2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Presentación

El Lado Oscuro del Correo Electrónico

ASOCIACION BANCARIA DE PANAMA
ABP

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

El Lado Oscuro del Correo Electrónico:

Proteja sus Correos Electrónicos con Seguridad Impulsada por AI

technologies

2023 CELAES
Congreso Latinoamericano
de Seguridad Bancaria

El Panorama del Correo Electrónico

El número de correos electrónicos enviados y recibidos a nivel mundial ha aumentado cada año desde 2017[1]

El correo electrónico es el vector de ataque más importante que los atacantes explotan para obtener acceso a empresas e individuos[2]

Trabajar desde la casa ha aumentado en más del 55%[3] en los últimos años y, como resultado, las amenazas de seguridad cibernética también han aumentado específicamente a través de los correos electrónicos a una tasa del 32% interanual[4]

65% de las empresas globalmente se enfrento a un ataque de compromiso de correo electrónico empresarial en 2020[5]

El 91 % de todos los ataques dirigidos comienzan con el correo electrónico[6]

1- Statista	2- Information Age	3- The economist	4- IT pro	5- Kaseya	6- Knowbe4

Algunos Desafios de las Empresas

Independientemente del tamaño de la empresa, todas las organizaciones enfrentan problemas de seguridad de correo electrónico

- Las empresas en industrias altamente reguladas (seguros, finanzas, atención médica) deben enviar miles de correos electrónicos cifrados con datos confidenciales a sus clientes a diario. Sin embargo, los destinatarios no abren la mayoría de esos correos electrónicos debido a la complejidad de las soluciones de cifrado actuales.

- Las empresas tienen recursos de TI y seguridad cibernética muy limitados. Se enfrentan a muchas prioridades en competencia y luchan por administrar muchos proveedores diferentes, por lo que a menudo quedan vulnerables.

- La seguridad del correo electrónico es una parte esencial de cualquier infraestructura empresarial. Sin embargo, para obtener una solución de seguridad holística, a menudo una organización necesita hasta 3 proveedores diferentes o más, lo que los deja con seguridad inadecuada o con demandas administrativas adicionales.

Compromiso de correo electrónico

¿Qué es un ataque BEC?

- Los ataques de compromiso de correo electrónico empresarial (BEC) son una forma de delito cibernético que utiliza el fraude por correo electrónico para atacar a las organizaciones para lograr un resultado específico que afecta negativamente a la organización objetivo.
- Un ataque BEC comienza con un ciberdelincuente que piratea y falsifica correos electrónicos para hacerse pasar por los supervisores, el CEO o los proveedores de su empresa.
- Los ciberdelincuentes utilizarán estas técnicas para filtrar datos confidenciales de PII, interceptar transferencias bancarias y robar credenciales.

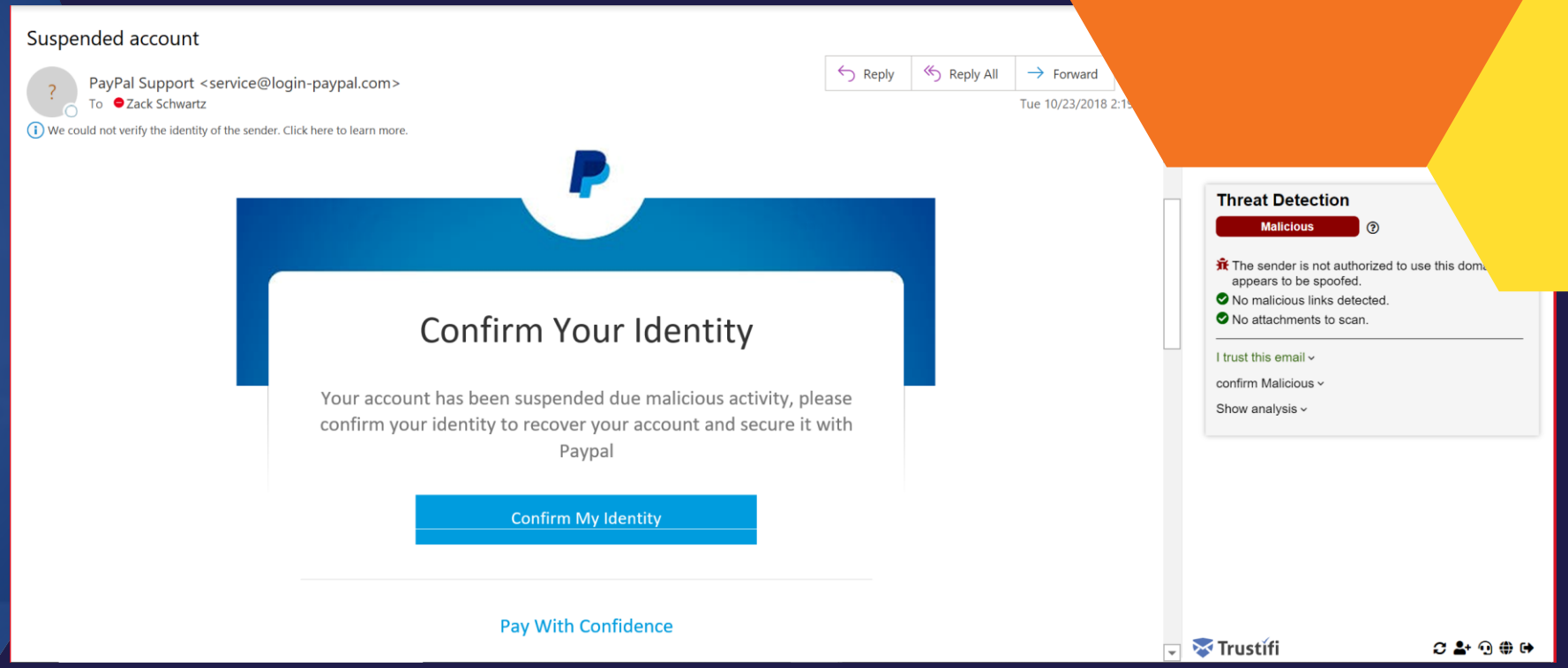
Compromiso de correo electrónico

¿Cómo ocurre un ataque BEC?

technologies

2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

¿Qué aspecto tiene un ataque BEC?

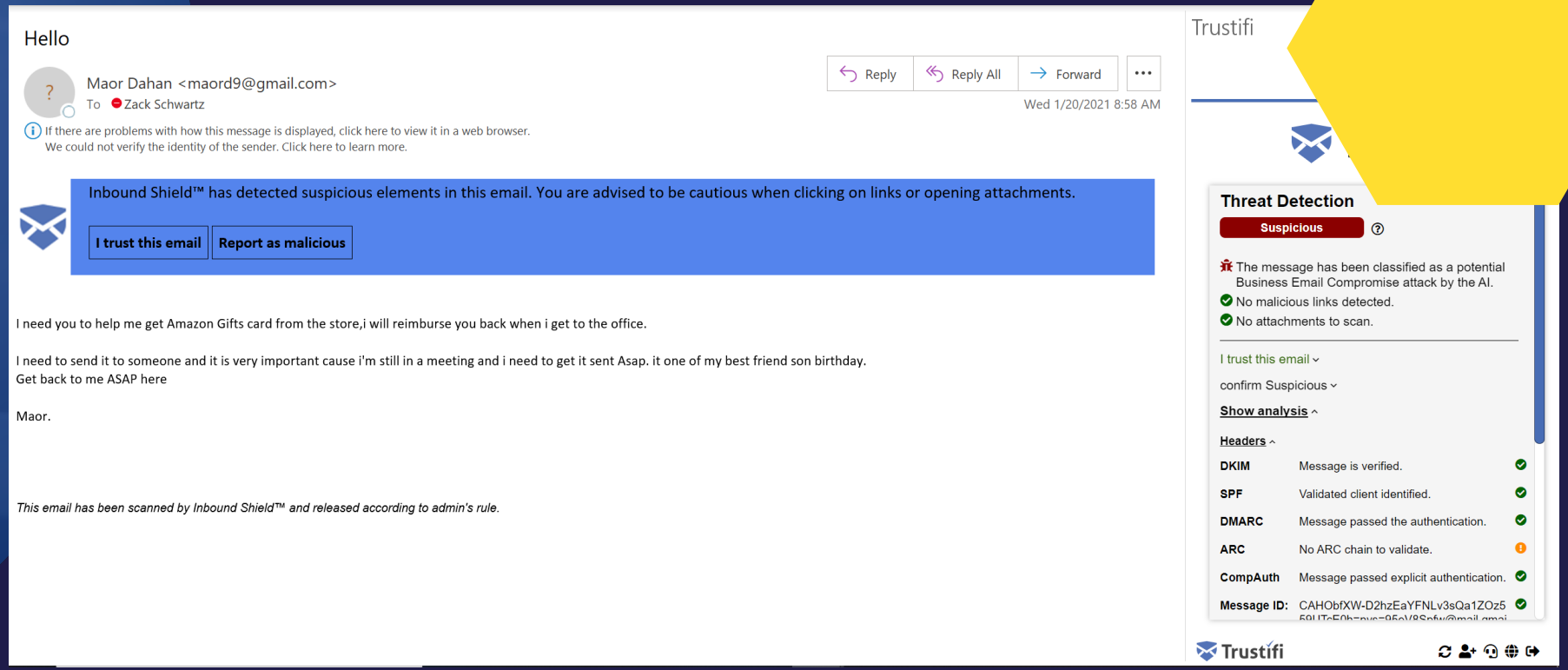


technologies

2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Ataques de Phishing

- El 91% de las violaciones de datos exitosas comienzan con un solo correo electrónico de phishing
- Office 365 es la plataforma número uno dirigida con campañas de phishing, con estafas comunes en torno a páginas de destino y facturas falsas.
- Los atacantes monitorearán su tráfico en tiempo real, identificando cuándo es más alto el tráfico y es más probable que un empleado responda a un correo electrónico de phishing porque está ocupado.

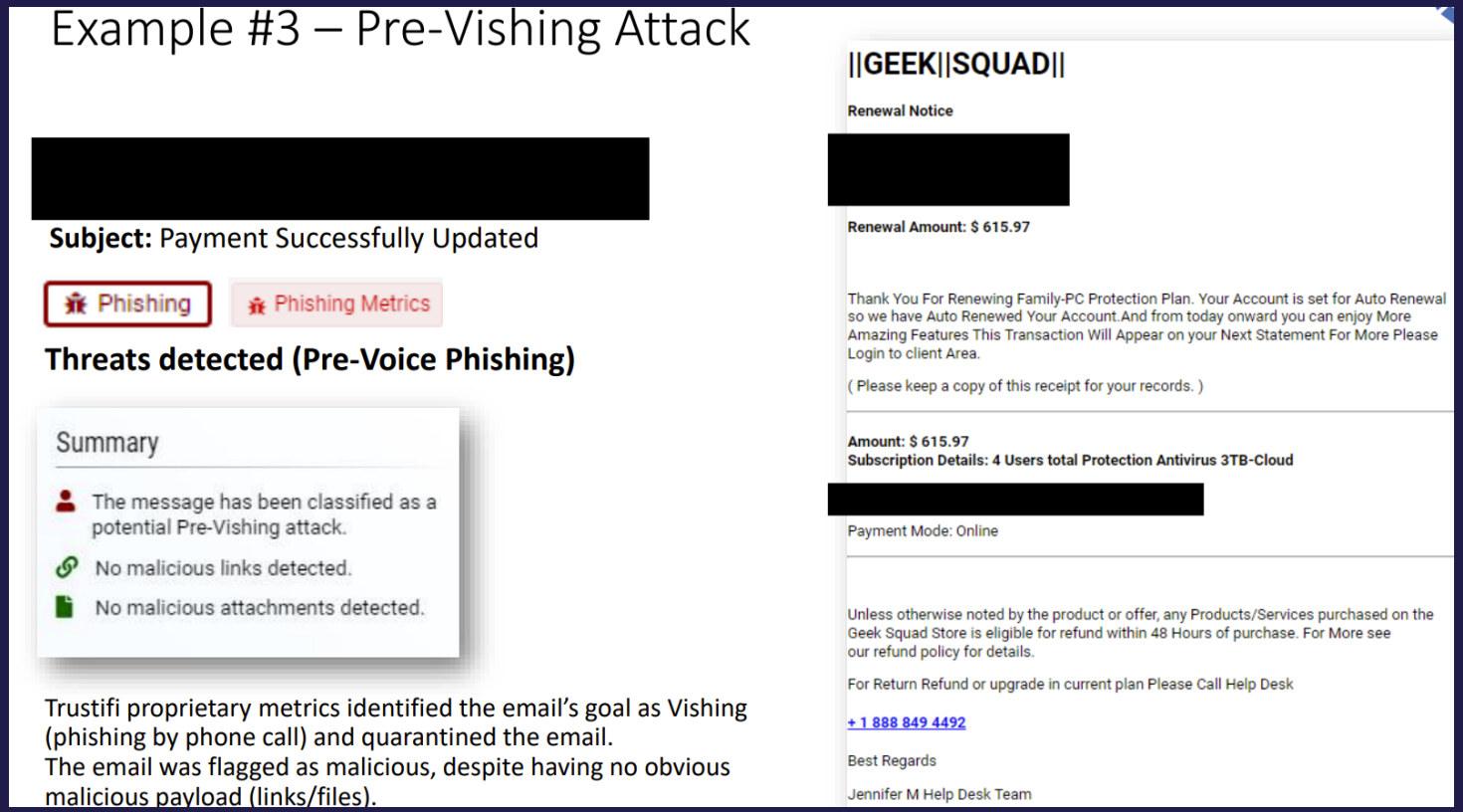


technologies

2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Ataques Previos al Vishing

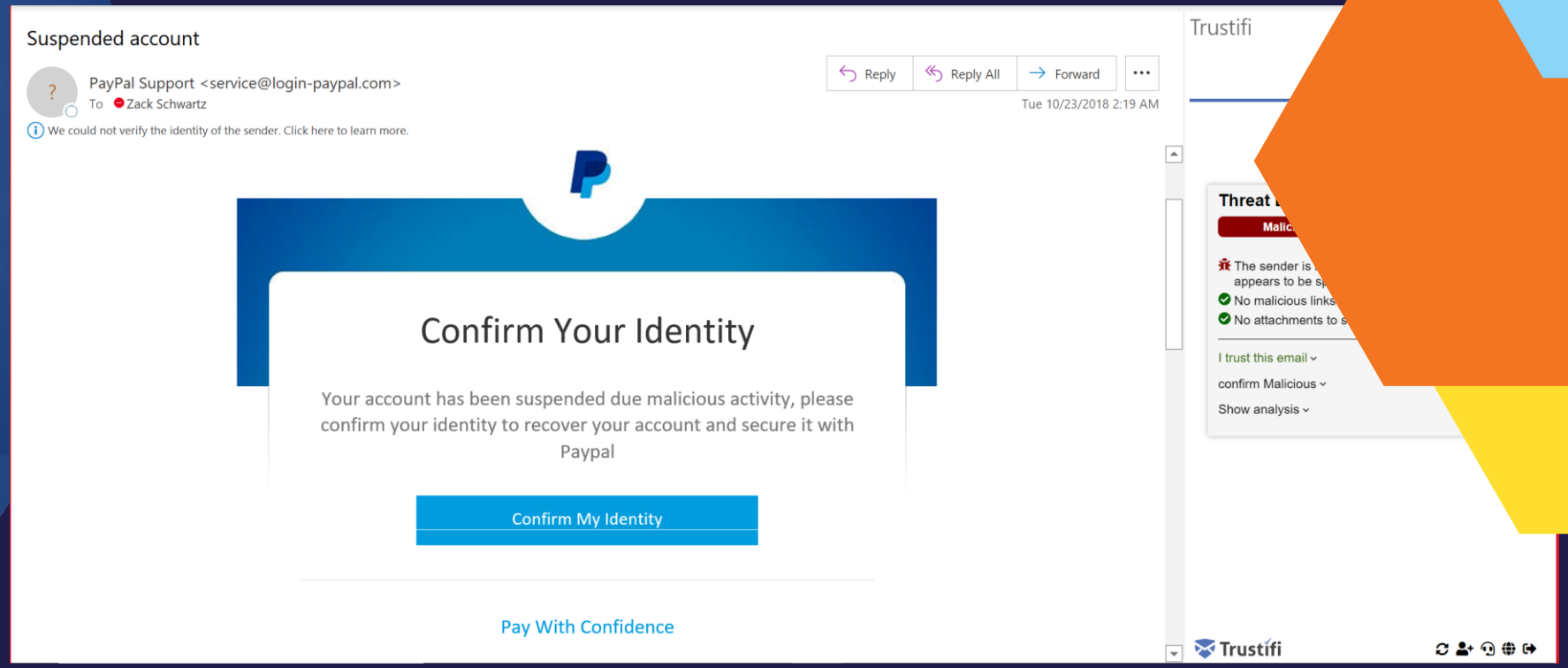
- Los ataques previos a Vishing solicitan al destinatario que llame al número proporcionado para proporcionar a la persona información personal o confidencial.
- Es posible que el correo electrónico en sí no tenga contenido malicioso incrustado, pero cuando el usuario llama al número, cree que es seguro porque hizo la llamada.



technologies
2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

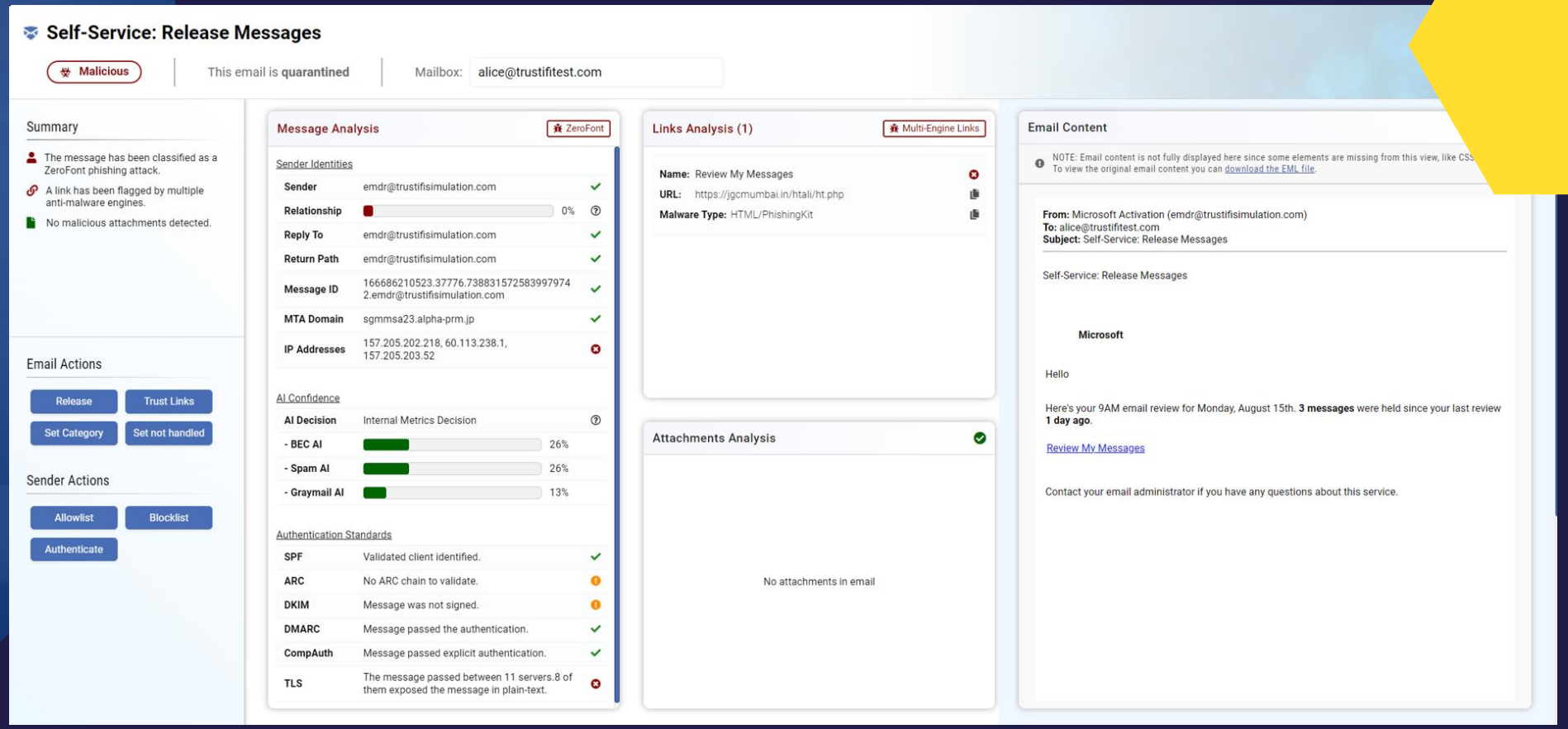
Adquisición de Cuentas

- Los ataques de adquisición de cuentas han aumentado un 307% desde el inicio de la pandemia
- Los ataques de adquisición de cuentas solicitarán al usuario que proporcione sus credenciales a un enlace malicioso. Una vez completado, el actor malicioso cambiará su contraseña bloqueando el acceso del usuario a su cuenta.



Ataque de Fuente Cero

El ataque de fuente cero implica insertar palabras ocultas con un tamaño de fuente de cero que es invisible para el destinatario.

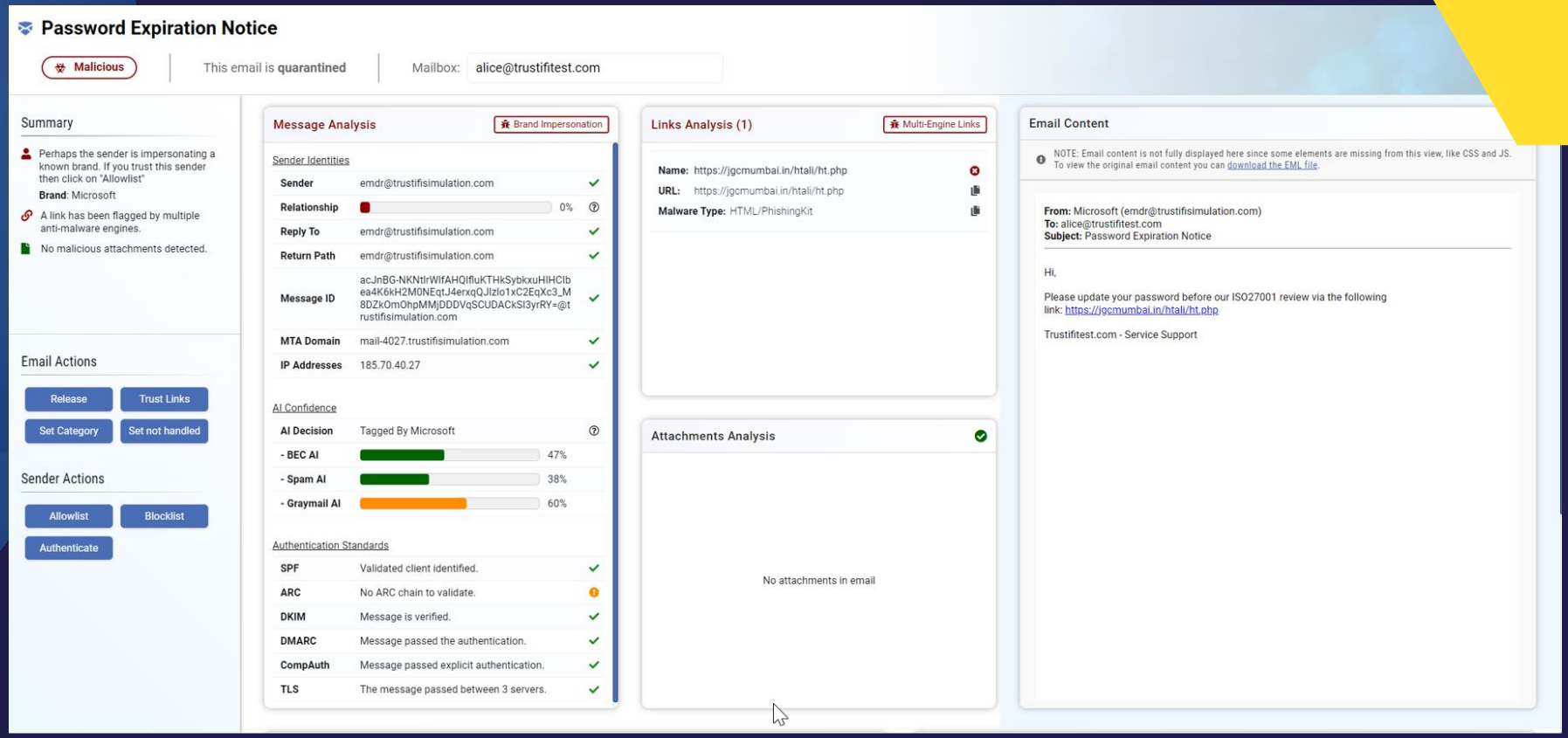


technologies

2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Personificación de Marca

La personificación de marca es un ataque que se hace pasar por una empresa de confianza o una marca para engañar a las víctimas para que respondan y divulguen información personal o confidencial.



technologies

2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

¿Qué se puede hacer para prevenir un ataque BEC?

- Desarrollar una estrategia sólida de prevención de pérdida de datos
- Cree una defensa de entrada en capas utilizando herramientas de IA / ML para detectar ataques sin archivos o enlaces maliciosos
- Analizar datos para comprender mejor si una cuenta se ha visto comprometida por un ataque BEC
- Capacitar a los empleados sobre las mejores prácticas al usar el correo electrónico corporativo

Why Isn't O365 Secure?

Almost 50% of organizations use third party security tools with Office 365. Why?

- Deployment can be complex, and many of O365's best security features are not configured by default
- Email is the most common attack vector; but O365 on it's own has a lack of advanced email security controls
- Skills gap: there is a lot of O365 features and functionality that is complex, and many admins do not configure it
- O365 is very accessible to cybercriminals: you can very easily grab a domain and test out phishing campaigns on the cheap

La seguridad del correo electrónico de Microsoft carece de

Capas adicionales de Protección de entrada

DLP sofisticado y gestión de cumplimiento

Usuario basado en IA Análisis de comportamiento

Guía de mercado de Gartner

Para la seguridad del correo electrónico

"La capacidad de seguridad de correo electrónico predeterminada de Microsoft (Protección de Intercambio En línea (EOP)) carece de capacidades avanzadas de protección contra phishing y otras amenazas. ...

"La ausencia de una capa adicional de protección, sistemas de correo electrónico heredados o puertas de enlace de correo electrónico seguras a menudo no pueden evitar ataques sofisticados de ingeniería social y correos electrónicos maliciosos".

technologies

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

O365 users are targeted with phishing in email and instant messaging

Phishing Attacks 27%

O365 accounts are compromised and used in high-level scams

Account Takeover 20%

O365 users are at risk of data loss and exfiltration

Data Loss & Exfiltration 39%

La Solución---AI & ML

Correos de salida:

- ✓ Cifrado de correo electrónico y autenticación multifactor de destinatarios
- ✓ Prevención de pérdida de datos y exfiltración de datos por correo electrónico
- ✓ Cumplimiento™ con un solo clic

Correos de entrada:

- ✓ Motores de IA para mantener limpia la bandeja de entrada
- ✓ Protección avanzada contra amenazas
- ✓ Protección contra Phishing y BEC
- ✓ Detenga el SPAM y el correo gris

Detección de compromiso de cuenta:

- ✓ Identifique instantáneamente las cuentas que se han visto comprometidas
- ✓ Bloquea automáticamente el acceso a cuentas comprometidas

Indexación inteligente Archivado en la nube:

- ✓ Comparta fácilmente datos, casos y consultas con destinatarios específicos
- ✓ Autenticación inteligente y acceso de monitoreo en tiempo real

Resumen

Dolor

El 91 % de todos los ciberataques dirigidos comienzan con el correo electrónico[1]. Las grandes empresas estadounidenses **pierden en promedio $ 14.8M anualmente por ataques de phishing**[2]. El costo promedio de la violación de datos **en 2021 fue de $ 4.2M con un aumento anual del 10%**[3].

Problema

Los SEG heredados son difíciles de implementar, administrar y no pueden abordar los ataques más sofisticados y avanzados que se utilizan. Los hackers están utilizando herramientas y estrategias de vanguardia para eludir las soluciones existentes, como Phishing, Pre-Vishing, Zero Font Attacks, BEC, Ransomware, Malware y están comprometiendo a terceros previamente aprobados y monitorearán su tráfico esperando el momento adecuado para cambiar la información bancaria o interceptar el tráfico.

Solución

Utilizando una solución avanzada de seguridad de correo electrónico que está diseñada para defenderse contra los ataques modernos y monitorea todos los aspectos de su tráfico de correo electrónico. Capacitación continua de concientización sobre seguridad que mantiene a su personal actualizado sobre los tipos de ataques más recientes.

1- 4- Knowbe4 | 2- Threatpost | 3- Upguard

PREGUNTAS

&

RESPUESTAS

technologies

2023 CELAES
Congreso Latinoamericano
de Seguridad Bancaria

IG TECHNOLOGIES

Simplifying Cybersecurity Solutions

Gracias