保安資訊--本周(台灣時間2023/07/21)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 69 萬 300 台受保護端點上總共阻止了 8,260 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/07/17)**

- 在**13萬6,100**台端點上，阻止了**3,190**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**23萬2,100**台端點上，阻止了**1,780**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬2,400**台**Windows**伺服主機上，阻止了**1,350**萬次攻擊。
- 在**9萬3,900**台端點上，阻止了**270**萬次嘗試掃描伺服器漏洞。
- 在**1萬5,900**台端點上，阻止了**88萬1,900**次嘗試掃描在**CMS**漏洞。
- 在**7萬900**台端點上，阻止了**150**萬次嘗試利用的應用程式漏洞。
- 在**23萬3,700**台端點上，阻止了**540**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,300**台端點上，阻止了**210**萬次加密貨幣挖礦攻擊。
- 在**14萬5,400**台端點上，阻止了**990**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,200**台端點上，阻止了**9萬500**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。

2023/07/20

AI熱，也燒到駭客圈的騙術～BundleBot惡意軟體冒充AI工具、常見應用程式或遊戲軟體

BundleBot 是同時具有竊密程式／殭屍電腦功能的精密惡意軟體。它使用 dotnet，這是一種單一檔案、獨立的格式，包括獨立執行的所有必要部分。這通常會建立一個非常大的檔案，並使分析和偵錯變得更加困難。

受害者經由臉書廣告和受感染的網站所引誘，這些網站以人工智慧 (AI) 工具、常見應用程式或遊戲軟體為幌子，其中較大的檔案可能會增加惡意軟體的被信賴程度而讓用戶更容易受騙上當。

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：

- Backdoor.Ratenjay
- Downloader
- Trojan Horse
- Trojan.Gen.2
- W97M.Downloader
- 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。

2023/07/20

APT41駭客組織 (又名Blackfly駭客組織)，操弄WyrmSpy和DragonEgg手機惡意軟體發動網路攻擊

最近，APT41 駭客組織 (又名 Blackfly、Winnti、Bronze Atlas) 發起的惡意攻擊中利用兩種名為 WyrmSpy 和 DragonEgg 的手機惡意軟體。該組織至少自 2010 年起就在駭客圈闖出名號，儘管其成員多次受到起訴，但該組織仍在繼續針對公共和私人企業的機構發動攻擊。WyrmSpy 和 DragonEgg 惡意軟體被歸類於網路監控惡意軟體，具有多面向的資料洩露功能。該惡意軟體的目標是收集資料檔案、照片、簡訊和錄音等。這兩種惡意軟體變種都嚴重依賴從 C&C 伺服器接收的指令，因此針對受感染設備的功能在每種情況下可能有所不同。

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。

- AdLibrary:Generisk
- AdLibrary:MoPub
- Android.Reputation.1
- Android.Reputation.2
- Android.Reputation.3
- 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。

2023/07/20

Zyxel的CVE-2023-28771漏洞，被開採利用於發動分散式阻斷服務(DDoS)攻擊的殭屍網路

CVE-2023-28771 是一個影響 Zyxel 設備的嚴重 (CVSS 評分 9.8) 命令注入漏洞。如果開採利用該漏洞，未經身份驗證的攻擊者可能會在目標系統上遠端執行任意程式碼。在真實網路傳出災情後，美國網路安全暨基礎設施安全局 (CISA) 也將該漏洞新增到『已知遭開採利用漏洞目錄』中。CVE-2023-28771 最近已被多個 DDoS 殭屍網路（例如：Dark.IoT 或各種 Mirai 變種）開採利用。

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.Lightaidra
- Linux.Mirai
- Trojan Horse
- Trojan.Gen.NPE
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2

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：

- Attack: Zyxel Command Injection CVE-2023-28771

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。

2023/07/18

故意的嗎？防毒品牌『Sophos』被勒索軟體拿來冠名

研究人員最近發現一種濫用合法防毒軟體公司名稱『Sophos』的全新勒索軟體。被加密的檔案會被冠上『.sophos』的副檔名。

除了加密檔案和留下贖金支付說明檔外等常見的勒索軟體面向，此會冠上『Sophos』字眼的勒索軟體還包含常見的遠端存取木馬 (RAT) 功能，包括掛鉤 (hook) 在鍵盤驅動程式的鍵盤側錄程式和使用 WMI 命令來分析系統。此外，勒索軟體還可以檢查受害者的電腦的語系配置，如果是俄語則不會執行。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- WS.Malware.2

基於機器學習的防禦技術：

- 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)：

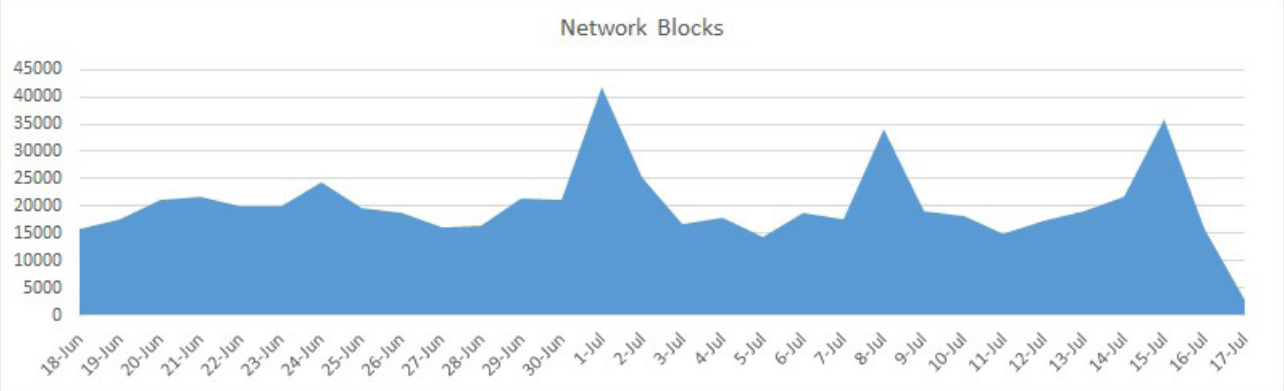
被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2023/07/18

防護亮點：BlackByte勒索軟體

惡名昭章的勒索軟體攻擊者多年來一直在利用各種與威脅相關的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs) 來執行攻擊並實現其目標。在這些攻擊者中，BlackByte 脫穎而出。最近報告顯示，他們可以在五天內就利用一系列的漏洞、後門和工具進行滲透、常駐、偵察、橫向移動、竊取資料和加密資訊，而完成致命性的攻擊。

ProxyShell 和 ProxyLogon 漏洞是各種威脅（包括勒索軟體）的目標，作為滲透系統的初始手段。下圖顯示了最近這些被封鎖的網路嘗試。



在 BlackByte 攻擊鏈中所採用的 TTPs 依 MITRE 所分類的包括以下內容：

* 濫用執行已簽章的代理程式：Rundll32 [T1218.011]
* 命令和腳本解釋器：Windows Command Shell [T1059.003]
* 啟動或登錄自動啟動執行：註冊表裡的Run Keys／啟動資料夾 [T1547.001]
* 軟體搜尋：安全軟體搜尋 [T1518.001]
* 遠端存取軟體 [T1219]
* 遠端系統搜尋 [T1018]
* 系統網路配置搜尋：Internet 連接搜尋 [T1016.001]
* 削弱防禦：禁用安全軟體或修改工具 [T1562.001]
* 禁止系統恢復 [T1490]
* 修改註冊表 [T1112]
* 網域信任搜尋 [T1482]
* 系統網路配置搜尋 [T1016]
* 帳戶搜尋 [T1087]
* 權限群組搜尋 [T1069]

BlackByte 勒索軟體最早在 2021 年首次發現，多年來，它針對醫療保健、製造和政府機構等不同行業所造成的災難而多次成為頭條新聞。目前，該攻擊者仍然活躍，據報導在過去兩個月裡已讓多個機構受害。

賽門鐵克針對BlackByte勒索軟體，提供完整的**零時差**保護，具體說明如下：

基於行為偵測技術(SONAR)的防護：

- SACM.Adfnd-Lnch!g1

端點偵測與回應(EDR)：

- 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訊息，請參閱此 GitHub 儲存庫。

賽門鐵克端點檢測和回應 (EDR) 使用機器學習和行為分析來檢測和揭露可疑網路活動。EDR 會發出有關潛在有害活動的警報，對事件進行優先級排序以便快速分類，並允許事件回應人員瀏覽設備活動記錄以對潛在攻擊進行鑑識分析。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Blackbyte

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：

- Audit: AnyDesk Remote Desktop Activity

- Audit: ADFind Tool Activity
- Attack: Microsoft Exchange Server CVE-2021-26855
- Web Attack: Microsoft Exchange Server RCE CVE-2021-34473
- Web Attack: Microsoft Exchange Server CVE-2021-34473
- Web Attack: Microsoft Exchange Server Elevation of Privilege CVE-2021-34523

SEP 的稽核用特徵資料庫 (Audit Signaturesare) 旨在提高對網路中潛在有害流量的認識。預設情況下，它們不會攔截。查看網路中 IPS 事件日誌的管理員可以記下這些稽核事件，並決定是否配置相應的簽章稽核來攔截流量。

基於機器學習的防禦技術：

- Heur.AdvML.B

基於安全強化政策(適用於使用DCS)：

- Symantec Data Center Security (DCS) 的Windows 版本，出廠即內建預設的強化策略提供針對未知威脅的零時差防護，包括以前未見過的勒索軟體變種和相關行為。
- Symantec DCS 針對 Microsoft Exchange 伺服器的預設強化策略就可防止 ProxyShell 漏洞。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

欲深入瞭解更多有關於賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲瞭解更多有關於賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。
欲瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲瞭解有關賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。
欲瞭解有關 Symantec 端點檢測和響應的訊息，請點擊此處。

2023/07/18

Muggle竊密惡意軟體

一種被稱為 Muggle 的全新竊密惡意軟體正在網路上大肆傳播。該惡意軟體是採用 Go 語言所撰寫的，並透過其他類似的竊密惡意軟體（例如：惡意網站或網路釣魚）也在使用的常用方法進行傳播。該惡意軟體從遭駭入的電腦收集系統資訊、收集螢幕截圖、擷取網頁瀏覽器中儲存的機密資料，包括憑證、cookie 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2023/07/18

FIN8駭客集團重新修改Sardonic後門，大肆傳播Noberus勒索軟體

網通晶片巨擘博通 (Broadcom) 旗下的企業安全部門～賽門鐵克威脅獵手團隊最近觀察到 Syssphinx（又名 FIN8）駭客集團部署 Sardonic 後門的變種來傳播 Noberus 勒索軟體。雖然對該後門的分析顯示它是該駭客集團之前使用的 Sardonic 框架的一部分，但該後門程式經過大改版似乎都已經脫胎換骨了。Syssphinx（又名 FIN8）是一個以經濟為動機的駭客集團，以酒店、零售、娛樂、保險、技術、化學品和金融領域的機構為目標。

在我們的部落格文章中有更多內容可供參考：FIN8 駭客集團重新修改 Sardonic 後門，大肆傳播 Noberus 勒索軟體

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：

- Hacktool.Mimikatz
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2023/07/17

APT29又名『Cloaked Ursa』駭客組織針對駐烏克蘭的外國機構

APT29 威脅組織 (也稱為 Cloaked Ursa) 最近參與針對駐烏克蘭的外國機構的惡意軟體散播行動。歹徒一直透過電子檔形式的汽車銷售廣告來發送誘餌給目標受害者。開啟惡意檔中嵌入的鏈結後，受害者將被重導向到上架在惡意軟體有效籌載的網站。被植入的有效籌載使用 Microsoft Graph 和 Dropbox API 與 C&C 伺服器進行通訊，並透過這些通道接收攻擊者的進一步命令。

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：

- Meterpreter
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Malscript
- Scr.Malcode!gdn34
- WS.Malware.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。

2023/07/17

AVrecon惡意軟體針對SOHO設備

AVrecon 是一種 Linux 的遠端存取木馬 (RAT)，針對小型辦公室／家庭辦公室 (SOHO) 的路由器和其他 ARM 嵌入式設備。惡意軟體透過開採利用未修補的漏洞或目標設備的常見錯誤配置來傳播。部署後，AVreckon 將收集有關受感染設備的相關資訊，開啟與預先配置的 C&C 伺服器的連線，並生成遠端 shell 來執行指令。它也可能下載其他任意檔案並執行。該惡意軟體最近被用於針對廣告欺騙活動、密碼噴灑（Password Spraying）和數據洩露等攻擊行動。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- 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。

2023/07/14

RedDriver瀏覽器劫持程式鎖定中文語系的用戶

RedDriver 瀏覽器劫持程式，應該可以說是專門針對中文環境而開發。是依附在驅動程式的瀏覽器劫持程式，可以安裝自己的憑證並在網路連線階段劫持所有瀏覽器的流量，這使得檢測其行為變得困難。它在程式碼和開發中使用多種開放原始碼工具，並偽造已簽核的憑證來繞過 Windows 檢測。

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：

- AGR.Terminate!g2
- AGR.Terminate!g5
- SONAR.Trafic2.RGC!g10

檔案型(基於回應式樣本的病毒定義檔)防護：

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

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。

2023/07/13

以薪資單為幌子的路釣魚行動，以更嚴謹的XHTML網頁格式檔來降低受害者的戒心

HTML、SHTML、XHTML 和 HTM 是 Web 開發中使用的不同副檔名，用於標示網頁中使用的標記語言類型。這些是廣泛使用的進行網路釣魚的格式，並充當惡意軟體的感染媒介。駭客傾向將 HTML 和 SHTML 作為首選，而 XHTML 則不太常用。這可能是由於 XHTML 本質上比 HTML 更嚴格，而 HTML 則以更可容受錯誤而聞名。

XHTML（eXtensible HyperText Markup Language，可延伸超文本標示語言），是一種標記式語言，表現方式與超文件標示語言（HTML）類似是遵循 XHTML 標準的 Web 檔，XHTML 標準是 HTML（超文本標記語言）更嚴格、更標準化的版本。XHTML 將 XML（可擴展標記語言）的語法和規則與 HTML 的靈活性和元素相結合。XHTML 檔的副檔名為“.xhtml”。它們可以像 HTML 檔一樣在 Web 瀏覽器中查看，但嚴格的 XHTML 檔可能無法在不支援 XML 或不遵守

XHTML 標準的舊版瀏覽器中正確顯示。

賽門鐵克最近發現到一場惡意電子郵件攻擊行動，據稱與薪資有關（subject：Payroll for period ending 12 July, 2023／郵件主旨：截至 2023 年 7 月 12 日的工資單），針對私人企業和公共部門。如果受害者被成功引誘，他們將看到一個假的 Microsoft 365 登錄頁面，該頁面主要在騙取他們的電子郵件憑證（帳密）。

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。