Security of Cloud Technology – How to Secure Cloud Email Senders from Impersonation

Omer Lahav – Principal SE

Sender Impersonation Case Study

October 5th , 2023

proofpoint.

Agenda

Sender Impersonation

The Very Unfortunate Tale of Trezor

SPF Flattening, Look A like Detection, Filter Email Relay

Summary

Sender Impersonation Impacts…

Brand Reputation

Customer Service | Marketing | Accounts Payable

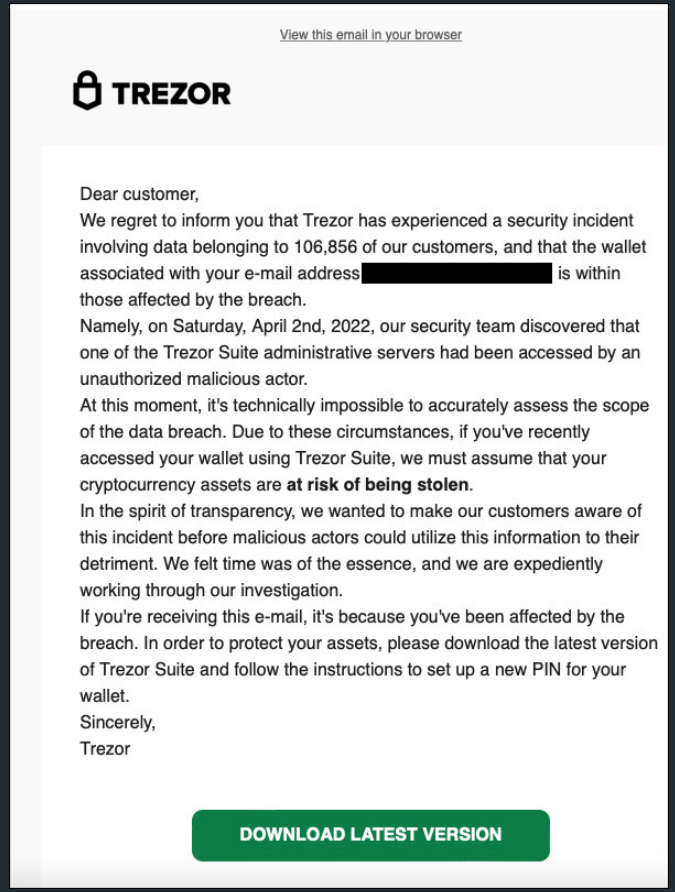
Sender Impersonation Can Come In Many Forms…

1) Domain Spoof
2) Domain Look A like
3) Legitimate sending system compromise

Trezor was targeted as part of a wider attack that took in over 100 Crypto and Finance companies

Multi vector, the attack depended on email

https://www.bleepingcomputer.com/news/security/fake-trezor-data-breach-emails-used-to-steal-cryptocurrency-wallets/



View this email in your browser

TREZOR

Dear customer,

We regret to inform you that Trezor has experienced a security incident involving data belonging to 106,856 of our customers, and that the wallet associated with your e-mail address [redacted] is within those affected by the breach.

Namely, on Saturday, April 2nd, 2022, our security team discovered that one of the Trezor Suite administrative servers had been accessed by an unauthorized malicious actor.

At this moment, it's technically impossible to accurately assess the scope of the data breach. Due to these circumstances, if you've recently accessed your wallet using Trezor Suite, we must assume that your cryptocurrency assets are **at risk of being stolen**.

In the spirit of transparency, we wanted to make our customers aware of this incident before malicious actors could utilize this information to their detriment. We felt time was of the essence, and we are expediently working through our investigation.

If you're receiving this e-mail, it's because you've been affected by the breach. In order to protect your assets, please download the latest version of Trezor Suite and follow the instructions to set up a new PIN for your wallet.

Sincerely,

Trezor

DOWNLOAD LATEST VERSION

Email Authentication – Critical Part of the Solution?

How can we be sure the sender is who they say they are?

DMARC

DMARC ensures the From address that users **see in their email client is trustworthy**

SPF

SPF allows organisations to declare (in DNS) what IP addresses **can send on their behalf.**

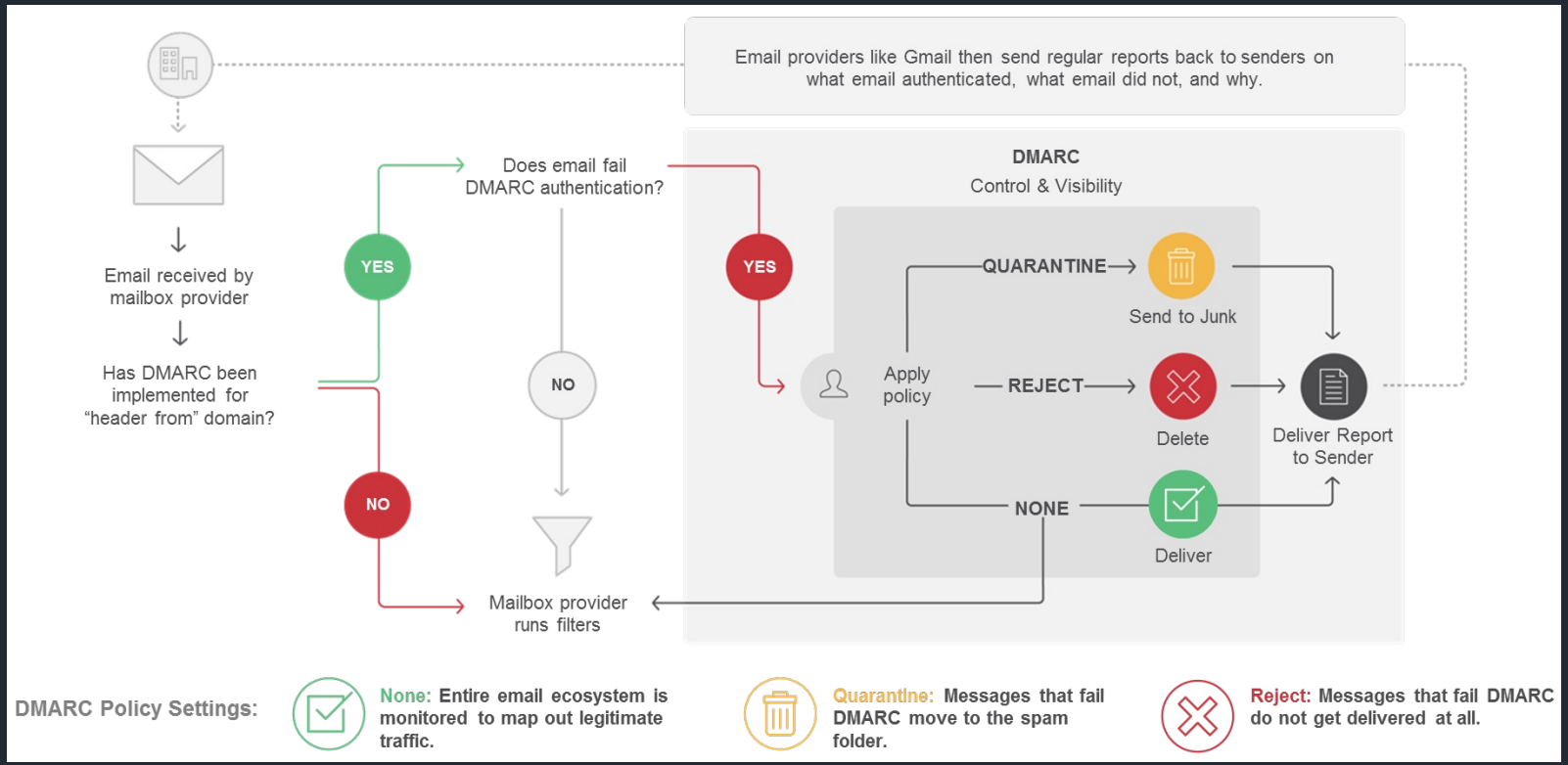
DKIM

DKIM ensures that messages **aren't tampered with in transit**, utilising cryptography.

DMARC Benefits

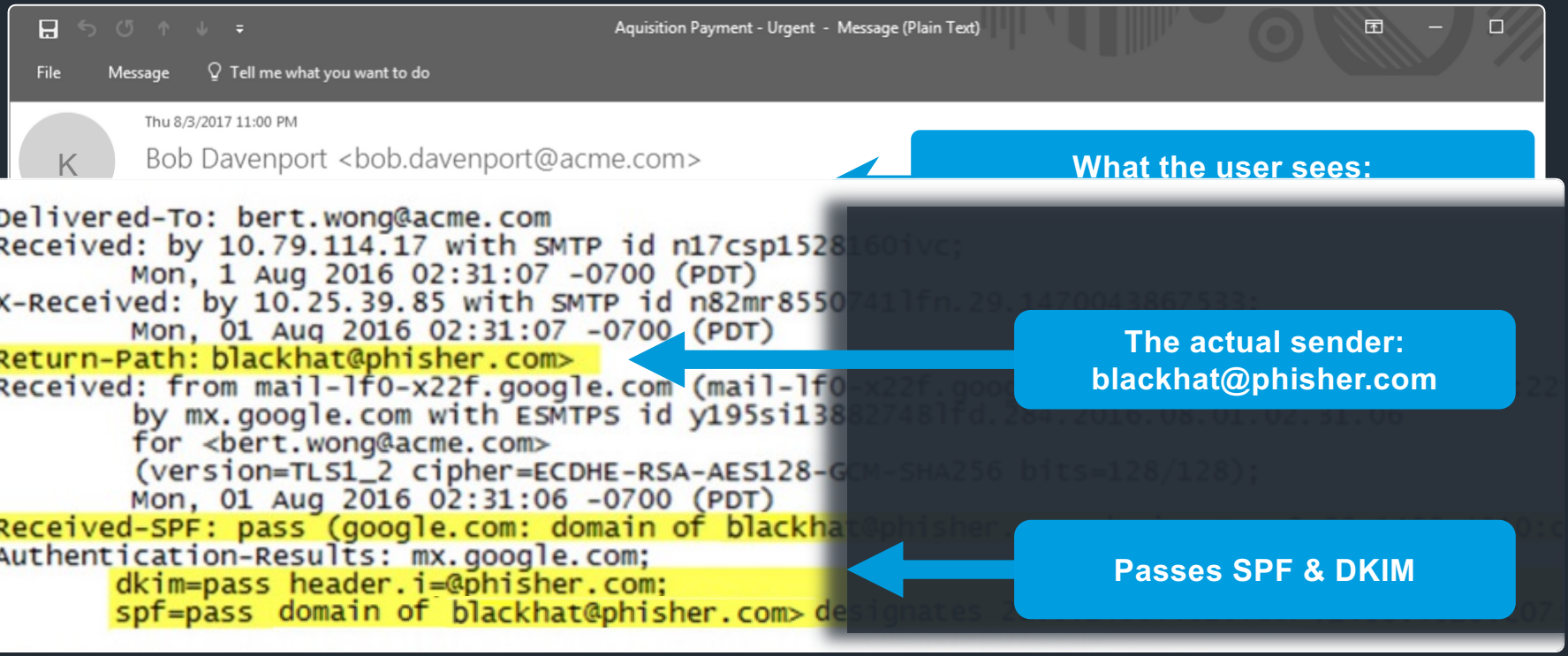
- SPF/DKIM authentication and alignment.
- Determine what to do with email that fails authentication.
- 'From' address can be trusted by users

How DMARC Works?



proofpoint.

Why Email Authentication is Important



proofpoint.

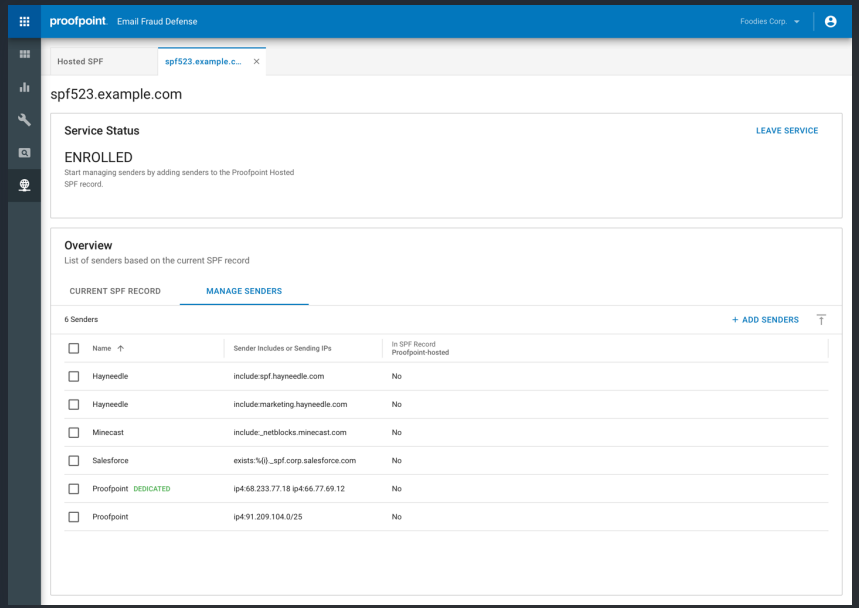
Trezor’s SPF Record at Time of Attack

- v=DMARC1; p=reject; rua=mailto:06b6370b8ec49e557257d38fd38e03-d@dmarc.report-uri.com

- v=spf1 include:spf.mandrillapp.com include:_spf.google.com include:servers.mcsv.net include:_spf.salesforce.com include:shops.shopify.com -all

SPF Flattening

Hosted Services



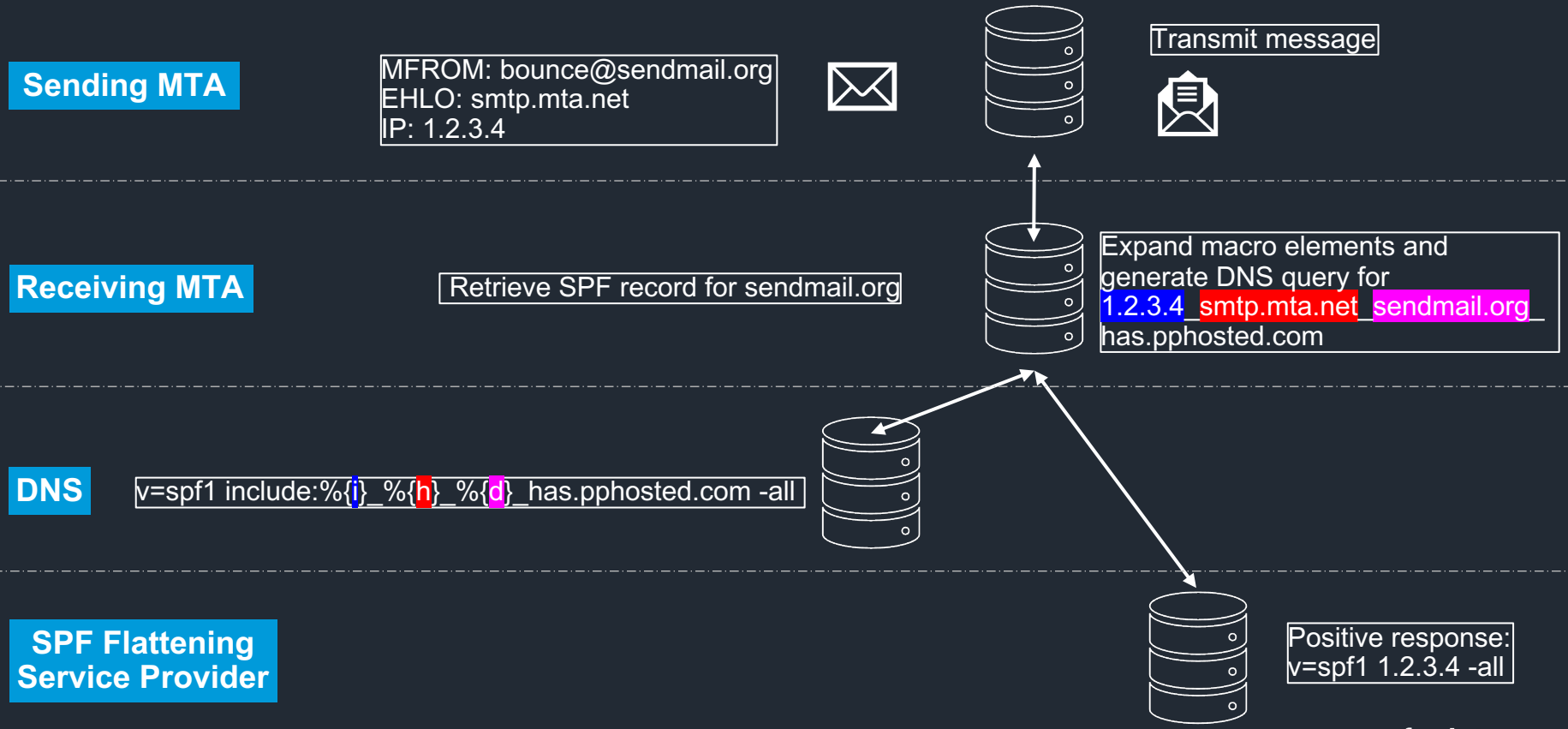
Improved efficiency

- Overcome the DNS lookup limit of 10
- Reduce overhead of making SPF updates
- Real-time propagation

Better security

- Obfuscate senders published in your SPF record
- Simplify SPF record by identifying authorized but unused IP addresses
- Eliminate 3rd party SPF risk by maintaining last known good SPF record.

SPF Macros In Mail Flow



proofpoint.

Lookalike

Dynamically Identify Lookalike Domains

SCAN

Continually scan over 400 million domains for threats

CLASSIFY

Automatically classify domains and identify potential BEC domains

INVESTIGATE

Provide detailed intel around registrant info, email traffic, web content; achieve workflow flexibility

RESPOND

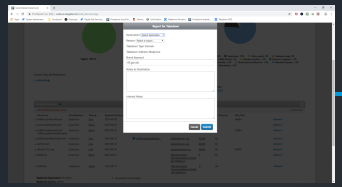
- Add to block list
- Limit access
- Permanently remove via Virtual Takedown add-on

Rapid Enforcement

4 Block lists accept or reject submission as per their criteria. Updated block list propagated to subscribers.

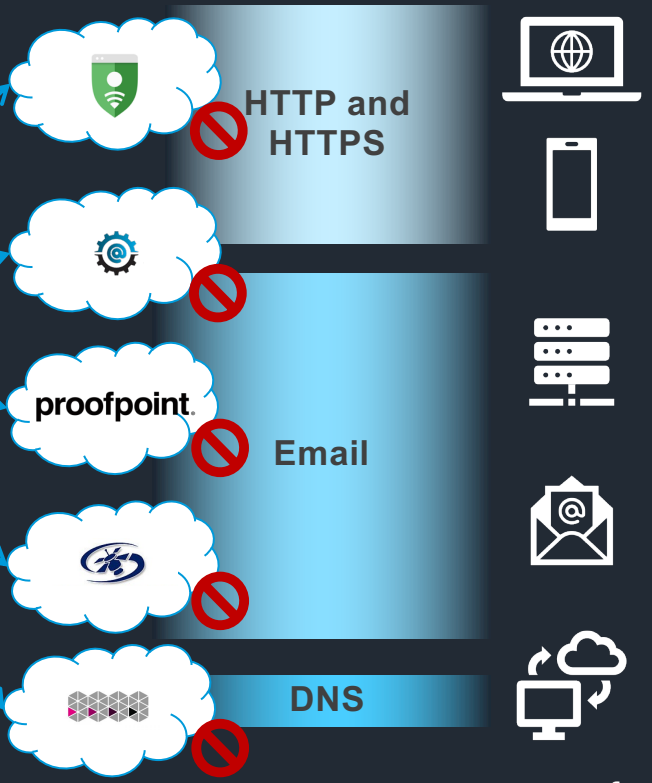
3 After successful vetting, submission to one or more block lists (depending on takedown type)

1 Domain submitted for takedown along with supporting evidence



Domain Discover

2 Takedown reviewed for submission by Proofpoint

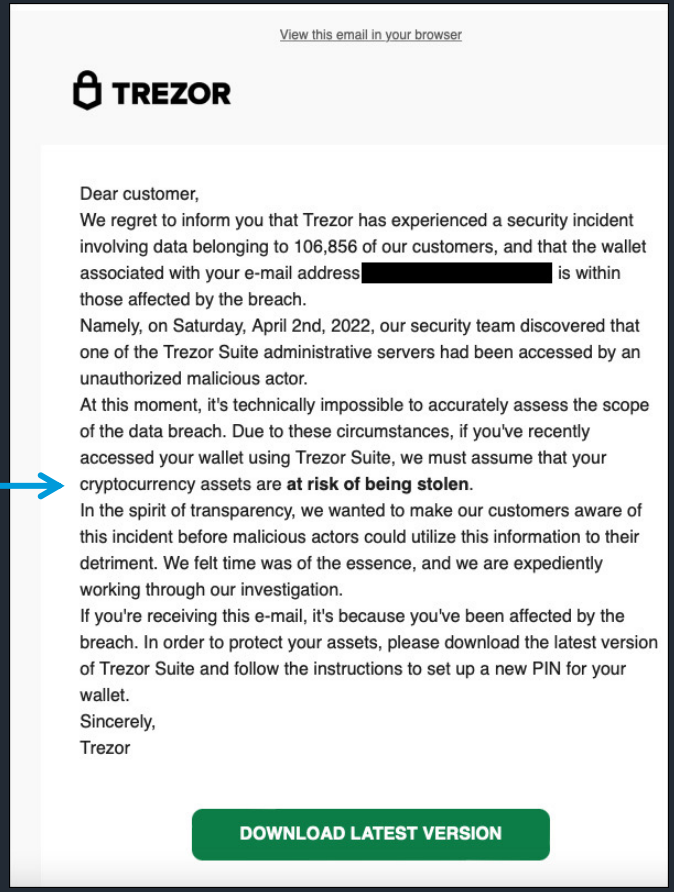


Wide-range of devices, apps, ISPs, consumer and enterprise Web services, and enterprise security offerings consume feeds from these various block lists

proofpoint.

Trezor was targeted as part of a wider attack that took in over 100 Crypto and Finance companies

Urgency
At Risk



View this email in your browser

TREZOR

Dear customer,
We regret to inform you that Trezor has experienced a security incident involving data belonging to 106,856 of our customers, and that the wallet associated with your e-mail address [redacted] is within those affected by the breach.
Namely, on Saturday, April 2nd, 2022, our security team discovered that one of the Trezor Suite administrative servers had been accessed by an unauthorized malicious actor.
At this moment, it's technically impossible to accurately assess the scope of the data breach. Due to these circumstances, if you've recently accessed your wallet using Trezor Suite, we must assume that your cryptocurrency assets are **at risk of being stolen**.
In the spirit of transparency, we wanted to make our customers aware of this incident before malicious actors could utilize this information to their detriment. We felt time was of the essence, and we are expediently working through our investigation.
If you're receiving this e-mail, it's because you've been affected by the breach. In order to protect your assets, please download the latest version of Trezor Suite and follow the instructions to set up a new PIN for your wallet.
Sincerely,
Trezor

DOWNLOAD LATEST VERSION

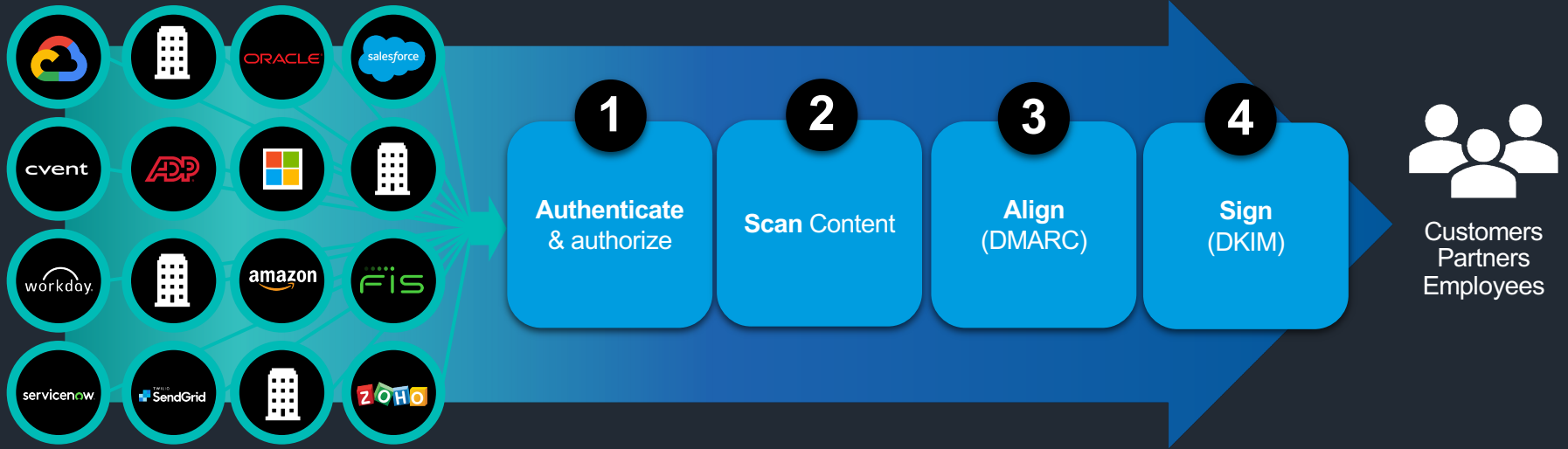
Multi vector, the attack depended on email

https://www.bleepingcomputer.com/news/security/fake-trezor-data-breach-emails-used-to-steal-cryptocurrency-wallets/

Filtering outbound Email from 3rd party Senders

Non-DMARC compliant
unsecure application email

Secure, DMARC compliant
application email



Secure Cloud Email Senders from Impersonation

1) **Domain Spoof** – Email Authentication and Obfuscate Senders

2) **Domain Look A Like** – Detection, Rapid Response and Take Down

3) **Legitimate Sending System Compromise** – Scan Outbound Email from all system, not just your corporate gateway…


proofpoint®