uptycs

SECURITY RISK
SEVERE

USPS Phishing Campaign Delivery

THREAT INTELLIGENCE

The Uptycs Threat Intel Team has identified a phishing campaign impersonating the United States Postal Service (USPS). The attackers target the victims by unsolicited text messages or web links. This type of attack is commonly known as smishing.

Smishing is a form of phishing that uses mobile phones as the attack platform. Victims will generally receive a fraudulent text message designed to entice the recipient into disclosing personal or financial information.

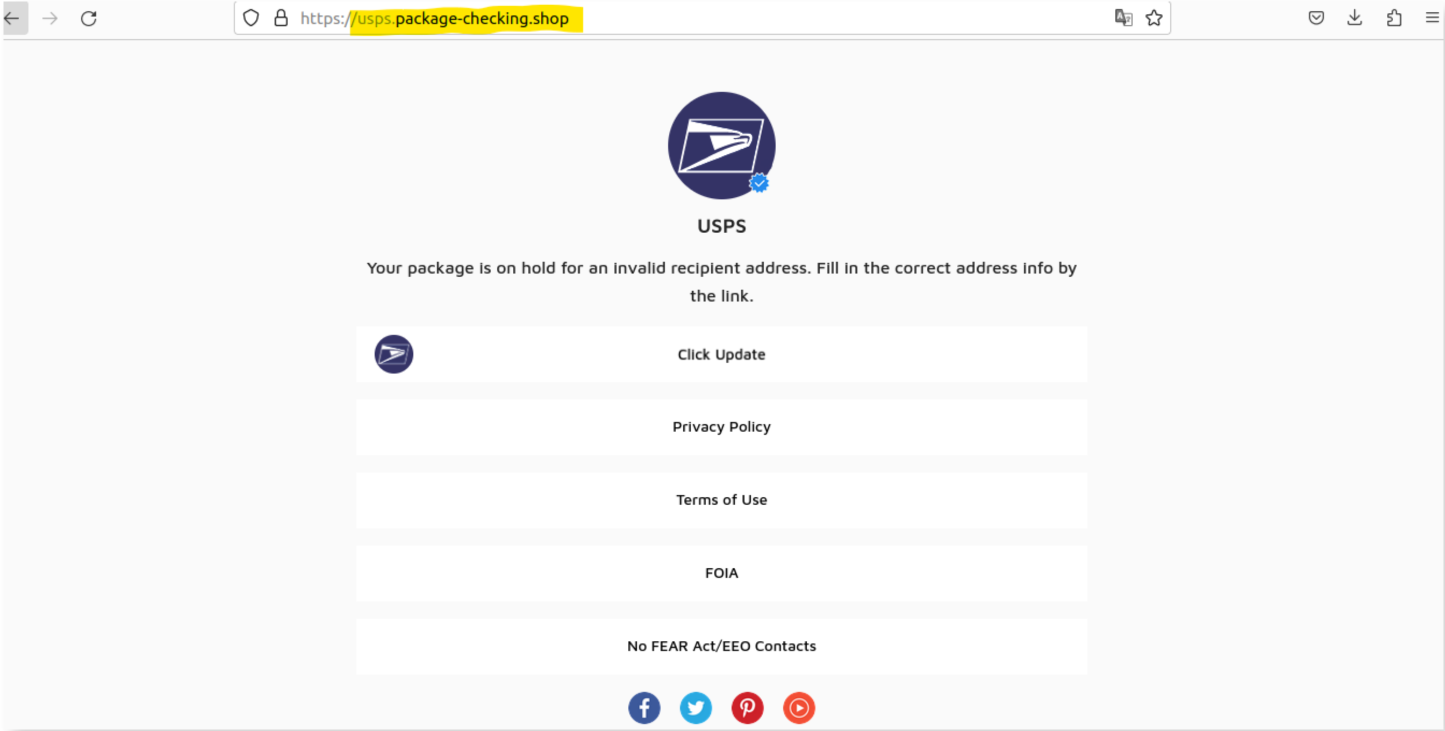
The criminal executes this type of attack with the intent to gather personal and financial information like credit card numbers.

Threat Intel Activity

In the reported smishing activity it was noted that the attackers reached out to the victims by initiating a text message stating that a USPS delivery requires a response from them.

On doing more research, Uptycs Threat Intel Team has discovered more than 1k live phishing websites associated with this campaign activity.

Analysis of one of the live websites masquerading as a USPS website in the phishing domain is outlined below.



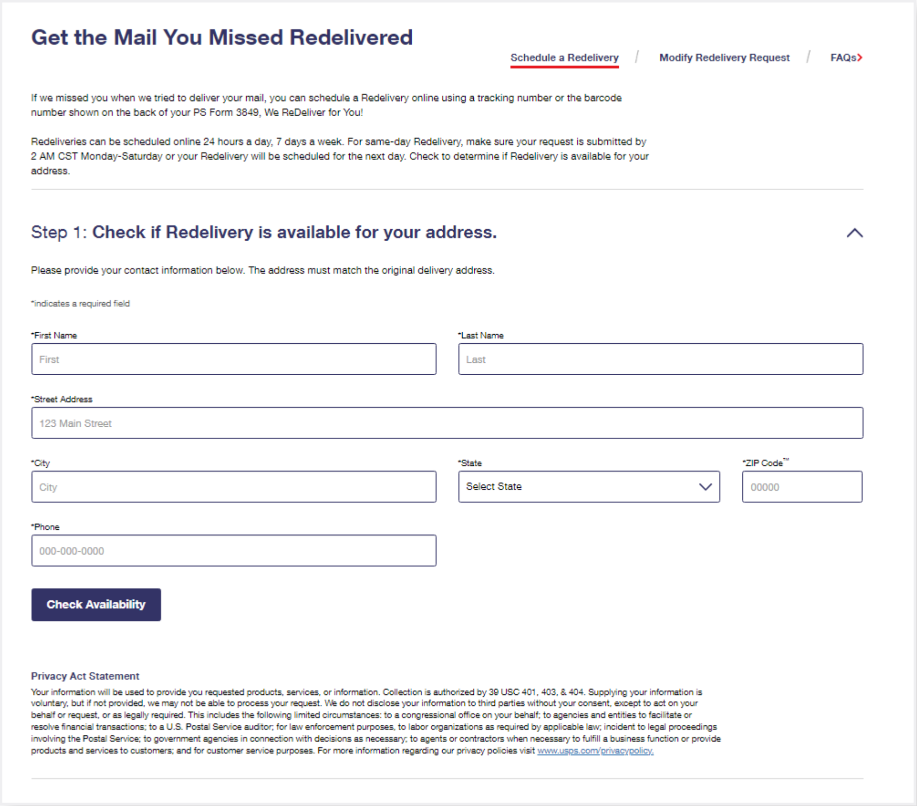
https://usps.package-checking.shop

USPS

Your package is on hold for an invalid recipient address. Fill in the correct address info by the link.

Figure 1: Fake USPS website link

SECURITY RISK
SEVERE



Get the Mail You Missed Redelivered

If we missed you when we tried to deliver your mail, you can schedule a Redelivery online using a tracking number or the barcode number shown on the back of your PS Form 3849, We ReDeliver for You!

Redeliveries can be scheduled online 24 hours a day, 7 days a week. For same-day Redelivery, make sure your request is submitted by 2 AM CST Monday-Saturday or your Redelivery will be scheduled for the next day. Check to determine if Redelivery is available for your address.

Step 1: Check if Redelivery is available for your address.

Please provide your contact information below. The address must match the original delivery address.

*indicates a required field

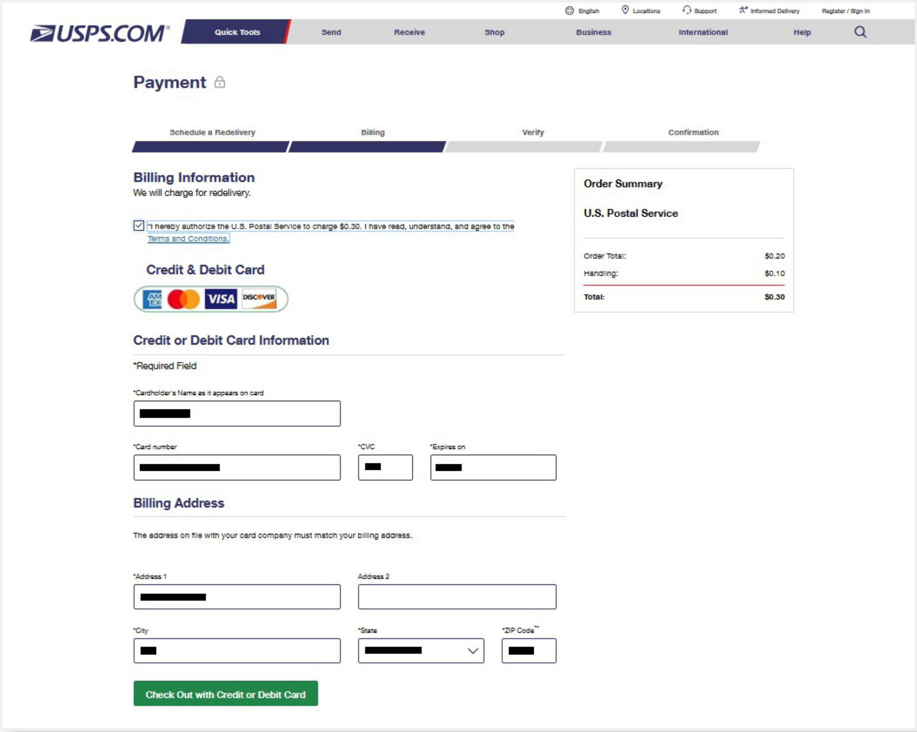
*First Name: First
*Last Name: Last
*Street Address: 123 Main Street
*City: City
*State: Select State
*ZIP Code™: 00000
*Phone: 000-000-0000

Privacy Act Statement

Your information will be used to provide you requested products, services, or information. Collection is authorized by 39 USC 401, 403, & 404. Supplying your information is voluntary, but if not provided, we may not be able to process your request. We do not disclose your information to third parties without your consent, except to act on your behalf or request, or as legally required. This includes the following limited circumstances: to a congressional office on your behalf; to agencies and entities to facilitate or resolve financial transactions; to a U.S. Postal Service auditor; for law enforcement purposes, to labor organizations as required by applicable law; incident to legal proceedings involving the Postal Service; to government agencies in connection with decisions as necessary; to agents or contractors when necessary to fulfill a business function or provide products and services to customers; and for customer service purposes. For more information regarding our privacy policies visit www.usps.com/privacypolicy.

Figure 2: Update page for personal details

Upon clicking on **Click Update**, it asks for personal details like name, address, phone number, etc.



Payment

Billing Information
We will charge for redelivery.

☑ *I hereby authorize the U.S. Postal Service to charge $0.30. I have read, understand, and agree to the Terms and Conditions.

Credit & Debit Card

Order Summary

U.S. Postal Service

Order Total:	$0.20
Handling:	$0.10
Total:	$0.30

Credit or Debit Card Information

*Required Field

*Cardholder's Name as it appears on card: [redacted]

*Card number: [redacted]
*CVC: [redacted]
*Expires on: [redacted]

Billing Address

The address on file with your card company must match your billing address.

*Address 1: [redacted]
Address 2:
*City: [redacted]
*State: [redacted]
*ZIP Code™: [redacted]

Figure 3: Payment details page

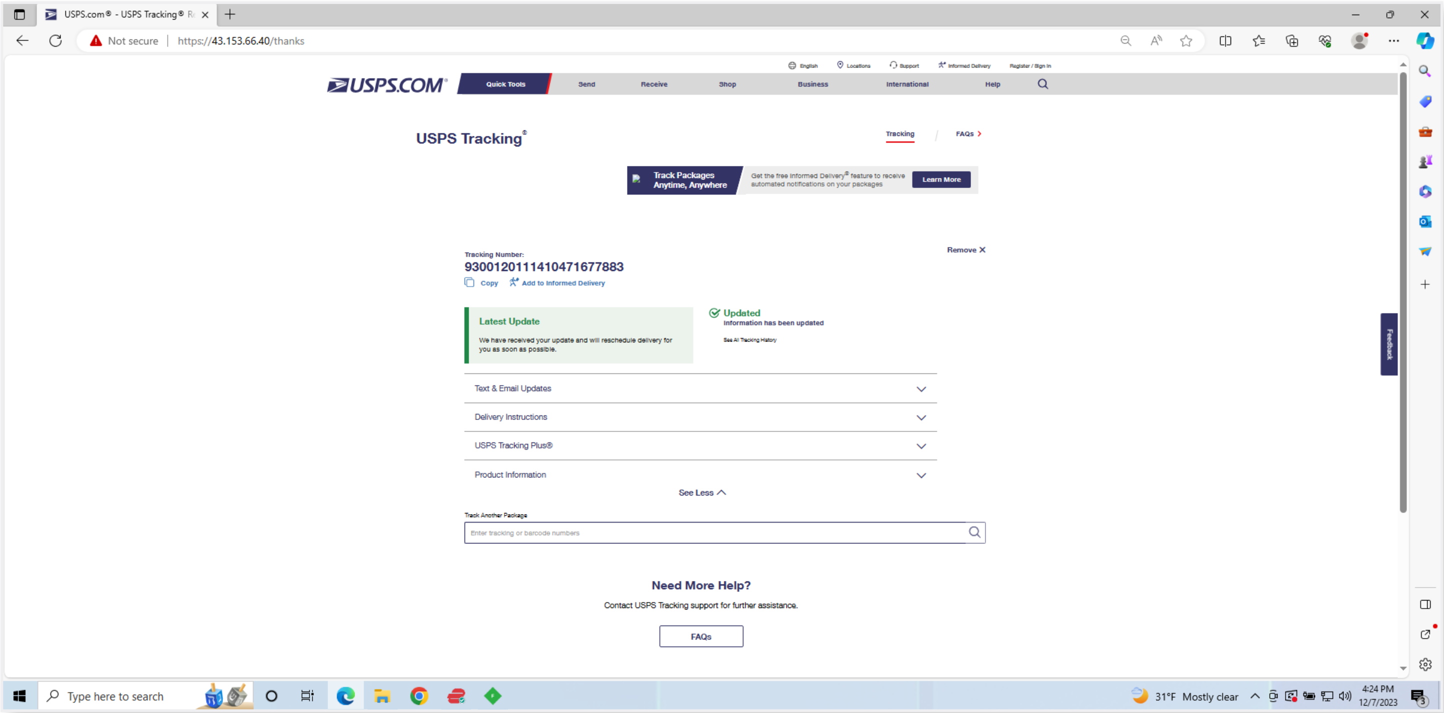
Upon entering all details and clicking on **Check Availability**, it goes to the payment details page as shown in Figure 3.

Here, it asks for billing information and **credit card** details like card number, CVV, and expiry date.

SECURITY RISK SEVERE

On providing all required details, it asks the victim to press the **Check Out** with **Credit** or **Debit Card**.

It next moves to the tracking page, stating that Information has been updated along with the tracking number.



USPS Tracking®

Get the free Informed Delivery® feature to receive automated notifications on your packages

Tracking Number:
9300120111410471677883

Copy Add to Informed Delivery Remove ✕

Latest Update

We have received your update and will reschedule delivery for you as soon as possible.

Updated
Information has been updated

See All Tracking History

Text & Email Updates

Delivery Instructions

USPS Tracking Plus®

Product Information

See Less

Track Another Package

Enter tracking or barcode numbers

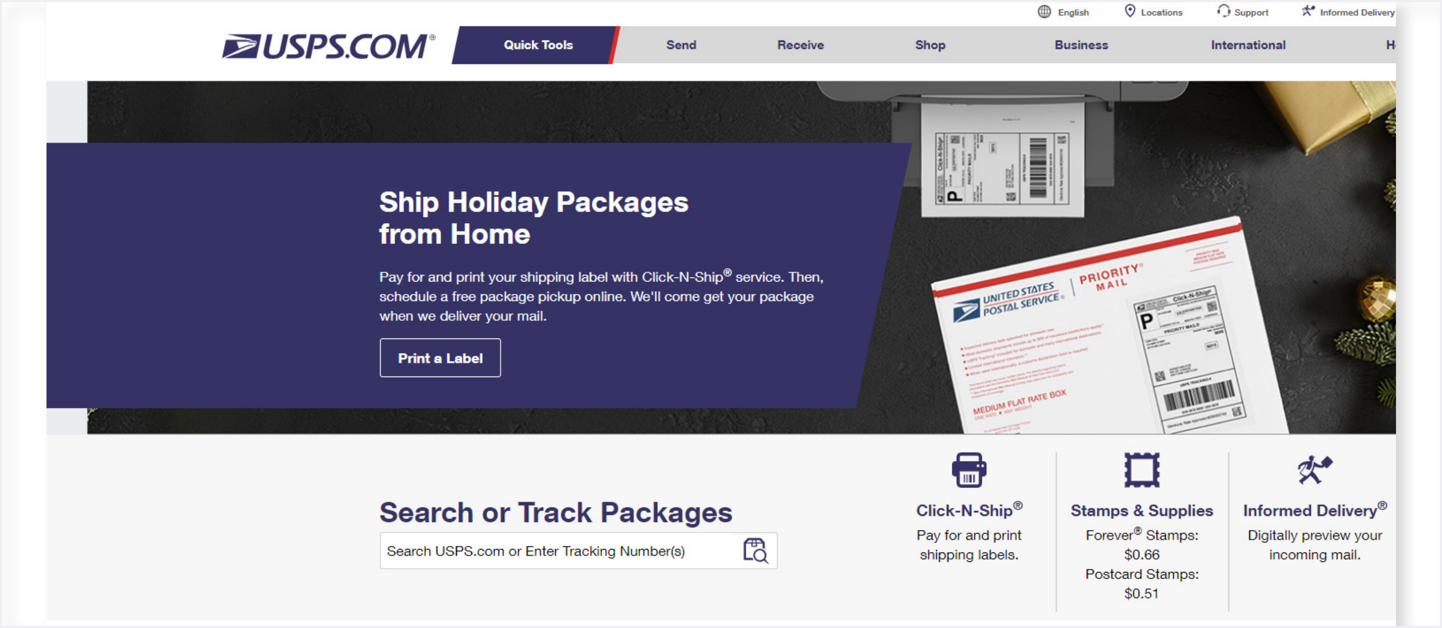
Need More Help?

Contact USPS Tracking support for further assistance.

FAQs

Figure 4: Tracking updated page

Later, the tracking page redirects quickly and goes to the legitimate website of USPS.



Ship Holiday Packages from Home

Pay for and print your shipping label with Click-N-Ship® service. Then, schedule a free package pickup online. We'll come get your package when we deliver your mail.

Search or Track Packages

Search USPS.com or Enter Tracking Number(s)

Click-N-Ship®
Pay for and print shipping labels.

Stamps & Supplies
Forever® Stamps: $0.66
Postcard Stamps: $0.51

Informed Delivery®
Digitally preview your incoming mail.

Figure 5: USPS legitimate website

Redirecting to legitimate websites is the usual method most phishing campaigns use to trick the victims, to make it appear that it is a common inquiry check.

Upon analysis, Uptycs Threat Intel Team found that the threat actor successfully collected the desired personal and financial information in their database.

Ultimately, the collected information could be used in multiple ways to impact the victim by leaking the information or selling these details to other cyber attackers.

Additionally, all the live websites checked are titled **USPS - Linkfly**, as shown in Figure 6.

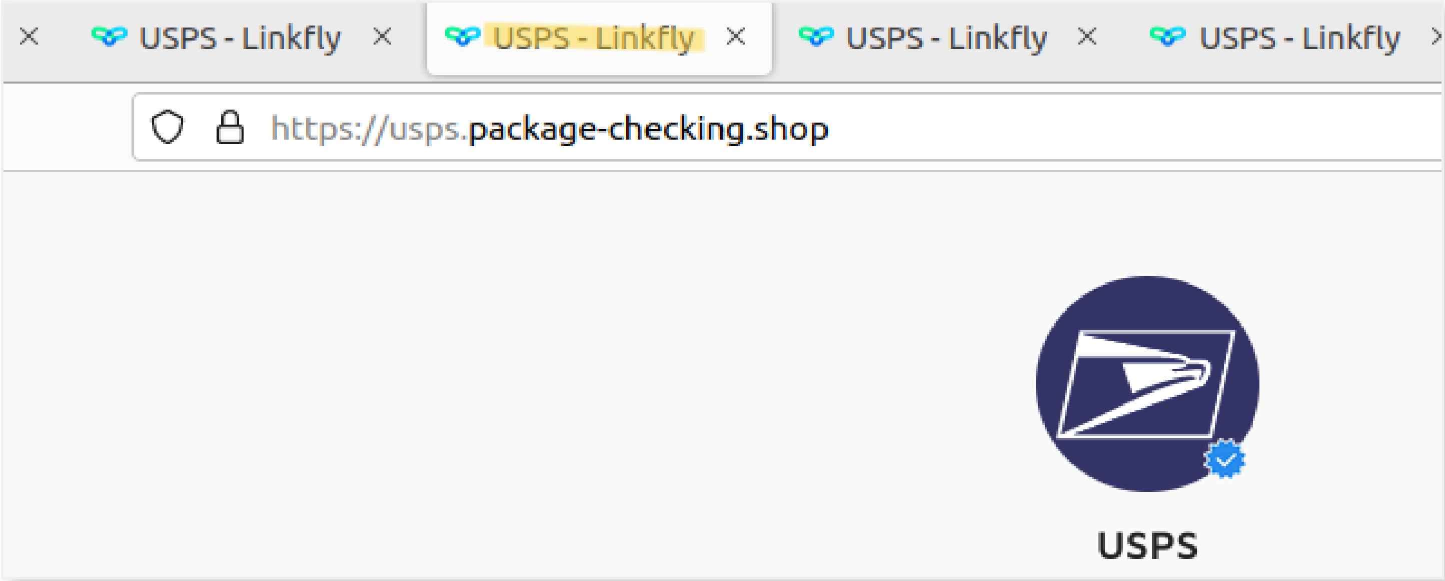


Figure 6: USPS - Linkfly title website

After in-depth analysis, Uptycs Threat Intel Team concluded that there is a high possibility this phishing campaign activity is being organized by **Chinese** threat actors.

Additionally, it’s been discovered that the campaign targets span worldwide.

Most of the observed servers/domains were hosted in the United States, and other countries like Canada, Germany, China, Singapore, and Russia.

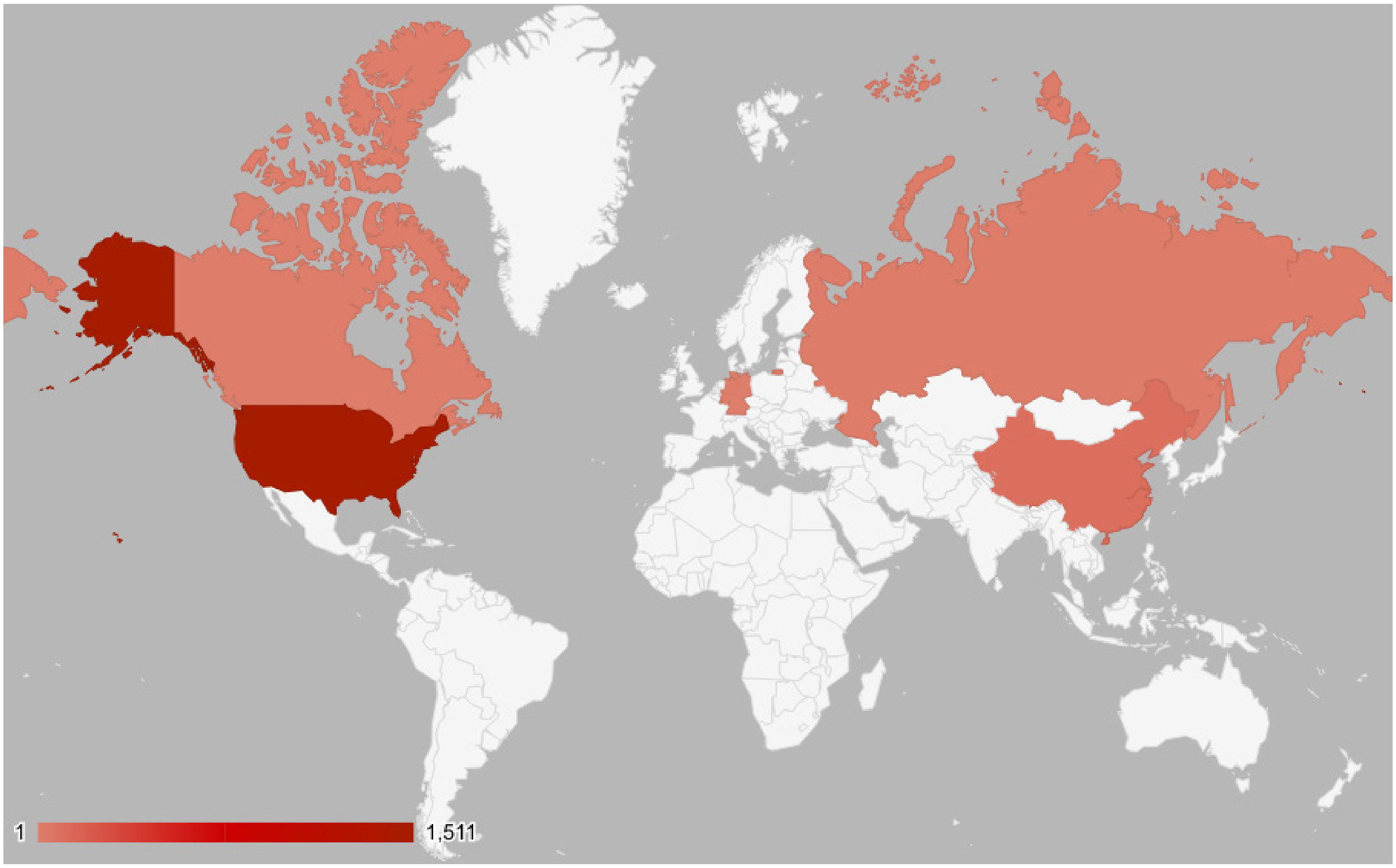
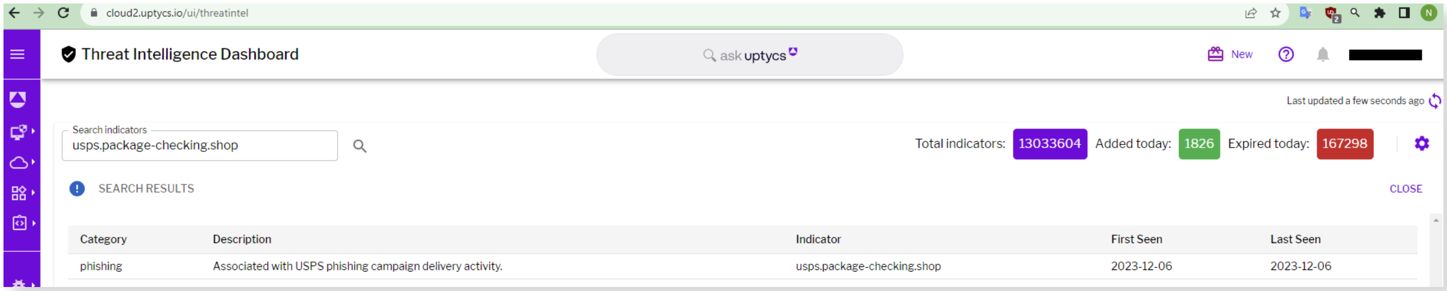


Figure 7: Server/domain host countries

In response to this threat, Uptycs has **blocked** all the 1050+ indicators that were found while investigating this phishing campaign.



Threat Intelligence Dashboard [redacted]

Last updated a few seconds ago

Search indicators: usps.package-checking.shop

Total indicators: 13033604 Added today: 1826 Expired today: 167298

SEARCH RESULTS CLOSE

Category	Description	Indicator	First Seen	Last Seen
phishing	Associated with USPS phishing campaign delivery activity.	usps.package-checking.shop	2023-12-06	2023-12-06

Figure 8: Presence of indicator in database

Recommendations

- Avoid clicking on links, phone numbers, or attachments in suspicious text messages.
- Contact the concerned entity directly through their official website or published contact information.
- Be wary of messages that create a sense of urgency.
- Never provide sensitive information like passwords or account recovery codes via text.
- Use legitimate anti-malware software for protection against cyber-attacks.

About Uptycs

Uptycs helps drive DevSecOps excellence, bringing teams together to master threat operations, meet compliance mandates, and reduce risk across clouds, containers, and endpoints. Take back control of your security data, get the correlated insights you care about most, and take decisive action.

Shift up your cybersecurity with Uptycs. Learn how at: Uptycs.com

uptycs