



Insights Report

Dropbox Exploits

Resurgence of Compromised
Dropbox-Hosted PDF Phishing & Malware
Campaigns

Executive Summary

In 2020, MailGuard first detected large-scale phishing and malware distribution campaigns leveraging compromised **Dropbox** accounts to send seemingly legitimate emails with links to PDF attachments.

Those **PDFs, hosted on Dropbox, contained embedded URLs pointing to credential-harvesting and malware sites.**

Despite initial takedowns, this tactic re-emerged in late 2024, and many leading security providers still fail to block these messages because they originate from Dropbox's own infrastructure and host benign-looking PDF files.



Email is the starting point for
91% of cyberattacks.

Source: [Microsoft.com](https://www.microsoft.com/en-au/security/business/security-101/what-is-business-email-compromise-bec)

References:

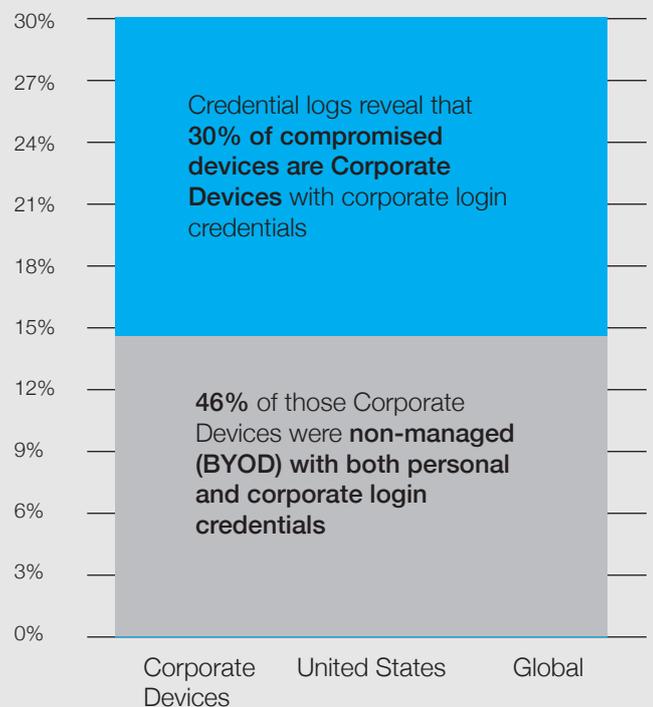
<https://www.microsoft.com/en-au/security/business/security-101/what-is-business-email-compromise-bec>

Key Threat Insight - Dropbox

How Compromised Dropbox Drives Phishing & Malware Delivery

- **Legitimate Sender Infrastructure:** Emails are dispatched from genuine @dropbox.com addresses or via OAuth-authenticated SMTP, bypassing SPF/DKIM/DMARC checks and trusted-sender filters.
- **PDF Trojan Horse:** The message body links to a PDF on Dropbox (e.g., an “Invoice” or “Proposal”); opening the PDF reveals embedded HTML links or JavaScript that redirect to external phishing portals or initiate drive-by downloads.
- **Persistent Reappearance:** After peak activity in mid-2020, the same technique resurfaced in organizations’ inboxes during Q4 2024, demonstrating that many email defences still allow Dropbox-hosted attachments through.

Compromised Devices Based on Credential Log Analysis



Verizon Data Breach Investigation Report

References:

<https://www.verizon.com/business/resources/reports/dbir/#2025DBIRNR>

Key Threat

Insight - Dropbox

Attack Method

1. Account Compromise

- a. Cybercriminals phish or brute-force into Dropbox accounts, often those used for business document sharing.

2. Message Crafting & Dispatch

- a. Using the compromised account's SMTP or Dropbox's "Share link" API, attackers send emails with genuine dropbox.com links and branding.
- b. Subjects mimic urgent business communications: "Project Proposal Attached," "Invoice #12345 – Expires in 24 Hours," etc.

3. PDF Payload Delivery

- a. The shared PDF appears innocuous but embeds hidden hyperlinks (or JavaScript redirects) to phishing sites or malware-hosting servers.
- b. Recipients click through believing they are accessing a safe document.

4. Secondary Exploit & Persistence

- a. Phishing portals harvest Office 365, Dropbox, or corporate VPN credentials.
- b. Malware sites deliver remote-access trojans, info-stealers, or ransomware via silent downloads.

Key Threat Insight - Dropbox

Why It's So Effective

- **Trusted Hosting & Sender:** Dropbox's high-reputation IP ranges and @dropbox.com domains evade allow-lists and authentication checks.
- **Content Camouflage:** A PDF attachment on a trusted link isn't typically scanned by most filters, and static analysis tools often ignore file-sharing domains.
- **User Expectation:** Remote workers routinely exchange PDFs via Dropbox, especially post-2020. Urgent wording ("file will expire in 24 hours") drives quick clicks.

"Credential exfiltration through Dropbox-hosted PDFs is particularly insidious: By exploiting OAuth-authenticated SMTP and Dropbox's share-link API, adversaries weaponize high-reputation infrastructure to deliver PDF payloads that embed stealthy phishing and malware redirects, undermining traditional email-authentication and sandbox defences."

— Anwar Ibrahim, CTO, MailGuard

Technical Deep Dive

SMTP & API Abuse

- Attackers leverage the legitimate account's OAuth token to send mail via smtp.dropbox.com or through the Dropbox API's share endpoint.

PDF Link Embedding

- PDFs contain <a> tags redirecting to shortened URLs (bit.ly, tinyurl) that forward to malicious payloads.
- Some use embedded JavaScript in PDF annotations to auto-launch external links upon opening.

Defence Evasion

- Static URL-based detectors skip dropboxusercontent.com links.
- Sandboxing solutions often whitelist known cloud-storage endpoints.

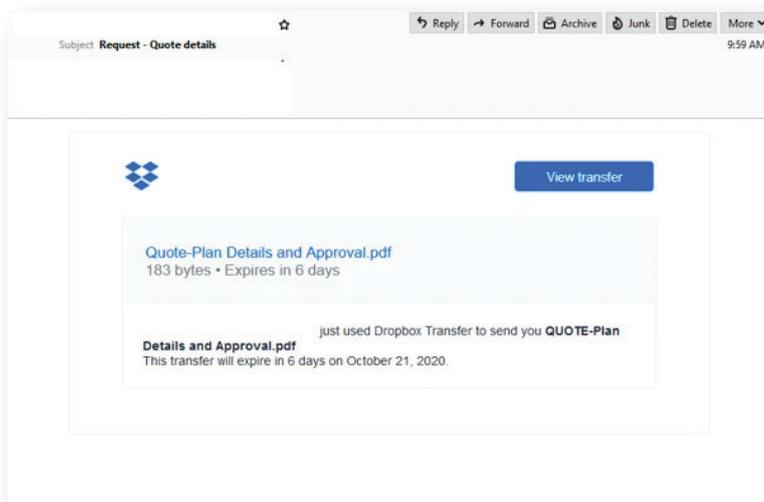
Re-emergence Mechanics

- In late 2024, threat actors automated account takeovers via credential stuffing, scaling the PDF-drop method across thousands of business users with minimal detection.

“Our forensic analyses show these PDFs use multi-stage redirect chains, often via URL shorteners, before landing on malware payloads. Each stage is designed to evade both static and dynamic scanning engines.”

— Prathik Chandrashekar, Head of Engineering, MailGuard

Dropbox Compromise Example 1

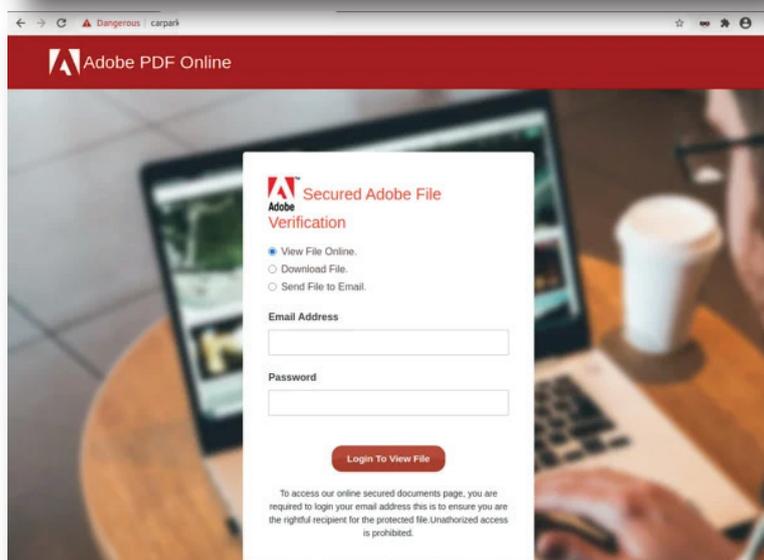


In this first example, a simple subject line of **'Request - Quote details'** aims to spike the curiosity of the recipient.

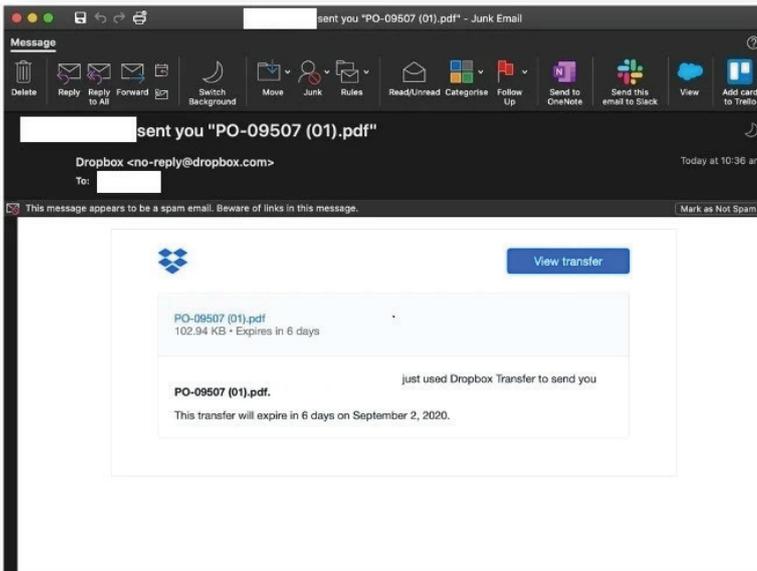
Carrying **Dropbox** brand elements, the email features a link to a **'Quote-Plan Details and Approval'** PDF document.

Clicking the **'View Transfer'** button leads users to a phishing page impersonating **Adobe**, that **aims to steal the users email and password**.

After entering credentials and clicking **'Login to View File'**, the PDF document may also be a **malicious download**.



Dropbox Compromise Example 2

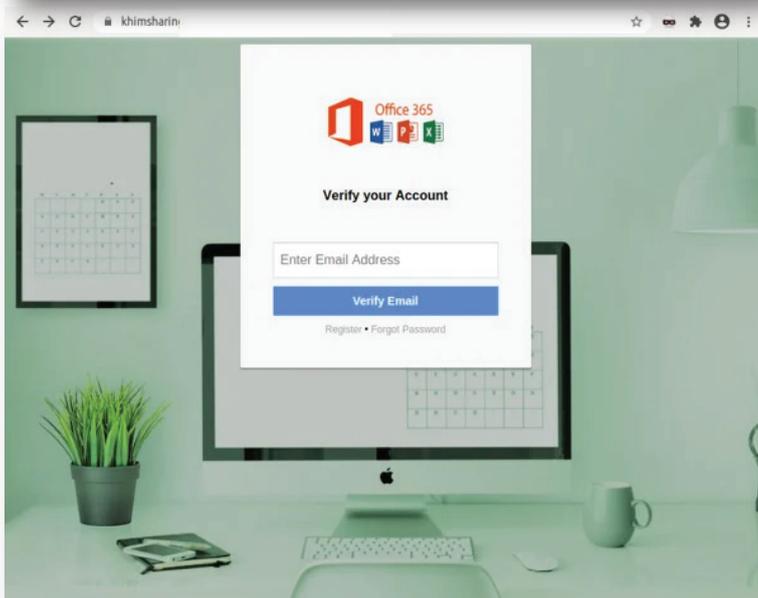


This example leverages **Dropbox** branding and its file transfer mechanism to capture the details of unsuspecting users.

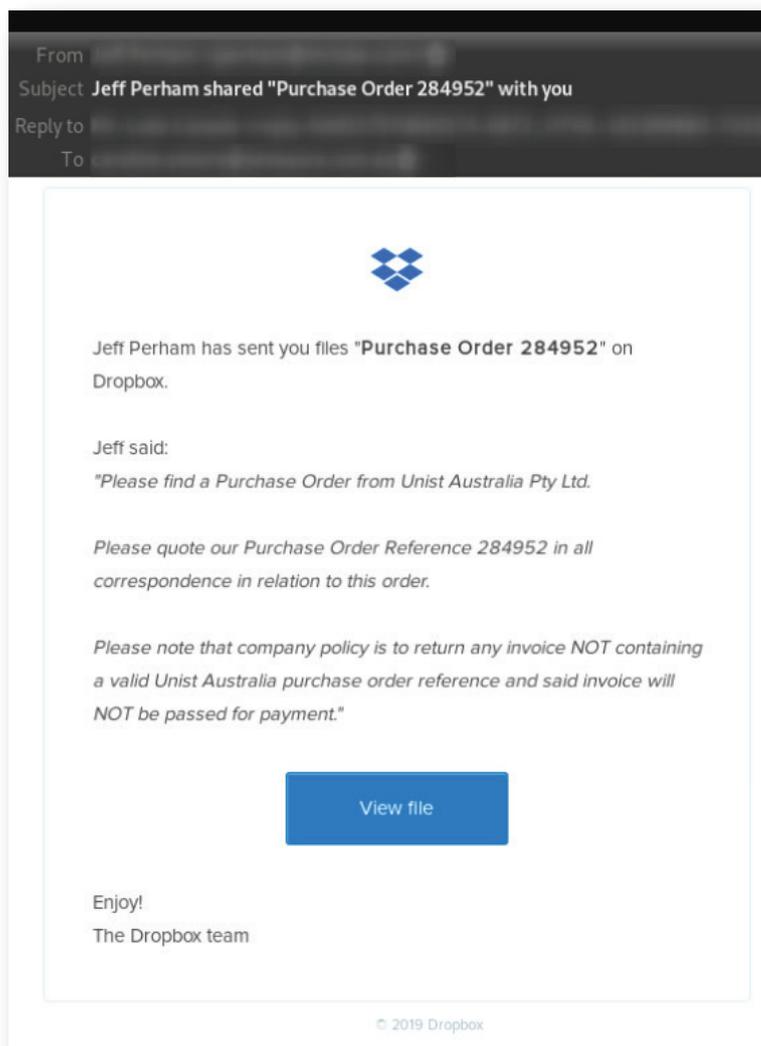
The initial email is **masquerading as a purchase order**, inviting users to click the **'View Transfer'** button to learn more.

Upon doing so, the user is taken to a phishing page that's impersonating an **Office 365 signin**. By entering their email and password, the user is disclosing to the criminals their **Office 365 credentials**.

As with the previous example, once the user has signed in, the purchase order file may indeed be a **malicious download** in disguise.



Dropbox Compromise Example 3

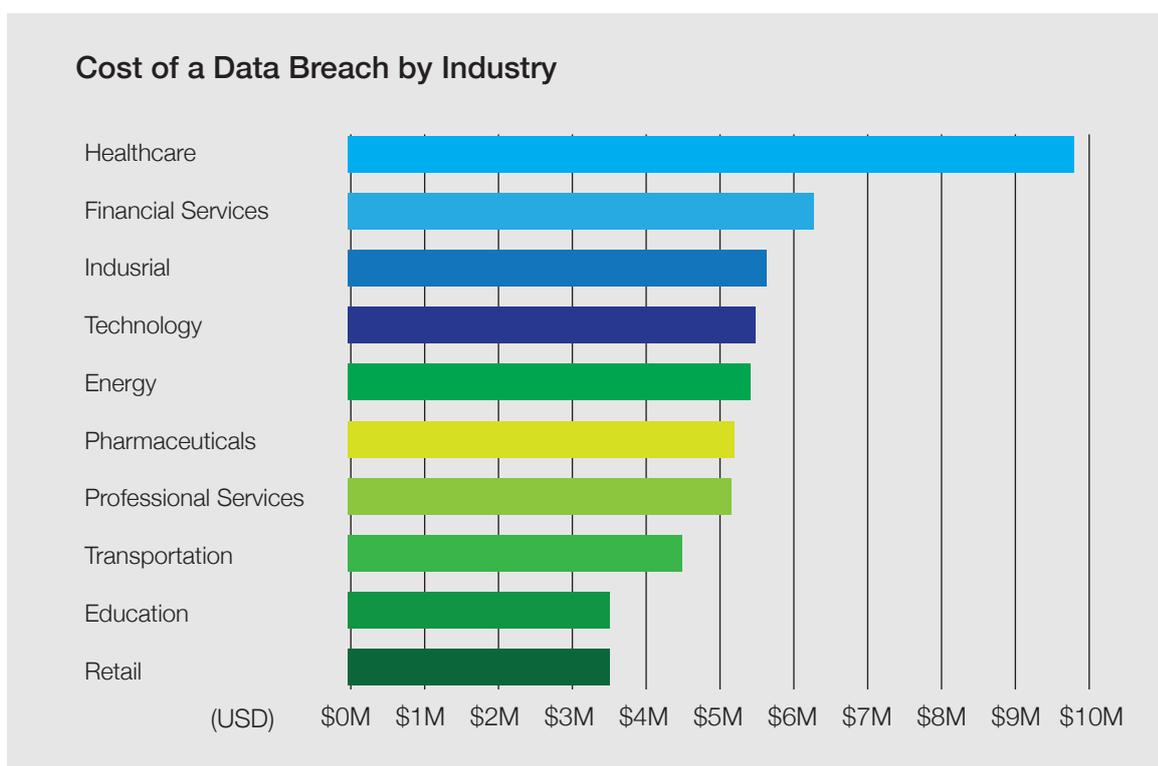


And again, this third example **impersonates a Dropbox file sharing email**, with a more well-formed email inviting the user to view another **'Purchase Order'**.

The scam follows the same dynamic, presenting a **phishing page to capture the user's credentials**, and then **downloading a malicious file to their network**.

Consequences of Inaction

- **Credential Theft:** Harvested credentials enable unauthorized access to Office 365, VPNs, and other cloud services.
- **Malware Infection:** Drive-by downloads can deploy ransomware or remote-access tools, leading to network infiltration.
- **Data Exfiltration:** Compromised credentials allow attackers to steal sensitive corporate documents.
- **Regulatory & Reputation Risk:** Breaches expose organisations to GDPR, ISO 27001, and SOC 2 non-compliance fines, plus brand damage.



IBM Cost of a Data Breach Report 2024

References:

<https://www.ibm.com/reports/data-breach#Key+stats>

Why MailGuard Is Critical

MailGuard delivers:

- **Cloud-Link Analysis:** Behavioural scanners detect anomalous use of Dropbox share links and embedded PDF payloads.
- **Content-Aware PDF Parsing:** Inline inspection of PDF attachments identifies hidden redirect links and JavaScript objects.
- **Account-Takeover Detection:** Monitors for unusual OAuth-email-sending patterns from file-sharing services.
- **Seamless Integration:** Frictionless deployment inline with Microsoft 365 and Google, blocking threats before they reach users.

Don't Settle for Compromises

All observed Dropbox-PDF phishing and malware campaigns (2020 & 2024 waves) were intercepted by MailGuard prior to delivery.



A Strategic Call To Action

Cloud-storage platforms are alluring vectors for attackers due to their trusted status. Email authentication and sandboxing alone cannot stop PDF-based weaponization.

Security teams must deploy advanced, behaviour-driven defences, like MailGuard, that parse and analyse cloud-hosted attachments in real time.

Let's **schedule a time** to review your organisation's security posture and explore how MailGuard can deliver precision defence against the similar persistent threats.

"I couldn't speak more highly of MailGuard as a reliable service provider."

— **IT Manager, Porsche**

"The entire implementation process was very simple and easy to manage"

— **Help Desk Specialist, Lincraft**

"We've seen email-based attacks surge. MailGuard and Defender 365 together have helped us stay protected."

— **CISO, Silk Logistics**

Built in Australia. Trusted Globally.

MailGuard is a global leader in email threat detection. A pioneer in cloud email security since 2001, MailGuard invented the concept of pre-filtering email threats before inbox delivery, laying the foundation for the Secure Email Gateway (SEG) category.

Today, MailGuard protects organisations globally with AI-powered threat detection, seamlessly deployed inline with Microsoft's ecosystem and Google, among other email providers.

At the heart of our platform is **MyGuard**, our proprietary AI threat engine developed with over **A\$35 million in R&D**. MyGuard combines:

- Gen-AI powered LLMs
- Bayesian and fingerprint-based classifiers
- Real-time behavioural heuristics

...to stop advanced threats on first encounter before they reach staff inboxes, including those that bypass Microsoft and other cloud email security vendors

MailGuard is **ISO/IEC 27001:2022 certified**, trusted by **over 5,500 organisations**, including governments, law firms, banks, hospitals, and ASX-listed companies. Recognised for our unmatched speed in detecting zero-day email threats, we have consistently stopped sophisticated exploits, like **QR code phishing**, **Dropbox-based malware**, and **Azure AD Guest Invite fraud**, months ahead of Microsoft, and other leading platforms.

In an era of rising cyber regulation and board-level accountability, MailGuard enhances your Microsoft 365 or Google security stack with minimal disruption, easy activation, and elite-speed protection, fulfilling your fiduciary and operational responsibilities.

Trusted by Global Leaders. Since 2001.

- A leader in advanced 'zero zero-day' email threats missed by Microsoft 365 and other 3rd party vendors.
- Achieve peace of mind with MailGuard, a solution **trusted by global leaders** that ensures your email is secure.
- Benefit from **A\$35M+ in R&D, including proprietary AI & ML-powered threat detection**, to boost your cybersecurity confidence.
- AI-powered email threat detection and inline architecture intercepts and blocks threats hours faster, on first encounter.



"It's the type of innovation that we want to see."

— **Satya Nadella, CEO & Chairman, Microsoft**



"MailGuard has developed world-leading cloud and email security IP. This is IP that is unique to Australia; it's among the leading cloud and email security solutions anywhere in the world."

— **Hon. Malcolm Turnbull, Former Australian Prime Minister**



"You are being led by what I see as one of the world's best, at preventing and protecting your secure infrastructure, securing your people, and securing your business"

— **Steve Miller, COO, Microsoft Asia**



www.mailguard.com.au

Let's Connect

Make time today to talk to our local team of experts about fortifying your inboxes.

expert@mailguard.com.au