Abuse of Microsoft 365 Direct Send to Bypass Email Security

TL;DR

Threat actors are abusing Microsoft 365's Direct Send feature to deliver spoofed phishing emails that bypass email gateways and security filters, including Cisco Email Security.

These emails appear to originate from trusted internal users but are malicious. Microsoft now allows tenants to disable Direct Send using PowerShell.

Overview

Multiple organizations have reported phishing emails bypassing their email security gateways, particularly Cisco Email Security, by exploiting a Microsoft 365 feature known as Direct Send. This feature allows unauthenticated devices and applications to send email using an organization's domain without credentials. Direct Send is a legacy SMTP method supported in Microsoft 365 that allows internal systems like printers or scanners to send mail to M365 users without authentication.

Affected Technologies

- Microsoft 365 / Exchange Online
- Any third-party email security gateway (e.g., Cisco ESA, Proofpoint)
- Organizations using legacy or unmonitored mail connectors

Threat actors are using this feature to send spoofed phishing emails that impersonate internal users. These messages often fail Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conference (DMARC) checks, yet still get delivered to inboxes or junk folders due to how Microsoft Exchange Online processes them. Microsoft has released new controls to allow organizations to reject Direct Send traffic, but they are not enabled by default. Microsoft recommends that users disable Direct Send in Microsoft 365 to avoid compromise.

Aspire Protects

- Disable Direct Send in Microsoft 365 by using the following PowerShell command:
  - ***Set-OrganizationConfig -RejectDirectSend $true***

- Restrict mail flow connectors to trusted IPs or authenticated applications only.
- Enforce strict SPF, DKIM, and DMARC policies - ideally set DMARC to p=reject.
- Quarantine internal-looking mail that fails SPF/DKIM/DMARC, especially if it originates from untrusted IPs.
- Conduct user awareness training about fake internal emails, especially those urging action on HR, finance, or security topics.

TTPs to Watch

Initial Access

- Phishing via Internal Spoofing [T1566.002] – The attacker may send emails that impersonate internal users using unauthenticated Direct Send channels.

Defense Evasion

- Email Gateway Evasion [T1086] – The attacker bypassed third-party filtering solutions by routing messages directly to Exchange Online, avoiding MX-based inspection.

Credential Access

- Phishing for Credentials [T1566.001] – Emails often include fake login pages or links intended to steal usernames and passwords.

IoCs

IP Addresses

- 139.28.36[.]230
- 163.5.112[.]86
- 163.5.160[.]28
- 163.5.160[.]119
- 163.5.160[.]143

Self-Signed SSL Certificate

- Common Name (CN): *WIN-BUNS25TD77J*

Email Header Indicators

- Authentication-Results: compauth=fail
- X-Forefront-Antispam-Report: CAT:SPOOF;SFTY:9.11 or SFTY:9.22
- X-MS-Exchange-CrossTenant-Id mismatch with your organization's tenant ID

User-Agent/Behavioral Indicators

- PowerShell or CLI-based mail senders
- Emails sent from a user to themselves
- No typical client headers (e.g., no Outlook or webmail fingerprints)

Email Content Patterns

- Subject lines like:
  - "New Missed Fax-msg"
  - "Voicemail from HR"
  - "Urgent Request"
- Attachments:
  - PDF files containing QR codes (used for quishing attacks)
  - HTML redirectors
  - Links to fake Microsoft 365 login pages

Targeted Industries

Any organization using Microsoft 365 and third-party email security tools like Cisco is exposed:

- Manufacturing
- Finance
- Government
- Education
- Energy
- Retail
- Technology

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations

center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
    - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
    - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

What is Direct Send and how to secure it | Microsoft Community Hub

Attackers Exploit M365 for Internal Phishing | Proofpoint US

Ongoing Campaign Abuses Microsoft 365's Direct Send to Deliver Phishing Emails

Arctic Wolf Observes Microsoft Direct Send Abuse I Arctic Wolf