Remote access, real cargo: cybercriminals targeting trucking and logistics

⋮ 10/29/2025

- Platform
- Products
- Solutions
- Partners
- Resources
- Company

Search

Login

English: Americas

Platform

Products

Solutions

Partners

Resources

Company

Threat Protection

Stop all human-centric threats with industry-leading AI and global threat intelligence.

Core Email Protection
Prime Threat Protection
How to Buy

Data Security & Governance

Transform your data security and governance with a unified, omni-channel approach.

Unified Data Security
Adaptive Email DLP
Enterprise DLP
Insider Threat Management
Digital Communications Governance
How to Buy

Data & SaaS Security Posture

Remediate data and SaaS exposures by understanding your risk posture.

Account Takeover Protection
Data Security Posture Management (DSPM)

Human Resilience

Unlock full user risk visibility and drive behavior change.

ZenGuide

Premium Services

Leverage our strategic guidance and hands-on expertise to optimize your Proofpoint solutions.

All Products

Browse the full Proofpoint product suite.

More products

More Proofpoint Products

Account Takeover Protection (ATO)

Detect, investigate and remediate account takeovers with sophisticated machine learning.

Adaptive Email DLP

Detect and prevent accidental and malicious email data loss with advanced ML and behavioral AI.

Archive

Securely store enterprise communications and search with deep data insights.

Automate

Streamline compliance supervision by reducing low-risk content and analyst review fatigue using machine learning models.

Capture

Collect and retain all digital communications for compliance, legal discovery, and long-term information retention.

CASB

Protect cloud apps and data with visibility, control, and threat prevention.

Collab Protection

Extend protection beyond email for all messaging and collaboration tools.

Core Email Protection

Protect your people from email threats using AI and global threat intelligence.

Discover

Process, analyze and cull more archived information in-house for e-discovery.

Data Security Posture Management (DSPM)

Discover, classify, and protect sensitive data across cloud and hybrid environments.

Email DLP & Encryption

Prevent email data loss and encrypt sensitive emails with granular and dynamic rules-based controls.

Endpoint DLP

Detect and prevent data loss at the endpoint.

Enterprise DLP

Detect and resolve data loss risk across email, cloud, and endpoints with centralized policies.

Email Fraud Defense

Protect your brand reputation, meet DMARC requirements to increase deliverability and identify lookalikes of your domains.

Insider Threat Management

Detect and prevent insider threats with deep visibility into risky behavior.

Patrol

Monitor and manage social media compliance with automated workflows and reporting.

Prime Threat Protection

Stop all human-centric attacks across multiple channels and stages with AI threat detection.

Secure Email Relay

Increase control and security for application-generated email and accelerate DMARC implementation.

Supervision

Monitor and supervise digital communications to enable compliance with SEC, FINRA, and other regulations.

Track

Track, audit, report on and reconcile all content in your capture stream for compliance.

ZenGuide

Strengthen human resilience through automated, risk-based learning.

Solutions by Use Case

How Proofpoint protects your people and data.

Ensure Acceptable GenAI Use

Empower your workforce with safe GenAI practices.

Authenticate Your Email

Protect your email deliverability with DMARC.

Combat Email and Cloud Threats

Protect your people from email and cloud threats with an intelligent and holistic approach.

More use cases

Solutions by Industry

People-centric solutions for your organization.

Federal Government

Cybersecurity for federal government agencies.

State and Local Government

Protecting the public sector, and the public from cyber threats.

More industries

Comparing Proofpoint

Evaluating cybersecurity vendors? Check out our side-by-side comparisons.

View comparisons

Solutions By Use Case

How Proofpoint protects your people and data.

Change User Behavior

Help your employees identify, resist and report attacks before the damage is done.

Combat Data Loss and Insider Risk

Prevent data loss via negligent, compromised and malicious insiders.

Modernize Compliance and Archiving

Manage risk and data retention needs with a modern compliance and archiving solution.

Protect Cloud Apps

Keep your people and their cloud apps secure by eliminating threats and data loss.

Prevent Loss from Ransomware

Learn about this growing threat and stop attacks by securing ransomware's top vector: email.

Secure Microsoft 365

Implement the best security and compliance solution for Microsoft 365.

Solutions By Industry

People-centric solutions for your organization.

Higher Education

A higher level of security for higher education.

Financial Services

Eliminate threats, build trust and foster growth for your organization.

Healthcare

Protect clinicians, patient data, and your intellectual property against advanced threats.

Mobile Operators

Make your messaging environment a secure environment.

Internet Service Providers

Cloudmark email protection.

Small and Medium Businesses

Big-time security for small business.

Proofpoint vs. the competition

Side-by-side comparisons.

Proofpoint vs. Abnormal Security
Proofpoint vs. Mimecast
Proofpoint vs. Cisco
Proofpoint vs. Microsoft Purview
Proofpoint vs. Legacy DLP
Proofpoint vs. Check Point Harmony
Proofpoint vs. SSE Vendors
Proofpoint vs. Symantec

Resources

Find reports, webinars, blogs, events, podcasts and more.

Resource Library
Blog

Keep up with the latest news and happenings.

Webinars

Browse our webinar library to learn about the latest threats, trends and issues in cybersecurity.

Cybersecurity Academy

Earn your certification to become a Proofpoint Certified Guardian.

Podcasts

Learn about the human side of cybersecurity.

Threat Glossary

Learn about the latest security threats.

Events

Connect with us at events to learn how to protect your people and data from ever-evolving threats.

Customer Stories

Read how our customers solve their most pressing cybersecurity challenges.

Company

Proofpoint protects organizations' greatest assets and biggest risks: their people.

About Proofpoint
Careers

Stand out and make a difference at one of the world's leading cybersecurity companies.

News Center

Read the latest press releases, news stories and media highlights about Proofpoint.

Privacy and Trust

Learn about how we handle data and make commitments to privacy and other regulations.

Environmental, Social, and Governance

Learn how we apply our principles to positively impact our community.

Support

Access the full range of Proofpoint support services.

Platform

Discover the Proofpoint human-centric platform.

Learn More
Proofpoint Satori

The power behind agentic security operations.

Proofpoint Nexus

Advanced AI and threat intelligence to detect threats and assess data risk.
Proofpoint Zen

Integrated control points to protect people and data, wherever work happens.

November 03, 2025 Ole Villadsen, Selena Larson, and the Proofpoint Threat Research Team

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.

Overview

Proofpoint is tracking a cluster of cybercriminal activity that targets trucking and logistics companies and infects them with RMM tooling for financial gain. Based on our ongoing investigations paired with open-source information, Proofpoint assesses with high confidence that the threat actors are working with organized crime groups to compromise entities in the surface transportation industry — in particular trucking carriers and freight brokers — to hijack cargo freight, leading to the theft of physical goods. The stolen cargo most likely is sold online or shipped overseas. Such crimes can create massive disruptions to supply chains and cost companies millions, with criminals stealing everything from energy drinks to electronics.

In the observed campaigns, threat actors aim to infiltrate companies and use their fraudulent access to bid on real shipments of goods to ultimately steal them. The observed campaigns described in this report are similar to activity Proofpoint researchers previously detailed in September 2024. However, we cannot assess with high confidence whether historic and current campaigns are conducted by the same or multiple groups; thus, Proofpoint is not attributing the activity to a tracked threat actor.

Old crimes, new tools: the digital transformation of cargo theft

According to the National Insurance Crime Bureau, cargo theft leads to $34 billion in losses annually. Cargo theft can refer to many different types of activities leading to the theft of commercial shipments while cargo is in transit. Much of this activity is conducted by organized criminal groups, according to U.S. law enforcement, and Congress has introduced legislation to combat organized retail theft as it has skyrocketed since the COVID-19 pandemic. (Cargo theft conducted by organized crime has been a problem for decades – from "Old West Train Robbers" to 1960s mobsters to our modern cyber-enabled heists.) Proofpoint previously published details on a similar type of cybercrime targeting cargo that impersonates various companies to steal medical and electronic equipment.

While the campaigns that Proofpoint discusses in this report relate to North American cargo theft, it's a global problem. According to Munich RE, global cargo theft hotspots include Brazil, Mexico, India, the U.S., Germany,

Chile, and South Africa, while the most targeted commodities are food and beverage products.

Cyber-enabled theft is one of the most common forms of cargo theft and relies on social engineering and a knowledge of how the trucking and transportation industries work. According to IMC Logistics, opportunities for cyber-enabled theft are partly responsible for the dramatic increase in cargo theft in recent years: "…the digitization of domestic and international supply chains has created new vulnerabilities and thus opportunities for [Organized Theft Groups] to exploit gaps using sophisticated and ever-evolving cyber capabilities. These groups can steal freight remotely by exploiting the technology that has been embedded into supply chains to move cargo more efficiently."

The attack chain in the observed campaigns leading to cargo theft attempts, which will be described in subsequent sections, is as follows: the threat actor will compromise a broker load board account (a marketplace companies use to facilitate booking loads for trucks), post a fake load, and kick off the attack chain when a carrier responds.

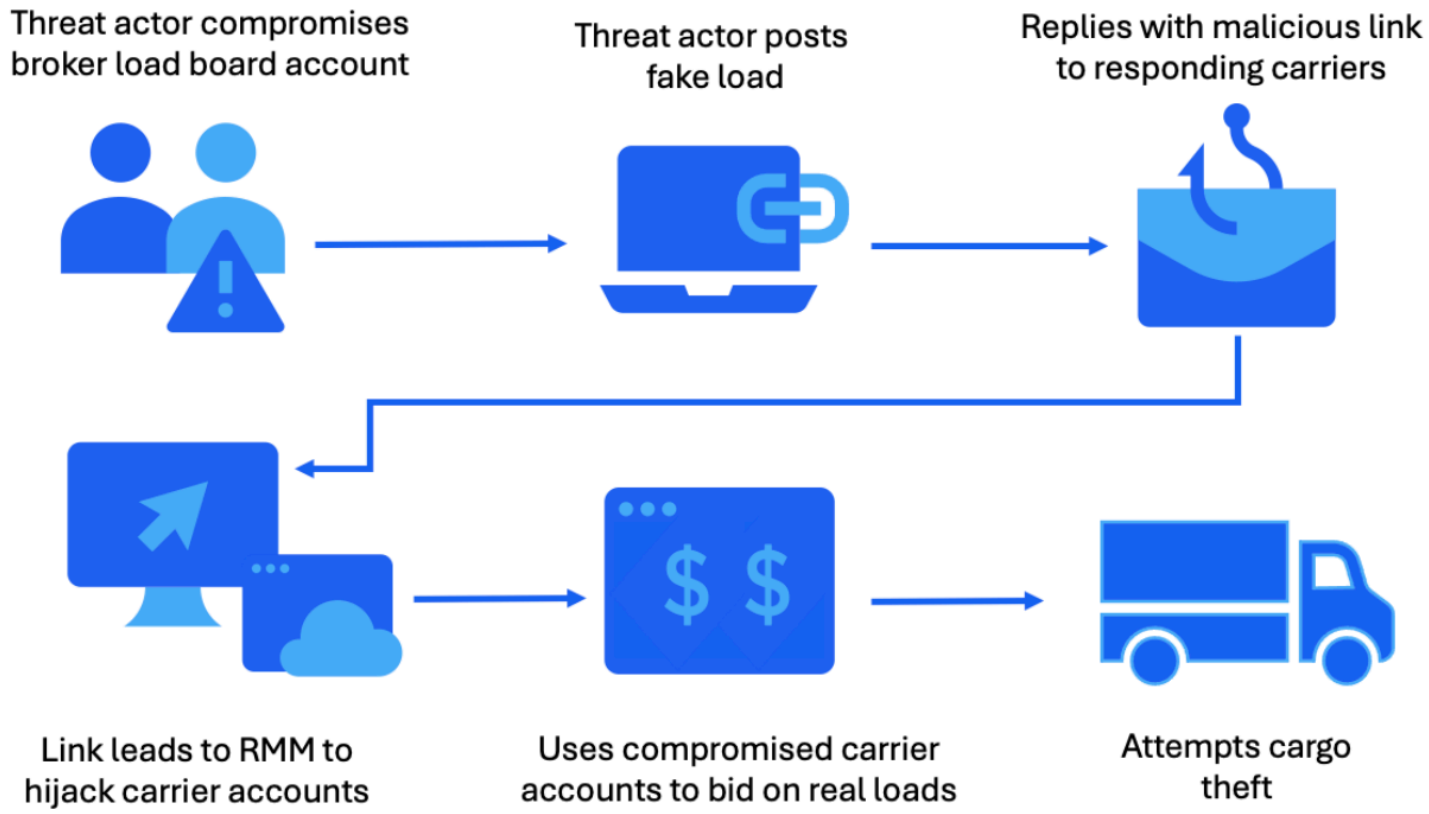

Figure 1. *Attack flow.*

Campaign details

The threat cluster engaged in suspected cargo theft has been active since at least June 2025, though evidence suggests the group's campaigns began as early as January. The actor has delivered a range of RMM tools (or in some cases remote access software), including ScreenConnect, SimpleHelp, PDQ Connect, Fleetdeck, N-able and LogMeIn Resolve. These RMMs/RAS are often used in tandem; for example, PDQ Connect has been observed downloading and installing both ScreenConnect and SimpleHelp. Once initial access is established, the threat actor conducts system and network reconnaissance and deploys credential harvesting tools such as

WebBrowserPassView. This activity indicates a broader effort to compromise accounts and deepen access within targeted environments.

Researchers have identified related network infrastructure and similar tactics, techniques, and procedures (TTPs) in campaigns delivering NetSupport and ScreenConnect going back to January 2025, suggesting a longer operational timeline. Separately, from 2024 through March 2025, Proofpoint also tracked a threat actor targeting ground transportation organizations distributing DanaBot, NetSupport, Lumma Stealer, and StealC, which we previously reported on. It is possible these clusters of activity are all related; however, we cannot attribute this with high confidence. All appear to have knowledge about the software, services, and policies around how the cargo supply chain operates. Regardless of the ultimate payload, stealers and RMMs serve the same purpose: remotely access the target to steal information. However, using RMM tools can enable threat actors to fly further under the radar. Threat actors can create and distribute attacker-owned remote monitoring tools, and because they are often used as legitimate pieces of software, end users might be less suspicious of installing RMMs than other remote access trojans. Additionally, such tooling may evade anti-virus or network detections because the installers are often signed, legitimate payloads distributed maliciously. Cargo theft actors using RMMs aligns with an overall shift in the cybercrime landscape where threat actors increasingly are adopting RMMs as a first stage payload.

In just the last two months, Proofpoint has observed nearly two dozen campaigns, with volumes ranging from less than 10 to over 1,000 messages per campaign.

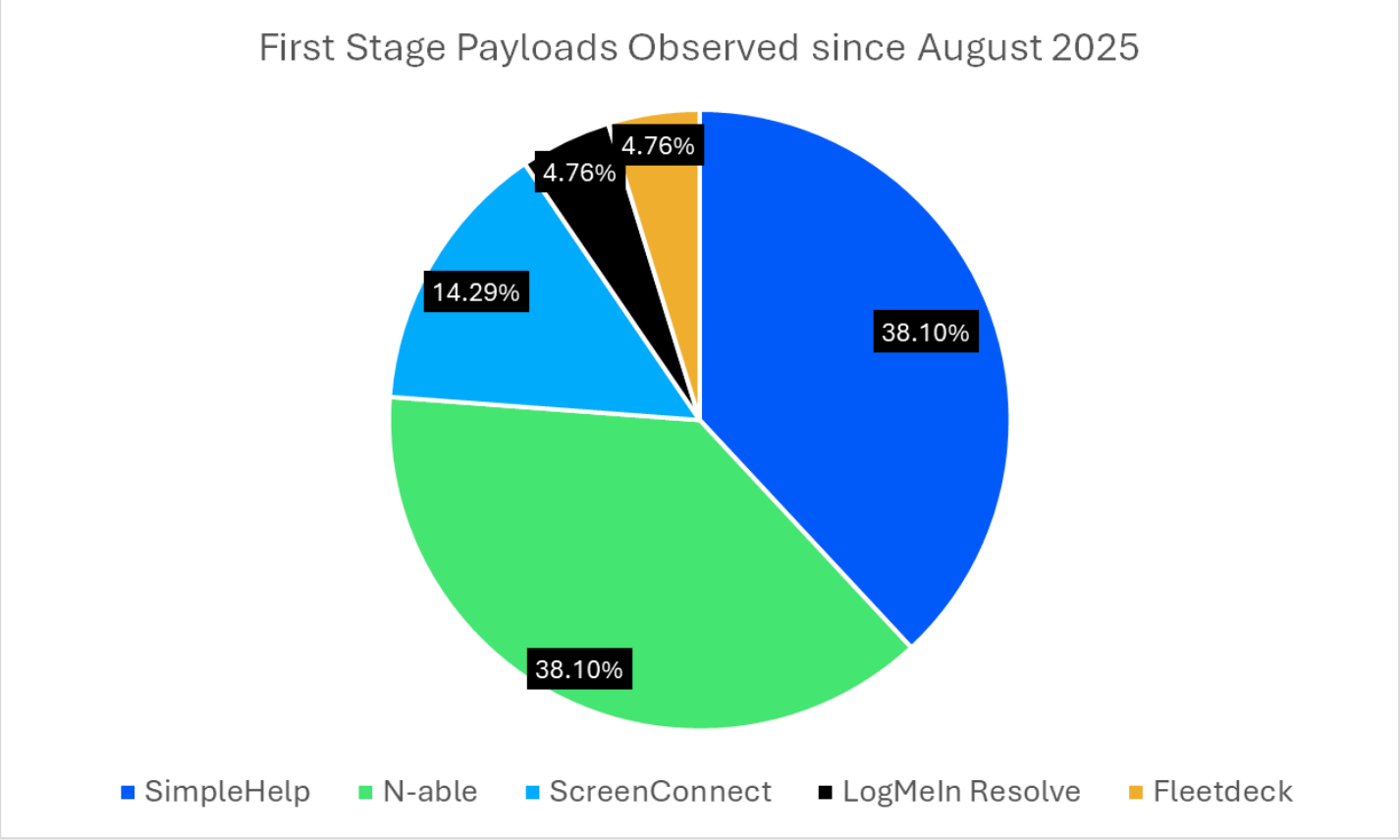

Figure 2. *Most frequently observed first-stage payloads targeting surface transportation since August 2025.*

The threat cluster has employed three tactics to deliver RMM tools:

- **Compromising load boards.** The actor posts fraudulent freight listings using compromised accounts on load boards and then sends emails containing malicious URLs to carriers who inquire about the loads. This tactic exploits the trust and urgency inherent in freight negotiations (see Figure 3).
- **Email thread hijacking.** Using compromised email accounts, the threat actors inject malicious content and URLs into existing conversations (see Figure 4).
- **Direct targeting via email campaigns.** The cluster has launched direct email campaigns against larger entities, including asset-based carriers, freight brokerage firms, and integrated supply chain providers. Gaining access to these entities may allow the actors to identify high-value freight loads or uncover other opportunities to further their objectives—such as posting fraudulent loads on load boards (see Figure 5).

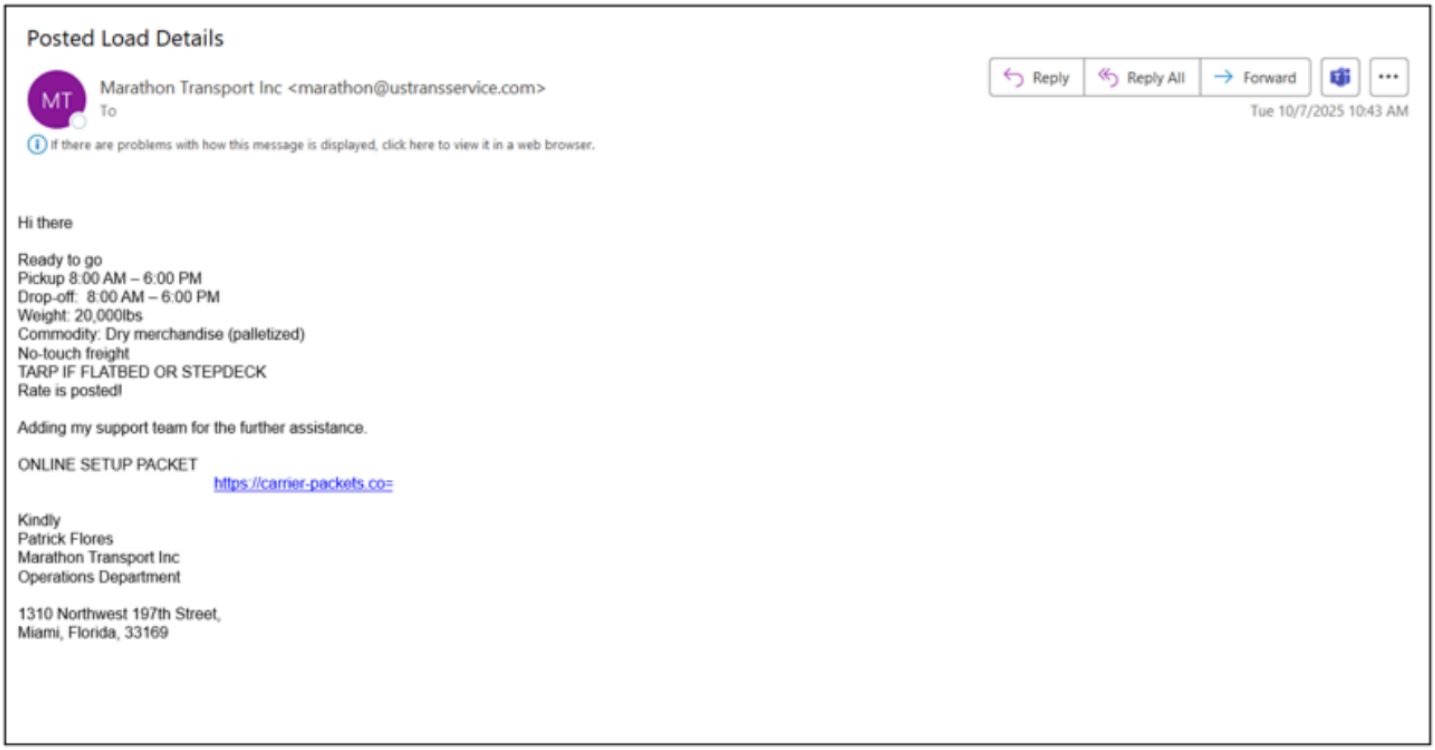

Figure 3. *Email sent to a carrier responding to a fraudulent load posted on a load board.*

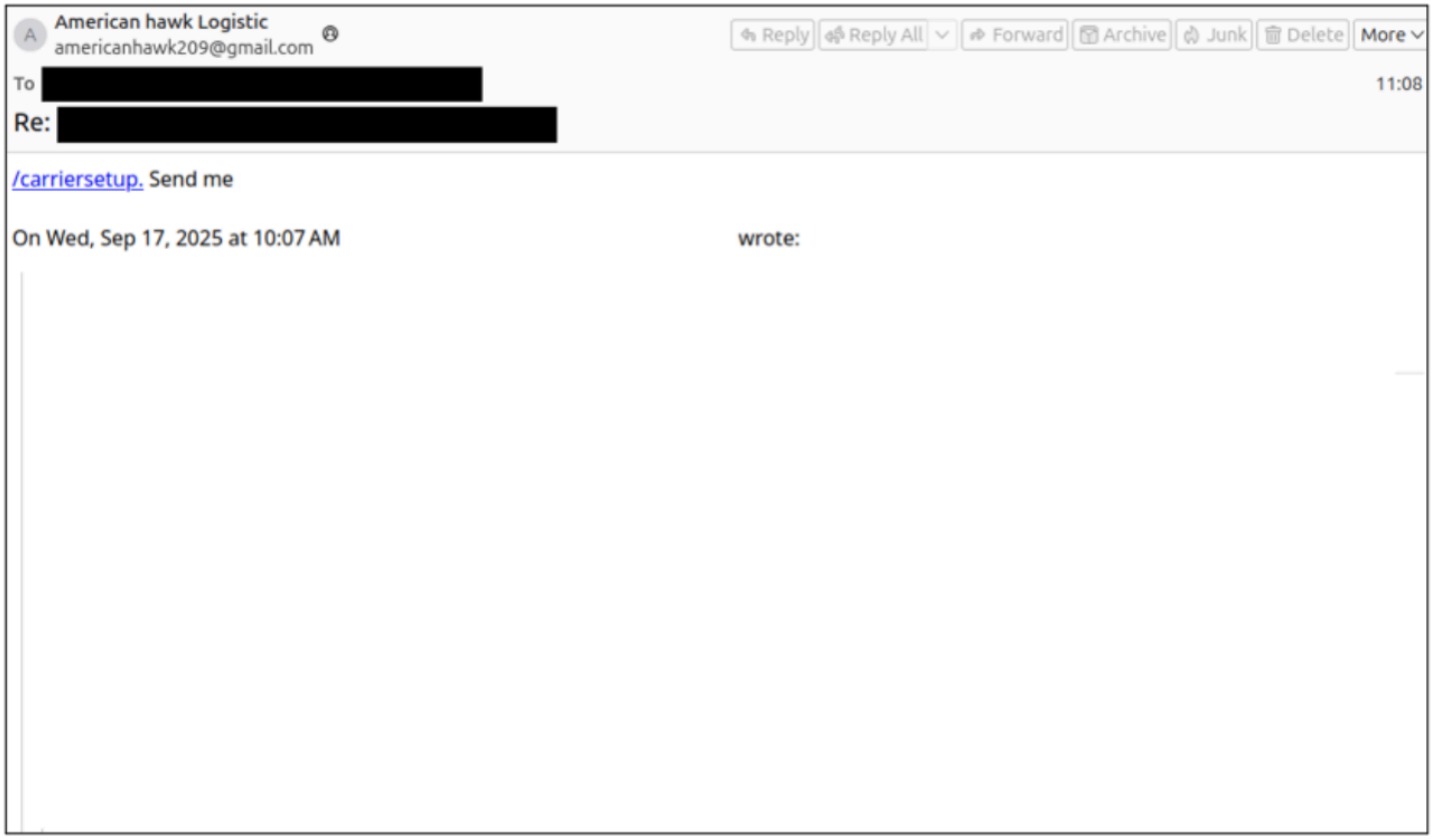

Figure 4. *Threat actor using a compromised email account and inserting a malicious link into an ongoing conversation.*

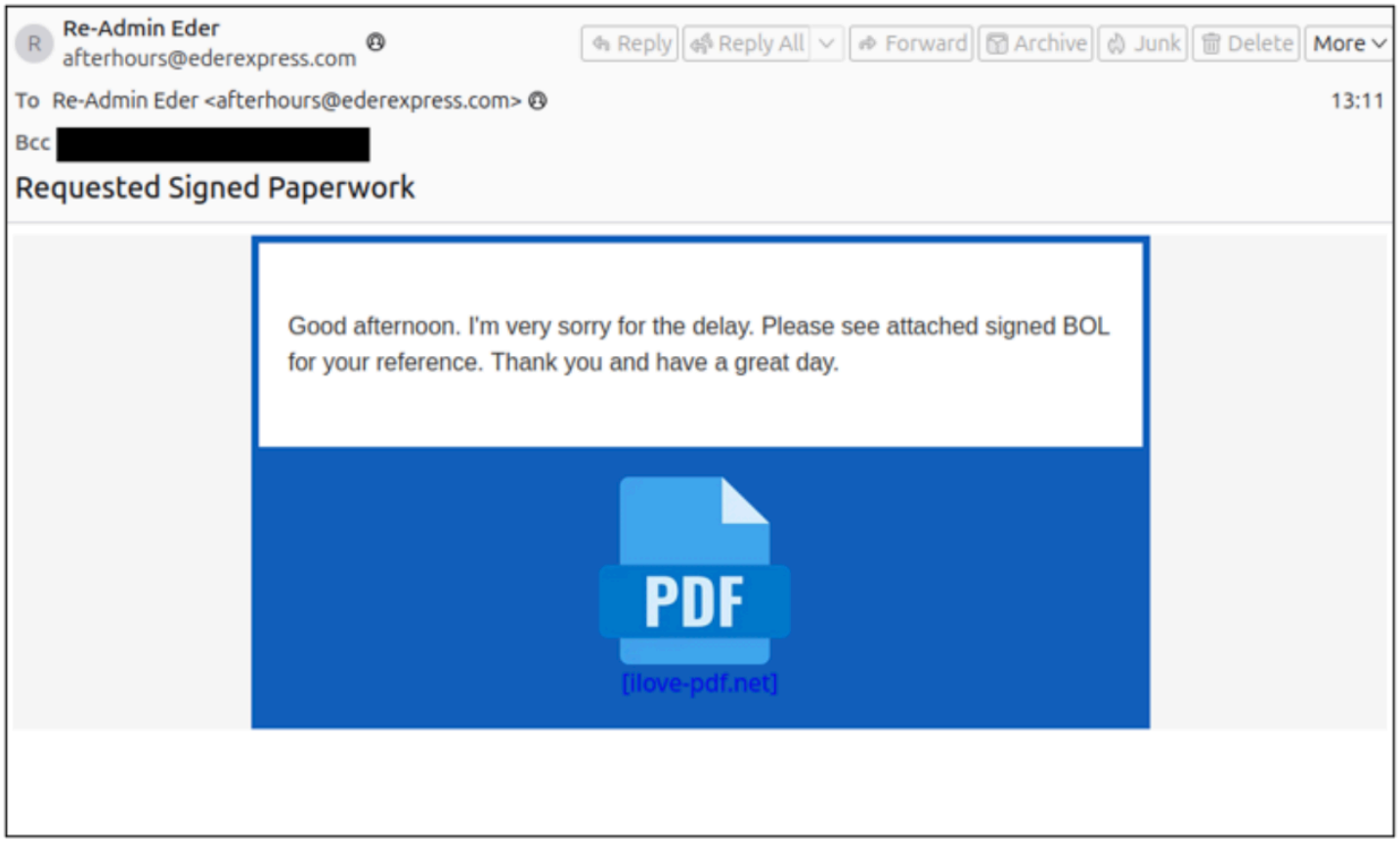

Figure 5. *Direct email sent to hundreds of organizations in the ground transportation industry.*

Typically, emails contain URLs that lead to an executable (.exe) or an MSI (.msi) file. When clicked, these files install an RMM tool, granting the threat actor full control of the compromised machine. In some cases, the threat actor will create domains and landing pages that impersonate legitimate brands or generic transportation terms to further the believability of the social engineering.

Based on campaigns observed by Proofpoint, the threat actor does not appear to attack specific companies, and targets range from small, family-owned businesses to large transport firms as described above. The threat actor appears to be opportunistic about the carriers that it targets and will likely attempt to compromise any carrier who responds to the fake load posting. Once a threat actor has compromised a carrier, they probably will use their knowledge of the industry and any insider information derived from other compromises to identify and bid on loads that are likely to be profitable if stolen.

While investigating the objectives of this threat cluster, Proofpoint researchers found multiple public discussions on social media websites that aligned precisely with the phishing and account takeover activity we had observed by this actor. One public Reddit post shared an experience in which the attacker compromised the company via RMM delivery, deleted existing bookings and blocked dispatcher notifications, added their own device to the dispatcher's phone extension, booked loads under the compromised carrier's name, and coordinated the transport. According to the post, the initial compromise was a "nextgen.Carrierbrokeragreement type of link" which notably aligns with a payload URL from this cluster that Proofpoint researchers observed active in July, likely distributing ScreenConnect: hxxp://nextgen1[.]net/carrier.broker.agreement[.]html.

Best practices

Organizations operating in the surface transportation industry or other industries at risk of cargo theft may benefit from reviewing the National Motor Freight Traffic Association Cargo Crime Reduction Framework.

To defend against RMM abuse, Proofpoint recommends the following:

- 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 – including using the Emerging Threats ruleset – and use endpoint protection. This can alert on any network activity to RMM servers.
- Do not download and install executable files (.exe or .msi) 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.

Conclusion

According to NICB, cargo theft losses increased 27 percent in 2024, and losses are expected to increase another 22 percent in 2025. Cargo theft is a profitable criminal enterprise, and based on Proofpoint data, cybercriminals are increasingly targeting surface transportation entities to steal real, physical goods. Proofpoint has observed nearly two dozen campaigns since August 2025 targeting such entities to deliver RMMs. Public discussion and reporting on cyber-enabled cargo theft suggests the problem is widespread, impacting organizations nationwide, and only increasing in scope and spread. Based on the growth of this activity in email threat data between 2024 and 2025,

Proofpoint assesses this threat will continue to increase. Organizations should be aware of the cyber-enabled tactics and payloads used by cargo theft criminals, and implement cybersecurity measures to prevent successful exploitation.

Proofpoint would like to thank our colleagues at ConnectWise ScreenConnect, Red Canary, and the DFIR Report for collaborating on information sharing related to this activity.

Example Emerging Threats signatures

2837962 – ScreenConnect - Establish Connection Attempt

2050021 – Observed DNS Query to Known ScreenConnect/ConnectWise Remote Desktop Service Domain

2054938 – PDQ Remote Management Agent Checkin

2065069 – Observed RMM Domain in DNS Lookup (n-able .com)

2065076 – Observed RMM Domain in DNS Lookup (remote .management)

2049863 – simplehelp Remote Access Software Activity

2047669 – fleetdeck Remote Management Software Domain in DNS Lookup (fleetdeck .io)

2061989 – Observed DNS Query to RMM Domain (gotoresolve .com)

Select IOCs

Indicator	Description	First Seen
carrier-packets[.]net	Payload Staging Domain	October 2025
claimeprogressive[.]com	Payload Staging Domain	October 2025
confirmation-rate[.]com	Payload Staging Domain	October 2025
wjwrateconfirmation[.]com	Payload Staging Domain	October 2025
rateconfirm[.]net	Payload Staging Domain	October 2025
ilove-pdf[.]net	Payload Staging Domain	October 2025
vehicle-release[.]com	Payload Staging Domain	October 2025

carrierpack[.]net	Payload Staging Domain	October 2025
car-hauling[.]com	Payload Staging Domain	October 2025
carrier-packets[.]com	Payload Staging Domain	October 2025
i-lovepdf[.]net	Payload Staging Domain	September 2025
fleetcarrier[.]net	Payload Staging Domain	September 2025
scarrierpack[.]com	Payload Staging Domain	September 2025
carrieragreements[.]com	Payload Staging Domain	September 2025
brokeragepacket[.]com	Payload Staging Domain	September 2025
brokerpackets[.]com	Payload Staging Domain	September 2025
centraldispach[.]net	Payload Staging Domain	September 2025
carriersetup[.]net	Payload Staging Domain	September 2025
brokercarriersetup[.]com	Payload Staging Domain	September 2025
carrierpacket[.]online	Payload Staging Domain	September 2025
billpay-info[.]com	Payload Staging Domain	August 2025
nextgen223[.]com	Payload Staging Domain	August 2025
fleetgo0[.]com	Payload Staging Domain	July 2025

nextgen1[.]net	Payload Staging Domain	July 2025
nextgen01[.]net	Payload Staging Domain	June 2025
ratecnf[.]com	Payload Staging Domain	June 2025
ratecnf[.]net	Payload Staging Domain	June 2025
dwssa[.]top	ScreenConnect C2	June 2025
ggdt35[.]anondns[.]net	ScreenConnect C2	August 2025
qtq2haw[.]anondns[.]net	ScreenConnect C2	September 2025
officews101[.]com	ScreenConnect C2	September 2025
instance-hirb01-relay[.]screenconnect[.]com	ScreenConnect C2	September 2025
185[.]80[.]234[.]36	SimpleHelp C2	August 2025
147[.]45[.]218[.]66	SimpleHelp C2	September 2025
70983c62244c235d766cc9ac1641e3fb631744bc68307734631af8d766f25acf	LogMeIn SHA256 Hash	October 2025
4e6f65d47a4d7a7a03125322e3cddeeb3165dd872daf55cd078ee2204336789c	N-able SHA256 Hash	October 2025
cf0cee4a57aaf725341d760883d5dfb71bb83d1b3a283b54161403099b8676ec	ScreenConnect SHA256 Hash	October 2025
913375a20d7250f36af1c8e1322d1541c9582aa81b9e23ecad700fb280ef0d8c	Fleetdeck SHA256 Hash	September 2025
8a00b3b3fd3a8f6b3ec213ae2ae4efd41dd5738b992560010ab0367fee72cd2a	SimpleHelp SHA256 Hash	September 2025
559618e2ffbd3b8b849a6ad0d73a5630f87033976c7adccbd80c41c0b2312765	PDQ Connect SHA256 Hash	September 2025

Previous Blog Post

Subscribe to the Proofpoint Blog