保安資訊--本周(台灣時間2023/09/08)
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 67 萬 9,900 台受保護端點上總共阻止了 9,000 萬次攻擊。這些攻擊中有 88.2% 在感染階段前就被有效阻止：**(2023/09/04)**

- 在**14萬5,600**台端點上，阻止了**3,750**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**22萬2,300**台端點上，阻止了**1,650**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬8,200**台**Windows**伺服主機上，阻止了**1,420**萬次攻擊。
- 在**8萬6,300**台端點上，阻止了**310**萬次嘗試掃描伺服器漏洞。
- 在**2萬2,200**台端點上，阻止了**140**萬次嘗試掃描在**CMS**漏洞。
- 在**7萬5,700**台端點上，阻止了**170**萬次嘗試利用的應用程式漏洞。
- 在**23萬6,600**台端點上，阻止了**510**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2,900**台端點上，阻止了**180**萬次加密貨幣挖礦攻擊。
- 在**14萬800**台端點上，阻止了**890**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**8萬6,300**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。

2023/09/07

交易員和投資者請小心～惡意廣告攻擊行動，傳播Atomic竊密程式(AMOS)

Atomic 竊密程式 (又名AMOS) 於 2023 年4 月左右被發現。該惡意軟體可以從遭入侵的電腦竊取各種機敏資料據，包括系統資訊、Keychain 密碼、使用者的文件檔案、cookie、瀏覽器資料、信用卡詳細資訊、加密貨幣錢包和其他……。最近在真實網路情境發現傳播該惡意軟體的新一波惡意廣告攻擊行動。攻擊者將其惡意下載網站偽裝成交易員和投資者經常使用的熱門圖表平台和社交網路：TradingView。該偽裝的惡意網站提供多種平台的虛假 TradingView 應用程式下載。後果是在 Windows 和 Linux 上會下載 NetSupport 遠端存取木馬 (RAT)，而在 macOS 上則會安裝 Atomic 竊密程式 (AMOS)。

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。

2023/09/07

還是有人不信邪～新一波Agent Tesla傳播行動繼續開採利用五、六年前的老舊漏洞

Agent Tesla 是惡名鼎鼎的竊密程式，具有遠端存取功能，在過去幾年中一直屹立不搖於威脅領域。每天都有該惡意軟體相關的災情傳出，其主要是透過惡意電子郵件進行傳播。最近傳播此惡意軟體的網路釣魚行動在其攻擊鏈中利用相對較舊的 Microsoft 漏洞 CVE-2017-11882 和 CVE-2018-0802。攻擊者一直在傳播偽裝成出貨明細發票的網路釣魚電子郵件，並夾帶惡意 Excel 附件，這些附件檔又包含針對上述漏洞的利用。被植入的 Agent Tesla 模組具有從各種瀏覽器、電子郵件收發程式和應用程式中竊取憑證／帳密、鍵盤側錄以及從受感染的電腦中截取螢幕截圖等功能。

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：

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：

- Exp.CVE-2017-11882!g5
- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Gen.MBT

基於機器學習的防禦技術：

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

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: Microsoft Office CVE-2018-0802
- 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。

2023/09/07

小心！WhiteSnake竊密程式透過Python套件(Package)散布

WhiteSnake 竊密程式，可以危害 Windows 和 Linux 平台。過去，這種惡意軟體被發現以惡意 PyPl 套件包散播。一旦遭入侵，就會收集並洩漏資訊，並採用 OpenSSH 和 serveo\.net 等開源工具將資料上傳到某些遠端伺服器，並透過 Telegram 頻道通知幕後主使者，以躲避檢測。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- 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。

2023/09/07

Warp惡意軟體散布Stealerium竊密程式的新變種

據報導，在真實網路情境發現到一起全新攻擊行動利用 Warp 惡意軟體向受害者散布 Stealerium 竊密程式的新變種。涉入該行動的 Warp 惡意軟體包含一個基於 Go 的 Warp 載入器元件，被夾帶在惡意電子郵件附件發送給受害者，以及一個負責派送和執行竊密程式的的 Warp 植入器惡意酬載。Stealerium 竊密程式的主要功能在竊取系統資訊、憑證、銀行詳細資訊、加密錢包和網路瀏覽器 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 Horse
- Trojan.Gen.MBT
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!500
- 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。

2023/09/07

Ivanti Sentry行動裝置安全閘道的CVE-2023-38035嚴重等級漏洞

CVE-2023-38035 是最近披露的一個嚴重等級，必須馬上修補 (CVSS 評分：9.8) 身份驗證旁路／繞過 (authentication bypass) 漏洞，影響 Ivanti Sentry (以前稱為MobileIron Sentry) 版本 9.18 及更早版本，這是一個 In-Line 模式的行動裝置安全閘道和管理系統。如果利用該漏洞，遠端攻擊者可以利用 root 權限在易受攻擊的系統上執行任意程式碼。可開採利用該漏洞的程式碼已於近期被公開發布，並在真實網路情境傳出災情，隨即被美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：

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: Ivanti Sentry API CVE-2023-38035

2023/09/06

鎖定SQL資料庫的FreeWorld(*自由世界)勒索軟體

已有報導稱，被稱為 FreeWorld 的Mimic 勒索軟體新變種，專門鎖定 SQL 資料庫進行加密勒索。該勒索軟體背後的攻擊者採用針對 Microsoft SQL(MSSQL) 服務的暴力攻擊技術。一旦遭感染後，它會濫用被稱為檔案搜尋神器的合法應用程式：Everything 來快速搜尋目標檔案，並在加密後附加 .FreeWorld 的副檔名。

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!gen6
- SONAR.SuspBeh!gen616

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

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

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

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。

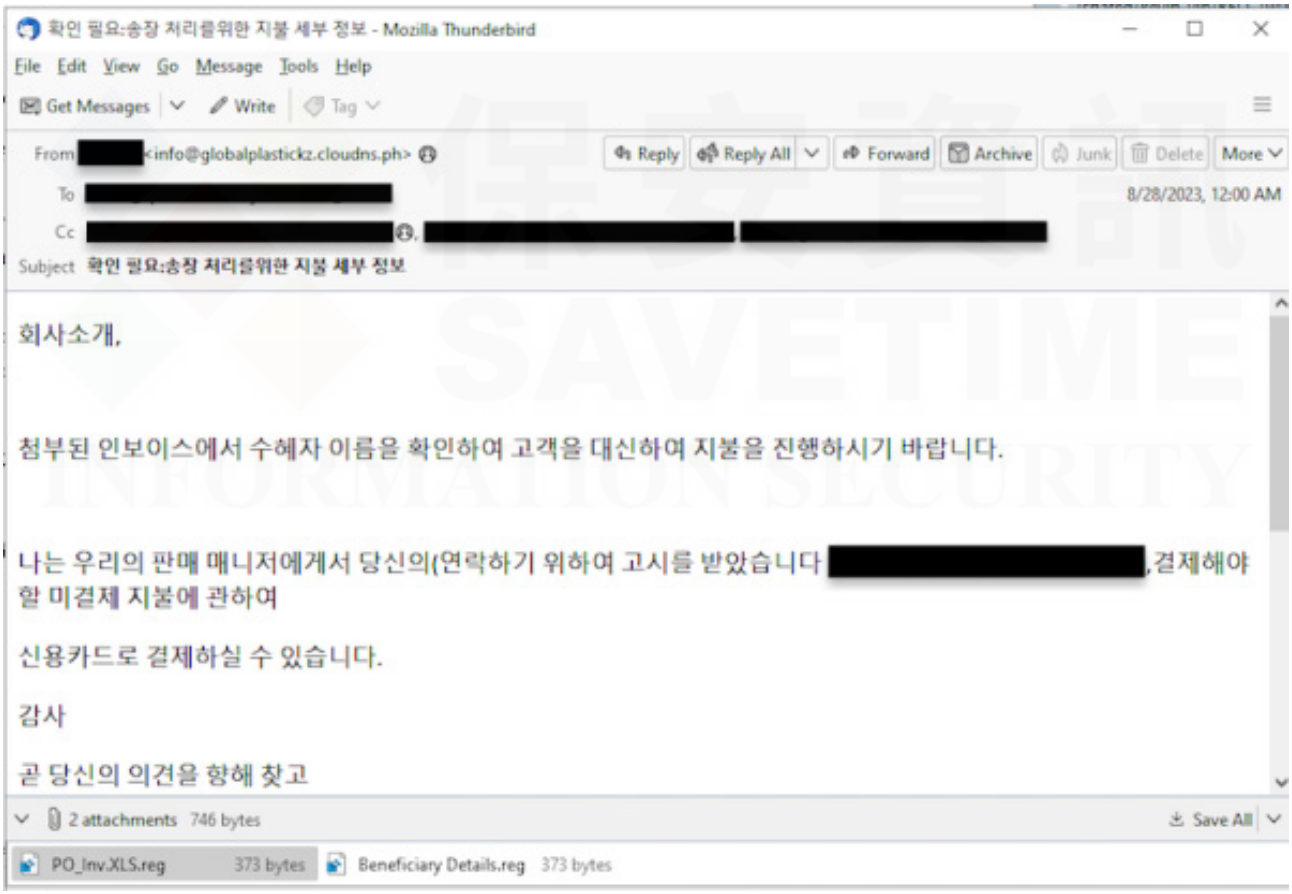
2023/09/05

防護亮點：韓國正遭受登錄註冊檔濫用的惡意郵件攻擊

.reg 登錄註冊檔是 Microsoft Windows 作業系統中用於新增、修改或刪除登錄子機碼和值的文字格式的登錄檔的腳本檔，而登錄檔是 Microsoft Windows 操作系統和其應用程式中的一個重要的層次型資料庫，用於儲存作業系統、硬體、軟體以及使用者喜好設定等資訊。

雖然 .reg 檔案通常用於合法目的，它的特性也讓網路犯罪分子可以在受害者的系統上下載和執行惡意軟體。在當今的威脅形勢下，雖然它們並不普遍，但它們仍然被世界各地的特定駭客組織和個人在其攻擊鏈中積極運用。

最近賽門鐵克觀察到針對韓國機構組織 (本地和跨國) 的惡意垃圾郵件行動。惡意電子郵件 (主旨：『**확인 필요:송장 처리를 위한 지불 세부 정보**』) 夾帶兩個惡意 .reg 檔案『PO_Inv.XLS.reg』和『Beneficiary Details.reg』。如果執行成功，後續將會下載惡意 PowerShell 腳本和bat 批次檔。



該批次檔 (ld.bat) 將執行 PowerShell 腳本檔 (ld.ps1)，隨後，PowerShell 腳本將嘗試修改電腦的註冊表和隱藏的 %APPDATA% 檔案夾，使其豁免 Windows Defender 的掃描。它還會下載一個冒充 PuTTY（是個開源的Telnet／SSH 安全遠端連線程式）的竊密程式。所有下載的檔案將存儲在%APPDATA%資料夾中。

這個基於 Python 的竊密程式名為『REG STEALER 2023』，經過高度混淆和加密。它與各種 Discord 和 Telegram 竊密程式有許多相似之處。經過分析，我們認為該竊密程式很可能源於 Blank

Grabber 的原始碼，該原始碼已發佈在熱門的版本控制和協作軟體開發平台上的網站。以下是它可以從受感染的電腦擷取並透過 Discord Webhooks 和 Telegram 機器人發送的一些資料。

- 瀏覽器密碼、cookie、自動填寫 (autofills) 機制的帳密和網頁瀏覽記錄
- Discord (一款在諸多系統上都可執行且功能完備的社交應用程式) 的 Token 憑證
- 已保存的 WIFI 密碼
- 系統資訊
- 螢幕截圖
- Telegram 連線
- Common files 檔案資料夾
- 加密錢包
- 擷取鏡頭影像
- 各種遊戲和遊戲平台的 cookie 和連線

賽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：

- Downloader
- Trojan Horse
- Trojan.Regsteal
- Web.Reputation.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。

2023/09/05

BlueShell惡意軟體在針對韓國和泰國的網路攻擊中被大肆散播

BlueShell 是一個由 Go 語言撰寫的惡意後門程式，有一段時間曾在 GitHub 上公開發布過，並且很容易被眾多 APT 駭客組織使用。該惡意軟體支持各種作業系統，包括 Windows、Linux 和 macOS。BlueShell 功能包括執行從遠端 C&C 伺服器接收的命令以及上傳和下載檔案。該惡意軟體能夠在遭入侵的裝置上設置 SOCKS5 代理，以達到惡意流量隱藏和檢測規避的目的。最近觀察到傳播 BlueShell 惡意軟體的網路攻擊行動主要針對韓國和泰國的用戶。

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
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Hacktool.Jsprat
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!500
- 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。

2023/09/04

SuperBear(*超級熊)遠端存取木馬(RAT)惡意軟體

SuperBear是最近鎖定韓國記者的網路攻擊行動中所傳播的一種遠端存取木馬 (RAT)。初始的攻擊媒介是一封包含快捷列 .LNK 附件檔的網路釣魚電子郵件，該附件檔案一旦被執行就會導致惡意 PowerShell 腳本執行。在攻擊鏈的再進一步發現，歹徒一直在利用具有程序注入功能的 AutoIT3 編譯腳本。該攻擊行動的最終有效籌載就是 SuperBear RAT，它能夠從遭入侵的端點竊取資料以及下載／執行任意 shell 命令和動態連結 (DLL) 函式庫。

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.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。

2023/09/04

Black Berserk(*暗黑狂暴戰士)勒索軟體

Black Berserk 是最近在網路上發現另一種常見勒索軟體。該惡意軟體會加密檔案並冠上 .Black 的附檔名。檔名為『Black_Recover.txt』的贖金支付說明檔會被放置在每個被加密檔的資料夾，指引受害者透過指定的電子郵件聯繫加害者。該惡意軟體還能夠刪除受感染端點上的陰影複製 (shadow copies) 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：

- AGR.Terminate!g2
- SONAR.Cryptolocker!g42
- SONAR.SuspLaunch!g18

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Generic.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/09/01

Remo(*羅密歐)～安卓平台上的網路銀行金融木馬

Remo 是安卓平台上新發現的全新惡意軟體，由多個冒充幣安交易平台的網路釣魚網站傳播。據報導，該惡意軟體以各種銀行和加密貨幣交易／錢包APP為目標，以竊取資料。Remo 會濫用遭入侵裝置上的輔助服務來側錄按鍵、竊取剪貼簿資料或暗中擷取受害者螢幕上顯示的內容。傳播該惡意軟體的最新行動主要針對東南亞的行動手機／裝置用戶。

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
- Android.Reputation.1
- 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。