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

By Tom Barnea

Published: 2025-06-26 · Archived: 2026-04-06 02:00:57 UTC

Varonis Threat Labs has uncovered a novel phishing campaign targeting more than 70 organizations. In this post, we dive into the specifics to help you better understand what happened, how to detect the attack and how to prevent it moving forward.

This campaign exploits a lesser-known feature in Microsoft 365: Direct Send.

Designed to allow internal devices like printers to send emails without authentication, Varonis warns that threat actors are abusing the feature to spoof internal users and deliver phishing emails **without ever needing to compromise an account**. Identified victims spanned multiple verticals and locations but were predominantly US-based organizations.

In many of their initial access attempts, the threat actor utilized M365 Direct Send functionality to target an individual organization with phishing messages that were subject to less scrutiny compared to standard inbound email.

These individual events were linked to one another based on commonalities in the attack vector, such as email subject, sender IP address and other factors. The campaign appears to have started in May 2025 with consistent activity over the past two months.

In this blog, we'll break down how Direct Send works, how attackers are abusing it with real-world examples from the incidents we investigated and how your organization can detect and defend against this tactic.

What is Direct Send?

Direct Send is a feature in Exchange Online that allows devices and applications to send emails within a Microsoft 365 tenant **without authentication**. It uses a smart host with a format like: **tenantname.mail.protection.outlook.com**

This setup is intended for internal use only. But here's the catch: no authentication is required. That means attackers don't need credentials, tokens, or access to the tenant — just a few publicly available details.

Identifying vulnerable organizations is trivial. Smart host addresses follow a predictable format as shown above and internal email formats (like *first.last@company.com*) are often easy to guess or scrape from public sources, social media, or previous breaches.

Once a threat actor has the domain and a valid recipient, they can send spoofed emails that appear to originate from inside the organization, without ever logging in or touching the tenant. **This simplicity makes Direct Send**

an attractive and low-effort vector for phishing campaigns.

How attackers exploit Direct Send

In the campaign observed by our forensics experts, the attacker used PowerShell to send spoofed emails via the smart host. Here's an example PowerShell command:

The email appears to come from a legitimate internal address, even though it was sent by an unauthenticated external actor.

Why this method works:

- No login or credentials are required
- The smart host (e.g., *company-com.mail.protection.outlook.com*) accepts emails from any external source
- The only requirement is that the recipient is internal to the tenant
- The "From" address can be spoofed to any internal user

Because the email is routed through Microsoft's infrastructure and appears to originate from within the tenant, it can bypass traditional email security controls, including:

- **Microsoft's own filtering mechanisms**, which may treat the message as internal-to-internal traffic.
- **Third-party email security solutions**, which often rely on sender reputation, authentication results, or external routing patterns to flag suspicious messages.

Detection: What to look for

To detect this kind of abuse, you'll need to dig into message headers and behavioral signals:

Message header indicators:

- **Received headers**: Look for external IPs sent to the smart host.
- **Authentication-Results**: Failures in SPF, DKIM, or DMARC for internal domains.
- **X-MS-Exchange-CrossTenant-Id**: Should match your tenant ID.
- **SPF record:** Look for a smart host to be present.

Behavioral indicators:

- Emails sent from a user to themselves.
- PowerShell or other command-line user agents.
- Unusual IP addresses (e.g., VPNs, foreign geolocations).
- Suspicious attachments or filenames.

How can I separate legitimate use from abuse?

Not all Direct Send usage in emails is malicious. Some legitimate use cases include:

- Automated notifications from internal tools.

- IT scripts sending alerts or reports.
- Third-party integrations (e.g., HR or marketing platforms).

That's why context is key — don't assume, validate.

Real-world example: Direct Send in action

Varonis Threat Labs has observed multiple instances across different environments where organizations received alerts for, "**Abnormal behavior: Activity from stale geolocation to the organization**."

In one case, the alert was triggered by a Ukrainian IP address, an unexpected and unusual location for the affected tenant.

Typically, alerts tied to abnormal geolocation are accompanied by authentication attempts. This time, however, there were no login events, **only email activity**. Even more unusual, users were sending emails **to themselves** with PowerShell as the user agent.

This pattern was distinct from other geolocation-related incidents and immediately pointed us toward a likely root cause: **Direct Send abuse**.

The lack of authentication, combined with internal-looking spoofed messages and scripting behavior, aligns perfectly with how Direct Send can be exploited.

Further forensic analysis revealed that the emails were crafted to resemble voicemail notifications, complete with a PDF attachment. The PDF contained a **QR code** that redirected users to a phishing site designed to harvest Microsoft 365 credentials.

Header analysis confirmed our hypothesis: the attacker was leveraging Direct Send to spoof internal users without needing to authenticate.

- Received: from [127.0.0.1] (139.28.36[.]230) by company.mail.protection.outlook.com
- authentication-results: spf=softfail (sender IP is 139.28.36[.]230) smtp.mailfrom=company.com; dkim=none (message not signed) header.d=none;dmarc=fail action=oreject
- x-ms-exchange-crosstenant-id: [tenant-id]

The email originated from an external IP, failed SPF and DMARC checks, and lacked DKIM signatures, yet it was accepted and delivered internally via the smart host. This is a textbook example of how Direct Send can be exploited when left unprotected.

Prevention: What you can do to protect your org

- Enable "Reject Direct Send" in the Exchange Admin Center.
- Implement a strict DMARC policy (e.g., p=reject).
- Flag unauthenticated internal emails for review or quarantine.
- Enforcing "SPF hardfail" within Exchange Online Protection (EOP).
- Use Anti-Spoofing policies.

- Educate users on the risks associated with QR code attachments (Quishing attacks).
- It’s always recommended to enforce MFA on all users and have Conditional Access Policies in place, in case a user’s credentials are stolen.
- Enforce a static IP address in the SPF record to prevent unwanted send abuse — this is recommended by Microsoft but not required

Indicators of Compromise (IOCs)

- **IP Addresses:**
    - 185.101.38.41
    - 141.95.79.227
    - 176.107.181.26
    - 62.90.188.108
    - 38.22.104.236
    - 185.174.101.87
    - 45.83.43.192
    - 163.5.149.5
    - 212.95.55.172
    - 51.38.109.135
    - 51.38.106.141
    - 176.107.181.26
    - 83.229.70.9
    - 51.89.53.34
    - 51.89.109.70
    - 51.195.53.217
    - 139.28.36[.]230
    - The Threat Actor used multiple IP addresses within the 139.28.X.X space in this campaign to launch emails
- **Domains:**
    - hxxps://voice-e091b.firebaseapp[.]com
    - hxxps://mv4lh.bsfff[.]es
- **Email Subject Lines often contain:**

    - Caller Left VM Message * Duration
    - Fax-msg mm/dd/yyyy, hh:mm:ss AM/PM (2 Pages) RefID: XXXX
    - New Missed Fax-msg
    - New Missed Fax-Msg (2 pages)
    - You have received a new (2 pages) *Fax-Msg* to email@****
    - Fax Received: Attached document for review REF
    - Wireless Caller Left Vm

- **Email Attachments often contain:**
    - Fax-msg
    - Caller left VM Message
    - Listen
    - Wireless Caller Left Vm
    - A Caller Left VM MSG * DURATION

Direct Send is a powerful feature, but it becomes a dangerous attack vector in the wrong hands. If you're not actively monitoring spoofed internal emails or haven't enabled the new protections, now is the time. Don't assume internal means safe.

This list has been updated with more IoCs as of September 9, 2025.

Author's Note: A special thanks to Michael Solomon and his internal research surrounding Microsoft Direct Send.

Don't wait for a breach to occur.

A combination of Varonis' leading threat detection and response capabilities for Exchange Online and our Managed Data Detection and Response (MDDR) service is the ultimate defensive measure for detecting and stopping email-based threats in their tracks.

Our team of world-class cybersecurity experts proactively hunts for indicators of compromise to protect your organization and data 24x7x365. Threat actors don't take breaks — neither do we.

If you are not a Varonis customer and need assistance securing and monitoring your data, please contact our team.

×

Tom Barnea Tom is a Forensics Specialist at Varonis who helps unravel cybersecurity cases, protect organizations, and provides answers quicker than a "Can you hear me?" moment during a virtual meeting. He is always ready to devise creative solutions to new challenges.
