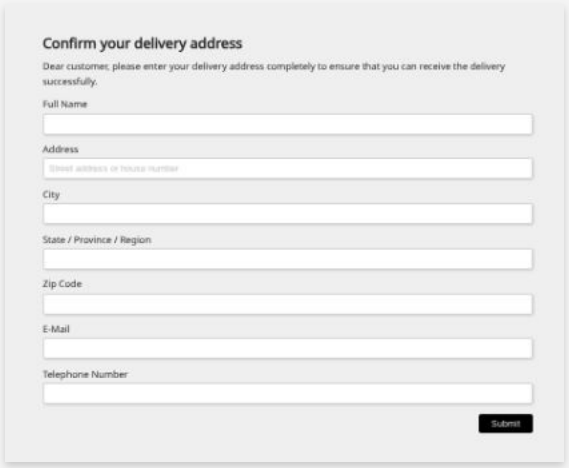


Rewards Points Scam (PointyPhish)

CTM360 OBSERVATIONS

Step 4: PII Harvesting

After selecting fake rewards or attempting to pay the supposed toll bill, victims are prompted to provide personal information under the pretense of claiming their prize, verifying their identity or completing the payment. The fraudulent form requests details such as full name, date of birth, phone number and home address, tricking victims into submitting their personal data.

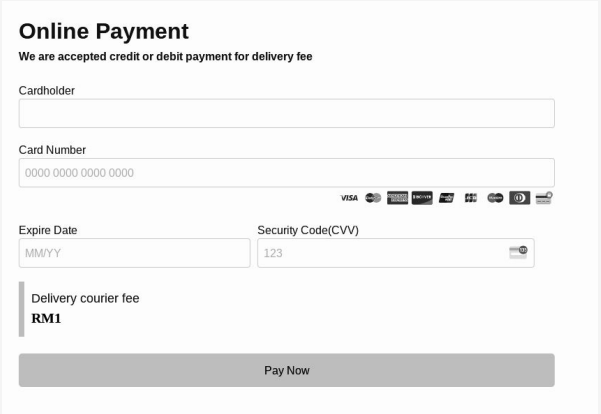


Rewards Points Scam (PointyPhish)

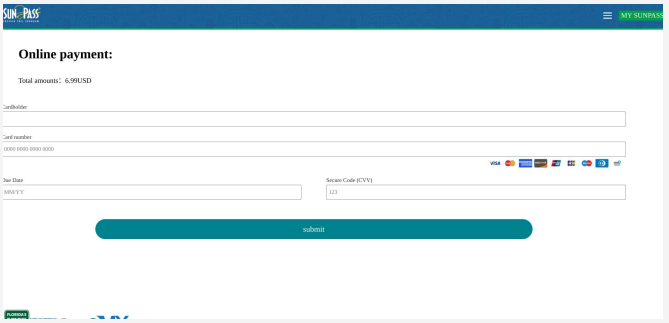
Toll Scam (TollShark)

Step 5: Credit/Debit Card Harvesting

At checkout, victims are prompted to provide sensitive financial information. The payment form requests details such as the name on the card, card number, expiration date and CVV.



Rewards Points Scam (PointyPhish)



Toll Scam (TollShark)

A DEEPER LOOK INTO DARCULA PHISHING ENVIRONMENT

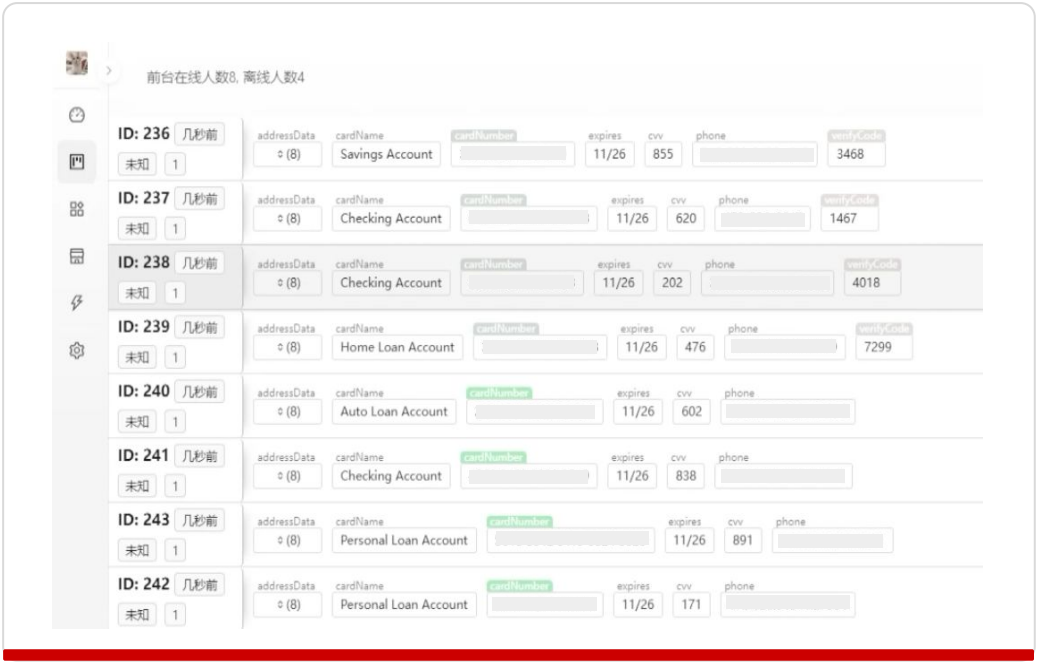
(Darcula Admin Panel)

During the investigation, we discovered an exposed directory that revealed Darcula PhaaS admin console, with direct access to key components of the phishing environment. The panel serves as the control center for attackers to manage phishing campaigns, track stolen data, and configure SMS-based phishing attacks.

Findings from the Admin Console:

- **Threat Actor Accounts & Credentials:** Multiple attacker accounts were found in the system with associated hashed passwords.
- **Phishing Campaign Management:**
  - Manage active phishing domains and deploy attack templates/kits.
  - Track victim interactions and submission logs in real-time.
  - Configure SMS-based phishing attacks, targeting specific regions.
- **Subscription Model & Access Controls:**
  - Some accounts required active keys, suggesting a licensing system.
  - Download counters indicated phishing kits were shared among threat actor.
- **Timestamps & Operational Activity:**
  - Admin logs showed continuous registration of new attacker accounts.
  - Campaigns were actively managed and regularly updated.

This exposed admin panel provided a **direct insight into how Darcula PhaaS operates**, revealing attacker coordination, credential storage, and phishing kit distribution.



A screenshot from the Darcula console

Darcula Capabilities & Functionalities (1)

Threat Actor Accounts & Credentials

Through an open directory, we found account management information containing threat actors credentials, including usernames, hashed passwords, and account creation timestamps. Some accounts had active keys, indicating a subscription-based access model.

The logs showed continuous new registrations, confirming an active and expanding user base. Download counters suggested phishing kits were being shared among users, reinforcing the organized structure of Darcula PhaaS.

Phishing Templates Deployment

Another open directory exposed a list of targeted organizations along with their corresponding phishing kit codes and versions. This suggests that the kits are continuously updated, refined, and distributed among Darcula PhaaS subscribers to evade detection.

The structured format and versioning indicate that Darcula PhaaS operates systematically, ensuring that phishing templates remain relevant, adaptable, and widely available to attackers.

Darcula Capabilities & Functionalities (2)

Phishing Site Configuration Analysis

The configuration file shown in the below screenshot reveals how Darcula PhaaS customizes and manages phishing campaigns. Key findings include:

- **Geo-Targeting:** The phishing site restricts access to specific regions, ensuring only victims from targeted countries can interact with it.
  - \"MY\",\"SG\" → For Malaysia and Singapore IP addresses.
- **Device Restrictions:** The site blocks desktop access, forcing victims to use mobile devices, which created a defensive layer and more likely to have banking apps.
  - "disableCheckPC", "disableCheckIOS", "disableCheckAN"
- **Directory Gated:** The configuration allow customizing the required directory that display the phishing kit.
  - "Entrypoint": "limit" → Domain gated with /limit directory
- **Versioning & Tracking:** The presence of version numbers and internal tracking codes suggests the kit is regularly updated and distributed among users.
  - "Version": "4"
- **Verification & MFA Bypass:** Display a fake two-step verification prompt asking for payment password (PIN) or OTP to mimics security features.
  - "verify-page"

These configurations highlight a well-structured and evolving phishing operation, designed to evade detection, steal sensitive data, and maximize success rates.


```
  {
    "language": "en",
    "domain": "[\"\\t hctrads.homes\",\"hctraas.lol\",\"hctrads.click\",\"hctrasda.my\"]",
    "entrypoint": "limit",
    "allowIp": "[\"MY\",\"SG\"]",
    "disableCheckIp": "0",
    "pay-description": "",
    "pay-price": "",
    "verify-page": "[{\"page-title\":\"支付密码\",\"page-text\":\"For added security, enter your payment password (PIN) for two-step
    verification.\",\"input-1\":\"Please enter your pin\",\"button\":\"Submit\",\"deny-msg\":\"Wrong Password\"},null,null,null,null]"
    "card-error-msg": "",
    "card-deny-msg1": "",
    "card-deny-msg2": "",
    "disableCheckPC": "1",
    "disableCheckIOS": "0",
    "disableCheckAN": "0",
    "digital-code": "1",
    "indexVerify": "0",
    "indexVerifyMessage": "",
    "title": "www.hctra.org",
    "description": "hctraETC",
    "icon": "",
    "version": "4",
    "code": "hctra182"
  }
]
```


Configuration page to customize phishing kits

Darcula Capabilities & Functionalities (3)

The data collection system used to capture and store victim payment data, revealing how Darcula PhaaS collects and organizes stolen information.

Key findings include:

- **Victim Information Logging:** The system records IP addresses, device details, and user agents, allowing attackers to track user activity and adjust phishing tactics.
- **Stolen Personal & Payment Data:** The collected data includes names, addresses, phone numbers, and full credit card details (number, expiration date, CVV), enabling fraud and unauthorized transactions.
- **Session Tracking:** A unique visitor ID is assigned to each victim, helping attackers monitor interactions and prevent duplicate entries.
- **Live Data Updates:** The timestamps indicate real-time logging, meaning credentials are collected and processed instantly as victims submit their details.

```
{
  "id": 416,
  "num": 416,
  "domain": "https://hectedhdf.lol",
  "ip": "121.123.96.9, 162.158.192.167",
  "ua": "{\"ua\":\"Mozilla\\/5.0 (Linux; Android 11; SAMSUNG SM-G973U) AppleWebKit\\/537.36 (KHTML, like Gecko) SamsungBrowser\\/14.2 Chrome\\/87.0.4280.141
  Mobile Safari\\/537.36\",\"lang\":\"en-US,en;q=0.5\",\"device\":\"android\"}",
  "visitor_id": "2e3c85a0034760b26c31004b4f106f82a92b31d8084500b5a3b9863033ade32a",
  "theme": "hctra",
  "page": "在填卡页",
  "card_type": "",
  "bank_type": "",
  "data": "{\"\\u5728\\u9996\\u9875\":{\"phone\":\"111111111\"},\"show\":{\"phone\":\"111111111\"},\"\\u5728\\u5730\\u5740\\u9875\":{\"first_name\":\"111\",\"ad
  dress\":\"111\",\"city\":\"111\",\"detailed_address\":\"111\",\"state\":\"111\",\"zip\":\"111111\",\"phon
  e\":\"111111111\"},\"\\u5728\\u586b\\u5361\\u9875\":{\"ccnum\":\"1111 1111 1111
  1111\",\"ccname\":\"111\",\"date\":\"01\\/29\",\"cccvv\":\"111\"},\"bin_highlight\":\"\"}",
  "status": 0,
  "hide": 0,
  "admin_id": 0,
  "created_at": "2025-03-20 08:37:04",
  "updated_at": "2025-03-20 08:38:35",
  "bin_data": "[]"
},
{
```


Victims logs that store inputted details

This structure confirms that Darcula PhaaS is designed for efficient **credential theft**, ensuring that sensitive data is captured, stored, and ready for exploitation with minimal attacker effort.

ABOUT US

CTM360 provides a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and unlimited managed takedowns), security ratings, third party risk management, email intelligence (dmarc) and cyber threat intelligence.

CONTACT US:

+973 77 360 360

info@ctm360.com

www.ctm360.com

21st Floor, East Tower Bahrain Financial Harbour, Kingdom of Bahrain

CTM360®