

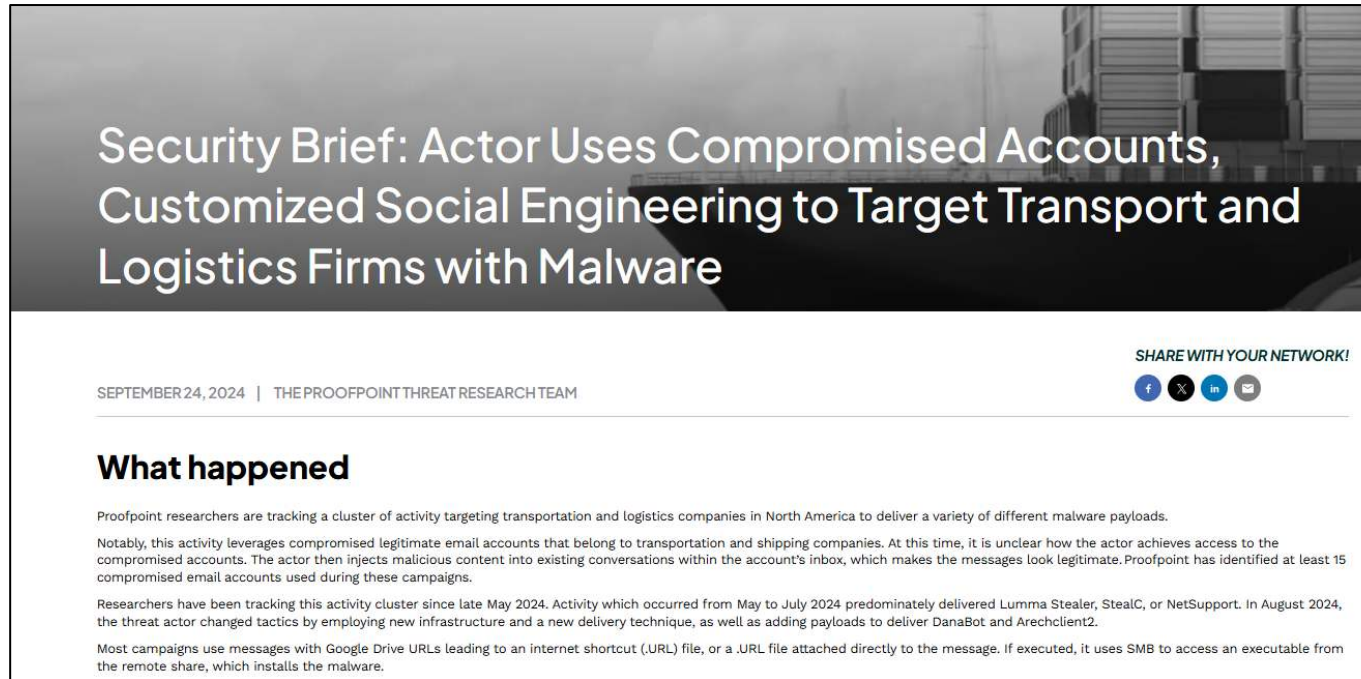
From Inbox to Freight Theft: How Cybercriminals Use RMMs, Malware, and Phishing to Steal Cargo Across North America and Europe



Ole Villadsen
Staff Threat Researcher
Proofpoint

Background: *How we came to track actors targeting transportation*

- **Fall 2024:** Identified unusual emails targeting Carriers with malware often using compromised emails and “thread hijacking”



Security Brief: Actor Uses Compromised Accounts, Customized Social Engineering to Target Transport and Logistics Firms with Malware

SEPTEMBER 24, 2024 | THE PROOFPOINT THREAT RESEARCH TEAM

SHARE WITH YOUR NETWORK!

What happened

Proofpoint researchers are tracking a cluster of activity targeting transportation and logistics companies in North America to deliver a variety of different malware payloads.

Notably, this activity leverages compromised legitimate email accounts that belong to transportation and shipping companies. At this time, it is unclear how the actor achieves access to the compromised accounts. The actor then injects malicious content into existing conversations within the account's inbox, which makes the messages look legitimate. Proofpoint has identified at least 15 compromised email accounts used during these campaigns.

Researchers have been tracking this activity cluster since late May 2024. Activity which occurred from May to July 2024 predominately delivered Lumma Stealer, StealC, or NetSupport. In August 2024, the threat actor changed tactics by employing new infrastructure and a new delivery technique, as well as adding payloads to deliver DanaBot and ArechClient2.

Most campaigns use messages with Google Drive URLs leading to an internet shortcut (.URL) file, or a .URL file attached directly to the message. If executed, it uses SMB to access an executable from the remote share, which installs the malware.

Background: *How we came to track actors targeting transportation*

- **Fall 2025:** Discovered an actor systematically targeting Carriers with Remote Monitoring and Management (RMM) tools.
 - Linked this activity to compromised Load Boards **and Cargo Theft.**



Remote access, real cargo: cybercriminals targeting trucking and logistics

NOVEMBER 03, 2025 | OLE VILLADSEN, SELENA LARSON, AND THE PROOFPOINT THREAT RESEARCH TEAM

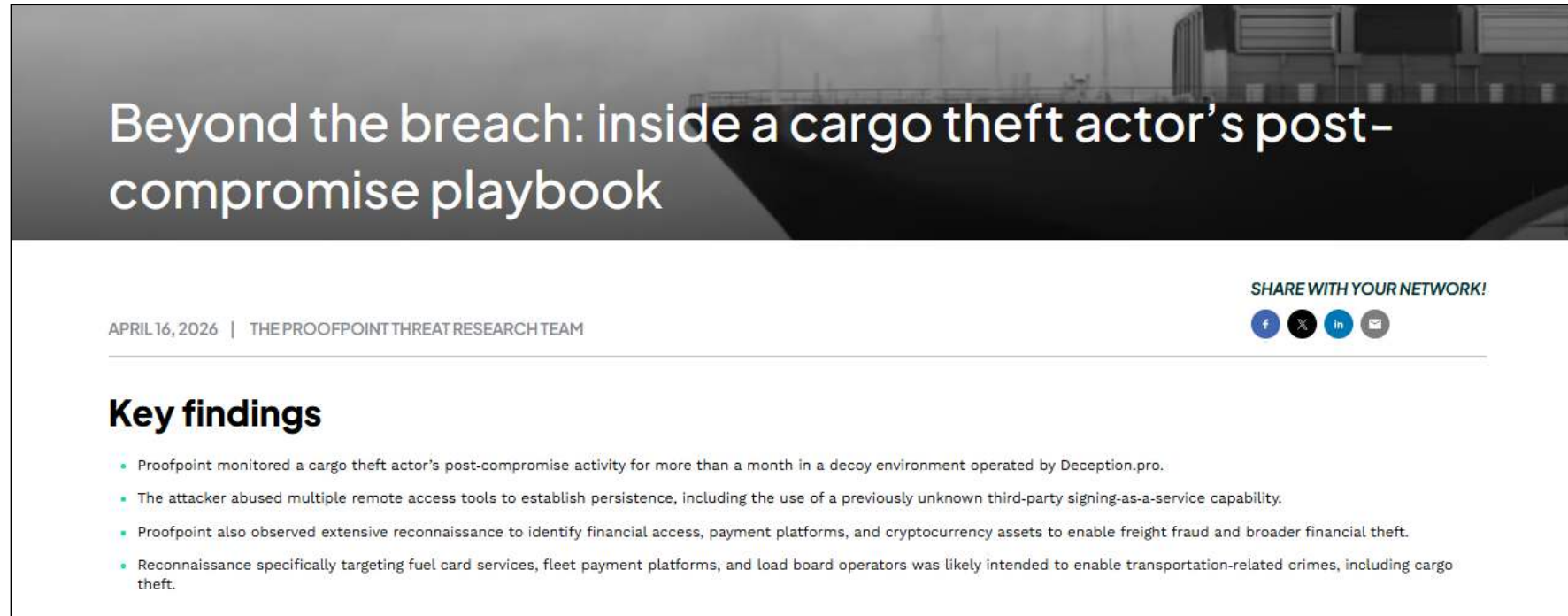
SHARE WITH YOUR NETWORK!

Key findings

- Cybercriminals are compromising trucking and freight companies in elaborate attack chains to steal cargo freight.
- Cargo theft is a multi-million-dollar criminal enterprise, and digital transformation has led to an increase in cyber-enabled theft.
- Threat actors compromise these companies and use their access to bid on cargo shipments, to then steal and sell them.
- The threat actors typically deliver remote monitoring and management (RMM) tools, aligning with the broader trend of cybercriminals adopting these as a first-stage payload across the threat landscape.

Background: *How we came to track actors targeting transportation*

- **Spring 2026:** Learned more about this actor's post-compromise activity



Beyond the breach: inside a cargo theft actor's post-compromise playbook

APRIL 16, 2026 | THE PROOFPPOINT THREAT RESEARCH TEAM

SHARE WITH YOUR NETWORK!

[f](#) [x](#) [in](#) [e](#)

Key findings

- Proofpoint monitored a cargo theft actor's post-compromise activity for more than a month in a decoy environment operated by Deception.pro.
- The attacker abused multiple remote access tools to establish persistence, including the use of a previously unknown third-party signing-as-a-service capability.
- Proofpoint also observed extensive reconnaissance to identify financial access, payment platforms, and cryptocurrency assets to enable freight fraud and broader financial theft.
- Reconnaissance specifically targeting fuel card services, fleet payment platforms, and load board operators was likely intended to enable transportation-related crimes, including cargo theft.

Background: *How we came to actors targeting transportation*

- **Present:** Have discovered and are tracking about 15 clusters targeting Carriers in North America and Europe delivering malware/RMMs and/or Credential Phishing lures

Key Findings

- Multiple distinct clusters (currently ~ 15) targeting Carriers with malware/RMMs and/or Credential Phishing
- Some clusters observed targeting the US *and* Europe
- Financially-motivated cyber-criminals performing Cargo theft as well as broader financial crimes
- Actors are well connected to the cybercriminal underground and know the transportation industry well

Delivery Methods

- Load Board Fraud
 - Responses from fraudulent load board postings
- Direct emails from actor -> recipient with malicious link.
 - Can come from actor-controlled or compromised accounts
 - Can be large, indiscriminate campaigns to small, highly targeted/tailored campaigns
- Benign conversation starter (imposter)
 - Potentially lead to malware, credential phishing, booking loads, or double brokering
 - Often seen with rate confirmation emails
- Thread Hijacking
 - Link inserted into a compromised email account pre-existing thread

Campaigns Delivering Malware/RMMs

Remote Management Tools (RMMs)

- Legitimate IT tools abused by actors
 - NetSupport*
 - ScreenConnect*
 - SimpleHelp
 - Fleetdeck
 - Datto
- Often used to quickly download additional payloads

Malware:

- Remote access trojans (RATs) and Information Stealers:
 - TryNodeRAT
 - AzaleaControl
 - StealC
 - CastleLoader
 - CastleRAT

TryNodeRAT (Load Board Fraud)

Auto: Load Info (was: DALLAS TO NASHVILLE)

 EASTERN EXPRESS INC <opentrailers@easternexpress.net>
To [REDACTED]

Good afternoon

Load Details:

-  Pickup: Today or Tomorrow
-  Pickup Hours: 8:00 AM – 7:00 PM
-  Delivery Hours: Monday – Friday, 8:00 AM – 9:00 PM
-  Weight: 30,000 lbs
-  Commodity: Cooker wire, NO TARP
-  Handling: No touch, Just strap and go
-  Rate: Posted

Please send your BEST RATE, ETA for pickup, and the payment option you prefer, we will get back to you.

You can also book this load directly through our portal:

 <https://packet-pro.com/>

If you need an onboarding invitation, please send a request to our team at: support@eastern-express.net

Best Regards

EASTERN EXPRESS INC
312 W 36TH AVE
GRIFFITH, IN 46519
MC# 148622
USDOT# 162408
Phone (219) 838-0000
FAX (219) 838-0011

Tue 8/25/2026 10:37 AM

Reply Reply All Forward

TryNodeRAT (Load Board Fraud)

Re: Load inquiry

 ONLINE FREIGHT SERVICES <loads@ofsbrokers.com>
To [REDACTED]

Hi there

Load Details:

-  Pickup: Today or Tomorrow
-  Pickup Hours: 8:00 AM – 7:00 PM
-  Delivery Hours: Monday – Friday, 8:00 AM – 9:00 PM
-  Weight: 30,000 lbs
-  Commodity: Rolled wire cables on pallets
-  Handling: No touch, No tarp, Just strap and go
-  Rate: Posted

Please send your **BEST RATE, ETA for pickup**, and the **payment option you prefer**, we will get back to you.

Best regards,
Debra Baker
ONLINE FREIGHT SERVICES
2275 WATERS DRIVE, MENDOTA HEIGHTS, MN 55120

Thu 9/3/2026 9:48 AM

  Reply  Reply All  Forward  

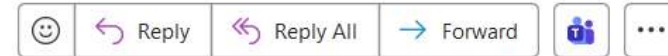
TryNodeRAT (Load Board Fraud)

[EXT] RE: [EXT] Re: Indianapolis to Detroit



ONLINE FREIGHT SERVICES <main@ofsbrokerageteam.com>

To



Thu 9/3/2026 11:16 AM

That works

Please take a moment to complete our onboarding through the portal using the link below.

<https://carrierpackready.com/>

We'll also need a few documents from you.

Once you've finished the packet, just let me know and I'll prepare the carrier confirmation for you.

Best regards,

Debra Baker

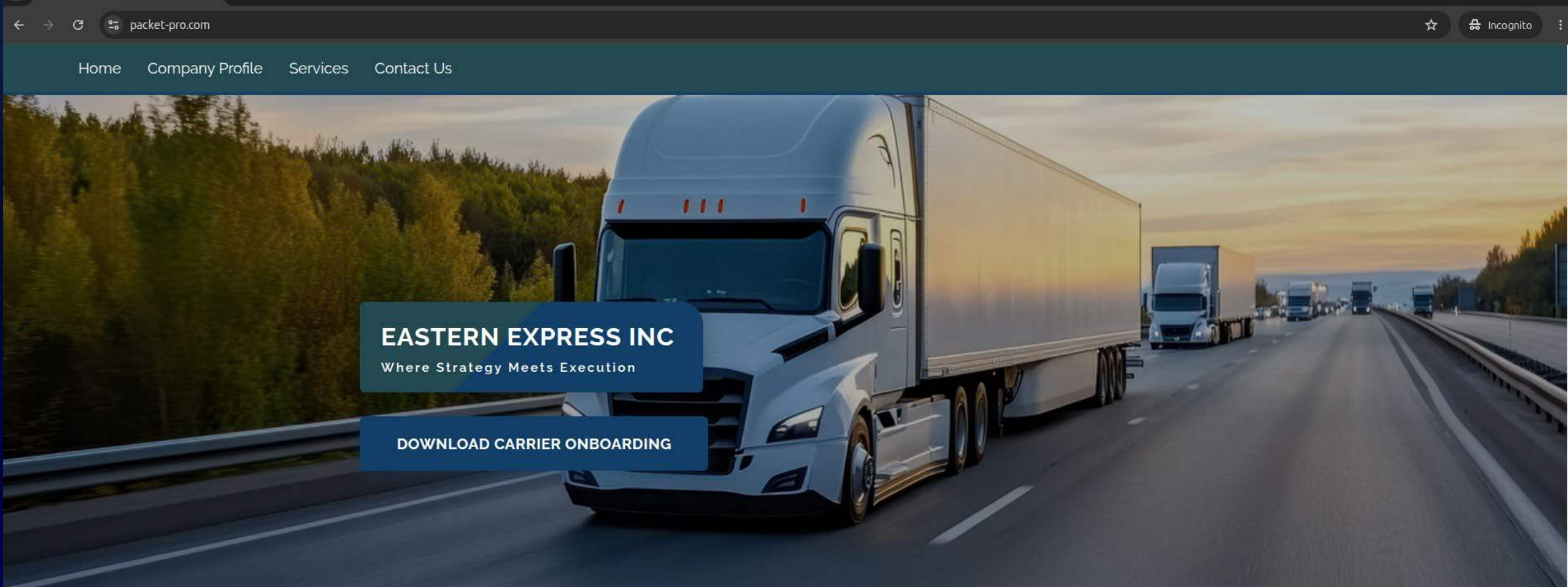
ONLINE FREIGHT SERVICES

MC# 315784 | DOT# 1563514

On Thu, 3 Sep 2026 15:55:37 +0000

wrote:





← → ↺ carrierpackready.com

CarrierPacket

What's Inside How It Works FAQ

Download Packet

+ Broker-ready in minutes

ONLINE
FREIGHTSERVICES

One professional packet with every document brokers ask for — W-9, insurance certificate, MC authority, WIP/NOA and more. Fill it once, send it to every broker.

Download Carrier Packet

Free · No sign-up required

CARRIER PACKET · CONTENTS

✓ W-9 Tax Form

✓ Certificate of Insurance (COI)

✓ MC Authority Letter

✓ WIP / NOA from Factor

✓ Carrier Profile & Contact Sheet

✓ Signed Broker–Carrier Agreement

Links to Cargo Theft

According to the post, the initial compromise was a “nextgen.Carrierbrokeragreement type of link” which notably **aligns with a payload URL from this cluster**, likely distributing ScreenConnect:
hxxp://nextgen1[.]net/carrier.broker.agreement[.]html.



reddit **FREIGHTBROKERS** comments

46 ↑
↓

How our company got hacked and almost lost 8 loads (trucking industry warning) (self.FreightBrokers)
submitted 28 days ago * by [jjjujoja](#)

(Im a carrier)

Wanted to share what happened to us — maybe it saves someone else the same headache. A broker sent a “setup” link. Our dispatcher, rushing, clicked it. The page asked to install remote access and a .exe file. We didn’t move forward with that load, but the damage was already done.

For about a week, nothing seemed wrong. Then the dispatcher noticed his email had random addresses added to the Block List. That’s when we realized: someone had gained access to his account.

Here’s what the hacker did:

- Deleted every booking email and blocked notifications so our dispatcher couldn’t see.
- Added his own device (tablet) to the dispatcher’s phone extension.
- When booking loads, he used our official MC email + phone (listed on FMCSA).
- Brokers, Highway, MyCarrierPackets would call our number and email — the hacker answered, verified everything, and got the loads.

Cargo Theft Attack Chain

Threat actor compromises broker load board account



Threat actor posts fake load



Replies with malicious link to responding carriers



Link leads to RMM to hijack carrier accounts

Uses compromised carrier accounts to bid on real loads



Attempts cargo theft

Beyond the Breach: Post Compromise Activity

Monitored this actor's post-compromise activity **for more than a month** in a decoy environment operated by Deception.pro.

- Abused multiple remote access tools to establish persistence
- Extensive reconnaissance using PowerShell scripts to enable freight fraud and broader financial theft
 - Accounting, Banking, Money transfer services, Cryptocurrency wallets
 - Fuel card services, fleet payment platforms, **and load board operators** - likely intended to enable transportation-related crimes, including cargo theft.

Public reporting on this threat actor

Remote access, real cargo: cybercriminals targeting trucking and logistics

NOVEMBER 03, 2025 | OLE VILLADSEN, SELENA LARSON, AND THE PROOFPOINT THREAT RESEARCH TEAM

SHARE WITH YOUR NETWORK!



Key findings

- Cybercriminals are compromising trucking and freight companies in elaborate attack chains to steal cargo freight.
- Cargo theft is a multi-million-dollar criminal enterprise, and digital transformation has led to an increase in cyber-enabled theft.
- Threat actors compromise these companies and use their access to bid on cargo shipments, to then steal and sell them.
- The threat actors typically deliver remote monitoring and management (RMM) tools, aligning with the broader trend of cybercriminals adopting these as a first-stage payload across the threat landscape.



FEDERAL BUREAU OF INVESTIGATION

Public Service Announcement



Alert Number: I-043026-PSA | 30 April 2026
Cyber-Enabled Strategic Cargo Theft Surging

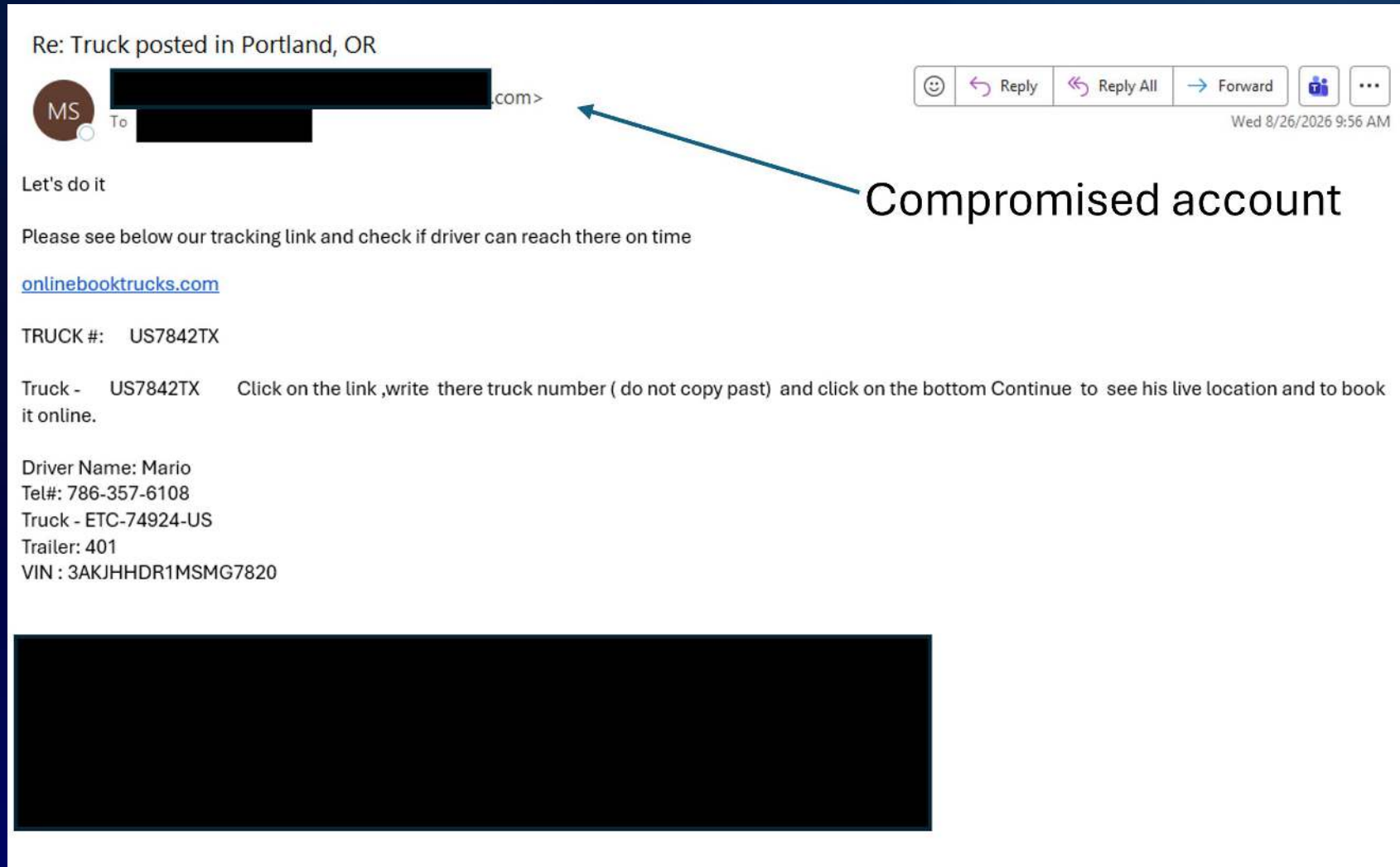
The Federal Bureau of Investigation is publishing this Public Service Announcement (PSA) to warn the public of cyber threat actors increasingly using sophisticated, cyber-enabled tactics to impersonate legitimate businesses to hijack freight, steal high-value shipments, and reroute deliveries, resulting in a surge of strategic cargo theft. Cyber threat actors target US transportation and logistics sectors, including companies with interests in shipping, receiving, delivering, and insuring cargo. Since at least 2024, cyber threat actors have gained unauthorized access to the computer systems of brokers and carriers — typically via spoofed emails, fake URLs, and compromised carrier accounts. The cyber actors pose as victim companies and post fraudulent listings on load boards¹ to deceive shippers, brokers, and carriers into handing over goods, which are redirected from their intended destination and stolen for resale. In 2025, estimated cargo theft losses in the United States and Canada surged to nearly \$725 million, (60 percent increase from 2024), while confirmed cargo theft incidents increased by 18 percent. The average value per theft rose 36 percent to \$273,990, driven by more selective, high-value targets.

HOW THE SCHEME WORKS

Threat actors² conducting cyber-enabled strategic cargo thefts use a multi-step process, often as follows:

NetSupport (Frequently Abused RMM)

- This actor targets the US and Europe



Compromised account

Same actor, responding to inquiry from compromised email account

Re: Newark, NJ Truck

 To gmail.com>



Thu 8/20/2026 9:50 AM

Let's do it

Please see below our tracking link and check if driver can reach there on time

usalivetracking.com

TRUCK #: ETC-74924-US

Truck - ETC-74924-US Click on the link ,write there truck number (do not copy past) and click on the bottom Continue to see his live location and to book it online.

Driver Name: Mario
Tel#: 786-357-6108
Truck - ETC-74924-US
Trailer: 401
VIN : 3AKJHHDR1MSMG7820

On Thu, 20 Aug 2026

Hello,

wrote:

Response from compromised account with malicious link

Legit inquiry on a truck availability



FreightLink Secure Access

For booking the truck and to have an access for live tracking
please enter the truck number

Enter truck number

Dispatcher sent you the truck number to view and book it
online. Enter it below to continue.

Truck number

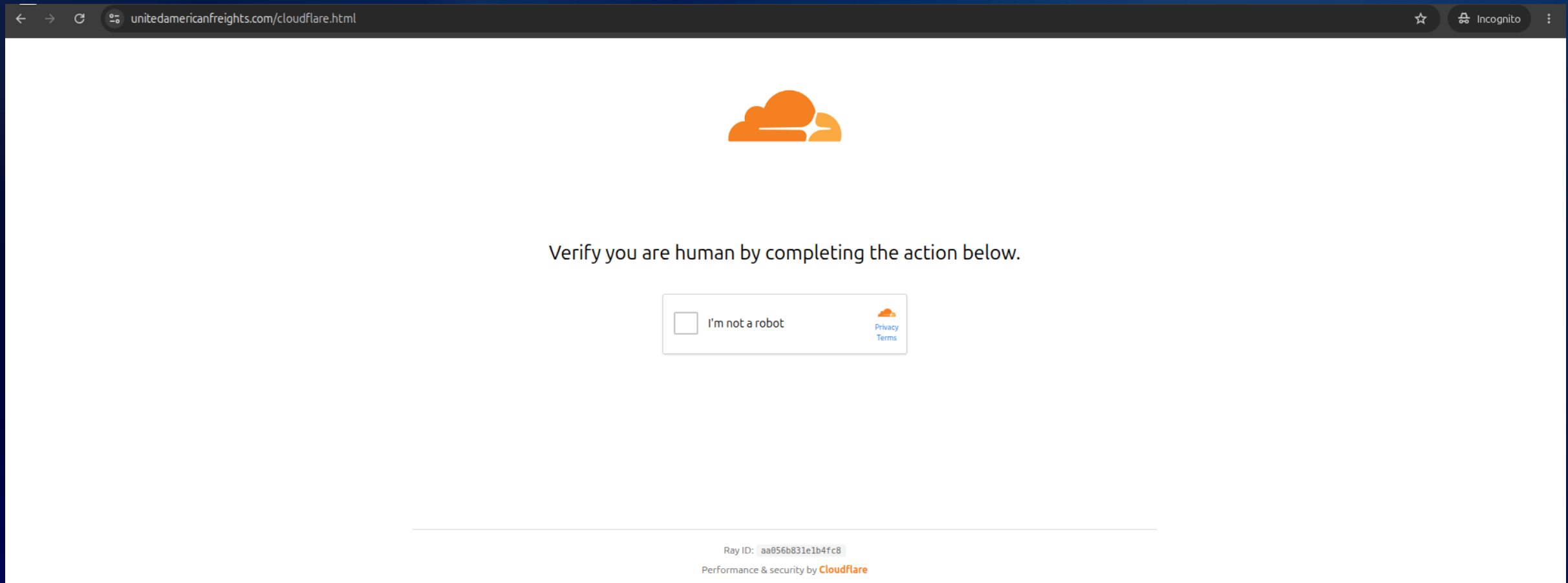
e.g. ETC-XXXX-US

Codes are single-use and expire after 24 hours.

Continue

256-bit encrypted connection. Your code is never stored.

Fake Cloudflare Challenge



ClickFix technique to install malware

← → ↻ unitedamericanfreights.com/cloudflare.html 🔍 ☆ Incognito ⋮



Verify you are human by completing the action below.

Verification Steps

Additional verification required

1. Press & hold **⌘** + **R**.
2. In the verification window, press **Ctrl** + **V**.
3. Press **Enter** on your keyboard to finish.

Verification prompt:

Cloudflare security check (Ray ID: aa056b831e1b4fc8)

Complete the steps above to continue

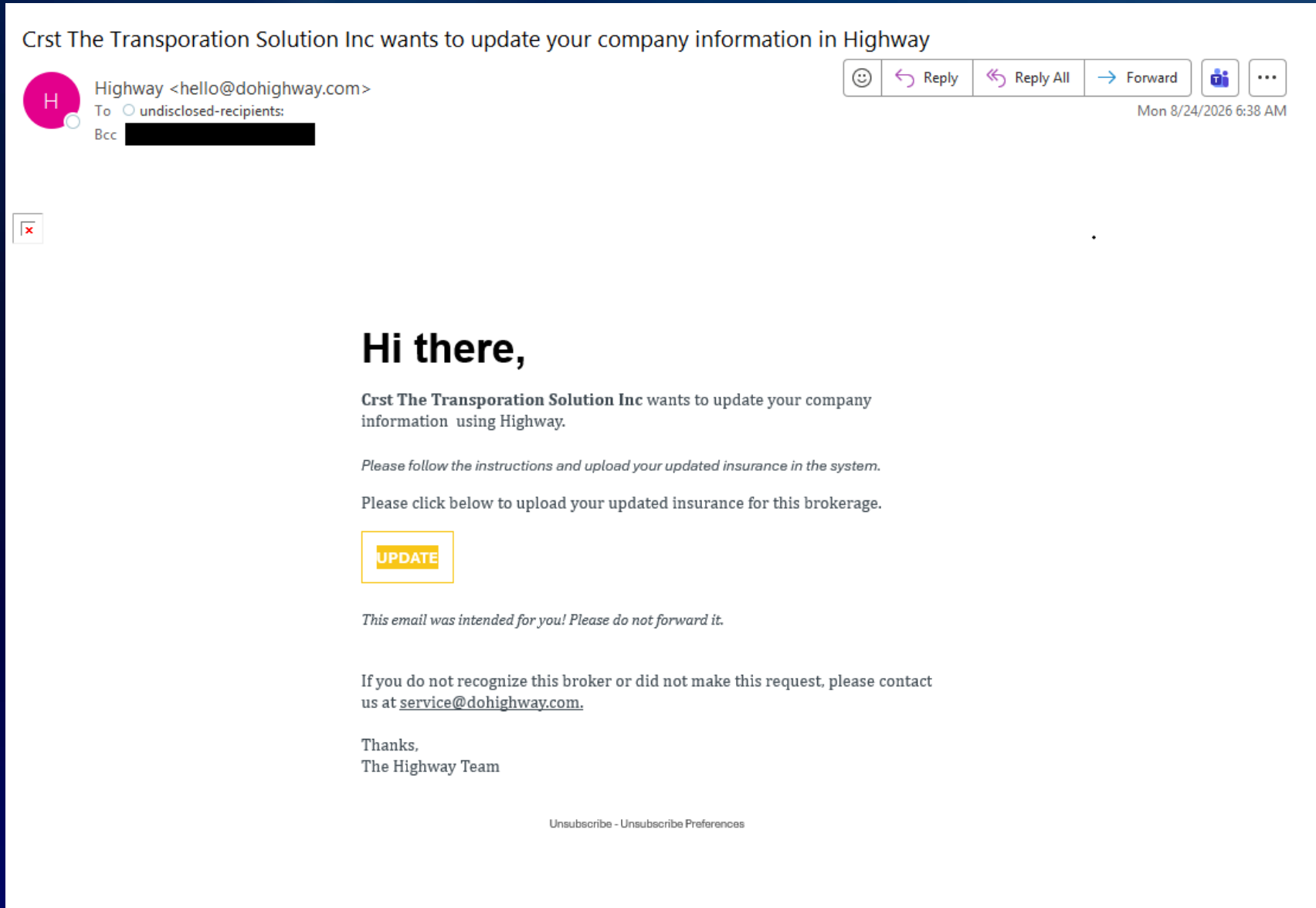
Verify

Ray ID: aa056b831e1b4fc8

Performance & security by Cloudflare

Following these directions will run a malicious script that ultimately installs NetSupport

AzaleaControl (Commodity RAT)



Highway - Sign In

highway.com-onboarding.com/carriers/

Incognito

If you need help, please call 806-HIGHWAY or email us at service@highway.com.

WELCOME TO

HIGHWAY

Let's get you onboarded with Highway.

FAST

Create a core profile faster than ever

EFFICIENT

Never re-enter your details again

PORTABLE

Use your profile with other Brokers

SECURE

Keep your company identity safe

FREE

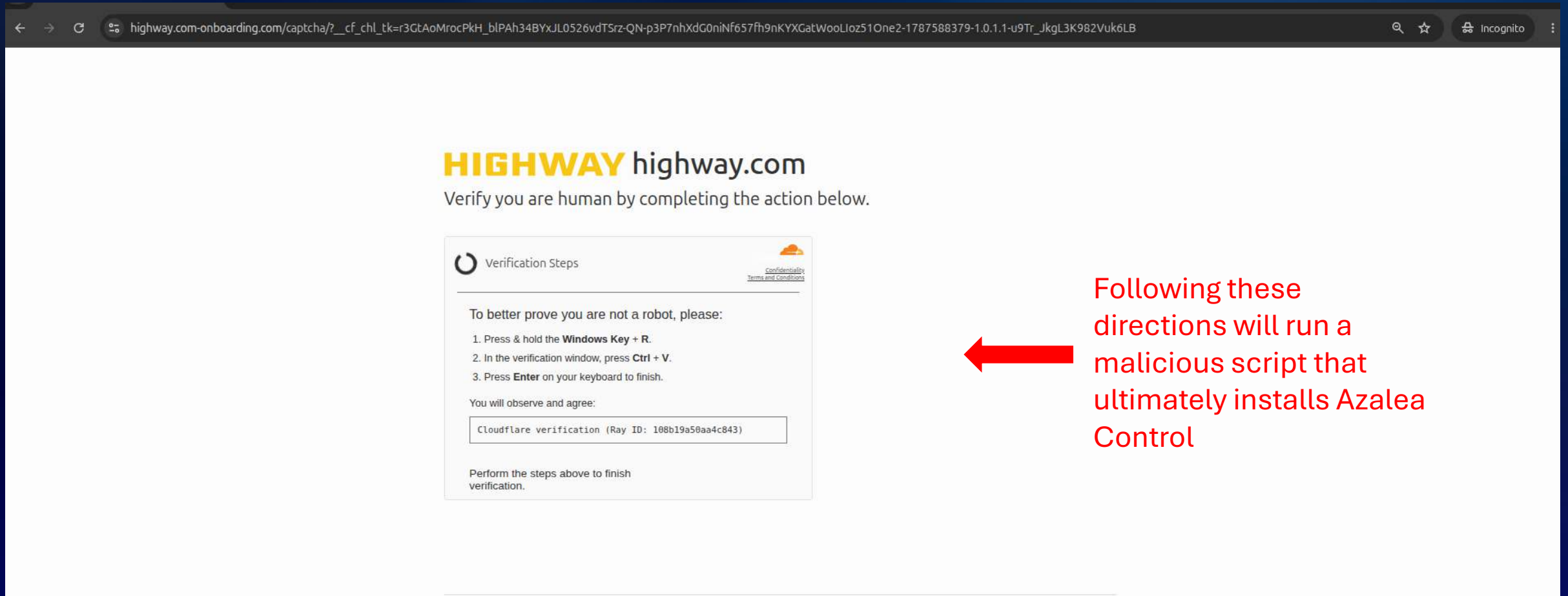
Do it all for no charge

Get Started

Already have an account?

[Log In](#)

ClickFix Technique to install malware



The screenshot shows a web browser window with the URL `highway.com-onboarding.com/captcha/?__cf_chl_tk=r3GtAoMrocPkH_bIPAh34BYxJL0526vdTSrz-QN-p3P7nhXdG0niNF657fh9nKYXGatWooLioz51One2-1787588379-1.0.1.1-u9Tr_JkgL3K982Vuk6LB`. The page displays the **HIGHWAY** logo and the text "highway.com". Below this, it says "Verify you are human by completing the action below." A "Verification Steps" box contains the following instructions:

- To better prove you are not a robot, please:
- 1. Press & hold the **Windows Key + R**.
- 2. In the verification window, press **Ctrl + V**.
- 3. Press **Enter** on your keyboard to finish.

Below the instructions, it says "You will observe and agree:" followed by a text box containing "Cloudflare verification (Ray ID: 108b19a50aa4c843)". At the bottom of the box, it says "Perform the steps above to finish verification." A red arrow points from the text on the right to the verification steps box.

Following these directions will run a malicious script that ultimately installs Azalea Control

NetSupport Commencing with Benign Conversation Starter (Rate Confirmation)

Re: Ref AJT-12314278 - Calhoun, GA to Charlotte, NC

 secure@mciexpresss.lat
To: [Redacted]

[Icons: Smile, Reply, Reply All, Forward, People, More]

Mon 8/31/2026 9:00 AM

[Ref:

I'm available by email right now. To confirm this load and secure our truck, please proceed to the link below. All carrier info, MC/DOT, and insurance details can be found there:

Link: <https://secure-highway.lat/secure/access/order39851>
Access code: DS-9841-FL

MC#186356 | DOT#263813

AJT TRUCKING

Nick Dalton
Logistics Manager · AJT Trucking Inc

T(305) 688-6622
Esafety@mciexpresss.lat
A11320 Nw 112th Ct, Doral, FL 33178-2152 [maps.google.com]
MC# 186356 DOT# 263813

----- On Mon, 31 Aug 2026 09:57:07 -0400

wrote -----

On Mon, Aug 31, 2026 at 9:54 AM <secure@mciexpresss.lat> wrote:

[Ref: CAL-KAN-0831]
Hello

Response with
malicious link

Recipient Response

Benign inquiry on a load

Need help with this verification? Contact the carrier that shared this secure request.



🔒 SECURE CARRIER VERIFICATION

CARRIER PROFILE REQUEST

Verify with confidence.

A carrier has shared their Highway verification profile with you. Enter the secure code from your message to review the authenticated details.

- Shared by carrier
- Read-only access
- Secure session



PROTECTED ACCESS

Enter secure code

Use the code provided by the carrier. This ensures the profile is only viewed by the intended recipient.

Secure code

Enter code

View verified profile

🔒 Your access is private. No account or personal information is required.

Highway secure verification · Request ID HWY-7F3A9C

← → 🔍 secure-highway.lat/secure/access/order39851/error.html

⚙️ 🔒 Incognito

⚠️ Session verification required — Manual download necessary

 **HIGHWAY**



Session Error

Your verification session couldn't be established automatically due to security restrictions. Please complete manual download to proceed.

Required action:

1. Click "Manual Download" below to retrieve the verification package
2. Open the downloaded file to complete carrier verification
3. Your session will be restored automatically

[Manual Download](#)

Secure connection - No personal data collected

Highway secure verification - Session recovery mode

🔒

SECURE CARRIER VERIFICATION

ⓘ

Anyone using this device can see downloaded files

📄

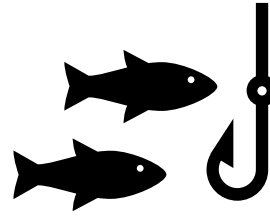
Rate_confirmation510_59ab.vbs

18.1 KB • Done

 **NMFTA**
CYBERSECURITY
CONFERENCE

 **NMFTA**
National Motor Freight
Traffic Association, Inc.

Credential Phishing

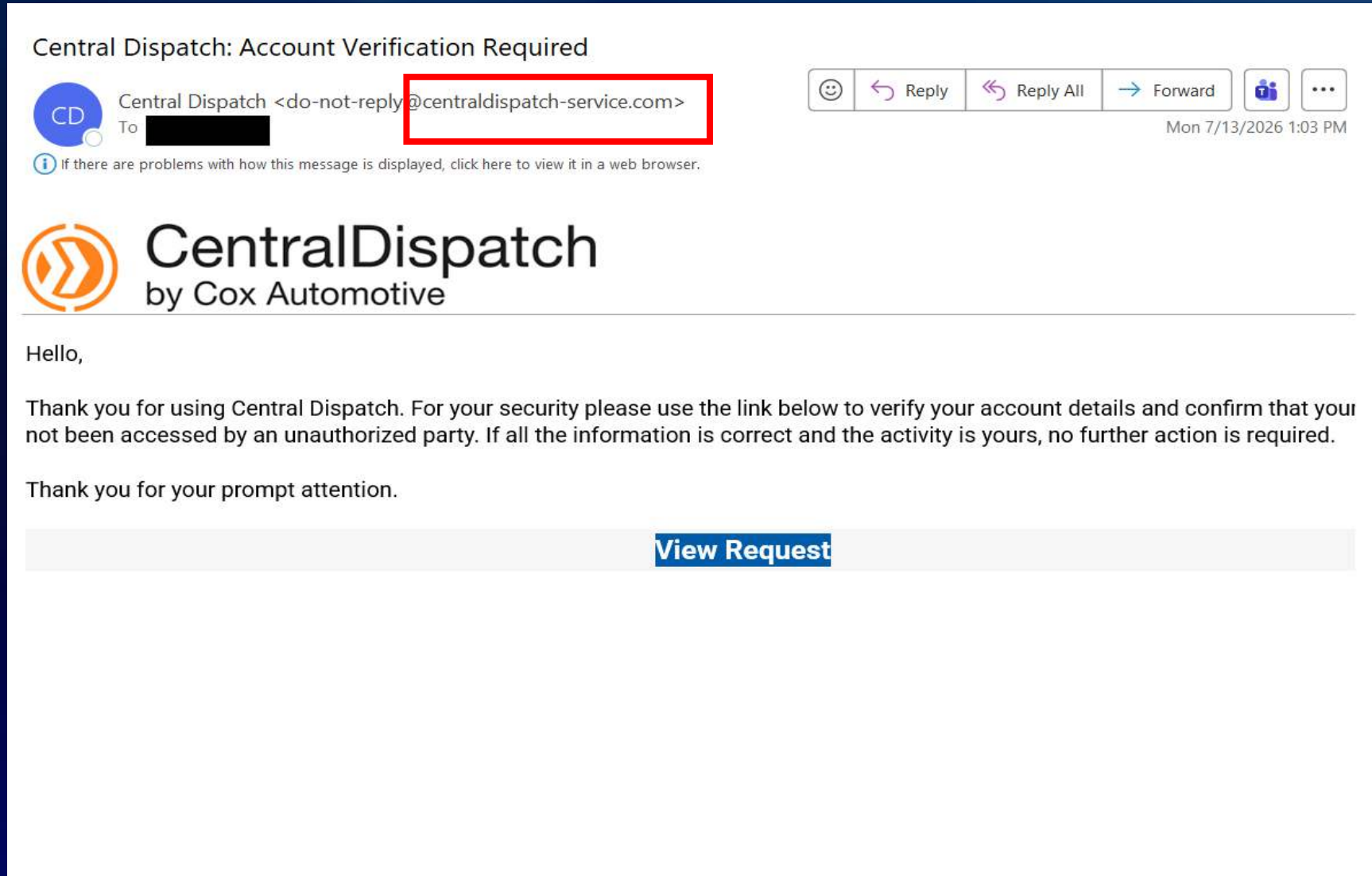


- 15 different phishing kits with 2 or more variations
- Targeting against US and Europe
- Kits include:
 - ✓ Credential/OTP Harvesters
 - ✓ Operator-gated “boutique” kits
 - ✓ Commodity Adversary-in-the-Middle (AiTM) phishing kits (e.g. Evilginx)

Quick Reference — Cluster Names

Cluster	Short Name	Primary Target
A	gpanel PHP AiTM PaaS — "RMIS Convoy"	RMIS/Truckstop, TIMOCOM
B	Socket.IO PhaaS — "LandingOnTheClouds"	Central Dispatch, TIMOCOM
C	UUID-Poll PHP AiTM — "DAT/Highway"	DAT, Highway
D	"Hello Friends" Telegram — FMCSA/Fuel Card	FMCSA/SAFER, EFS
E	Central Dispatch Static HTML AiTM	Central Dispatch
F	RMIS Onboarding Clone — "ProvideSupport" Operator	RMIS/Truckstop
G	Laravel Reverb "auth-status" AiTM	Amazon Relay, RMIS/Truckstop
H	Game-Camouflaged WebSocket Angular AiTM	RMIS/Truckstop
I	Highway Carrier-Onboarding Telemetry — Express <code>/api/log</code>	Highway
J	DAT-Directory Laravel Credential+OTP Harvester	DAT
K	Vercel/Next.js Telegram Relay — "Dream Big"	Central Dispatch
L	Flask-on-Vercel Page-Mirror Credential Recyclers	DAT, Central Dispatch
M	Netlify/React "Summit" Fabricated Brokerage	Central Dispatch
N	Express "Fenix" REST API State Machine	RMIS/Truckstop
O	Socket.IO E-Sign Freight Brokerage	Spooled freight brokerages

Operator-gated phishing kit



 **CentralDispatch**
by Cox Automotive

Sign-In

Central Dispatch will never ask for your password via email or text. Always verify the sender and URL before signing in. Learn how to identify legitimate Central Dispatch communications—including verified domains, trusted URLs, and common phishing red flags:

centraldispatch.com/staysafe

Username

Password

☐ Remember my Username

Sign In

Forgot? [Username](#) [Password](#)

Not a Member?

Create an Account

Potential relationship to this actor

Diesel Vortex: Inside the Russian cybercrime group targeting US & EU freight

FEBRUARY 24, 2026

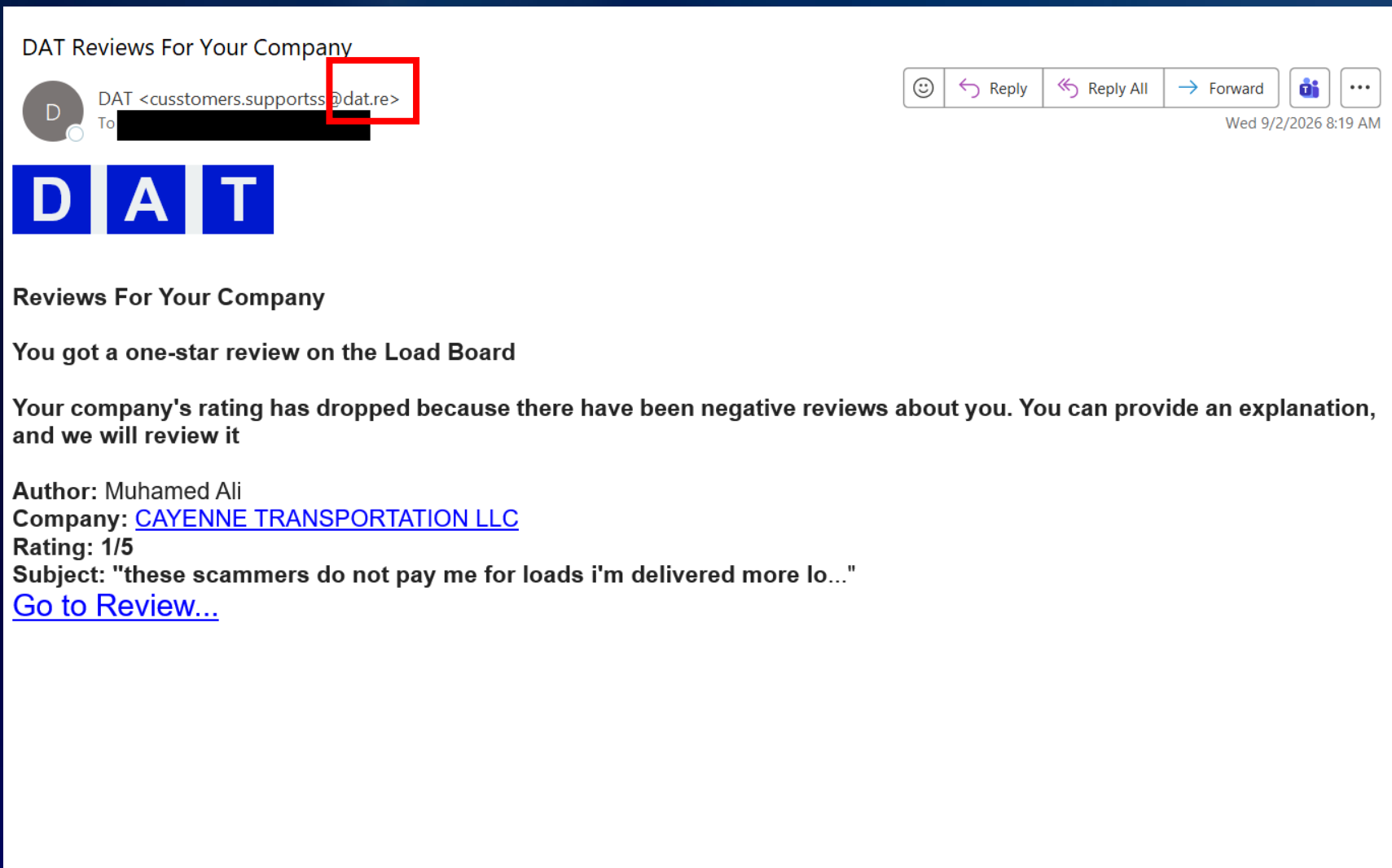
THREAT INTELLIGENCE

THREAT ACTOR

by Have I Been Squatted - 37 min read



Evilginx AiTM Phishing Kit



login.lldatlone.com/u/login/identifier?state=hKFo25B6VENBWDhichI5NE1GMkhHQVFjYjFxcUlfMUdyT1liZqFur3VuaXZlcnNhbc1sb2dpbqN0aWTZIEJyX011ZW03Z0VPVENhSVVkdFJ2RFhEN3Z2Z0daTnNT02NpZnkgZTlsek1YYm5XTkowRDUwQzJoY...

DAT Freight & Analytics

Log In

To continue to your DAT account

Email address*

CONTINUE

Don't have an account? [Sign up](#)

Credential & OTP/MFA Harvester

DAT DIRECTORY REPORT

 DAT <no-reply@datreports.com>
To [REDACTED]

😊

↩ Reply

↩ Reply All

➡ Forward

⋮

Tue 9/1/2026 1:10 PM

UNAUTHORIZED RE-BROKERING OF SHIPMENT
FRAUDULENT ACTIVITY
UNETHICAL OR DECEPTIVE BUSINESS PRACTICES

Submitted
DDID 37776239631F3315341F25341F5a42403101D2

1. SEPTEMBER 09/01/2026

REPORT AGE: 1 DAY

[VIEW REPORT](#)

DAT Freight & Analytics

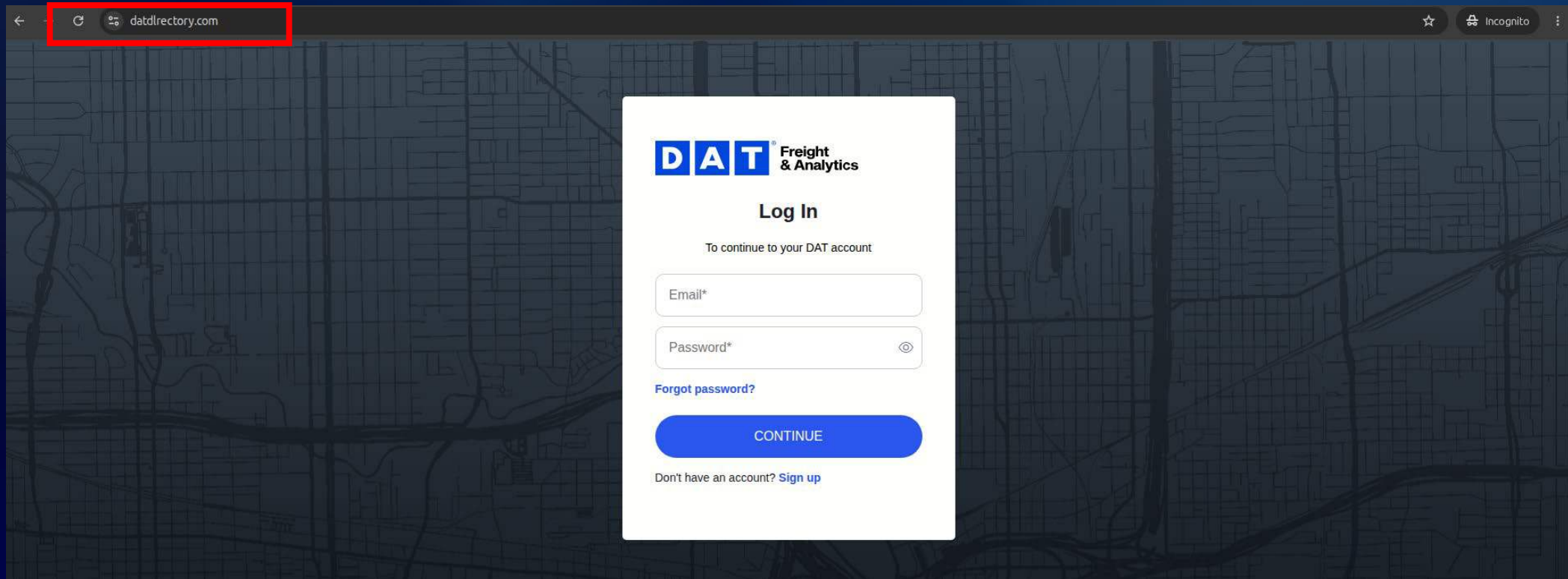
Our artificial intelligence engine detected this company has related companies or is associated with other companies. That could be a big red flag. Searches analyze archived FMCSA authority data since January 2005 to identify suspect conditions and related companies. They are not based on FMCSA census data



NMFTA
CYBERSECURITY
CONFERENCE



NMFTA™
National Motor Freight
Traffic Association, Inc.



datdrectory.com/verification

☆ Incognito

DAT

Freight
& Analytics

Verify your identity

We've sent a text message to:

+1XXXXXXXXXX

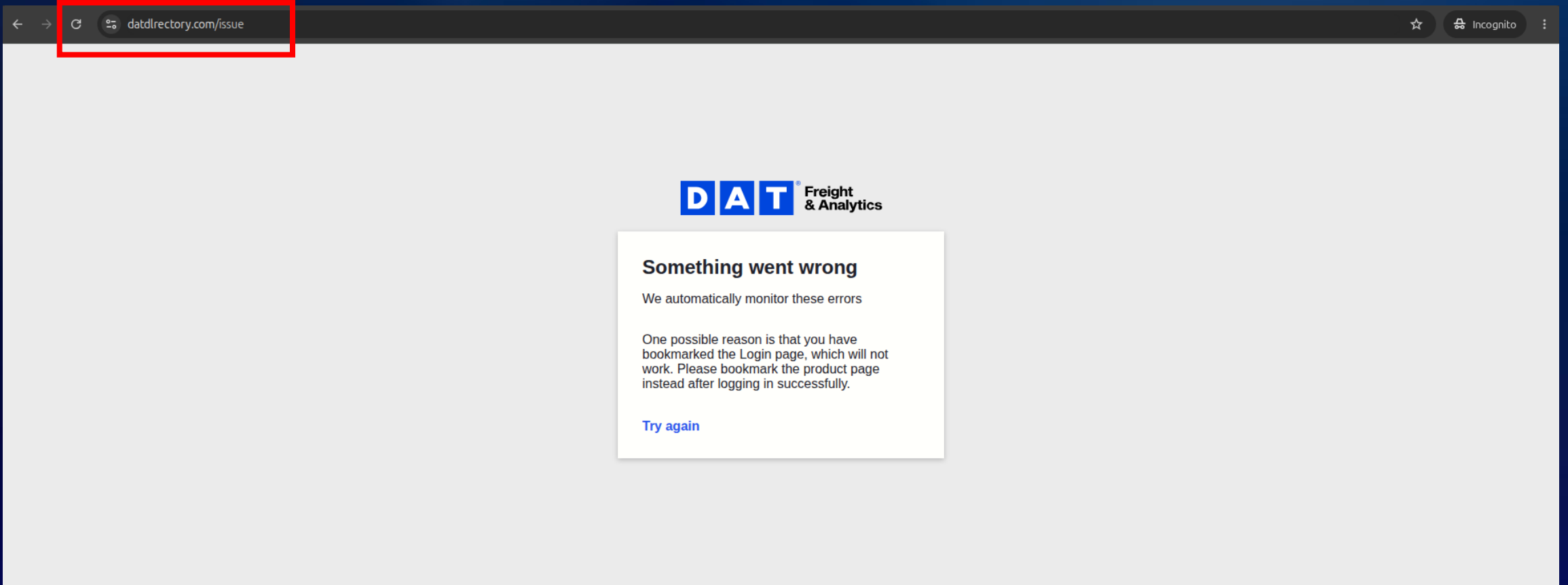
Enter the 6-digit code*

☐ Remember this device for 30 days

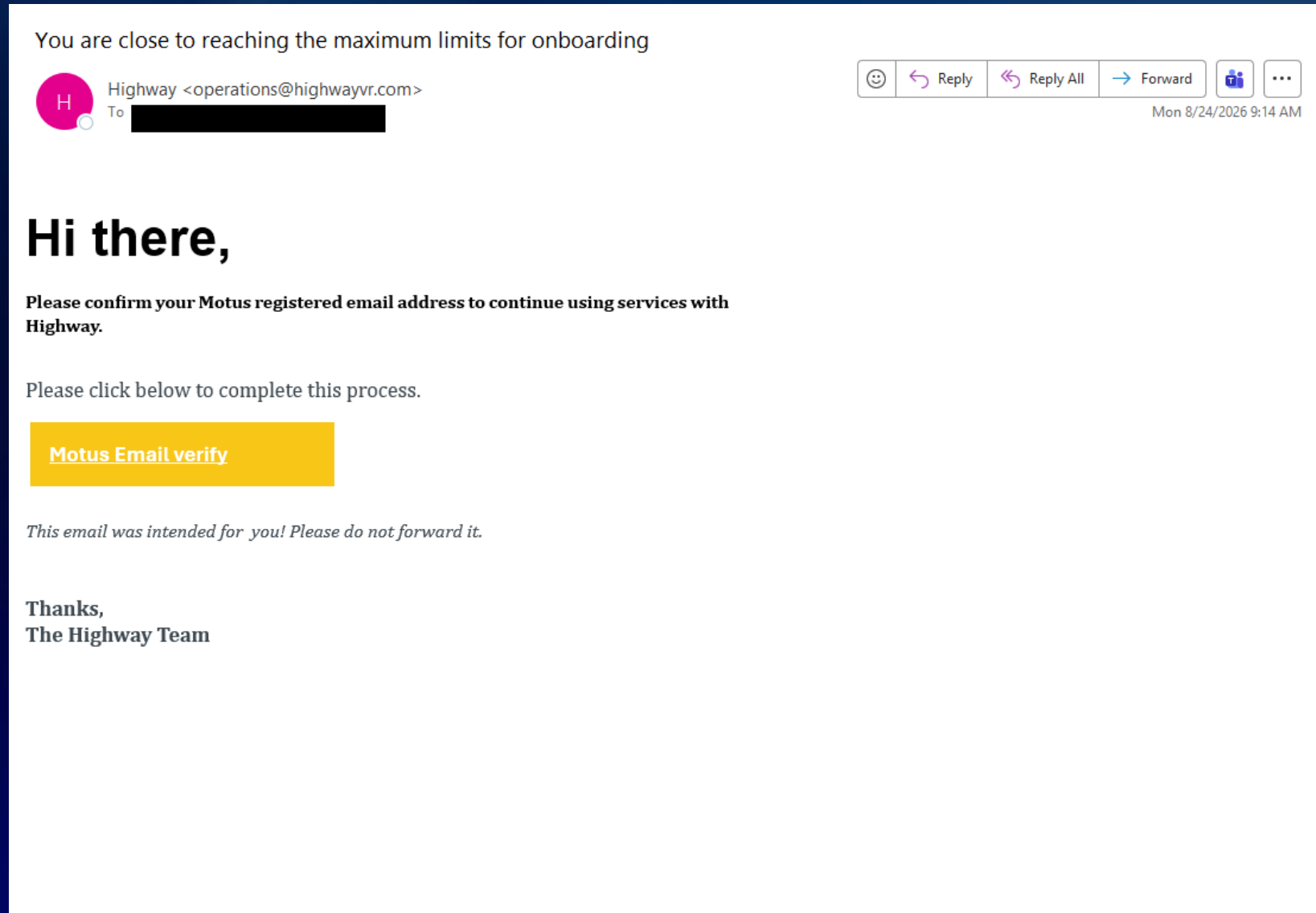
CONTINUE

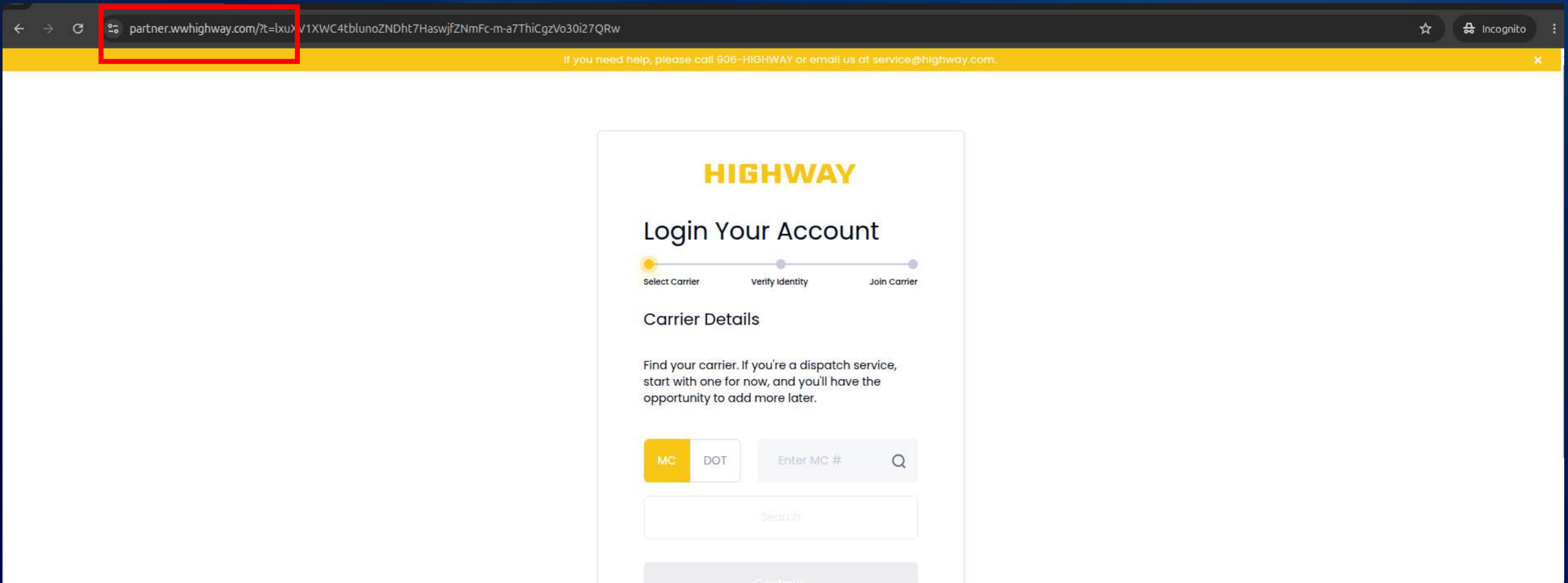
Didn't recive a code? [Resend](#) or [get a call](#)

TRY ANOTHER METHOD



Operator-gated Credential Phishing Kit: Highway





← → partner.wwhighway.com/?t=lxuV1XWC4tblunoZNDht7HaswjfZNmFc-m-a7ThiCgzVo30i27QRw ☆ Incognito

HIGHWAY

Login Your Account

Select Carrier Verify Identity Join Carrier

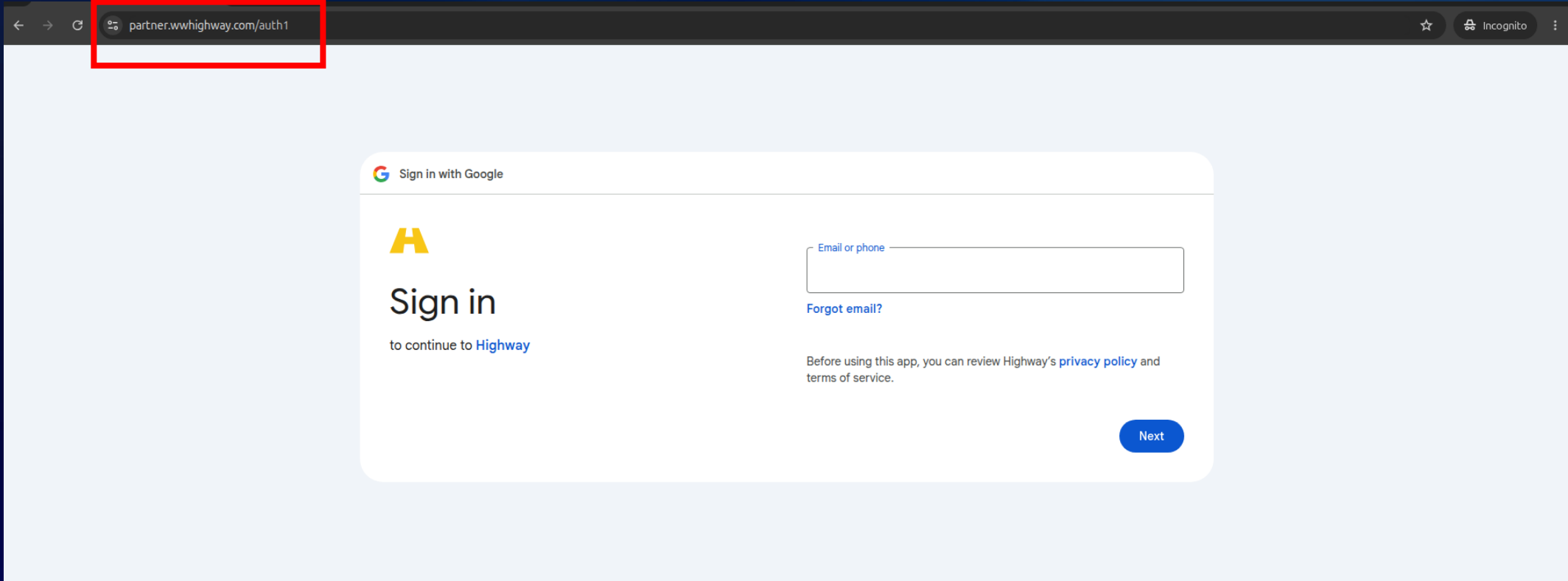
Enter Email Address

In order to protect your account, we need to verify your email address.

EMAIL ADDRESS

Enter Email Address

Continue



Operator-gated Credential Phishing Kit: RMIS/Truckstop

From: RMIS <rmis@registrymonitorings.com>

Subject: TRI-TECH LOGISTICS LLC - New Carrier Registration Invitation - [REDACTED]

New Carrier Registration Invitation

Dear [REDACTED],

TRI-TECH LOGISTICS LLC is now using Registry Monitoring Insurance Services Inc. (RMIS), as our online carrier compliance service provider. Although you may have registered with TRI-TECH LOGISTICS LLC in the past, we require all carriers to register using this new system. The RMIS online registration system will give you the ability to view your insurance, authority, and safety information that RMIS has on file to ensure you meet TRI-TECH LOGISTICS LLC minimum requirements and are on our approved carrier list.

Per our Corporate policy, TRI-TECH LOGISTICS LLC can only work with carriers that are listed as an approved carrier. The online system will also streamline the connection with your insurance provider, so we always have an up to date copy of your insurance certificate(s). Expired insurance certificate(s) are one of the biggest reasons we drop carriers from our approved carrier list. Please complete the online application today so we can continue working together; all carriers that we currently work with, or will work with going forward, must apply via the link below.

PLEASE CLICK HERE <[https://accordgoc.rmisecur.com/_s/reg/InvitationProcessing?invitation_key=\[REDACTED\]](https://accordgoc.rmisecur.com/_s/reg/InvitationProcessing?invitation_key=[REDACTED])> TO COMPLETE ONLINE REGISTRATION*

INVITATION TOKEN: [REDACTED]

For help or questions regarding the registration process on this website, contact a TRI-TECH LOGISTICS LLC representative at (646) 436-6729 <(646)%436-6729> or dispatch@tritechlogistic.com , to assist you.

Thank you and best regards,

Roman H.
TRI-TECH LOGISTICS LLC
2261 Market Street, PMB 85402, San Francisco, CA 94114

Copyright 2025 Registry Monitoring Insurance Services, Inc. 800-400-4924 <(800)%20400-4924>

← → ↻

accordgoc.rmisecur.com/_s/reg/invitationProcessing?invitation_key=

🔒 ☆ Incognito



Registration Client Login Carrier Login

Invitation Page

Please enter your invitation code. You cannot register without an invitation.

INVITATION CODE:

GO TO NEXT STEP

Already registered? [Click here to log in to your account.](#)

For help or questions regarding the registration process, contact RMIS at 888-643-8774 or click on the Live Chat icon.

© 2026 Truckstop. All rights reserved.
RMIS Privacy Policy | Do Not Sell My Personal Information
● RMIS Status - All Systems Operational

NEED HELP?
CHAT NOW!

← → ↻ [accordgoc.rmisecur.com/_s/reg/GeneralRequirements?invitation_key=\[REDACTED\]](https://accordgoc.rmisecur.com/_s/reg/GeneralRequirements?invitation_key=[REDACTED]) 🔍 🔄 ☆ Incognito



[Registration](#) [Client Login](#) [Carrier Login](#)

Welcome! Thank you for your interest in becoming an approved carrier for ACCORD TRANSPORTATION LTD. We look forward to working with you.

To become a certified carrier, you must:

- Provide your MC/MX# or DOT# to begin registration. Intrastate carriers without a DOT# may provide an applicable state registration number to begin registration.
- Supply your company contact information.
- Submit an electronic W9 (have your TaxID available).
- Complete the Carrier Profile.
- Read and ACCEPT the Agreement(s).
- Provide a Certificate of Insurance that meets the insurance minimum requirements below. Certificates must be submitted from your insurance producer (agent)
 - \$100,000 Cargo Coverage
 - \$1,000,000 Auto Coverage
 - \$1,000,000 General Liability Each Occurrence Limit
 - \$2,000,000 General Liability Aggregate Limit
- If RMIS does not already have a copy of your certificate on file, we will request one for you from your insurance agent (producer).
- You will be required to meet the following requirements:
 - Active Common or Contract Authority.
 - Safety Rating must be Satisfactory, Conditional or None.
 - Authority active for at least 180 days.

[GO TO NEXT STEP](#)

[NEED HELP?](#)

←→↻🔍 accordgoc.rmissecur.com/_c/std/reg/DOTLookupStd?invitation_key=[REDACTED]🔍🔒🌟📁 Incognito⋮



RegistrationClient LoginCarrier Login

Carrier Prequalification

Please select ONE carrier identifier for registration.

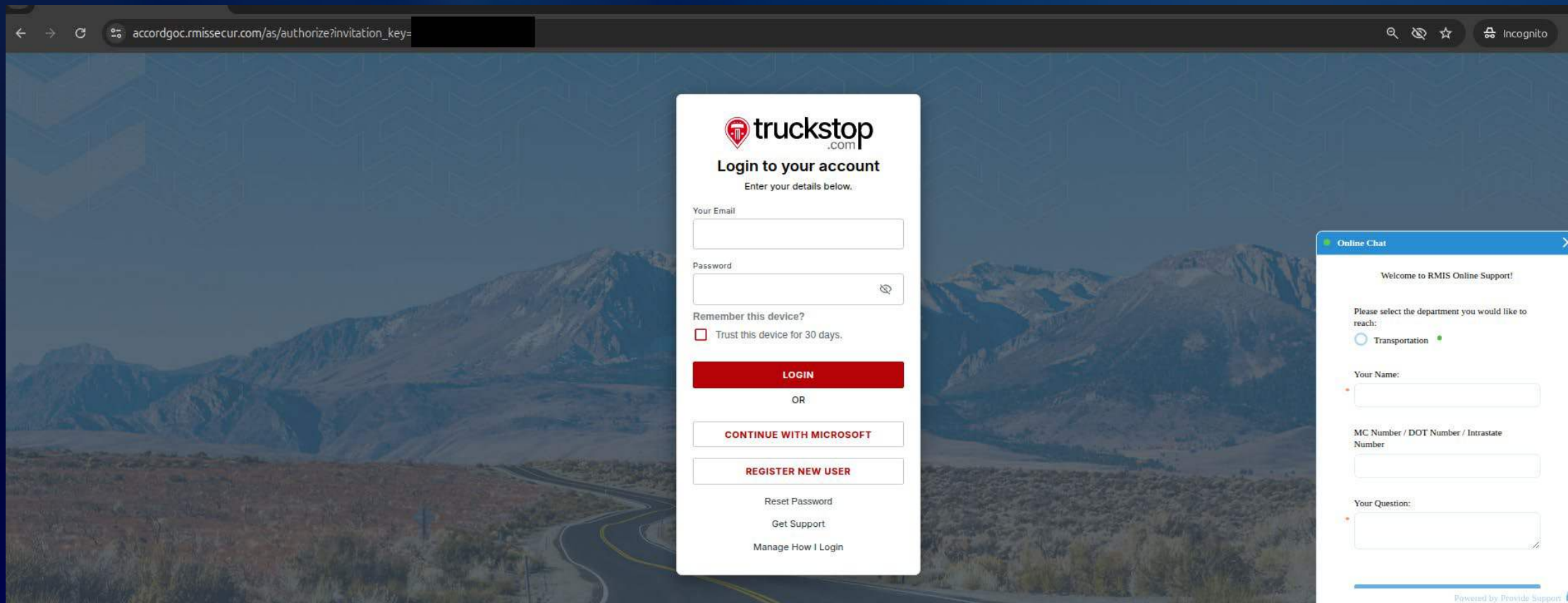
☐ Interstate (hauling across state lines) ☐ Intrastate US (hauling within a single state only) ☐ Intra Canada (hauling within Canada only)

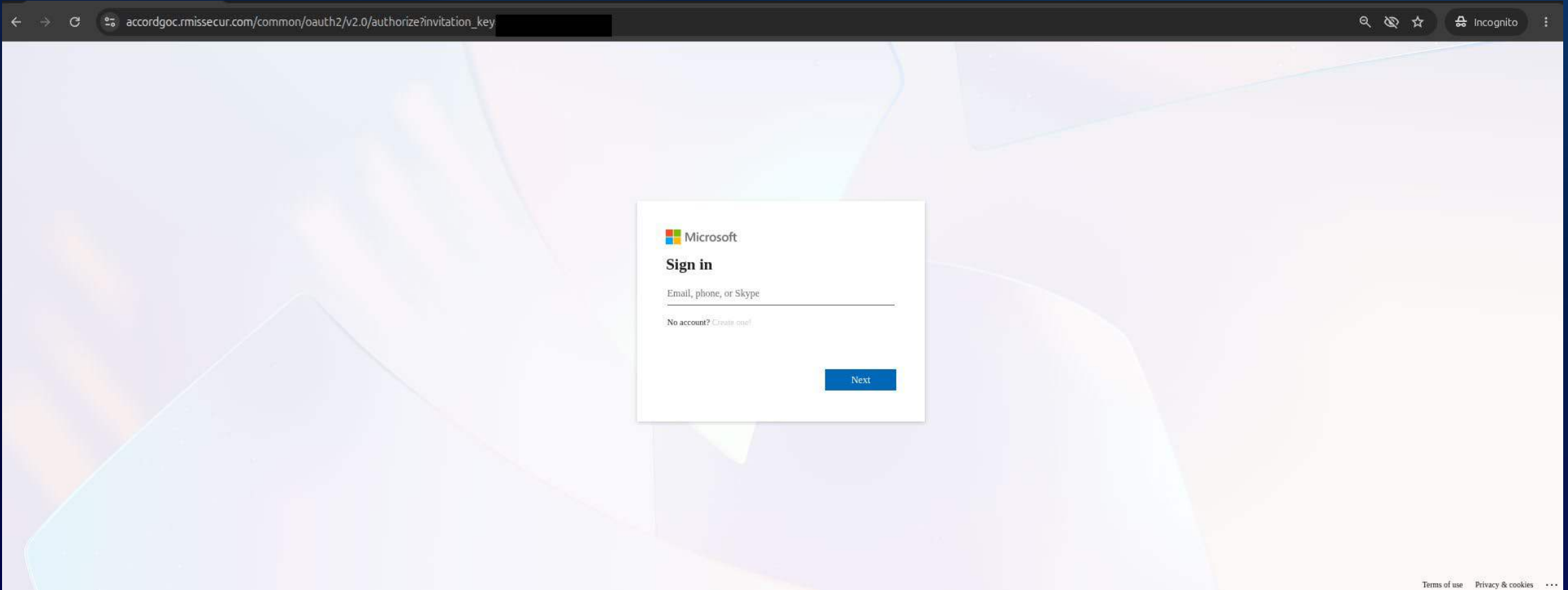
GO TO NEXT STEP

For help or questions regarding the registration process, contact RMIS at 888-643-8774 or click on the Live Chat icon.

© 2026 Truckstop. All rights reserved.
RMIS Privacy Policy | Do Not Sell My Personal Information
● RMIS Status - All Systems Operational

NEED HELP?
CHAT NOW!





← → ↻ accordgoc.rmisecur.com/common/oauth2/v2.0/authorize?invitation_key=[redacted]&email=[redacted] 🔍 🗑️ ☆ Incognito ⋮



[redacted]

Enter your password

Password

Next

[Help and feedback](#) [Terms of use](#) [Privacy and cookies](#)
Use private browsing if this is not your device. [Learn more](#)

Imposter – Benign Conversation Starters

Lyons, GA Atlanta, GA

 Joe Negron <cmt@chisellogisticsinc.com>
To [REDACTED] Wed 8/19/2026 8:29 AM

  Reply  Reply All  Forward  

Good day team, we have a load available for today.
Let me know if you have a capacity to cover this

Pick Up Today FCFS 08:00 - 22:00
Delivery Tomorrow 06:00-16:00
Weight: 8,000 LBS
Commodity: Palletized Clothing
What rate do you need to book this one?
MC#1559435

--
Regards,
Carrier Management Team
CHISEL LOGISTICS LLC
Address: 105 MAXESS ROAD MELVILLE, NY 11747
Cell - (516) 548 8937 | MC-1559435 | USDOT-4092596 | Website: [chisellogistics.com] | LinkedIn:
Emergency contact-
Team Leader - Simon Miller | Cell - (516) 548 8937 | Email - simon@chisellogistics.com
Manager - Tom James | Cell - (516-656-1020) | Email - tom@chisellogistics.com
If you are happy with our services or have any feedback do email us @ feedback@chisellogistics.com
"Your freight is more than cargo to us; it's a commitment we deliver with precision, care, and unwavering r

Toronto , ON Carrollton , MO

 Dario Maros <dario.maros@dsan.com>
To [REDACTED] 8/20/2026

Details?

Y&B TRANSPORTATION FOR THE FUTURE LLC
MC-1602162
184 CANNON CT APT 1
LOUISVILLE, KY 40229
Phone (502) 345-7058

Potential End Games:

- Send a link leading to credential phishing or malware/RMM
- Successfully book (and steal) a load
- Double brokering a load that was fraudulently booked

Why is this such a problem?

- **The urgency is built in.** No need to create a sense of urgency to compel the recipient to click on the link – the urgency to book loads quickly already exists.
- **Carriers are a soft target.** The vast majority (90%) of Carriers are small businesses or owner-operators who lack robust security and defenses – both tools and people.

Spotting malicious emails and payloads

Fundamentals matter:

- Slow down. Every email is potentially malicious.
- Check and verify all senders' domains and identifiers.
- Watch for ClickFix lures!
- Check the file extension before executing the download (vbs, wsf, cmd, exe, zip/rar)

Listen when your 6th sense says: *"That's weird"*:

- Unusual or misspelled domain or TLD (top level domain e.g. .lat)
- Content is out of context with the rest the thread
- Quick/clumsy response pushing a link in the conversation.
- Remember malicious emails will come from someone you know (i.e. compromised account)

Further Recommendations

- Restrict the download and installation of any RMM tooling that is not approved and confirmed by an organization's information technology administrators.
- Have network detections in place and use endpoint protection. This can alert on any network activity to RMM servers.
- Do not download and install executable files/scripts (.exe, .msi, vbs, wsf, cmd) delivered via email from external senders.
- Train users to identify the activity and report suspicious activity to their security teams. This training can easily be integrated into an existing user training program.

Dinner at Long Beach Beer Lab

Meet in the lobby at 5:30 pm for transportation to dinner

