TIR-20250813 DocSend - When a Trusted Tool Becomes a Threat Vector

8/13/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

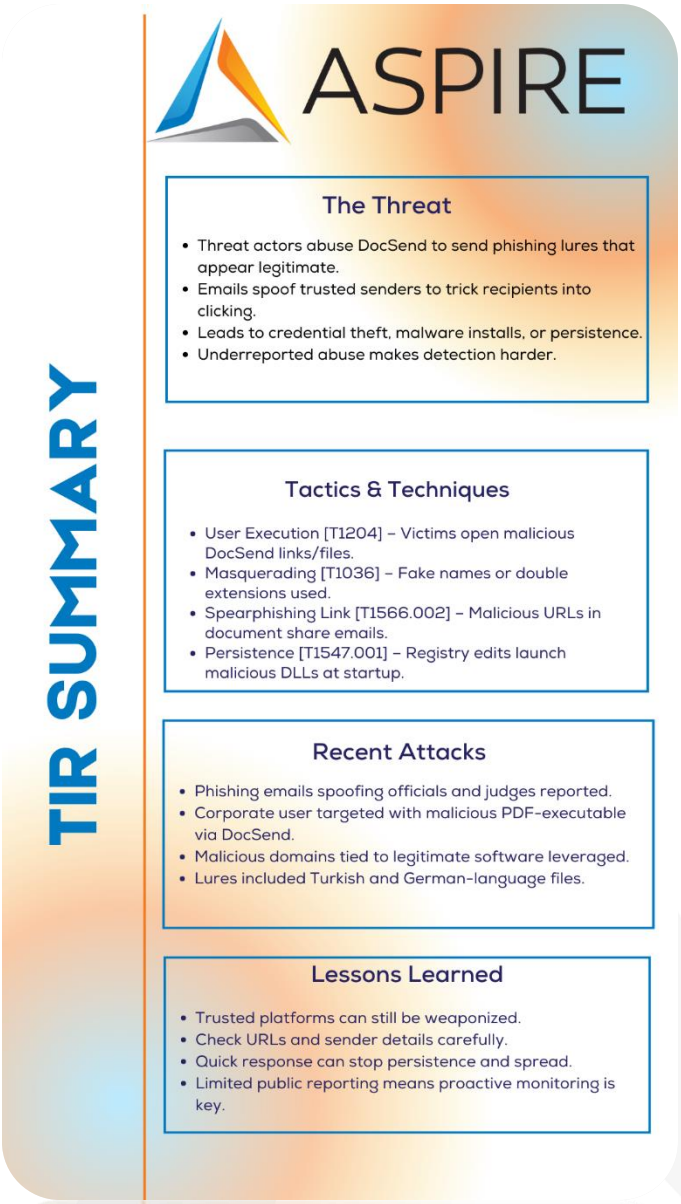
TABLE OF CONTENTS

Executive Summary

Threat actors are increasingly turning to DocSend (the file-sharing and document-tracking service Dropbox bought in 2021) to deliver phishing lures and malicious files. While the service was designed to securely share sensitive business documents, its reputation and ability to host content behind a harmless-appearing link have made it a convenient tool for bypassing traditional email security measures.

Over the past year, incidents involving DocSend abuse have escalated, with attackers using the platform to distribute credential-harvesting pages, malware installers, and socially engineered lures targeting both individuals and organizations.

Unlike mass spam campaigns that can be easily blocked, DocSend abuse exploits the trust users place in branded file-sharing links. Threat actors create convincing document share requests that appear to come from familiar contacts or reputable institutions. In many cases, the link directs victims to a malicious site outside of DocSend after an initial preview, making it harder for security filters to detect the threat before the user interacts with it. This tactic has



been effective in spear-phishing campaigns targeting government agencies, law firms, financial institutions, and small to mid-sized businesses. These are sectors where document exchange is routine and urgency is often high.

Recent investigations show attackers tailoring DocSend-based phishing lures to mimic official communications from law enforcement, courts, tax authorities, and corporate HR departments. Here's how threat actors are abusing DocSend, and the steps your organization can take to protect against it.

DocSend

DocSend is often described as a secure way to send sensitive documents. Think of it as the digital equivalent of handing someone a folder sealed with a stamp. Introduced by DocSend, Inc. in the early 2010s, it was acquired by Dropbox in 2021, and its integration with Dropbox's storage and collaboration tools has made it easier for people to adopt.

Over the years, DocSend has become a trusted for business roles, such as legal counsel sharing contracts, sales teams sending proposals, or HR sending onboarding material.

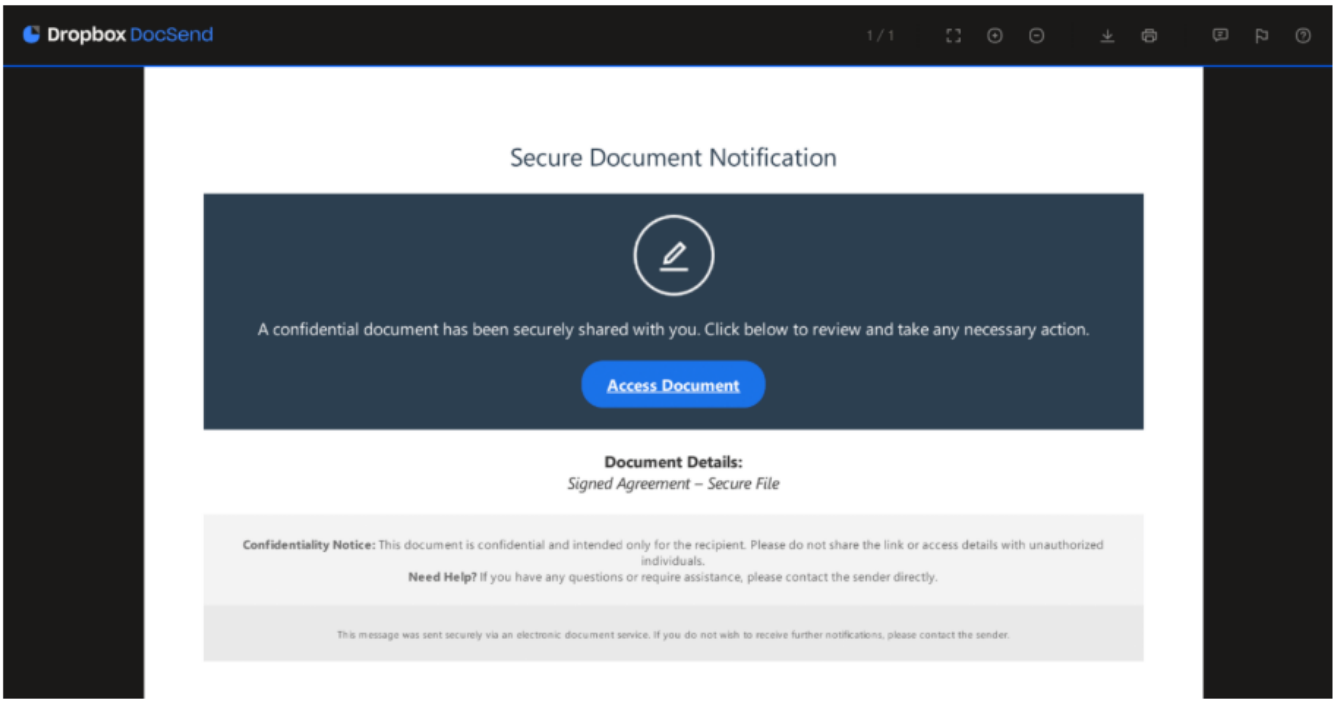
What makes DocSend appealing?

- Control and visibility - Senders can set document access to expire after one view, revoke links, and track who clicked and when. That makes it much more controlled than traditional email attachments.
- Minimal friction - Recipients don't need accounts or installs. Typically, you click and preview in-browser.
- Legitimacy in inboxes - DocSend's domain is recognized widely; many organizations allow it by default in their Secure Email Gateways.

That same convenience is exactly what makes it risky. Email filters tend to let DocSend links through because they're assumed safe. Many users don't bat an eye when a link says "Sent via DocSend." It becomes even riskier when attackers disguise it with social engineering, such as using a manager's name or a legal-sounding document title, before sending the victim to a phishing site. The risk grows because DocSend links work with a single click and can expire, leaving little for investigators to trace. In practice, it can act like an unintentional trusted front desk for attackers.

Since DocSend phishing hasn't been tied to major headlines or widely publicized breaches, it's often not on an organization's radar. Add to that the fact phishing emails containing DocSend links often continue to reach inboxes unchallenged, and attackers have room to flourish behind the scenes. Exploiting DocSend is less about technology flaws and more about exploiting trust patterns baked into workflows.

Image 1: DocSend Lure



Source: Keepware.com

How Does This Happen?

Threat actors exploiting DocSend don't usually operate on impulse. Most campaigns start with reconnaissance, where attackers gather intelligence on potential targets. This could include scanning LinkedIn for job titles, reviewing company press releases for vendor relationships, or purchasing breached email lists from underground forums. The goal is to craft an email that feels contextually relevant, which increases the odds of a click.

Once a victim profile is built, the attacker creates or hijacks a DocSend link to host malicious content. Because DocSend is a legitimate service, its URLs often bypass security filters. The attacker can then monitor engagement and swap out payloads without sending a new link. Threat actors can also restrict access to make detection harder. The malicious content might be a credential phishing page or a disguised executable.

Typical attack chain for DocSend abuse:

- Target identification – Harvesting email addresses and context on the target from public sources or stolen data.
- Lure creation – Drafting a convincing email with relevant subject matter, such as legal notices or HR forms.
- DocSend setup – Uploading malicious files or embedding phishing pages within a DocSend link.
- Delivery – Sending the email to the target, using DocSend's legitimate domain to evade filters.
- Click & redirect – Victim clicks the link, often landing first on DocSend, then being redirected to a malicious site or download.
- Execution – Malicious payload runs or the phishing page captures credentials.
- Persistence – In some cases, the attacker uses registry edits, scheduled tasks, or DLL injection to maintain access.

- Data exfiltration or further compromise – Stolen credentials or data are sold, reused, or leveraged for lateral movement within the network.

Exploitation and Case Studies

Let's walk through some case examples to see what was detected, how it was handled, and what they reveal about attacker methods and risks.

Case A: Professional Services Firm, U.S. (July 2025)

At a midsized professional services firm (~500 staff), an employee received a DocSend link titled "Quarterly Finance Overview." Clicked by the user expecting a PDF, what appeared on screen was a DocSend interface. However, everything looked unusually generic and the interface displayed German text ("Dokument anzeigen"), even though the firm operated entirely in English and only in the U.S.

That context immediately off alarm bells. The link then forwarded to a page asking the user to re-enter their email to verify access, with no preview or download. Microsoft Defender flagged the page, citing unusually obfuscated JavaScript with dozens of function definitions stashed inside. Because the link only opened once, there was no easy way to re-create it for forensics.

The security operations team triaged the incident by tracing the original email source, verifying there was no malware on the host, and confirming that no credentials had been sent to the attacker. Investigators mapped this to MITRE - link-based phishing (T1566.002) combined with defense evasion via obfuscated landing (T1027). They recommended tightening DocSend flow control and applying sandboxing to unrecognized DocSend links. It was a clear example of a "trusted preview" turning suspicious because of odd wording and unexpected access steps.

Case B: Legal Sector, U.S. (July 2025)

At a law firm, an associate clicked on what appeared to be an internal DocSend link labeled “Contract for Review.” The link delivered a ZIP archive (esign-documents.zip) to the downloads folder. Inside was an executable disguised as a PDF file (...Signature_Form_for_jBB5375.PDF.exe) placed in a temporary directory. Once executed, the file attempted persistence by creating a registry run key named “criticalUpdates,” which pointed to a DLL executed through rundll32.

This DLL, identified as a variant of Penguish malware, initiated a DNS lookup as part of its beaconing process. Penguish, an infostealer and loader, is known for exfiltrating browser data, cryptocurrency wallet files, and authentication tokens, as well as deploying second-stage payloads.

In this case, Cisco Umbrella blocked the outbound request to vovsoft[.]com, a legitimate Turkish freeware/shareware domain, which Penguish was abusing for staging or command-and-control purposes. CrowdStrike flagged the registry change as “RegistryPersistEdit” and quarantined the process before exfiltration or additional malware deployment could occur.

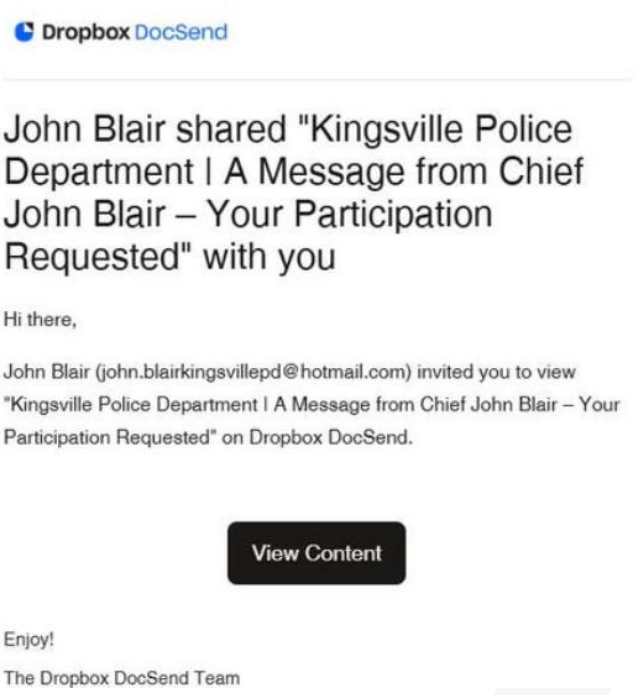
Analysis showed the executable carried a valid Sectigo-issued signature tied to a legitimate Vovsoft PDF tool, consistent with Penguish’s tactic of abusing trusted signatures for camouflage. While VirusTotal initially marked the file as legitimate, its runtime behavior revealed its malicious intent. The MITRE mapping for this activity includes phishing link (T1566.002]), double-extension execution (T1204), run key persistence (T1547.001), signed proxy execution (T1218.011), and masquerading with a trusted signature (T1036). Similar DLL names, executable structures, and registry keys were later identified in other Penguish-related incidents, indicating this was part of a broader campaign rather than a standalone intrusion.

Case C: Organizational Impersonation, U.S. (Mid-2025)

A human resources professional got a “Reminder: Your Participation is Requested” link from no-reply@docsend.com, with a display name reading “Judge AppleTree.” Recognizing that DocSend should come directly from the sender with original context, not impersonated, she paused. They discovered the link pointed to a free webmail alias in the header, not a government domain, and contained a hidden redirect button. No

harm occurred, but this user's reflexive question (and quick escalation) showed how awareness is a workforce's strongest filter.

Image 2: An Example of What the HR Professional May Have Seen



Source: Facebook/Klebergcoso

Because the link never opened a landing page, the team used the incident to tighten policy. Now, any email with a DocSend link and an authority-style title, like "Judge" or "City Manager", paired with a mismatched domain gets flagged as medium risk automatically.

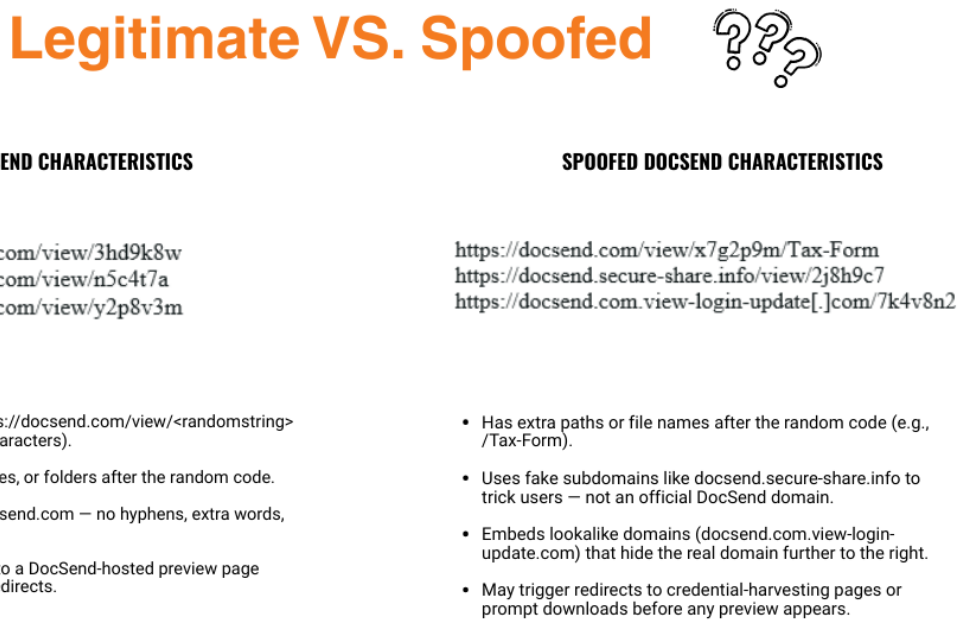
Pulling it together

These three examples show the range of attacks. From DocSend previews that looked almost legitimate to blatant executable traps hidden behind trusted redirects. In each case, defenders relied on a mix of:

- Endpoint detection (CrowdStrike) catching registry-write triggers
- Network filtering (Umbrella) blocking second-stage domains

- User training and policy enforcement, stopping impersonation attempts before any click
- Threat hunting, drawing link patterns across cases to treat them as campaigns (turkish/german gates, vovsoft.exe, persistent run keys)

Image 3: Legitimate VS. Spoofed DocSend Links



CYBER THREAT INTELLIGENCE

ATTRIBUTION

From what we've seen, there are clues that point to threat actors with ties to both Turkey and Germany. Some of the malicious DocSend links delivered PDFs written in Turkish, while other activity included German-language elements buried in the file properties or infrastructure setup. That mix of languages doesn't look random, it could mean someone with familiarity in those regions is behind at least part of the activity. Whether it's one group with multilingual capabilities or multiple actors using the same playbook, the evidence leans toward operations rooted in, or at least closely connected to, Turkey and Germany.

OTHER LOTL ATTACK CAMPAIGNS

The DocSend abuse campaign is generally considered a "living-off-the-land" (LotL) abuse of a legitimate service combined with phishing-as-a-delivery tactics.

It doesn't involve exploiting a software vulnerability, instead, it misuses a trusted third-party platform to deliver malicious files or links. Security researchers often categorize this type of attack under:

- WMI and admin scripting - Windows Management Instrumentation (WMI) and system scripting languages are turned into attack platforms. Threat actors use them to move laterally, steal data, or persist without dropping new binaries.

- PowerShell abuse - Attackers run scripts entirely in memory using PowerShell. This means no files are written to disk - nothing suspicious to antivirus, just invisible commands doing the dirty work. TechRadar highlights that PowerShell is one of the most frequently misused native tools in attacks.

- Network tool misuse (e.g., netsh.exe) - Cybercriminals use built-in networking commands like netsh.exe to reconfigure settings, route traffic, or open backdoors. Bitdefender found it's involved in about one-third of high-severity attacks—practically invisible because it's a trusted tool.

ASPIRE'S RECOMMENDATIONS

While DocSend itself is a legitimate and secure file-sharing service, its features can be exploited by threat actors in highly convincing phishing and malware campaigns. The challenge is that these attacks often bypass technical defenses and rely on user trust, making human awareness just as important as technical safeguards.

Preventing successful exploitation requires a layered approach. Organizations must combine email security best practices and proactive technical controls. See the following recommendations:

1. Verify Before You Click

- If you receive an unexpected DocSend link (even from someone you know) verify its legitimacy through a separate communication channel (phone call, direct message, or in-person).
- Hover over links before clicking to confirm the URL points to a legitimate DocSend domain (docsend.com) and not a spoofed site.

2. Strengthen Email Security Filters

- Configure your secure email gateway to flag or quarantine messages containing links to external file-sharing services that are not commonly used within your organization.
- Enable URL rewriting and scanning to analyze links in real time before the user can access them.

3. Train Employees on Social Engineering Awareness

- Include DocSend-specific phishing examples in security awareness training, emphasizing that attackers often impersonate known institutions or colleagues.
- Teach staff to recognize subtle signs of spoofing, such as misspelled domains or unexpected requests for sensitive data.

4. Apply Technical Protections on Endpoints

- Maintain up-to-date endpoint detection and response (EDR) tools capable of detecting suspicious file executions and registry modifications.

- Block known malicious domains and IP addresses linked to DocSend phishing activity via DNS filtering solutions.

5. Limit External File-Sharing Permissions

- If DocSend is not part of your official workflow, consider blocking it at the network level or limiting access through a secure web gateway.
- If DocSend is required for business purposes, enforce authentication and limit sharing to pre-approved contacts or email domains.

6. Implement Incident Response Procedures

- Have a clear, documented process for reporting suspected phishing emails, including DocSend links.

Conclusion

The abuse of DocSend is part of a larger problem in cybersecurity. Attackers are turning trusted platforms into tools for phishing and malware. DocSend was built for secure sharing, but that trust can work in the attacker's favor.

This tactic does not require advanced exploits. Attackers take everyday business tools and use them for harmful purposes. Just as DocSend links can be turned into phishing lures, other trusted platforms and built-in utilities can be repurposed in the same way, often slipping past defenses because they look like routine activity.

The real risk comes from how people interact with these tools. When something looks routine, it is more likely to be opened without question. The solution is a mix of strong security controls and better user awareness. Security tools can block many attempts, but training can help users think twice before clicking.

MITRE MAP

DocSend

Initial Access	T1566 – Phishing T1566.002 – Phishing: Spearphishing Link
Execution	T1204 – User Execution
Persistence	T547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Defense Evasion	T1036 – Masquerading T1027 – Obfuscated Files or Information
Command and Control	T1071.001 –- Application Layer Protocol: Web Protocols
Exfiltration	T1567.002 - Exfiltration Over Web Service: Exfiltration to Cloud Storage

ASPIRE PROTECTS

- **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 cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.

  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **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.

INDICATORS OF COMPROMISE (IOCS)

DocSend

Note: These IoCs were compiled from publicly available reports on DocSend-related attacks and from Aspire's internal case notes.

Domains

- thecalebgroup[.]top
- rz8js7sjbef[.]latovafineart[.]life

- qhozd[.]ru
- upx[.]sf[.]net
- drlve[.]rnweb[.]co

IP Address

- 193[.]222[.]96[.]91

URLs

- docsend[.]com/view/vcdmsmjcskw69jh9
- docsend[.]com/v/zpd8s/xhbgwejpyhiffaqgdqfdjfxrwtamkmgpqvbvfrtvbvrtajmqtqbmtnwbqyxr
- docsend[.]com/v/zpd8s/wjvpgnmniinyczibuvrkqnhtadwiwwzzqtkhm=
- docsend[.]com/v/zpd8s/wjvpgnmniinyczibuvrkqnhtadwiwwzzqtkhmmizgpncjkvetqbfxtgfudzr
- docsend[.]com/view/h9t85su8njxtugmq

Email Subjects

- 1st Quarter Profit Sharing Plan & Salary Increase 2025 (401k) Ref: XXXXXXXX
- Reminder: [Company Name/Important Individual] shared '…Your Participation is Requested'

SUPPORTING DOCUMENTATION

Behind the Veil: Darktrace's Detection of VPN Exploitation in SaaS Environments

How We Were(n't) Phished

Detecting Attacks Across Email, SaaS, and Network Environments with Darktrace's ActiveAI Security Platform

Suspicious shared link from sender. | The Dropbox Community

Officials urge neighbors to watch out for recent Dropbox/DocSend scam

📢 **SCAM ALERT: Dropbox... - Kleberg County Sheriff's Office | Facebook

JEFFERSON COUNTY SHERIFF'S OFFICE WARNS OF EMAIL SCAM (04/08/2025) - Press Releases - Jefferson County Sheriff AR

Living Off the Land(LOTL): Turning Trusted Tools into Silent Weapons | by Aenosh Rajora | Aug, 2025 | InfoSec Write-ups

Living Off The Land: The Cyberattack You'll Never See Coming - Brandefense

Kaspersky Threats — Trojan.Win32.Penguish.fs

Trojan:Win32/Penguish!MSR threat description - Microsoft Security Intelligence

Appendix II: Disclaimer

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.