保安資訊--本周(台灣時間2023/09/22)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 66 萬 5,200 台受保護端點上總共阻止了 8,370 萬次攻擊。這些攻擊中有 87% 在感染階段前就被有效阻止：**(2023/09/18)**

- 在**13萬500**台端點上，阻止了**3,510萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**20萬7,700**台端點上，阻止了**1,640萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬7,300**台**Windows**伺服主機上，阻止了**1,490萬**次攻擊。
- 在**8萬1,400**台端點上，阻止了**270萬**次嘗試掃描伺服器漏洞。
- 在**1萬4,500**台端點上，阻止了**110萬**次嘗試掃描在**CMS**漏洞。
- 在**6萬6,900**台端點上，阻止了**150萬**次嘗試利用的應用程式漏洞。
- 在**22萬8,500**台端點上，阻止了**460萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**8,200**台端點上，阻止了**200萬**次加密貨幣挖礦攻擊。
- 在**13萬5,000**台端點上，阻止了**900萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**2,000**台端點上，阻止了**9萬8,000**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。

2023/09/22

Gelsemium進階持續威脅組織(APT)鎖定東南亞政府機構

安全研究人員在遭入侵的某個東南亞政府機構的伺服器進行調查時發現一個名為 Gelsemium 的進階持續威脅組織 (APT) 的感染鏈。

攻擊者最初安裝 AspxSpy、China Chopper 和 reGeorg Web shell，以便在受感染的伺服器上建立常駐能力，進而讓該組織發動更多攻擊。OwlProxy 和 SessionManager 是後續使用的主要後門，目的是從敏感的 IIS 伺服器收集情報。

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
- Hacktool.Ace
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.2
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

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

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。

2023/09/22

是真的由人資部門(HR)所發出的現上自我評估調查？請三思而後行

安全研究人員最近提出報告：有發生冒充人力資源部門 (HR：人資) 發送新版員工手冊或自我評估調查表的網路釣魚事件。這些網路釣魚的鏈接可連到網頁式的表單，誘騙沒有戒心的員工的登入憑證／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。

2023/09/21

Remcos和GuLoader駭客工具集被包裝成有品牌的合法軟體來銷售

GuLoader 是一種基於 shellcode 的初始攻擊程式，經常在垃圾郵件中發現其蹤跡，它可以提供攻擊鏈後續所需的各種有效籌載包括勒索軟體、竊密程式、銀行木馬、遠端存取木馬 (RAT) 等。另一方面，Remcos 也作為遠端控制和監視軟體進行商業銷售。

研究人員最近發現一些電子商務網站將 Remcos 和 GuLoader 工具加以品牌化以作為合法產品來出售。經營這些網站的個人經常在他們的 Telegram 頻道上發布這些偽裝產品的行銷影片。有證據顯示他們參與惡意軟體的傳播，包括 Formbook 和 Amadey Loader。

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：

- Ransom.Pots
- SONAR.TCP!gen1
- Trojan.Remcos

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn30
- Scr.Malcode!gdn32
- Scr.Malcode!gdn34
- Scr.Malcode!gen36
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

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

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。

2023/09/21

Snatch勒索軟體仍然是一個重大的威脅

賽門鐵克安全回應中心了解到 CISA 和 FBI 最近發出的警報，觀察到 Snatch 勒索軟體涉入大量的針對式攻擊行動。Snatch 是一個勒索軟體家族，至少自 2019 年以來就出現在威脅領域中。根據已發布的報告，Snatch 背後的威脅組織一直積極針對關鍵基礎設施部門，包括國防工業基地(DIB)、食品和農業以及 IT 部門在涉及資料外洩和雙重勒索的活動中。攻擊者一直在利用暴力破解 RDP 連線，但也非法取得被入侵的憑證來初次存取受害者的網路。Snatch 勒索軟體會在加密檔案中冠上隨機的副檔名，並以「HOW TO RESTORE YOUR FILES.TXT」檔案的形式留下勒索贖金支付說明等資訊。

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.RansomSnatch!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Snatch
- Trojan.Gen.MBT
- Trojan.Malscript
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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：

- Malicious Site: Malicious Domains Request

2023/09/20

攻擊中東電信公司的全新惡意軟體

中東的電信公司正在成為全新惡意軟體鎖定的目標，這些惡意軟體偽裝成合法的安全軟體，包括 Palo Alto Networks 的 Cortex XDR 程式和 Microsoft 的 Exchange Web Services (EWS) 平台，使檢測變得更加困難。

攻擊者似乎對有提供網際網路服務的伺服器發動漏洞利用攻擊，將名為 HTTPSnoop 後門程式部署到受害者網路上來發動初始攻擊，讓他們監聽特定 HTTP(S) 網址 (URL) 的傳入請求並在受感染的端點上執行該內容。另一種新的惡意軟體稱為 PipeSnoop，它可以接受來自具名管道的任意 shellcode 並在受感染的端點上執行它。

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.Cridex
- Trojan.Gen.9
- Trojan.Gen.MBT
- WS.Malware.1

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

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

2023/09/20

專騙資安人員～攻擊者透過假的概念驗證(PoC)散播VenomRAT遠端存取木馬

已公開發布的專為 CVE-2023-25157 所建立的概念驗證 (PoC) 已被修改為可下載並執行 VenomRAT 遠端存取木馬的惡意酬載。這是為了欺騙安全研究人員，讓他們認為新的 PoC 現在可用於後續的新漏洞「CVE-2023-40477」。這種遠端存取工具可以竊取資料、執行命令並接管遭入侵電腦的控制權。

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
- Scr.Malcode!gdn14
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

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

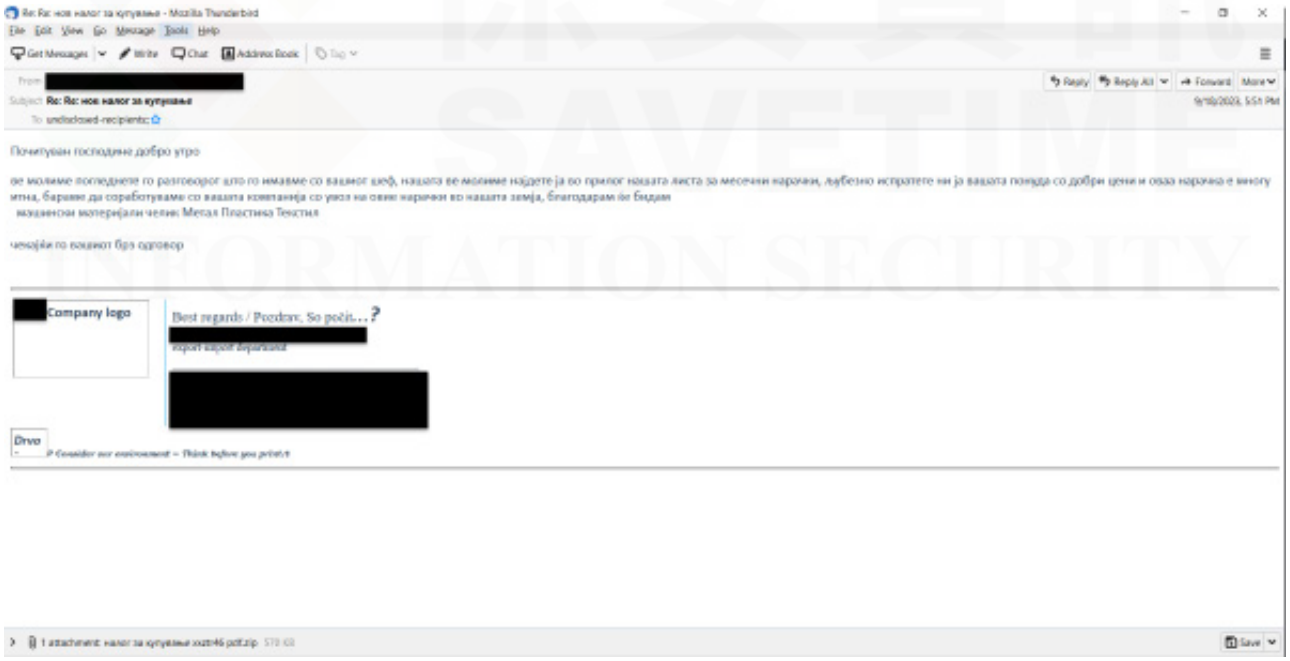
基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

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。

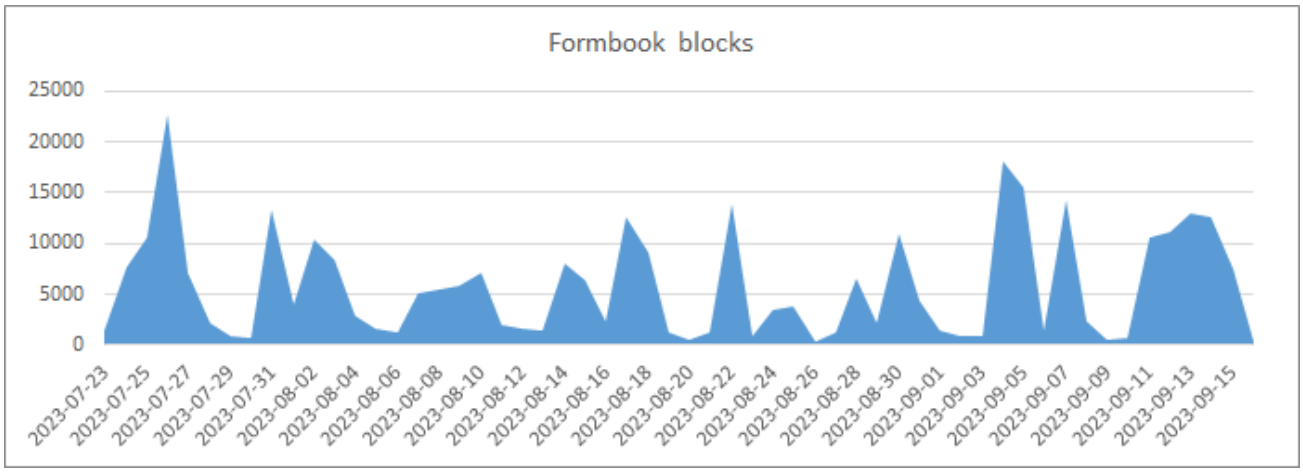
2023/09/19

防護亮點：在巴爾幹地區發現的Formbook竊密程式

Formbook 雖然是較老牌的竊密程式，但其威脅無所不在，遍及全世界，每天總有人回報其活動，並且廣受許多駭客組織及網路壞蛋所青睞，絲毫沒有退流行的跡象。最近，賽門鐵克發現這種老當益壯、陰魂不散的的威脅正在巴爾幹半島肆虐。這次在巴爾幹的攻擊行動的幕後黑手試圖透過惡意電子郵件 (主旨：нов налог за купување) 來引誘某些公司，這些電子郵件聲稱來自馬其頓的家電製造商。這些電子郵件附帶一個惡意 ZIP 壓縮附件檔，內容包含偽裝成採購訂單的 PDF 檔案其實就是 Formbook 竊密程式。



Formbook 至少從 2016 年開始就相當活躍，在網路安全領域廣為人知，是一個在地下論壇上銷售排名很前面的商業化竊密程式。它能夠從受遭入侵的系統中劫取非常多的資訊，包括網頁瀏覽器相關資訊 (儲存的登入資訊、cookie、表單數據等)、按鍵紀錄、螢幕截圖和電腦上儲存的檔案。以下是最近賽門鐵克所偵測攔截到的 Formbook 竊密程式的狀態表。



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 多重防護技術能在第一時間就偵測到該惡意程式及有效對應**零時差**攻擊的防護機制及其威脅名稱：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn34

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g310
- SONAR.SuspBeh!gen752

基於機器學習的防禦技術：

- Heur.AdvML.B

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)。

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。
欲深入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。
欲深入瞭解更多有關於賽門鐵克郵件安全雲端服務(Email Security.Cloud)詳細資訊，請點擊此處。

2023/09/19

中國駭客在間諜行動中導入的全新Linux後門程式：SprySOCKS

SprySOCKS 是中國駭客針對多個國家政府機構所發動的間諜行動中所導入全新 Linux 後門。該後門源於 Windows 平台上的開源惡意軟體 (Trochilus)，將其移植到 Linux 平台，並有 RedLeaves 和 Derusbi 等其他惡意軟體的影子。攻擊者最近將未修補已知漏洞有提供網際網路服務的不安全伺服器作為初始攻擊的目標，並安裝 Cobalt Strike 和攻擊鏈後續需的工具，例如：SprySOCKS 後門。

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
- Linux.Mirai
- 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。

2023/09/19

Dottless IP將其混入垃圾郵件中

賽門鐵克最近觀察到一場利用 Dottless IP 的網址，試圖逃避連結偵測和反垃圾郵件技術的垃圾郵件行動。雖然普通 Dottless IP 的網址，可能包含一種類型的混淆（十六進制、八進制、十進制），但這些最近觀察到的連結包含所有三種類型。即 hxxp://0xFF.255.0337.0xFF/。

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。

2023/09/18

APT36駭客組機(又稱透明部落)：透過模仿YouTube外觀的Android安裝套件(APK)來傳播CapraRAT遠端存取木馬

APT36 駭客組織 (又稱透明部落) 在威脅領域相當活躍，這次散播 CapraRAT 遠端存取木馬的活動再次讓他聲名大噪，CapraRAT 是一個模仿 YouTube 外觀的 Android 安裝套件 (APK)。被安裝後，該 APP 將列出所需的多項權限，如果接受，攻擊者隨後將獲得對受害者設備的存取權限，這將使他們能夠收集和竊取個人資訊。

CapraRAT 具有以下的功能：

- 使用麥克風錄音、前後鏡頭的錄影
- 收集簡訊內容和多媒體訊息內容、通話記錄
- 傳簡訊、封鎖簡訊
- 打電話
- 螢幕截圖

- 更改系統設定，例如：GPS 和網路
- 修改儲存在手機上的檔案。

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：

- WS.Malware.1

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.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。

2023/09/15

針對Webex用戶的BatLoader惡意廣告攻擊行動

這是一個濫用 Google Ads 詳細目錄摘要的購物廣告範本設定來針對 Webex 使用者的惡意程式。如果用戶點擊這些廣告，他們將被重新導向到誘騙使用者下載安裝程式以傳播的 BatLoader 惡意軟體的網站。顧名思義，該惡意軟體用於載入攻擊鏈後續所需的檔案。在檢查時，下載並執行的惡意軟體是 DanaBot，但這可以根據攻擊者的意願進行變更。DanaBot 是一種銀行金融木馬，可用於竊取資訊、遠端連接到遭入侵系統以及載入和執行更多惡意軟體，包括勒索軟體。

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：

- Trojan Horse
- Trojan.Whispergate
- WS.Malware.1

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
- Heur.AdvML.B!200
- 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。