保安資訊--本周(台灣時間2024/04/05)賽門鐵克原廠防護公告重點說明

前言

賽門鐵克原廠首要任務就是保護我們的顧客，被譽為賽門鐵克解決方案專家的保安資訊更能發揮我們被高度認可的專業知識與技能、豐富經驗以及專為幫助客戶成功的服務熱忱，與顧客共同創造賽門鐵克解決方案的最大效益，並落實最佳實務的安全防護。攻擊者從不休息，我們更不會。一支技術精湛且敬業的團隊不斷創造新的防護措施，以應對每天發布成千上萬的新威脅。儘管不可能詳述我們已經可以防禦的每種新威脅，但該站點至少反映了我們的努力。這些公告分享針對當前熱門新聞話題有關威脅的保護更新，確保您已知道自己受到最佳的保護。點擊此處獲取賽門鐵克原廠防護公告(Protection Bulletins)。

關於 保安資訊有限公司 | 從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

在端點啟用賽門鐵克入侵預防系統(IPS) 的好處(以下皆為美國時間)

賽門鐵克的入侵預防系統 (IPS) 是業界一流的深層封包檢測技術引擎，可保護包括財富 500 強企業和消費者在內的數億個端點(桌機／筆電／伺服主機)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在 51 萬 5,700 台受保護端點上總共阻止了 5,720 萬次攻擊。這些攻擊中有 84.3% 在感染階段前就被有效阻止：**(2024/04/01)**

- 在**10萬9,600**台端點上，阻止了**1,980**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**14萬6,900**台端點上，阻止了**1,100**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬6,300**台**Windows**伺服主機上，阻止了**8,700**萬次攻擊。
- 在**6萬5,900**台端點上，阻止了**210**萬次嘗試掃描伺服器漏洞。
- 在**1萬8,100**台端點上，阻止了**99**萬次嘗試掃描在**CMS**漏洞。
- 在**5萬400**台端點上，阻止了**150**萬次嘗試利用的應用程式漏洞。
- 在**17萬7,200**台端點上，阻止了**420**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**8,300**台端點上，阻止了**420**萬次加密貨幣挖礦攻擊。
- 在**10萬1,900**台端點上，阻止了**770**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**550**台端點上，阻止了**7萬700**次加密勒索嘗試。

強烈建議用戶在桌機／筆電／伺服主機上啟用 IPS (不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用 IPS 的說明，或與保安資訊聯繫可獲得最快最有效的協助。

有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點(桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在 13 萬 2,700 個受保護端點上阻止了總計 510 萬次攻擊。**(2024/04/01)**

- 使用網頁信譽情資，在 **119.5K** 個端點上阻止 **450** 萬次攻擊。
- 攔截 **28K** 個端點上 **516.6K** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在 **11.3K** 個端點上攔截 **129.6K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **424** 個端點上攔截 **21.8K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

2024/04/05

在針對金融行業活動中觀察到JsOutProx惡意軟體的新變種

在最近針對非洲、中東、南亞和東南亞金融業的網路攻擊行動中，發現 JsOutProx 惡意軟體的新變種涉入其中。JsOutProx 遠端存取木馬 (RAT) 是歸屬於 Solar Spider 駭客組織所有。該駭客組織過去一直把惡意有效酬載上架在 GitHub 儲存庫，而最新的攻擊則利用 GitLab 平臺上的儲存庫。JsOutProx 採用模組化架構，具有執行 shell 命令、上傳／下載檔案、修改系統檔、螢幕截圖和擷取各種系統資訊等功能。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- JS.Downloader
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2024/04/05

Byakugan(*百樂甘)惡意軟體

最近在真實網路情境發現到 Byakugan 惡意竊密程式，它具有模組化的架構。該惡意軟體被偽裝成 Adobe Reader 安裝程式進行傳播。該惡意軟體接收來自遠端 C&C 伺服器的命令，該伺服器還充當攻擊者的控制台。Byakugan的功能包括鍵盤側錄、螢幕截圖、加密貨幣挖礦劫持、竊取存儲在網路瀏覽器中的資訊以及下載任意檔案等。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Ps-SvcReg!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Pidief
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.C

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2024/04/04

Phorpiex惡意軟體涉入針對歐洲和北美的金融業的網路攻擊

觀察到一起傳播 Phorpiex 殭屍網路的惡意軟體網路攻擊行動，該行動針對歐洲和北美的金融機構組織。攻擊鏈包含使用嵌入惡意巨集的捷徑檔來感染使用者的系統並下載額外的惡意軟體籌載。Phorpiex可以在沒有活躍的 C&C 伺服器的情況下運行，主要是利用加密貨幣剪貼簿竊密器 (Clipper) 伎倆來置換加密錢包的地址進而竊取加密貨幣。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-Http!g2

- ACM.Ps-CPE!g2
- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen6
- SONAR.SuspProfileRun

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen205
- ISB.Downloader!gen221
- Trojan Horse
- Web.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2024/04/04

印尼正在流行--以喜帖作為誘餌的「簡訊內容轉發」惡意程式

早在 2023 年年中，就發現有人向印尼的智慧型手機用戶發送簡訊，誘使他們安裝一個冒充婚禮邀請函的 APP。在過去幾個月中，此類惡意 APP 日益增多。該類惡意軟體主要目的是收集簡訊，並透過 Telegram 機器人的 API 將其轉發到作者的 Telegram 頻道。

觀察到的 APP 安裝檔檔名：

- UNDANGAN PERNIKAHAN DIGITAL_1.0.apk
- Surat Undangan.apkAcara Resepsi_1.0.apk
- Surat Undangan Online0.apk
- Surat Undangan Wedding Digital_ok.apk
- Undangan-resmi.apk
- Undangan pernikahan-1.0.apk

「簡訊內容竊取／轉發」日益受到惡意行為者的覬覦，原因有幾個。首先，簡訊通常包含一次性密碼 (OTP) 和金融交易確認等敏感資訊，可被用於金融欺詐或身份盜用。其次，透過攔截包含驗證碼的簡訊，惡意軟體可以繞過雙因素驗證，在未經授權的情況下接管帳戶。此外，截獲的簡訊還可用於間諜、監視或個人間諜活動，使攻擊者能夠監控通訊或跟蹤個人。利用竊取的簡訊內容製作令人信服的網路釣魚資訊，可為社交工程攻擊提供更高的信任。此外，攻擊者還可能利用從簡訊中獲取的洩露資訊進行勒索或敲詐。最後，被盜的簡訊資料可在暗網上出售牟利，或出售給其他有興趣利用這些資料的惡意行為者。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- Android.Reputation.1
- AppRisk:Generisk

2024/04/04

Latrodectus惡意軟體

Latrodectus 是 2023 年 11 月首次發現的惡意軟體載入器 (loader)。該惡意軟體最近在 TA577 和 TA578 威脅組織的惡意行動中被大肆傳播。該惡意軟體載入器主要用於攻擊的初始階段，以執行遠端命令和下載附加有效酬載。值得注意的是，它在傳播行動中採用的技術和基礎設施與之前的 IcedID 行動有許多雷同之處。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-Wscr!g1
- ACM.Wscr-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspBeh!gen805
- SONAR.SuspLaunch!g360

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Heuristic!gen20
- Scr.Malcode!gen
- Scr.Malcode!gen137
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Latrodectus
- Trojan.Pikabot!gen13
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2024/04/03

XZ Utils程式庫被植入隱密後門的程式碼

3 月 29 日發佈一個安全警報，警告用戶某些版本的 XZ Utils 程式庫中嵌入惡意後門程式碼，XZ Utils 是一個流行的資料壓縮工具庫，幾乎存在於所有 Linux 發行版本中。該惡意程式碼被追蹤為 CVE-2024-3094，嵌入在 XZ Utils 5.6.0 和 5.6.1 版本中，可允許遠端惡意行為者破解 sshd 身份驗證並在未經授權的情況下存取整個受影響的系統。

大多數主要 Linux 發行版本的穩定分支都使用較舊版本的工具程式，因此不太可能影響生產系統。運行最新版本 Linux 用戶最有可能受到影響。美國網路安全暨基礎設施安全局 (CISA) 建議開發人員和使用者根據發行版本維護者的指示，將 XZ Utils 降級／回溯到未受影響的版本。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於端點偵測與回應(EDR)：

- IF.CVE-2024-3094!Lg1
- IF.CVE-2024-3094!Lg2
- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多資訊，請參閱此鏈接：https://github.com/Symantec/threathunters/tree/main/Trojan/IcedID
- 賽門鐵克的端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.NPE

基於安全強化政策(適用於使用DCS)：

DCS 強化

- 透過在 sym_unix_protection_sbp 政策中的全域檔案規則--禁止存取資源清單中新增 */liblzma.so.5.6.0、*/liblzma.so.5.6.1，以防止 sshd 或任何應用程式載入易受攻擊的 liblzma 程式庫版本。
- 透過使用應用程式規則將 xz 程式 (/usr/bin/xz*) 路由至 deny_ps 沙箱，防止在不需要的環境中執行 xz 程式。DCS 應用程式搜索將會回報這些應用程式。
- Sym_unix_protection_sbp 政策預設鎖定 sshd 程式，並受到預設的 daemon 沙箱限制。

DCS 監控

- 透過新增檔案監視規則來監視 /lib/x86_64-linux-gnu/liblzma.so.* 和 /usr/lib/x86_64-linux-gnu/liblzma.so.* 的更改，進而檢測 xz 程式庫是否被篡改。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/04/03

MacOS使用者成為惡意竊密程式覬覦的目標

MacOS 用戶繼續經由惡意廣告和虛假網站的傳播而感染惡意竊密程式。在最近一次網路攻擊行動中，我們發現一個提供免費會議室預約系統軟體的假冒網站。該網站安裝的惡意竊密程式能夠提取使用者的「鑰匙圈存取」資料、網路瀏覽器中存儲的憑證以及加密貨幣錢包中的資訊。該惡意軟體與基於 Rust 的名為 Realst 的惡意竊密程式系列具有相似的特徵，並採用 AppleScript 工序指令來提示使用者輸入 macOS 登錄密碼，以執行其惡意活動。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Trojan.Gen
- WS.Malware.1

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2024/04/03

TA588駭客組織繼續在拉丁美洲開展間諜活動

TA558 駭客組織以針對拉丁美洲各行業而聞名，最近發現該組織利用帶有惡意附件的垃圾郵件傳播 Venom 遠端存取木馬 (RAT)，這是一種源於 Quasar RAT 的遠端存取木馬。該惡意軟體具有擷取敏感性資料和遠端控制被入侵系統的功能。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn32
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2024/04/03

YouTube 帳號劫持：傳播惡意竊密程式的攻擊活動增多

據觀察，利用 YouTube 發動的網路攻擊活動越來越多，威脅行為者劫持現有的熱門 YouTube 帳戶來傳播 Vidar 和 LummaC2 惡意竊密程式。使用者被聲稱提供 Adobe 等常用程式破解版的影片所引誘。評論區提供的連結指向上傳到 MediaFire 的惡意套裝程式 (MediaFire 是一家存放使用者檔案和圖像的服務網站)。結果，使用者在不知情的情況下載並執行惡意程式碼，而不是所需的程式，從而受到感染。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn32
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2024/04/03

Napoli(*那不勒斯)勒索軟體

最近在真實網路情境發現 Chaos 勒索軟體的變種--Napoli。該惡意軟體會加密使用者檔案，並冠上 .napoli 副檔名，還會更改受感染電腦的桌布。攻擊者會以名為『read_it.txt』的文字檔形式發送贖金支付說明，並要求用戶用比特幣支付。此外，該惡意軟體還具有刪除受感染機器上磁碟區陰影複製的功能。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RLsass!g1
- ACM.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2024/04/03

手機／行動裝置威脅環境中出現全新的Vultur銀行金融木馬種

在真實網路情境出現一種新版本的安卓 Vultur 銀行金融木馬種。該版本具有更強的規避技術和先進的遠端控制能力。在最近網路攻擊行動中，受害者透過簡訊發送的連結和電話提供的說明被誘騙安裝被木馬化的安全軟體 APP。然而，這個 APP 實際上是 Brunhilda 惡意程式植入器，它會啟動初始攻擊，後續會引爆 Vultur 惡意軟體有效酬載的下載和執行。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- AppRisk:Generisk
- AdLibrary:Generisk
- Other:Android.Reputation.1

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

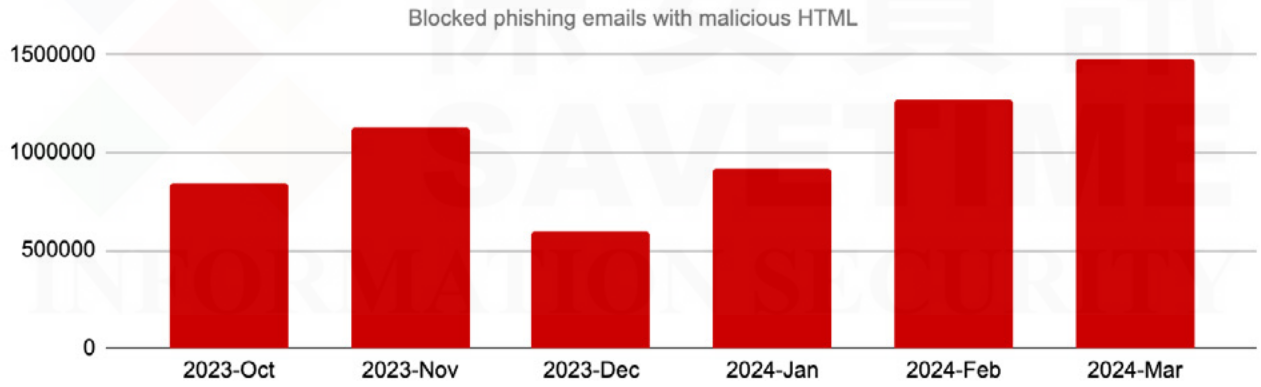
被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2024/04/02
防護亮點：HTML附件在網路釣魚呈現日益增長的趨勢

網路威脅情勢的不斷發展，網路釣魚應該是最禁得起時間考驗的資安威脅。網路釣魚攻擊的歷史幾乎與網際網路本身一樣悠久，一直困擾著全球的組織和個人。與利用技術漏洞的複雜網路攻擊不同，網路釣魚利用人為因素，利用心理操縱來實現其目標。

儘管網際網路上的通訊方式和技術一直推陳出新、行動裝置上的簡訊網路釣魚攻擊也持續上升，但是電子郵件仍然是網路釣魚攻擊的主要手段。說到電子郵件的威脅，內嵌 HTML 類型的附件網路釣魚攻擊，包括 HTML、SHTML 和 XHTML，仍然是最常見的技術之一。它的人氣不墜主要因素是因為它易於建立和客製化。網路犯罪分子通常只需具備最低限度的專業技術，就能迅速利用現成的範本和線上教學，建立令人信以為真的合法網站翻版。

在大多數甚至全部情況下，以令人信服而且極具說服力的語言詳述、虛假的安全警報和營造一種有急迫性情景的資訊，塑造出讓人信服的假象，預先填寫收件人電子郵寄地址的登錄欄位，會令使用者難以辨別真假網站。此外，攻擊者採用各種混淆技術來隱藏 HTML 類型的釣魚頁面中惡意程式碼。編碼 (Encoding)、加密 (encryption) 和動態內容常被用來規避傳統的檢測機制並繞過資安檢查機制。



針對不同的受害者群體，網路釣魚行動的規模也大不相同。受害者可能是預先精準瞄準的特定目標、也可能是更廣泛的亂槍打鳥、或是具有一定的共同點，例如：地理區域或產業領域。雖然與勒索軟體或網路間諜等備受關注的網路威脅相比，網路釣魚攻擊似乎影響較小，但它們是引爆許多網路攻擊最關鍵的起點。它們導致各式各樣的危害，包括資料竊取、財務損失、身份盜用、勒索軟體感染、帳號填充攻擊、商業電郵詐騙、網路入侵和聲譽損害。

賽門鐵克的電子郵件雲端安全服務 (Email Security.Cloud) 和郵件安全閘道 (SMG：Symantec Messaging Gateway) 是抵禦此類網路釣魚和常見網路釣魚的完善解決方案，這要歸功於其精心設計的一整套先進技術，可保護企業免受此類威脅。

- **垃圾郵件過濾系統**：預測性過濾系統能針對附件檔的風險屬性和其他電子郵件特徵及時更新，高效攔截出現在不斷變化的威脅環境中瞬息萬變的電子郵件威脅。
- **模擬器和啟發式特徵／簽名**：我們的解決方案利用先進的模擬器和啟發式特徵／簽名來檢測電子郵件中嵌入的惡意 HTML。透過模擬程式碼執行和分析行為模式，我們可以在潛在威脅對組織造成危害之前將其識別出來並予以消除。
- **專利的 WebPulse 網頁分類技術**：以自動化群眾外包驅動的網頁聲譽生態系，這是一個

雲端的基礎架構，專門設計用於利用用戶驅動行為的力量，並將使用者輸入轉化為全球網路情資和網路威脅情資。

- **資料保護服務**：如果沒有合法的業務原因，HTML、SHTML 和 XHTML 等格式的附件檔--我們建議使用資料保護規則直接阻止這些 MIME 類型的附件檔。

我們知道威脅形勢不斷演變，網路犯罪分子會設計新戰術以規避檢測。這就是為什麼我們務必保持警惕，持續監控威脅環境，以識別新興、方法獨特的網路釣魚行動。

欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲深入瞭解更多有關賽門鐵克自建型郵件安全閘道(SMG：Symantec Messaging Gateawy)(實體／虛擬／Azure)，請點擊此處。
欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

2024/04/01

印尼企業成為Agent Tesla網路攻擊行動的目標

賽門鐵克最近觀察到一個個體戶或駭客團體，對準印尼的機構組織進行有針對性的惡意垃圾郵件攻擊行動，儘管在鄰近國家也出現類似情況。這些惡意行為者自稱是印尼一家指標領先的銀行，並採用金融交易社交工程伎倆。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn34
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.B!200