REPORT

SLASHNEXT

Real-Time Threat Observability

Email Risk Report

Summary

This report has been designed to identify the many linked-based attacks, natural language-based attacks, malicious attachments, and exploits missed by your current email security services.

Based on the analysis of **869,364** email messages covering a **30-day** period, **86,465** messages have been identified as carrying threats. The assessment identified **1,436** total users of which **1,149 (80%)** were targeted by these attacks. **38** users were identified as executive targets as they received more than **15** messages within the observability period.

Threat Breakdown

Type	Email
Malicious Links / Identity Credential Phishing	**Zero-hour**: 19,022 **Out of Total**: 54,467 (63%)
Attachment Exploits / Ransomware	**Zero-hour**: 9,986 **Out of Total**: 20,749 (24%)
BEC / Financial Fraud	**Zero-hour**: 6,221 **Out of Total**: 11,239 (13%)
Total	**86,456**

Review

Based on this report, you have a company-wide threat exposure of over **$700,000/year**. With SlashNext Integrated Cloud Email Security, based on these results your exposure would be $0, all threats identified here would have been stopped before they caused any harm.

To learn more about the SlashNext Integrated Cloud Email Security service and to discuss the full details of this assessment and a prescribed solution, schedule and full review with a SlashNext security professional at https://www.slashnext.com/.

869,364
EMAILS SCANNED

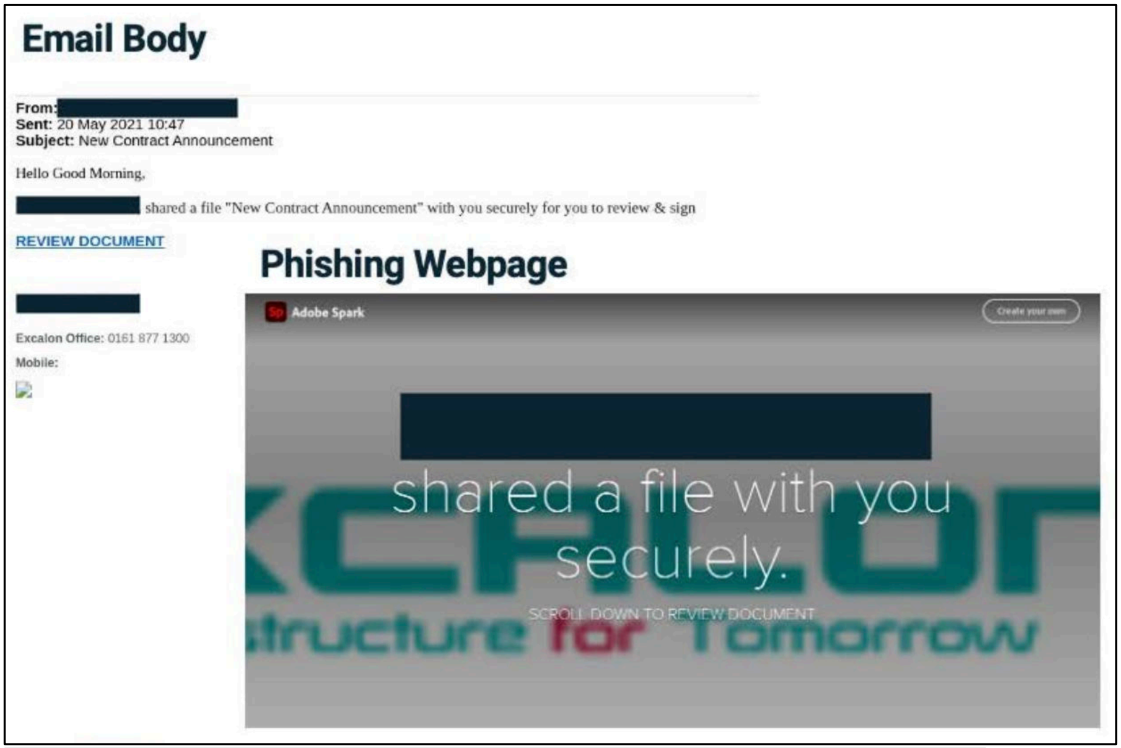
86,465
MALICIOUS EMAILS

38
EXECUTIVES TARGETED

80
RISK SCORE

EMAIL THREAT ANALYSIS

THREAT EXAMPLES FOUND DURING THE OBSERVATION PERIOD



Email Body

From: [redacted]
Sent: 20 May 2021 10:47
Subject: New Contract Announcement

Hello Good Morning,

[redacted] shared a file "New Contract Announcement" with you securely for you to review & sign

REVIEW DOCUMENT

[redacted]

Excalon Office: 0161 877 1300

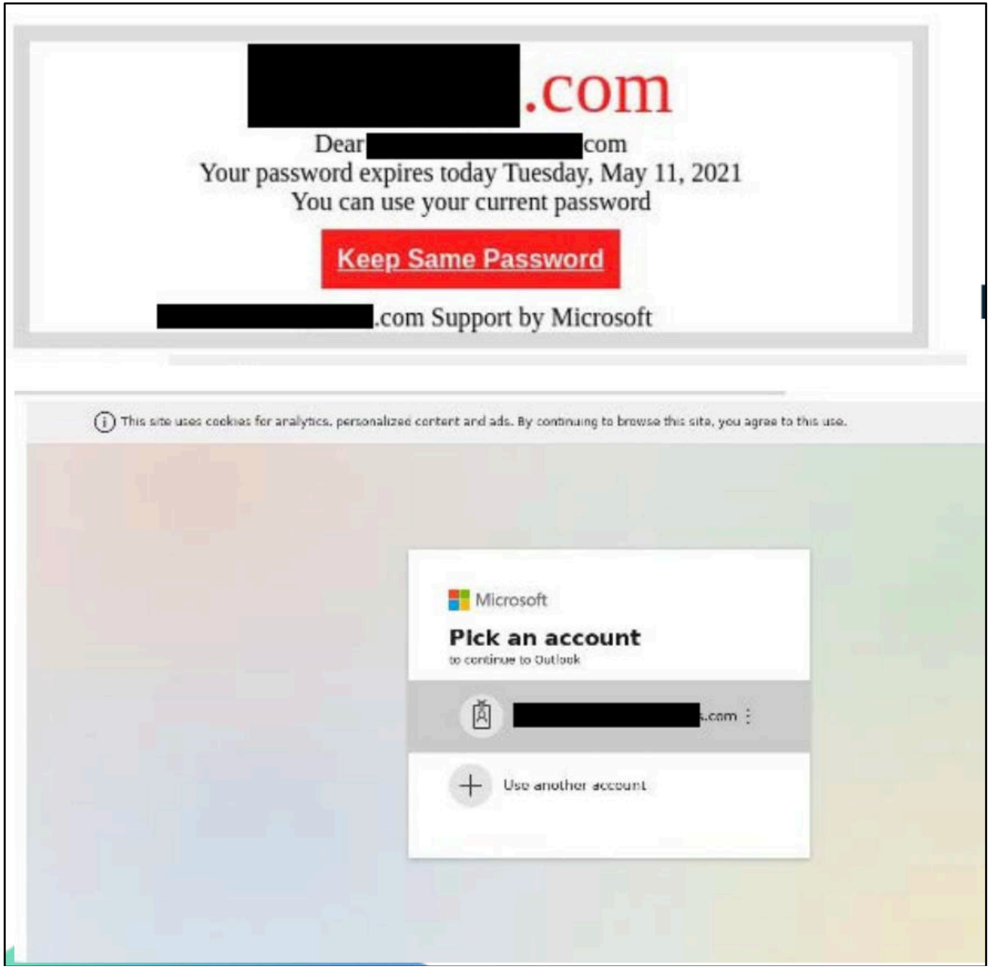
Mobile:

Phishing Webpage

[redacted]

shared a file with you securely.

SCROLL DOWN TO REVIEW DOCUMENT



[redacted].com

Dear [redacted]com
Your password expires today Tuesday, May 11, 2021
You can use your current password

Keep Same Password

[redacted].com Support by Microsoft

ⓘ This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you agree to this use.

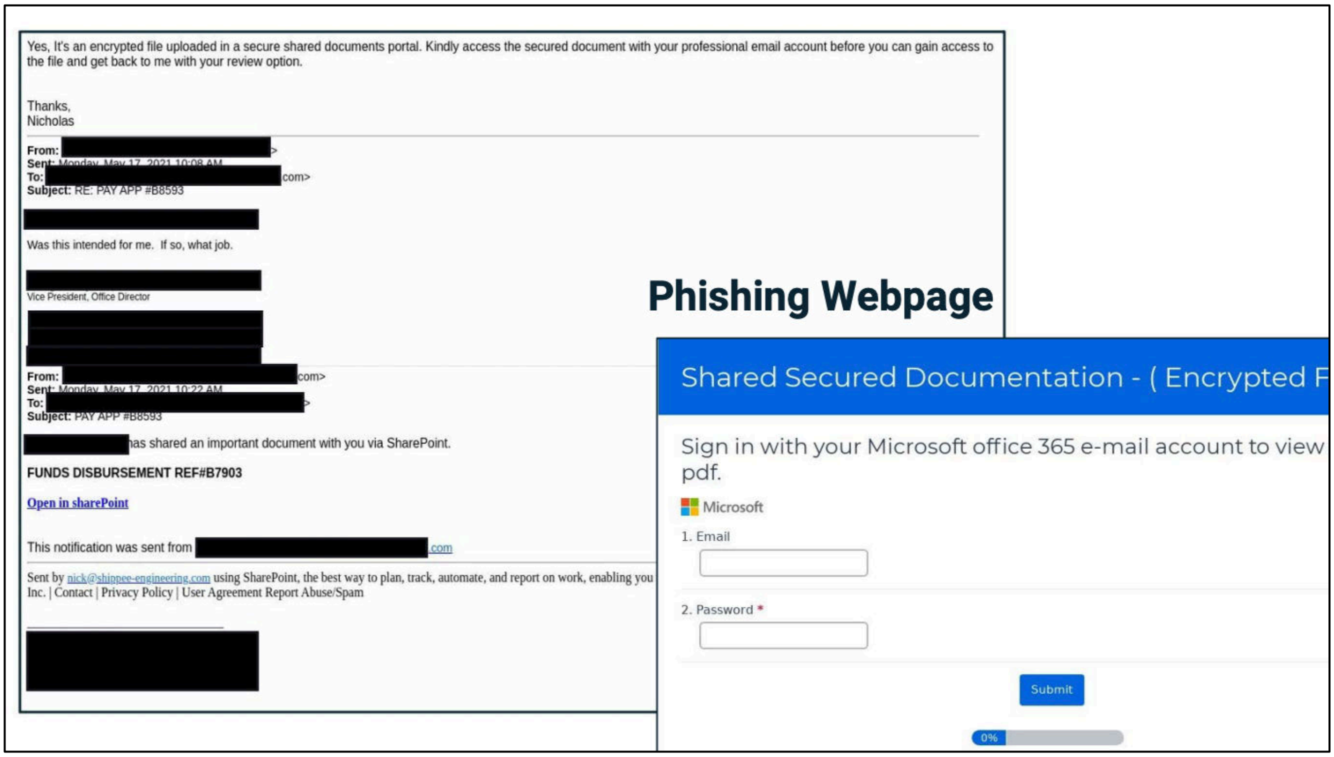
Microsoft

Pick an account

to continue to Outlook

[redacted].com ⋮

+ Use another account



Yes, It's an encrypted file uploaded in a secure shared documents portal. Kindly access the secured document with your professional email account before you can gain access to the file and get back to me with your review option.

Thanks,
Nicholas

From: [redacted]>
Sent: Monday, May 17, 2021 10:08 AM
To: [redacted]com>
Subject: RE: PAY APP #B8593

[redacted]

Was this intended for me. If so, what job.

[redacted]
Vice President, Office Director

[redacted]

From: [redacted]com>
Sent: Monday, May 17, 2021 10:22 AM
To: [redacted]>
Subject: PAY APP #B8593

[redacted]has shared an important document with you via SharePoint.

FUNDS DISBURSEMENT REF#B7903

Open in sharePoint

This notification was sent from [redacted].com

Sent by nick@shippee-engineering.com using SharePoint, the best way to plan, track, automate, and report on work, enabling you
Inc. | Contact | Privacy Policy | User Agreement Report Abuse/Spam

[redacted]

Phishing Webpage

Shared Secured Documentation - (Encrypted F

Sign in with your Microsoft office 365 e-mail account to view
pdf.

Microsoft

1. Email

2. Password *

82% of successful breaches start with a human compromise threat, includes ransomware, malware, data exfiltration and financial fraud. SlashNext protects the modern workforce from malicious messages across all digital channels. SlashNext's patented HumanAI^{TM,} a combination of computer vision, natural language processing, and behavioral contextualization, detects threats in real time with 99.9% accuracy. SlashNext Complete™ integrated cloud messaging security platform stops zero-hour threats in email, mobile, and web messaging apps across M365, Gmail, LinkedIn, WhatsApp, Telegram, Slack, Teams, and other messaging apps to detect and prevent threats before they become a breach.