保安資訊--本周(台灣時間2023/01/06)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 73 萬 1,700 台受保護端點上總共阻止了 9,250 萬次攻擊。這些攻擊中有 92% 在感染階段前就被有效阻止：**(2023/01/02)**

- 在**13萬9,000**台端點上，阻止了**3,550**萬次嘗試掃描**Web**服務器的漏洞。
- 在**26萬9,100**台端點上，阻止了**2,110**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬9,000**台**Windows**伺服主機上，阻止了**1,710**萬次攻擊。
- 在**8萬8,100**端點上，阻止了**260**萬次嘗試掃描伺服器漏洞。
- 在**2萬**台端點上，阻止了**120**萬次嘗試掃描在**CMS**漏洞。
- 在**4萬4,500**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**23萬7,800**台端點上，阻止了**610**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬7,500**台端點上，阻止了**240**萬次加密貨幣挖礦攻擊。
- 在**4萬3,000**台端點上，阻止了**460**萬次向惡意軟體**C&C**連線的嘗試。
- 在**4,300**台端點上，阻止了**15萬3,600**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。

2023/01/05

需要安裝軟體，請到原廠網站下載～IcedID 惡意軟體透過造假的Zoom安裝程式暗度陳倉

IcedID 是一種眾所周知的金融惡意軟體，通常扮演攻擊鏈中惡意酬載或模組的啟動器／載入程式 (Loader) 的角色。在近期全新的攻擊行動中被散佈的惡意軟體，利用網路釣魚網站提供偽裝成 Zoom 應用程式安裝檔的惡意軟體。釣魚網站設計成模仿合法的 Zoom 下載中心頁面，並誘騙用戶下載與惡意軟體檔案捆綁在一起的 Zoom 用戶端安裝程式。一旦下載的安裝程式被執行，惡意軟體就會被啟動，但為了避免用戶懷疑，還會同時安裝合法版本的 Zoom 應用程式。

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：

- Trojan Horse
- Trojan.Gen.2
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2023/01/05

錢多之處就是江湖～SpyNote 手機行動惡意軟體持續鎖定銀行客戶

在去年年底前後，SpyNote 手機行動惡意軟體家族變本加厲鎖定銀行客戶。該惡意軟體的功能包括從受感染裝置中收集資訊和竊取憑證、鍵盤側錄、Google身份驗證器雙重驗證碼和通話／相機記錄等。最新的 SpyNote.C 變種甚至以 CypherRAT 的名稱透過 Telegram 頻道進行廣告和銷售，還標榜新增一些額外的遠端存取木馬 (RAT) 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：

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
- Android.Reputation.2
- AppRisk:Generisk

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。

2023/01/05

Bluebottle駭客集團：鎖定非洲法語系國家金融機構發動攻擊行動

賽門鐵克最近發布一篇關於 Bluebottle 的網路犯罪組織近期活動的部落格。眾所周知，該組織專門針對金融單位。最近觀察到的攻擊行動延續這一趨勢，受害者居住在非洲的法語系國家。攻擊手法、技術與過程 (TTPS) 包括使用就地取材、兩用工具和商品化的惡意軟體，在此攻擊行動中並沒有部署自定義惡意軟體。

在我們的部落格文章中有更多資訊可供參考：Bluebottle：鎖定非洲法語系國家金融機構的攻擊行動。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Hacktool
- Hacktool.Mimikatz
- Hacktool.Mimikatz!g4
- Hacktool.Rootkit
- Hacktool.SharpHound
- Infostealer
- MSIL.Downloader!gen8
- Packed.NSISPacker!g14
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Guloader
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.3
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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。

2023/01/04

透過GoogleAds散佈的Rhadamanthys竊密程式

駭客使用 GoogleAds 散播網路釣魚和惡意軟體攻擊是很常見，但最近發生多起此類事件引起媒體的關注。其中一個情境涉及透過 GoogleAds 宣傳 Notepad++ 軟體的假網站。如果用戶從該網站下載假冒的安裝程式，他們會在背後默默安裝一個名為 Rhadamanthys 的竊密程式。

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：

- Trojan.Gen.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2023/01/04

瞄準歐洲的金融機構的Raspberry Robin惡意軟體

在真實網際網路環境發現 Raspberry Robin 惡意軟體所涉及的新一波網路攻擊。攻擊鏈採用了惡意 MSI 安裝程式檔 (大小約為 500MB)，這些檔案會被植入到受害者的電腦上。解壓後檔案變得很小，已知的案例會嘗試連接到攻擊者所操控的 C&C 伺服器以下載其他惡意軟體模組。最近 Raspberry Robin 行動背後的攻擊者一直在濫用幾個知名的資料代管服務提供商，例如：Discord 或 Azure 來存放二進位的惡意酬載檔案。

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：

- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2023/01/04

利用CHM檔案發動的攻擊行動，鎖定銀行、酒店和在線上預約平台

賽門鐵克發現，在多個散佈惡意軟體的垃圾郵件攻擊行動中，CHM 檔案的使用有所增加。CHM 是由 Microsoft 開發的一種已編譯並壓縮為 HTML 格式的檔案格式。它們可以包含文本、圖像和超鏈接。例如：我們發現一個垃圾郵件攻擊行動，在該行動中，攻擊者透過發送主旨為“Pagaamento Reserva”的電子郵件以及指向代管在 Google Drive 上的惡意 CHM 檔案的鏈接，以知名酒店、預約平台網站和銀行為目標。如果受害者被誘騙開啟惡意 CHM 檔案，他們會在不知不覺中被三種惡意軟體感染他們的機器：兩個遠端存取木馬 (Babylon 和 Venom) 和一個簡單的螢幕截圖程式。

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)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen11
- Downloader
- SMG.Heur!gen
- Trojan.Malscript

基於機器學習的防禦技術：

- Heur.AdvML.C

2023/01/03

Chaos 勒索軟種變種充斥全球，干擾消費者和企業

以 Chaos 為基底的勒索軟體變種最近在全世界大爆發，多個駭客組織與個人建立自己的版本以進行廣泛但相對簡單的加密攻擊。消費者和企業都面臨成為攻擊目標的風險。賽門鐵克最近觀察到一個攻擊者透過將 Chaos 勒索軟體偽裝成 Minecraft 安裝程式來攻擊 Minecraft 玩家。如果加密成功，將勒索1500美元的贖金，沒有採用雙重勒索的手段。

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：

- Ransom.Sorry

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/01/03

École Française de Téhéran 遭到冒名拿來發動電郵憑證的網路釣魚行動

數十年來，網路犯罪分子一直透過網路釣魚和惡意軟體攻擊將電子郵件憑證鎖定為目標。最近，賽門鐵克偵測到瞄準全球銀行、保險公司、房地產公司、能源公司以及研究和教育單位的網路釣魚行動。在這次網路釣魚行動中，歹徒採用航運主題欺騙受害者，偽裝成位於德黑蘭的法國國際學校 École Française de Téhéran。受害者收到一封帶有 PDF 附件的電子郵件，其中包含導引向一個網站的鏈接，該網站似乎是一份語意不清的裝運單據 (Shipping documents)。當他們點擊網址鏈接時，系統會提示他們輸入電子郵件憑證 (帳密) 以查看該檔。

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。

2023/01/03

CatB勒索軟體～附加植入程式功能

CatB (又名 Fishcat) 最近在真實網際網路上被發現的一種全新勒索軟體。該惡意軟體能夠透過 DLL 劫持 MSDTC 服務在背景執行其有效籌載以避免檢測。CatB 勒索軟體附加植入程式功能，可在受感染機器上執行多次 anti-VM (虛擬環境偵測) 檢查後最終交付勒索軟體有效載荷。雖然 CatB 釋出的贖金說明與 Pandora 勒索軟體變種有一些相似之處，但與這些惡意軟體似乎無關。

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：

- Ransom.Gen
- Trojan.Dropper
- Trojan.Gen.2
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.C

2023/01/02

ArkeiStealer竊密程式偽裝成熱門手機交易應用程序App

ArkeiStealer 惡意軟體最近以偽裝成合法 TradingView 應用程式的安裝程序形式傳播。ArkeiStealer 是過去幾年活躍於威脅領域的一種竊密惡意軟體。該惡意軟體能夠從受感染的機器中竊取資訊，包括瀏覽器保存的資訊、憑證、cookie、加密錢包等。在最近佈署此惡意軟體的攻擊行動中，攻擊者一直在利用一個包含後門版本的 TradingView 應用程序下載器的假網站。攻擊鏈還涉及從攻擊者操控的 C&C 伺服器執行 Smokeloader 惡意軟體。被執行後，Smokeloader 將進一步下載 ArkeiStealer 的最終有效籌載。

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：

- Infostealer
- Trojan.Dropper
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2023/01/02

日本信用卡公司UCS用戶成為網路釣魚攻擊行動鎖定的目標

賽門鐵克最近偵測到一場網路釣魚攻擊行動，攻擊者假裝來自日本知名信用卡公司 UCS。網路釣魚者發送虛假電子郵件（主題：[UCS]UCSネットサーブ一時的な利用停止、ログインして確認してください）聲稱通知臨時暫停服務，並包含指向虛假 UCS 登錄頁面的鏈接。如果受害者登入鏈接並輸入他們的登錄憑證，網路釣魚者將收集並可能濫用此資訊。用戶在收到聲稱來自金融機構的電子郵件時要謹慎，並在點擊之前驗證任何鏈接的真實性，這一點很重要。另外，請注意在觀察到的電子郵件和假冒網站中使用的日語包含語法錯誤，這是一個主要的警告訊號。

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。

2023/01/02

日本熱門服務遭受無止盡的網路釣魚攻擊

某些國家比其他國家更頻繁地成為網路釣魚活動的目標並不少見，日本就是其中之一。日本可能成為網路釣魚行動的目標有多種原因。原因之一可能是該國網際網路和技術使用率高，這使其成為網路犯罪分子的誘人目標。此外，日本是許多大型知名公司和組織的所在地，這些公司和組織可能會成為網路釣魚者攻擊的目標。最後，日本可能只是其自身成功和知名度的受害者，因此在全球發生的網路釣魚攻擊總量中所佔比例更大。

日本的許多網路釣魚攻擊都針對 Amazon、Rakuten、Aeon、Docomo 等熱門服務，試圖從日本用戶那裡獲取敏感資訊和信用卡詳細資訊。以下是最近針對日本的網路釣魚行動中使用的一些電子郵件主旨的範例：

- 【重なら】お客様のお支払い方法が承認されません。
- 【Amazon 重要なお知らせ】あなたのAmazonアカウントはセキュリティ環境上の理由で中断されました
- Amazonのお支払いにご指定いただいたお客様のお支払い方法が承認されないため
- ETC会員再確認のご知らせ
- Rakutenお支払い方法のお知らせ【緊急の連絡 】イオンカード ご利用確認のお願い
- 【重要】AEONいご利用の会員IDとサービスについて

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。

2023/01/01

網路犯罪分子濫用Discord網路勾手(webhook)的情況有所增加

在過去的幾個月裡，有越來越多的竊密程式使用 Discord，透過 Discord 網路勾手 (webhook) 的自動發送訊息功能來回傳遭竊資訊。這些普通的竊密程式通常在他們的程式碼中有相似之處，其中許多是基於其他竊密程式的副本或分支。它們通常透過公共資源共享，例如：軟體開發和版本控制代管服務，以及駭客論壇和網站。Creal、Prisonizme 和 Vert 是賽門鐵克最近在真實網際網路環境發現的竊密程式範例，通常偽裝成破解軟體或駭客工具的偷渡式下載進行傳播。

註：來自網路 Discord 內置網絡鉤手 (Webhooks) 功能，來為您方便地在服務器的文字頻道中獲取自動訊息以及更新數據。

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：

- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2023/01/01

NJRAT濫用退休基金社交工程詐騙，瞄準西班牙語系的用戶

在景氣動盪時期以退休基金為主題的社交工程攻擊特別有效，例如：2022 年某些事件後續影響。賽門鐵克最近偵測到一個針對西班牙語系用戶的惡意電子郵件攻擊行動，它偽裝以管理養老金和遣散費知名的哥倫比亞金融公司要匯入退休金。這些電子郵件包含一個帶有兩個惡意 VBS 檔案的 RAR 壓縮檔附件，如果打開附件，將使用 NJRAT 遠端存取木馬感染受害者的裝置。

NjRat，也稱為 Bladabindi 或 Ratenjay，是一種非常熱門的遠端存取木馬 (RAT)，在過去十年中被廣泛使用。它允許攻擊者從受感染的裝置中擷取資訊，包括按鍵記錄、儲存的憑證和瀏覽器歷史記錄。NjRat 的一些較新變種也針對加密貨幣錢包。除了擷取資訊之外，這個 RAT 還使攻擊者能夠透過遠端 shell 發送命令、修改登錄機碼以及下載其他檔案。

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)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen

2022/12/30

Shc惡意軟體用於散佈加密貨幣挖礦程式和分散式阻斷攻擊的殭屍電腦(DDoS IRC)的二進製檔案

在真實網際網路環境發現一起利用 Linux 環境下的 Shc 惡意軟體傳播 XMRig 加密貨幣挖礦程式的新行動。Shc 是 Shell 腳本編譯器，它依賴於可以轉換為 .elf 的 Linux 可執行檔的 Bash shell 腳本。傳送到受感染端點的惡意腳本包含受控於於攻擊者的 C&C 伺服器以下載額外有效籌載及其後續執行的指令。除了散佈加密貨幣挖礦程式之外，還觀察到相同的攻擊者將分散式阻斷攻擊的殭屍電腦 (DDoS IRC) 的二進位檔案下載到受感染的端點上。

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：

- Linux.Coinminer
- Trojan Horse
- Trojan.Gen.NPE
- 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。