保安資訊--本周(台灣時間2023/05/19)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 76 萬 5,000 台受保護端點上總共阻止了 9,210 萬次攻擊。這些攻擊中有 92% 在感染階段前就被有效阻止：**(2023/05/14)**

- 在**15**萬**1,200**台端點上，阻止了**3,820**萬次嘗試掃描**Web**服務器的漏洞。
- 在**26**萬台端點上，阻止了**1,920**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5**萬**3,900**台**Windows**伺服主機上，阻止了**1,480**萬次攻擊。
- 在**8**萬**5,400**台端點上，阻止了**260**萬次嘗試掃描伺服器漏洞。
- 在**1**萬**5,600**台端點上，阻止了**95**萬**7,900**次嘗試掃描在**CMS**漏洞。
- 在**6**萬**400**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**27**萬**2,100**台端點上，阻止了**620**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**8**萬**6,000**台端點上，阻止了**240**萬次加密貨幣挖礦攻擊。
- 在**15**萬**7,700**台端點上，阻止了**1,090**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,400**台端點上，阻止了**9**萬**8,600**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。

2023/05/18

MEME#4CHAN網路攻擊行動發送XWorm有效負載

XWorm 是一種遠端存取木馬 (RAT)，已知在地下論壇上販賣。這種基於 .NET 的惡意軟體具有多種功能，目的在控制受駭的電腦、遠端指令執行、發起 DoS 攻擊和料外洩。XWorm 3.1 變種最近在名為 MEME#4CHAN 的惡意攻擊行動中傳播。攻擊者一直在他們的活動中採用多階段方法。初始攻擊始於惡意垃圾郵件和惡意 MS Office 檔案，其中包含已知的 Follina MSDT 遠端程式碼執行漏洞 CVE-2022-30190 漏洞利用程式。進一步攻擊階段包含 PowerShell 和 JavaScript 執行，這些執行會導致此攻擊行動的最終有效籌載。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

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!gen12
- ISB.Downloader!gen80
- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- W97M.Downloader

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!100
- 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: MSDT Remote Code Execution CVE-2022-30190
- 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。

2023/05/18

Greatness～PaaS(網路釣魚即服務)正在興起

Greatness 是一個網路釣魚即服務 (PaaS) 平台，其活動從 2022 年年中開始，最近知名度大增。據報導，這個相對較新平台已迅速受到網路犯罪分子的青睞，主要針對 Microsoft 365 憑證盜竊。世界各地都發現源於 Greatness 網路釣魚即服務平台的惡意電子郵件，如果他們成功被誘騙打開惡意 HTML 網頁檔附件，就會將受害者引誘到精密的攻擊鏈中。

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。

2023/05/18

提早支付贖金也有打折～Heeck4ever勒索軟體

除了專業級或國家級的勒索軟體駭客集團所發動的複雜攻擊，從滲透到遭駭的網路環境、加密關鍵電腦、竊取敏感資料並勒索受害者高額贖金登上新聞頭條的高調駭客集團外，還有許多其他勒索軟體是透過社交工程伎倆，來詐騙消費者和企業用戶的電腦，要求較小的贖金。

Heeck4ever 就是一種此類勒索軟體，已被發現到偽裝成假的 Windows 優化工具、Microsoft Office 安裝程式和 Windows 表單應用程式。一旦用戶成為這種詐騙的受害者，檔案會被加密且被提示支付價值 200 美元的比特幣，如果在 72 小時內付款，則可優惠只需支付 50 美元。此外，受害者也可以選擇其他付款方式，包括 PayPal。

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.SuspDrop!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/05/17

Minas惡意挖礦程式

Minas 是全新的惡意加密貨幣挖礦軟體。Midas 採用多種規避檢測伎倆，包括加密、注入機制、隨機名稱生成和常駐性技術等。感染鏈包含由 PowerShell 執行腳本已取得 .dll 類型的有效酬載並且在記憶體中啟動挖礦軟體 XMRig。

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

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/05/17

針對Linux平台的Maori勒索軟體

Maori 是一種由 Go 語言撰寫的普通勒索軟體，目前針對 Linux 平台。該惡意軟體將會加密使用者家 (home) 目錄中的檔案，並新增 .maori 的副檔名。加密完成後，“README_MAORI.txt”文字格式的贖金支付說明檔，將被存放到受感染的電腦上。贖金說明要求受害者透過 Tox 加密即時通訊軟體與攻擊者聯繫以獲取進一步指示。

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
- WS.Malware.2

2023/05/17

Geacon--適用於macOS的類似Cobalt Strike滲透測試工具

Geacon 是 macOS 平台上由 Go 語言撰寫，模擬常用滲透測試工具 Cobalt Strike 的惡意工具。雖然在網路上發現大多數 Geacon 樣本似乎仍主要用於紅隊測試，但各種攻擊者開始濫用它們以類似利用 Cobalt Strike 的方式進行惡意攻擊，只是時間早晚的問題。Geacon 最近在某些情況下被惡意使用，包括偽裝成中國業者網宿科技遠距辦公程式 SecureLink 的合法程式案例。此案例中 macOS 使用一個共用的 C&C 位址，該位址以前因與 Cobalt Strike 的信標連結而廣為人知。

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
- OSX.Trojan.Gen.2
- 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。

2023/05/16

Water Orthrus進階持續威脅(APT)駭客組織發起的CopperStealth和CopperPhish攻擊行動

被稱為 Water Orthrus 威脅組織最近一直在展開兩個全新的惡意攻擊行動，分別稱為 CopperStealth 和 CopperPhish。CopperStealth 攻擊行動偽裝成免費軟體安裝程式來傳播 Rootkit 惡意軟體。一旦部署，rootkit 會將 CopperStealth 有效籌載注入系統程序。有效籌載預計會執行從 C&C 伺服器接收到的命令。CopperPhish 攻擊行動利用下載器惡意軟體變種，例如：PrivateLoader，再會下載負責最終執行 CopperPhish 植入程式。該攻擊行動的目的在對毫無戒心的受害者發起銀行帳號和信用卡資訊的網路釣魚。

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
- SONAR.TCP!gen1

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
- Trojan.Malfilter
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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：

- System Infected: Trojan.Backdoor Activity 502
- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 721
- 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。

2023/05/15

AndoryuBot～發動分散式服務阻斷(DDoS)攻擊的殭屍網路

最近一個名為 AndoryuBot 殭屍網路被曝光，該殭屍網路利用 Ruckus 設備 (CVE-2023-25717) 安全漏洞，發動分散式服務阻斷 (DDoS) 攻擊。CVE-2023-25717 是一個影響許多 Ruckus 無線設備的遠端程式碼執行 (RCE) 漏洞。攻擊手法首先利用漏洞開採取得 Ruckus 設備的存取權限，再使用 SOCKS 通訊協定與其 C&C 伺服器建立連接，然後惡意軟體從其 C&C 伺服器接收命令以發起 DDoS 攻擊。

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.Mirai
- WS.Malware.1

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: Ruckus Wireless Admin RCE CVE-2023-25717
- 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。

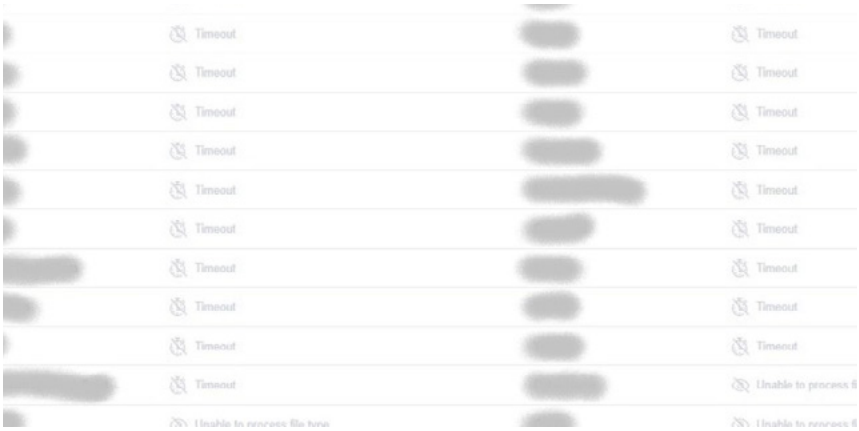
2023/05/15

防護亮點："模擬" Android阻斷服務攻擊(DoS)

～防護亮點～

在我們 7x24 的日常工作中，我們會不斷監控異常和跡象，這些異常和跡象可能顯示存在試圖逃避安全檢測的全新威脅或經過修改的威脅。我們的自動化系統最近提醒我們注意一個問題，即在檢測特定 Android 手動安裝包 .APK 的樣本時，我們的雲端掃描明顯變慢。快速瀏覽一下就會發現，幾個有問題的樣本也對更廣泛的自動化掃描系統效能產生輕微影響。

VirusTotal 其他供應商似乎受到的不利影響更大，在分析期間顯示逾時 (Timeout)，這實際上看起來像是一次行動裝置的分散式服務阻斷 (DDoS) 攻擊。



深入研究樣本顯示了以下特性：

- 每個容器樣本都包含大量（最多 32K）、很小的檔案
- 這些很小的檔案包含看起來像隨機字串的內容，並且似乎沒有被 APK 使用
- APK 本身似乎是自動化產成
- 手動安裝包名稱似乎也是隨機自動生成
  * hbjvuozxxuhpyfbnvxtd.dxgbesgyxlsvkccgozbi.deomdyhhwgeraghfzrds
  * dknmmohvktzcmopltehs.yrrnbpuvyctwiefeeycz.gtwxbuikrwakaehwpazg

透過行為分析，我們確定這些 APK 樣本主要是廣告軟體／灰色軟體，和其他可能不需要但不全然是惡意的程式，被統稱為潛在有害程式 (Potentially Unwanted Applications，PUAs)。其中某些連接到遠端伺服器以取得跟廣告相關的設定或與管理推送通知或位置服務的部份軟體開發套件 (SDK) 整合。

迄今為止，我們已經看到超過 11,000 個此類樣本（每個樣本包含超過 30,000 個檔案）。我們相信它們可能是某種測試--因此標題中使用“模擬”這個詞彙--但很難確定這種測試是由安全研究人員，還是有惡意意圖的人士所進行。

學習和適應的能力對於一家安全公司的成功非常重要，我們立即修改我們的自動化程序，以便更有效地分析這些樣本，有效地克服之前觀察到的處理性能下降。

賽門鐵克的端點安全企業版 (SESE)／端點安全完整版(SESC)內含防護 IOS／Android 的最先進防護技術，請點擊此處瀏覽更完整的資訊。

個別的內含在SES／SESC 賽門鐵克行動裝置威脅防禦型錄最新版下載，請點擊此處。

2023/05/15

Lancefly進階持續威脅(APT)駭客組織，濫用Merdoor後門

Lancefly 進階持續性威脅 (APT) 組織在針對南亞和東南亞組織的攻擊中濫用自定義撰寫的後門，該活動已持續數年。Lancefly 的自定義惡意軟體被稱為 Merdoor，是一個強大的後門程式，似乎自 2018 年以來就存在。賽門鐵克研究人員觀察到它被用於 2020 年和 2021 年的某些活動，還有最近的攻擊行動，該活動一直持續到 2023 年第一季度。這兩項攻擊行動背後的動機被認為是情報收集。此攻擊行動中的攻擊者也可以使用最新版本的 ZXShell rootkit。

在我們的部落格文章中有更多資訊可供參考：Lancefly：該組織使用客製化後門攻擊政府、航空以及其他行業

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
- SONAR.TCP!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Hacktool
- Hacktool.Gen

- Hacktool.Mimikatz
- PUA.Gen.2
- Trojan Horse
- Trojan.Dropper
- Trojan.Gen.MBT
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B
- 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：

- System Infected: Trojan.Backdoor Activity 634
- 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。

2023/05/15

TP-Link CVE-2023-1389漏洞被開採利用來傳播Mirai殭屍網路

CVE-2023-1389 是一個存在於 TP-Link Archer AX-21 韌體版本 1.1.4 Build 20230219 之前的命令注入 (Command Injection) 漏洞。一旦該漏洞被開採利用，未經身份驗證的攻擊者可以注入指令，這些指令將以 root 身份執行，具有簡單的 POST 請求。原廠早在今年 3 月份就發布該漏洞的修補。根據 Mirai 殭屍網路在網路上被開採利用的報告，該漏洞最近剛剛被國網路安全暨基礎設施安全局 (CISA) 新增到“已知遭開採利用漏洞目錄”中。

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：

- Downloader.Trojan
- Linux.Mirai
- Linux.Mirai!g2
- WS.Malware.1

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: TP-Link Router Remote Code Execution Vulnerability CVE-2023-1389

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。

2023/05/12

一箭雙鵰～Blacksuite勒索軟體，一問世就同時針對Windows和Linux系統

Blacksuit 是勒索軟體生態系的新成員。已經在網路上發現可同時針對 Windows 和 Linux 的系統的特色。該惡意軟體會加密使用者的檔案並對加密後的檔案新增 .blacksuit 副檔名。該惡意軟體具有停用與 VM 環境關聯的程序、停用特定 Windows 服務以及從受感染系統中刪除陰影副本的功能。成功加密後，Blacksuit 將以名為“README.BlackSuit.txt”的文字檔格式留下贖金支付說明，引導受害者透過 TOR 加密網站與攻擊者聯繫。

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.Blacksuit
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/05/12

雨後春筍般的惡意應用程式和網站冒充類似ChatGPT等AI(人工智慧)工具進行惡意軟體傳播

自今年年初以來，利用模仿 ChatGPT 和類似 AI (人工智慧) 工具的冒牌貨應用程式、安裝程式和假冒網站的惡意活動大幅增加。攻擊者採用包括透過熱門的搜尋引擎或媒體平台進行網路釣魚和惡意廣告等常用伎倆，目的是將惡意軟體部署到毫無戒心的用戶。最近發現攻擊行動包含偽裝成一些最熱門的人工智慧工具和平台的網站，包括 ChatGPT、Midjourney、Google Bard 或 Dall-e。此類攻擊行動中分佈的惡意軟體家族之一是 Redline 竊密程式，這是一種非常知名和熱門的惡意竊密程式，用於洩露機敏資料、憑證、cookie 或加密貨幣錢包等。

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：

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：

- Trojan Horse
- Trojan.Gen.NPE
- Trojan.RedLineStealer
- 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：

- System Infected: Redline Stealer Activity
- System Infected: Redline Stealer Activity 2
- System Infected: Trojan.Backdoor Activity 634
- 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。