

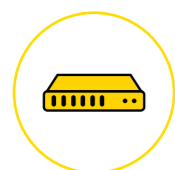


雲端安全

Google Workspace

Microsoft 365

Microsoft Exchange (Online)



地端安全

Microsoft Exchange (On-premises)

其他自建郵件系統



需要更多資訊 · 請上官網 www.cellopoint.com

Email: sales.tw@cellopoint.com

TEL: (02) 8969-2558 分機 820 彭小姐

Why CELLOPOINT

Secure Your Email 是我們的使命，也是 Cellopoint 致力於對抗全世界駭客與商業間諜的原動力。

根據統計，有85%的組織被新型態的釣魚郵件 (Phishing)、勒索病毒(Ransomware)、偽冒詐騙 (BEC)郵件所攻擊，這些進階威脅從以往的大量攻擊手法，轉變為少量目標式攻擊(Targeted attack)，用以突穿現有防線。

因應新型態威脅，Cellopoint 運用全新人工智慧 (AI)、機器學習(ML)、深度學習(DL)演算法，分析攻擊者的思維、行為、意圖與特徵，有效地分辨出幾可亂真的攻擊郵件，這是為什麼選擇 Cellopoint 的主因。



榮獲 Gartner 客戶之聲 4.7 分評價



Cellopoint Reviews 4.7 ★★★★★

CIO / CISO 不能不知道的3大電子郵件威脅



釣魚

Phishing



勒索

Ransomware



詐騙

Business Email Compromise

1 >> 釣魚 (Phishing)

[重要] IT部門通知

Jack Wu <btg13110@yahoo.com>
To: Shirley Lin <shirley.lin@yedotech.com>

週三 2021-07-12 13:15

Hello Shirley,

稍早發現公司有安全漏洞疑慮，為避免造成公司更大的損失，請各位同仁**盡快**更改個人密碼。連結如下：

密碼更改

Thank you,
Jack | IT 經理 | Yedo Technologies

- 內部員工顯示名稱偽冒
- 郵件地址與 Jack 的顯示名稱不同
- 寄件網域非該公司網域 yedotech.com
- 增加急迫感
- 憑證釣魚URL

釣魚攻擊透過社交工程手法來引誘收件人點擊郵件中的釣魚連結 (Phishing URL)，以竊取收件人的帳號、密碼、信用卡資訊或個資；釣魚攻擊也可能帶有惡意的偷渡式下載連結 (Malicious URL)，誘騙收件人點擊以觸發惡意軟體執行。

Cellopoint 釣魚解決方案提供以下偵測及防護機制來阻擋魚叉式釣魚、憑證釣魚及捕鯨式釣魚攻擊 (Whaling)：

- 點擊前與 100 類 URL 威脅情資比對。
- URL 重寫 (URL rewrite) 及 點擊當下的 ToC (Time of Click) 即時掃描。
- 回溯掃描 (Retroactive scanning)。
- 檢測 Microsoft Office 檔案、PDF 和 ZIP 文件中的 URL。

2 >> 勒索病毒 (Ransomware)

勒索病毒是一種惡意軟體 (Malware)，主要透過帶有惡意附檔或 URL 的電子郵件來傳播。一旦下載到勒索病毒，受害者的電腦系統就會被鎖住或檔案被加密，為取回電腦控制權或換取解密金鑰，受害者將支付龐大的贖金。

Cellopoint 勒索病毒解決方案提供以下偵測及防護機制來阻擋勒索病毒攻擊：

- 靜態程式碼分析 (Static code analysis)。
- 動態沙箱引爆及分析 (Sandbox simulation and analysis)。
- 壓縮檔檔案偵測(如：ZIP、TAR、TBZ、TGZ、LZH、JAR 等)。
- 加密附檔偵測。
- 詳細的惡意軟體鑑識報告 (APT-File 模組)。

RE: Final Partnership Agreement

Allison Liao <lin81370@gmail.com>
To: Mandy Lee <mandy.lee@yedotech.com>

Belltech Partnership Agreement 2021083.doc

Tue 2021-08-31 09:53

Hi Mandy,

Sorry, I just saw a critical error, can you review the changes in the attachment **asap**?

Thanks,
Allison | Legal | Yedo Technologies

- 內部員工顯示名稱偽冒
- 郵件地址與 Allison 的顯示名稱不同
- 寄件網域非該公司網域 yedotech.com
- 帶有勒索病毒的附檔
- 增加急迫感

Vasti-Yedotech-匯款資訊變更&envoiceDH20211032

Luke Smith <luke.smith@vast1.com>
To: Jessie Jones <jessie.jones@belltech.com>

envoiceDH20211032.pdf 匯款資訊.pdf

週三 2021-08-11 05:38

Hi Jessie,

感謝您對 Vasti 的支持，在此通知您 Vasti 的匯款資訊已變更，詳細資訊請見附檔。

另附上此次服務的電子發票DH202111032，再麻煩您將此次的款項新台幣 800,000 元及未來的款項匯進我們的新帳戶，謝謝。

因該筆款項的匯款期限已到，提醒您**於今日完成匯款**。

Thank you,
Jack | 財務部 | Yedo Technologies

- 供應商顯示名稱偽冒
- 以相似網域偽冒供應商網域
- 假的附檔，不帶有惡意軟體
- 增加急迫感
- 可疑的匯款要求

>> 商業電子郵件詐騙 (BEC)

BEC (Business email compromise) 商業電子郵件詐騙，又稱 BEC 變臉詐騙，是透過假冒成內部員工、高階主管或外部供應商來欺騙員工進行電匯付款或洩漏機密資料。

Cellopoint BEC 解決方案提供以下偵測及防護機制來阻擋 BEC 詐騙：

- DMARC 認證檢測。
- 顯示名稱偽冒 (Display name spoofing) 及相似域名 (Look-alike domain) 偵測。
- 寄件人行為塑模分析：分析寄件人與收件人間的通信模式以偵測異常訊息。
- 郵件內容與意圖檢測：偵測郵件主旨和內容中的特定用字，如：「匯款」、「電匯」、「緊急」或「請求」。

Next-generation AI-based Email Security

Cellopoint 推出新世代郵件安全解決方案，基於人工智慧 (AI) 及機器學習 (Machine Learning) 演算法進行塑模，分析駭客攻擊的思維、行為、意圖與特徵，結合 Cellopoint 全球電子郵件威脅情報 Email TI (Threat Intelligence)，可有效地分析少量的目標式攻擊 (Targeted attack)，及阻斷瞬間大量的病毒 (Virus outbreak) 攻擊。

針對 Microsoft 365 雲端郵件，透過 Graph API 整合，不需更動郵件路由 (DNS MX) 與使用者習慣，可無縫整合與補強郵件安全縱深防禦。

另外，All-in-one 全方位治理平台可提供寄外郵件 DLP 稽核與加密、郵件歸檔檢索，讓您有效地掌控郵件安全、郵件資料外洩防護、郵件數位資產保存與法規遵循等三大管理議題。

All-in-one Solution:

Security					DLP		Archiving			Signature
Anti-Spam SPAM AG	Anti-Virus AV	Anti-APT URL URL	Anti-APT File File	Anti-BEC BEC BEC	Audit AUD	Encryption ENC	Archive MA	Grid Search GDS	Case Management CAS	SIG
CelloOS™										
Azure, AWS, GCP / VMware, Hyper-V / x86 server, Appliance										