**D**IETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
**N**ationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
**I**nternet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

**Anleitung Phishing Beispiele**

# Soziale Netzwerke werden höchstwahrscheinlich von kriminellen Gruppen nachgeahmt, wobei LinkedIn jetzt für die Hälfte aller Phishing-Versuche weltweit verantwortlich ist

## *Check Point Research veröffentlicht seinen Q1 Brand Phishing Report und hebt die Marken hervor, die Hacker am häufigsten imitieren, um Menschen dazu zu bringen, ihre persönlichen Daten preiszugeben*

Unser aktueller Marken-Phishing-Bericht für das 1. Quartal 2022 hebt die Marken hervor, die im Januar, Februar und März 2022 am häufigsten von Kriminellen bei ihren Versuchen nachgeahmt wurden, persönliche Daten oder Zahlungsinformationen von Einzelpersonen zu stehlen.

Social-Media-Netzwerke haben inzwischen Schifffahrt, Einzelhandel und Technologie als die Kategorie überholt, die am ehesten von kriminellen Gruppen angegriffen wird. Bisher war LinkedIn in diesem Jahr mit mehr als der Hälfte (52 %) aller Phishing-bezogenen Angriffe weltweit in Verbindung gebracht worden, was das erste Mal war, dass das Social-Media-Netzwerk die Spitze der Rangliste erreichte. Dies stellt eine dramatische Steigerung von 44 % gegenüber dem Vorquartal dar, als LinkedIn auf dem fünften Platz lag und nur 8 % der Phishing-Versuche zu verzeichnen waren. LinkedIn hat jetzt DHL als die am stärksten angegriffene Marke überholt, die nun auf den zweiten Platz gefallen ist und im Quartal für 14 % aller Phishing-Versuche verantwortlich war.

Unser jüngster Bericht hebt einen aufkommenden Trend zu Bedrohungsakteuren hervor, die soziale Netzwerke nutzen, die jetzt die Kategorie Nummer eins sind, die vor Reedereien und Technologiegiganten wie Google, Microsoft und Apple angegriffen wird. Neben LinkedIn, das mit großem Abstand die am meisten angegriffene Marke ist, behauptete WhatsApp seine Position unter den Top Ten und war für fast 1 von 20 Phishing-Angriffen weltweit verantwortlich. Der Bericht hebt ein besonderes Beispiel hervor, bei dem LinkedIn-Benutzer über eine offiziell aussehende E-Mail kontaktiert werden, um sie dazu zu verleiten, auf einen bösartigen Link zu klicken. Dort würden die Benutzer erneut aufgefordert, sich über ein gefälschtes Portal anzumelden, wo ihre Anmeldeinformationen gesammelt würden.

Die Schifffahrt ist jetzt die am zweithäufigsten angegriffene Kategorie, wobei Bedrohungsakteure weiterhin den allgemeinen Anstieg des E-Commerce nutzen, indem sie Verbraucher und Schifffahrtsunternehmen direkt ins Visier nehmen. DHL steht hinter LinkedIn

an zweiter Stelle und ist für 14 % der Phishing-Versuche verantwortlich; FedEx ist vom siebten auf den fünften Platz vorgerückt und macht nun 6 % aller Phishing-Versuche aus; und Maersk und AliExpress haben es zum ersten Mal in die Top-Ten-Liste geschafft. Unser Bericht hebt eine bestimmte Phishing-Strategie hervor, bei der E-Mails der Marke Maersk verwendet wurden, um das Herunterladen gefälschter Transportdokumente zu fördern und Arbeitsstationen mit Malware zu infizieren.

Bei einem Marken-Phishing-Angriff versuchen Kriminelle, die offizielle Website einer bekannten Marke zu imitieren, indem sie einen ähnlichen Domainnamen oder eine ähnliche URL und ein ähnliches Webseitendesign wie die echte Website verwenden. Der Link zu der gefälschten Website kann per E-Mail oder SMS an Zielpersonen gesendet, ein Benutzer beim Surfen im Internet umgeleitet oder von einer betrügerischen mobilen Anwendung ausgelöst werden. Die gefälschte Website enthält oft ein Formular, das darauf abzielt, Anmeldeinformationen, Zahlungsdetails oder andere persönliche Informationen von Benutzern zu stehlen.

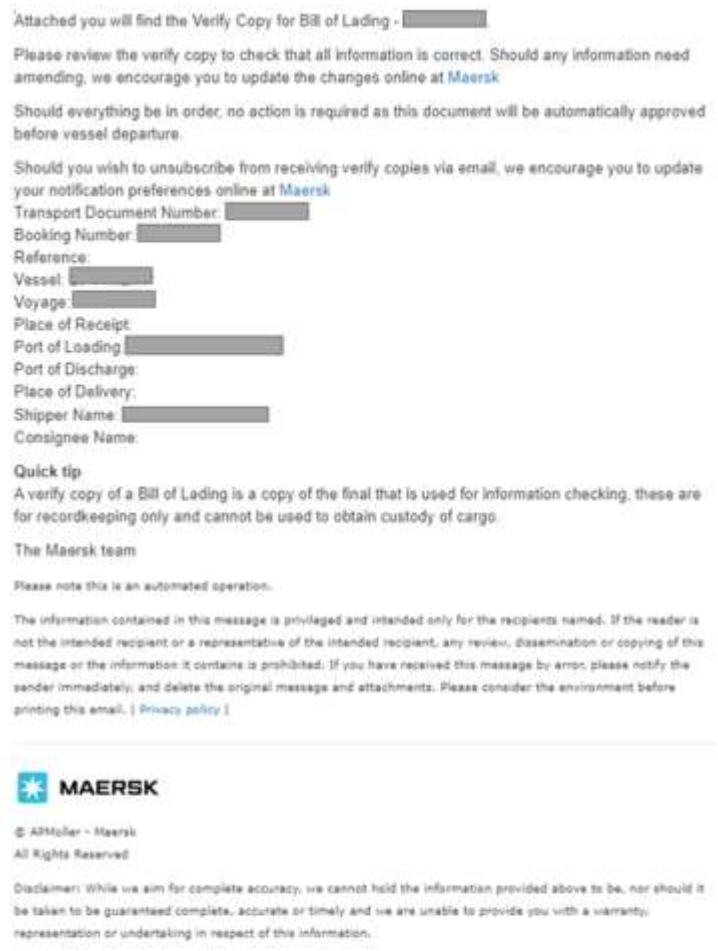
## Top-Phishing-Marken im ersten Quartal 2022

Unten sind die Top-Marken nach ihrem Gesamterscheinungsbild bei Marken-Phishing-Versuchen geordnet:

1. LinkedIn (im Zusammenhang mit 52 % aller Phishing-Angriffe weltweit)
2. DHL (14%)
3. Google (7 %)
4. Microsoft (6 %)
5. Fedex (6%)
6. Whatsapp (4%)
7. Amazonas (2%)
8. Maersk (1%)
9. AliExpress (0,8 %)
10. Apfel (0,8%)

## Maersk-Phishing-E-Mail – Malware-Beispiel

Im ersten Quartal 2022 beobachteten wir eine böswillige Phishing-E-Mail, die das Branding von Maersk verwendete und versuchte, den Agent Tesla RAT (Remote Access Trojan) auf den Computer des Benutzers herunterzuladen. Die E-Mail (siehe Abbildung 1), die von einer Webmail-Adresse gesendet und so getäuscht wurde, dass sie so aussah, als ob sie von „Maersk Notification ( service@maersk [.]com)“ gesendet worden wäre, enthielt den Betreff „Maersk : Verify Copy for Bill of Ladung XXXXXXXXX zur Verifizierung bereit.“ Der Inhalt forderte zum Herunterladen einer Excel-Datei „Transport-Document“ auf, die dazu führen würde, dass das System mit Agent Tesla infiziert wird.



Attached you will find the Verify Copy for Bill of Lading - [redacted]

Please review the verify copy to check that all information is correct. Should any information need amending, we encourage you to update the changes online at Maersk

Should everything be in order, no action is required as this document will be automatically approved before vessel departure.

Should you wish to unsubscribe from receiving verify copies via email, we encourage you to update your notification preferences online at Maersk

Transport Document Number: [redacted]
Booking Number: [redacted]
Reference:
Vessel: [redacted]
Voyage: [redacted]
Place of Receipt:
Port of Loading: [redacted]
Port of Discharge:
Place of Delivery:
Shipper Name: [redacted]
Consignee Name:

**Quick tip**
A verify copy of a Bill of Lading is a copy of the final that is used for information checking, these are for recordkeeping only and cannot be used to obtain custody of cargo.

The Maersk team

Please note this is an automated operation.

The information contained in this message is privileged and intended only for the recipients named. If the reader is not the intended recipient or a representative of the intended recipient, any review, dissemination or copying of this message or the information it contains is prohibited. If you have received this message by error, please notify the sender immediately, and delete the original message and attachments. Please consider the environment before printing this email. | Privacy policy |

MAERSK

© AP Moller - Maersk
All Rights Reserved

Disclaimer: While we aim for complete accuracy, we cannot hold the information provided above to be, nor should it be taken to be guaranteed complete, accurate or timely and we are unable to provide you with a warranty, representation or undertaking in respect of this information.

*Figure 1: The malicious email which was sent with the subject* ***"Maersk : Verify Copy for Bill of Lading XXXXXXXX ready for verification."***

## LinkedIn-Phishing-E-Mail – Beispiel für Kontodiebstahl

In dieser Phishing-E-Mail sehen wir einen Versuch, die LinkedIn-Kontoinformationen eines Benutzers zu stehlen. Die E-Mail (siehe Abbildung 1), die von der E-Mail-Adresse „LinkedIn ( smtpfox-6qhrg@tavic [.]com[.]mx)" gesendet wurde, enthielt den Betreff „M&R Trading Co.,Ltd 合作采购订单＃XXXXXXXX". Der Angreifer versuchte, das Opfer dazu zu verleiten, auf einen schädlichen Link zu klicken, der den Benutzer auf eine betrügerische LinkedIn-Anmeldeseite weiterleitet (siehe Abbildung 2). In dem schädlichen Link (https://carriermasr.com/public/linkedIn[.]com/linkedIn[.]com/login[.]php) musste der Benutzer seinen Benutzernamen und sein Passwort eingeben.

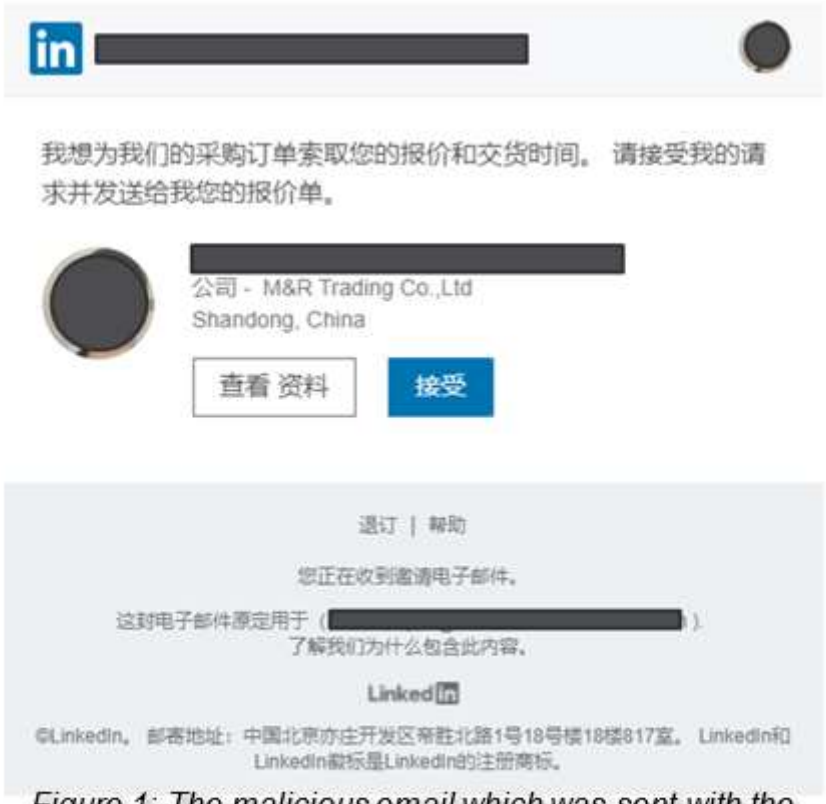



*Figure 1: The malicious email which was sent with the subject "**M&R Trading Co.,Ltd 合作采购订单 # XXXXXXXX**"*

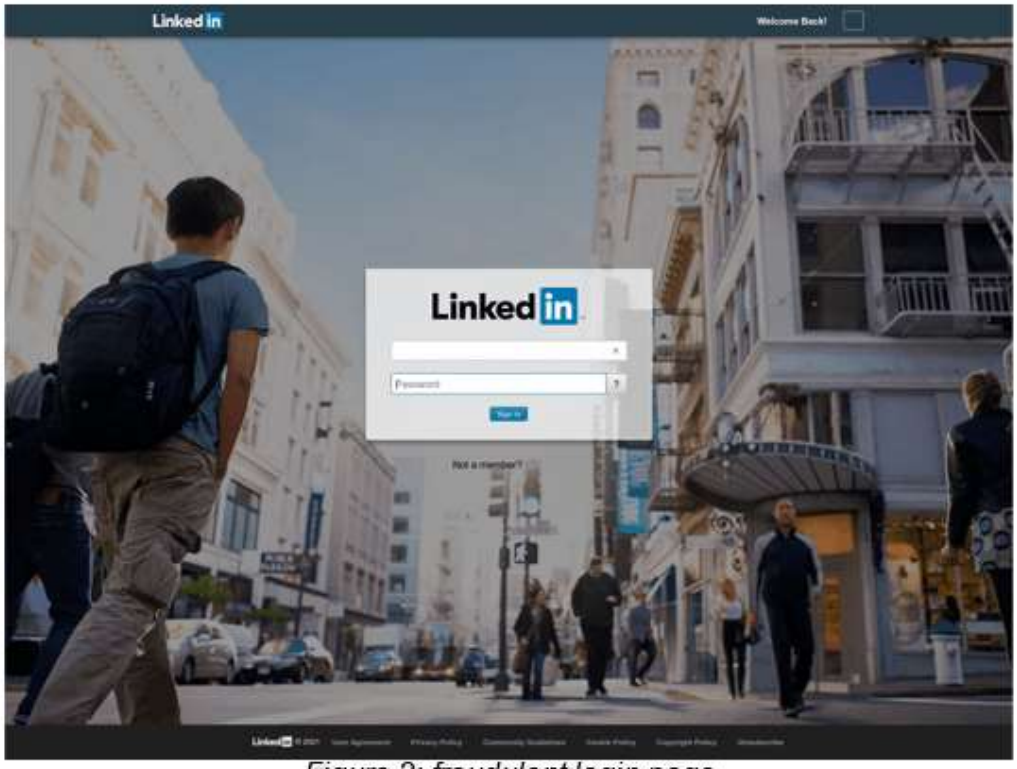



*Figure 2: fraudulent login page*
***https://carriermasr.com/public/linkedIn[.]com/linkedIn[.]com/login[.]php***

Wie immer empfehlen wir Benutzern, bei der Preisgabe persönlicher Daten und Zugangsdaten an Geschäftsanwendungen oder Websites vorsichtig zu sein und es sich zweimal zu überlegen, bevor sie E-Mail-Anhänge oder Links öffnen, insbesondere E-Mails, die vorgeben, von Unternehmen wie LinkedIn oder DHL zu stammen, wie sie es derzeit sind am ehesten imitiert.

Quelle: https://blog.checkpoint.com/2022/04/19/social-networks-most-likely-to-be-imitated-by-criminal-groups-with-linkedin-now-accounting-for-half-of-all-phishing-attempts-worldwide/