Stealthy Phishing Campaign Targets Global Transport and Logistics Sectors: New Threat Intel and Indicators

Source: [Security Brief: Actor Uses Compromised Accounts, Customized Social Engineering to Target Transport and Logistics Firms with Malware | Proofpoint US]

1. Relevance to the Community: This phishing campaign specifically targets the *transportation and logistics sector*, an industry that frequently engages in high-value financial transactions. Companies in this sector, which include partners, suppliers, and customers globally, are vulnerable to this type of threat due to the volume and nature of their financial communications.

Impact on the Community: Organizations in this sector risk financial losses, operational disruptions, and potential data breaches, particularly through compromised email communications used for transactions.

---

2. Threat Identification and Context:

- **Threat Actor:** The exact threat actor remains unidentified but is likely financially motivated, given the sector's vulnerability to fraud and high-value transactions.
- **Motivation:** Financial gain through phishing tactics aimed at compromising sensitive business communications.
- **TTPs:**
    - *Use of compromised legitimate email accounts.*
    - *Injection of malicious content into existing email threads.*
    - *Delivery of malware via Google Drive URLs and .URL files.*
    - *Use of "ClickFix" technique with Base64 encoded PowerShell scripts*.
    - Mapped to MITRE ATT&CK:
        - Initial Access: Phishing (T1566)
        - Execution: User Execution (T1204)
        - Persistence: Valid Accounts (T1078)
        - Command and Control: Application Layer Protocol (T1071)

---

3. Indicators of Compromise (IOCs):

The trail left behind by this campaign began to unfold like pieces of a larger puzzle. Each indicator represented a fragment of the attackers' meticulous planning, and understanding these fragments would help organizations mount a strong defense.

Indicator	Description	First Observed
199d6f70f10c259ee09e99e6f1d7f127426999a0ed20536f2662842cd12b5431	SHA256 .URL file	2024-05-22

Indicator	Description	First Observed
ac49ff207e319f79bbd9c80d044d621920d1340f4c53e5e4da39b2a0c758634e	SHA256 .URL file	2024-07-01
e7526dadae6b589b6a31f1f7e2e528ed1c9edd9f3d1ca88f0ece0dee349d3842	SHA256 .URL file	2024-07-12
e5ed1a273faf5174dbd8db9d6d3657b81dc2cbc2e0af28cfe76f41c3d2f2fc37	SHA256 .URL file	2024-07-24
f8b12e6d02ea5914e01f95b5665b3a735acfbb9ee6ae27b004af37547bc11e7f	SHA256 .URL file	2024-08-05
0931217eb498b677e2558fd30d92169cc824914c2df68cfbcff4f642600e2cc2	SHA256 .URL file	2024-08-24
582c69b52d68b513f2a137bbf14704df7d787b06752333fc31066669cd663d04	SHA256 .URL file	2024-09-06

The digital fingerprints of the attackers were also visible in the URLs they used to lure unsuspecting victims:

URL	Description	First Observed
hxxp://89[.]23[.]98[.]98/file/14242.exe	Payload	2024-05-22
hxxp://89[.]23[.]98[.]98/file/ratecon.exe	Payload	2024-07-01
hxxp://89[.]23[.]98[.]98/file/rate_confirmation.vbs	Payload	2024-07-12
hxxp://89[.]23[.]98[.]98/file/Rateconfirm.exe	Payload	2024-07-24
hxxp://89[.]23[.]98[.]98/file/carrier.exe	Payload	2024-08-05
hxxp://185[.]217[.]197[.]84/file/remittance.exe	Payload	2024-08-24
hxxp://185[.]217[.]197[.]84/file/information_package.exe	Payload	2024-09-06

But the campaign didn’t stop there. As investigators dove deeper, they unearthed more evidence of malicious URLs and files, each carrying payloads that varied in purpose—from stealing credentials to executing more nefarious operations:

URL	Description	First Observed
hxxps://live-samsaratrucking[.]com/true-tracking-32934.html	ClickFix	2024-08-19

URL	Description	First Observed
hxxp://ambcrrm[.]com/	ClickFix	2024-09-03
hxxps://ambccm[.]com/Astra/index.html	ClickFix	2024-09-10
hxxps://idessit[.]com/fn.msi	Danabot Payload	2024-08-19
hxxps://ambccm[.]com/3.msi	Danabot Payload	2024-09-05

Malware Hashes and Payloads: With their fingerprints becoming clearer, the attackers' weaponry also became more apparent. These payloads, hidden within files bearing innocent names, were part of a larger scheme involving various strains of malware.

SHA256	File Name	Malware Description	First Observed
957fe77d04e04ff69fdaff8ef60ac0de24c9eb5e6186b3187460eac6be561f5d	14242.exe	Suspected Lumma	2024-06-14
2436fe37d25712b68b2e1a9805825bcf5073efb91588c1b5193ba446d1edd319	rate_confirmation.vbs	Lumma	2024-07-12
8fe96fb9d820db0072fe0423c13d2d05f81a9cf0fdd6f4e2ee78dc4ca1d37618	ratecon.exe	StealC/NetSupport	2024-07-24
cdf160c63f61ae834670fdaf040411511dc2fc0246292603e7aa8cd742d78013	Rateconfirm.exe	StealC	2024-07-25
d45b6b04ac18ef566ac0ecdaf6a1f73d1c3164a845b83e0899c66c608154b93d	carrier.exe	Arechclient2	2024-08-05
fddacfe9e490250e62f7f30b944fcbe122e87547d01c4a906401049304c395f7	fn.msi	Danabot	2024-08-19
1a002631b9b2e685aeb51e8b6f4409daf9bc0159cfd54ef9ad3ba69d651ac2a3	information_package.exe	Lumma Stealer	2024-09-06
b94bcdf5d6b9f1eb6abe97090993e8c4f66b514dd9c51193f16673e842253d86	information_package.exe	StealC/NetSupport	2024-09-10

The indicators formed a clear path to the attackers' tactics—one rooted in persistence and evolving sophistication. By understanding these IOCs, organizations in the logistics and transportation sectors can better fortify their defenses and stay one step ahead of this stealthy threat.

---

4. Vulnerability and Exploit Information:

- **No specific CVEs** are mentioned in relation to this phishing campaign, but organizations are advised to ensure email protection systems are updated and phishing awareness training is provided to employees.

---

5. Attack Patterns and TTPs:

- The campaign uses social engineering to trick victims into clicking on links that lead to credential-harvesting websites. Attackers focus on exploiting weak email security defenses.
- **Detection Techniques:**
  - Implementing SPF/DKIM/DMARC policies to verify sender legitimacy.
  - Anomalous DNS traffic detection using SIEM solutions to monitor malicious domain resolutions.

---

6. Incident Reporting and Case Studies:

- **No specific case studies** were provided in the article, but similar phishing campaigns have been used in past incidents, such as the "Business Email Compromise" attacks, where similar tactics were employed to divert financial transactions.

---

7. Mitigation and Defense Recommendations:

- **Email Security Solutions**: Enforce strict filtering for phishing emails and implement multi-factor authentication (MFA) on all financial transaction systems.
- **User Awareness**: Regular phishing training and simulations to improve employees' ability to identify suspicious emails.
- **Endpoint Detection and Response (EDR)**: Deploy to monitor for unusual activity following email clicks or domain access.

---

8. Threat Actor Attribution and Profiling:

- **No clear attribution** is provided, but this type of campaign aligns with financially motivated cybercriminal groups that frequently target high-transaction industries.

---

9. Real-Time Updates and Alerts:

- The phishing campaign is active as of September 26, 2024, and companies in the logistics sector are being actively targeted. Immediate action is recommended.

---

10. Collaborative Tools and Resources:

- No specific open-source tools were mentioned. However, YARA rules or SIEM detection rules can be created based on the provided IOCs to track malicious domains or email headers in enterprise environments.

---

11. Vulnerability and Threat Intelligence Correlation:

- The phishing campaign correlates with tactics observed in broader financial phishing campaigns but does not link to specific known vulnerabilities (e.g., CVEs).

---

12. Legal and Regulatory Considerations (Global and Canada-specific):

- **GDPR and Data Breaches**: If customer or business partner data is compromised in phishing attacks, organizations may face legal consequences under data protection laws like the GDPR.

---

13. Continuous Monitoring and Feedback Loop:

- Continuous monitoring of email gateways and network traffic is crucial. Regular updates from cybersecurity vendors on threat intelligence feeds should be integrated into SIEM tools.

---

14. Anonymity and Data Sensitivity:

- No identifiable data handling or privacy concerns were raised in the article. Ensure that any shared sensitive business communication remains anonymous when reporting incidents to authorities.

---

15. Strategic Threat Trends and Predictions:

- The increasing sophistication of phishing campaigns targeting specific sectors, particularly those handling large financial transactions, suggests this will remain a preferred vector for cybercriminals.

Summary: The phishing campaign actively targeting transport and logistics companies exploits weak email defenses and operational dependencies on digital communications. Organizations within this sector should prioritize strengthening email security, monitoring malicious domains, and educating employees on phishing tactics to mitigate these risks effectively.