CYBERFORCE

THREAT BULLETIN

AUGUST 2025

EXPLOITATION OF MAIL DELIVERY FEATURE

OVERVIEW

A newly observed phishing technique is targeting Microsoft 365 organizations by spoofing emails to appear as though they come from the recipient themselves. This campaign exploits Microsoft's Direct Send feature and other mail delivery quirks to bypass traditional email security mechanisms.

Unlike typical impersonation or executive spoofing, this tactic leverages unauthenticated internal routing, trust in one's own email identity, and gaps in SPF/DKIM/DMARC enforcement to gain credibility and trick users into engaging with malicious content.

KEY OBSERVATIONS:

New Attack Patterns

Emails appear to originate from the recipient's own email address, exploiting trust and bypassing sender verification logic.

Abuse of Microsoft 365 Direct Send

Attackers use Microsoft's Direct Send service to route spoofed messages without needing authentication or account compromise.

Widespread Campaign

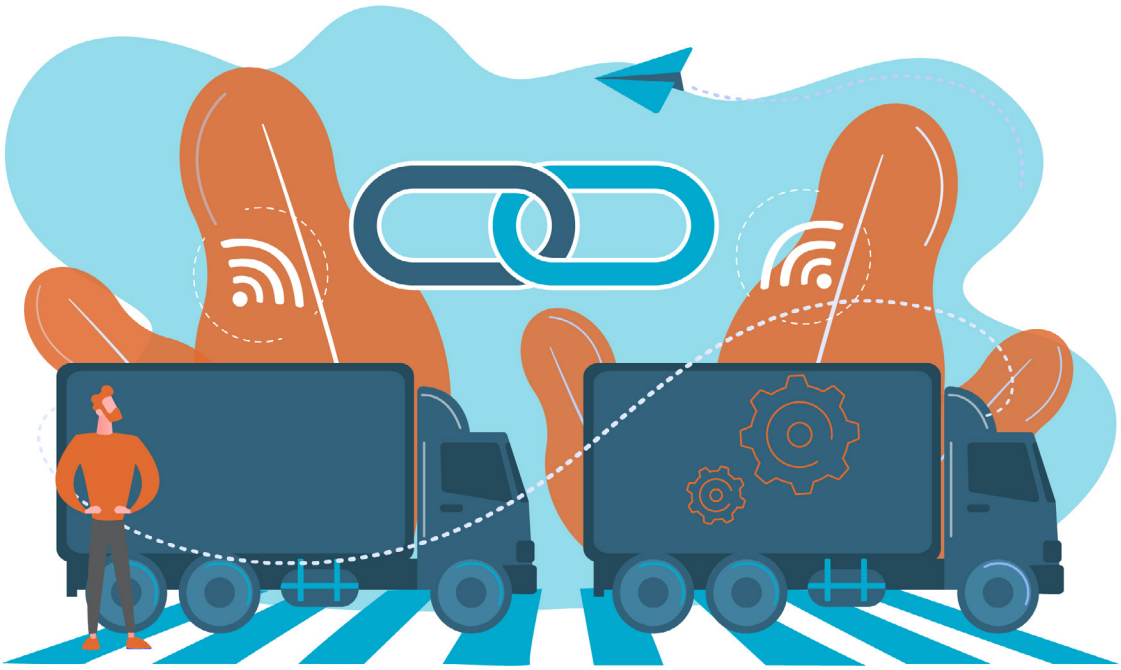
As reported by Varonis Threat Labs, the campaign has been active since May 2025, affecting over 70 US-based organizations. We expect this number to be much higher, as we have observed this activity in several participant environments in the past two months.

Other Exploits

- **Double-Bounce Loops:**
  Leverage SMTP bouncebacks to appear internal.
- **Forward-Based Spoofing:**
  Breaks email authentication via forwarding chains.

Authentication Limitations

SPF/DKIM/DMARC, while essential, are not foolproof against these internal-looking spoof attacks.



EXPLANATION:

01

Direct Send Exploit (Microsoft 365)

Microsoft allows devices like printers to send emails using Direct Send via predictable smart-host addresses. These require no authentication and are meant for internal use.

Attackers identify the organization's domain and construct emails using the Direct Send path to spoof internal addresses. Crucially, they can spoof the recipient's own address—making the email appear as though the recipient sent it to themselves.

02

Protocol Weaknesses & Email Trust

SMTP doesn't validate the "From" header against the sender's identity. As a result, attackers can forge headers to spoof any identity, including the target's. When no strong DMARC enforcement exists, these messages often pass basic email security filters.

03

Additional Tactics

Bounce Loops:
Spoofed messages sent to invalid addresses generate bouncebacks that appear to come from the user's own account.

Forwarding Chains:
Attackers exploit forwarding behavior to break authentication, allowing spoofing of well-known domains (even government and financial institutions).

MITIGATION & GUIDANCE:

Email Authentication & Policy Hardening

Enforce SPF, DKIM, and DMARC with strict policies (quarantine or reject).

Regularly audit your DMARC reports to identify spoofing attempts and misaligned sources.

Configure your domain to disallow ambiguous sources using DMARC "p=reject" once alignment is verified.

Restrict Use of Direct Send

Disable unauthenticated Direct Send where possible.

Only allow SMTP relay from known IP addresses or authenticated devices like printers or scanners.

Monitor traffic through smart-hosts for anomalies.

Implement Advanced Email Filtering

Deploy email gateways with forged-from detection capabilities (e.g., Cisco's Forged Email Detection).

Enable detection of mismatches between header "From" and envelope "From".

Use behavioral analysis tools (e.g., IdentityMailer) to flag deviations in normal sending behavior—even from valid accounts.

Strengthen Internal User Awareness

Train users to be cautious of emails from their own address, especially if they include links, attachments, or unusual requests.

Encourage verification via secondary communication channels.

Tag or banner all external messages, even those that appear internal, to break visual trust assumptions.

How CyberForceQ Can Help

For 29 years, CyberForceQ has been a trusted name in advancing cybersecurity programs. Our expertise lies in designing and executing measurable cybersecurity strategies tailored to organizations of all sizes. With a track record of proven results, we offer services such as customized security assessments, robust security operations centers, and comprehensive strategic guidance. Let us assist your organization in prioritizing its goals, elevating your cybersecurity capabilities, and providing meaningful measurements of progress. Our participants are innovative leaders who share optimal strategies to implement and advance a proven cybersecurity program. CyberForceQ, in collaboration with our participants, is protecting the cyber realm.

CONNECT WITH US

www.cyberforceq.com 248.837.1400 solutions@cyberforceq.com