保安資訊--本周(台灣時間2023/06/09)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 74 萬 6,000 台受保護端點上總共阻止了 9,310 萬次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2023/06/04)**

- 在**15萬3,900**台端點上，阻止了**4,360**萬次嘗試掃描**Web**服務器的漏洞。
- 在**26萬5,800**台端點上，阻止了**1,900**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬300**台**Windows**伺服主機上，阻止了**1,360**萬次攻擊。
- 在**8萬4,000**台端點上，阻止了**240**萬次嘗試掃描伺服器漏洞。
- 在**1萬5,700**台端點上，阻止了**86萬1,700**次嘗試掃描在**CMS**漏洞。
- 在**6萬5,800**台端點上，阻止了**150**萬次嘗試利用的應用程式漏洞。
- 在**25萬7,300**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**4萬5,000**台端點上，阻止了**190**萬次加密貨幣挖礦攻擊。
- 在**16萬500**台端點上，阻止了**900**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,200**台端點上，阻止了**12萬5,300**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。

2023/06/08

Stealth Soldier～被用於攻擊利比亞企業／組織的全新後門程式

Stealth Soldier 是一種全新後門程式，被用於針對利比亞企業／組織的間諜活動和監視活動。惡意軟體的功能包括鍵盤側錄、檔案滲出、螢幕截圖、網路瀏覽器資料和憑證竊取等。惡意軟體使用的命令和控制 (C&C) IP位址顯示與之前用於網路釣魚攻擊並偽裝成利比亞外交部網站的大量網域存在特定關係。

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.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。

2023/06/08

MFT檔案共享系統MOVEit Transfer存在零時差漏洞(CVE-2023-34362)，駭客已利用該漏洞展開攻擊

據報導，最近在 MFT 檔案共享系統 MOVEit Transfer 軟體中發現嚴重的 SQL 注入漏洞 (CVE-2023-34362) ，該漏洞已被駭客開採利用。如果被開採利用，該漏洞可能讓攻擊者未經授權存取未修補的系統，進而導致機密資料遭到入侵和洩漏。在網路上被開採利用的報告公布後，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。

觀察到 MOVEit 漏洞開採利用的攻擊行動之一是將 LEMURLOOT web shell 部署到受感染的目標。Web shell 已偽裝成“human.aspx”檔案，該檔案是 MOVEit MFT 軟體的合法元件。LEMURLOOT 具有從 MOVEit Transfer 系統目標竊取資料以及 Azure Blob 儲存容器的資訊和憑證功能。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- JS.Malscript!g1
- Trojan Horse
- Trojan.Gen.2

- Trojan.Gen.NPE
- Trojan.Malscript
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.C

基於安全強化政策(適用於使用DCS)：

DCS 內建的強化安全政策能防止任意部署 Webshells 和未經授權的軟體，可確實針對 CVE-2023-34362 漏洞提供零時差保護。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2023/06/07

以美國運通(American Express)為幌子，駭客鎖定日本企業發動網路釣魚詐騙

多年來，網路釣魚攻擊者一直在利用銀行相關主題來進行他們的社交工程詐騙，以從世界各地的消費者和企業那裡竊取銀行等財務資料。賽門鐵克每天都會監控到這些駭客行動。在最近一個例子中，攻擊者一直鎖定日本企業為目標，同時透過惡意電子郵件冒充美國運通。他們試圖以刷卡額度不夠或遭盜刷等問題的欺騙活動為由來引誘受害者。如果有人成功被引誘並點擊電子郵件中的網址鏈結 (URL)，他們將被重導到一個假冒的美國運通網站。

觀察到的電子郵件主旨：

- American Expressカード利用に関する重要なご案内
- ご利用金額の超過によるカード利用制限のご案内
- カード不正使用の防止にご協力をお願いします - カード利用制限のお知らせ
- 不正利用の疑いがあります - カードの停止手続きが必要です

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。

2023/06/07

Satacom惡意軟體傳播加密貨幣竊取程式

Satacom 下載器又名 LegionLoader 最近在向受害者傳播加密貨幣竊取程式的惡意攻擊行動中被發現。該惡意軟體最初透過標榜免費軟體或破解軟體的網站下載來傳播。Satacom 將多個檔案下載到受感染的電腦，包括為源於 Chromium 核心類型的網頁瀏覽器安裝惡意擴充功能的 PowerShell 腳本。安裝的擴充功能利用網頁注入伎倆，允許攻擊者操縱目標網站的內容，以竊取加密貨幣。

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.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。

2023/06/07

Gitlab路徑穿越漏洞CVE-2023-2825

CVE-2023-2825 是最近披露的嚴重 (CVSS 評分滿分：10.0) 路徑穿越漏洞，影響 Gitlab 社群版 (CE) 和企業版 (EE) 版本 16.0.0。如果利用該漏洞，則可能允許未經身份驗證的用戶通過路徑穿越錯漏洞誤讀取 Gitlab 伺服器上存在的任意檔案。這可能會導致機密資料、程式碼或其他機密資訊的洩露。GitLab 已在 16.0.1 版本中發布緊急安全更新以解決此漏洞。

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：

- Attack: Gitlab Path Traversal Vulnerability CVE-2023-2825

2023/06/07

MoneyBird勒索軟體(又名Agrius)

最近有新一波 Agrius 相關活動被報導，他們使用全新的勒索軟體，其別名被稱為MoneyBird。該組織自 2021 年以來一直相當活躍，與以色列等中東地區的各種勒索軟體和檔案刪除程式的攻擊行動也有關連。此外，Agrius 過往就有從受害者那裡竊取資料並公開洩露的紀錄。雖然他們使用新的勒索軟體，但他們的作案手法與之前的活動非常相似--從易受攻擊的網頁伺服器進行初始存取。

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.MoneyBird
- Trojan.Gen.MBT

2023/06/06

Xollam／Mallox勒索軟體

Xollam 是 TargetCompany 勒索軟體家族的最新變種。同一駭客集團在 2021 年和 2022 年使用的先前已知變種包括 Fargo 和 Mallox。Xollam 這個名字源於倒著寫的 Mallox，因為它是用相同的字母倒過來拼寫的。Xollam 於 2023 年在利用微軟的 OneNote 檔案進行初始存取和有效籌載傳遞的行動中首次被發現。該勒索軟體會加密使用者的檔案並在其後附加 .xollam 副檔名，然後以檔名為“FILE RECOVERY.txt”的文字檔投放勒索支付說明。

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!g36
- SONAR.CryptoLocker!g42
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g230
- SONAR.SuspLaunch!g253
- SONAR.SuspLaunch!gen4
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Mallox
- 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

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 568
- System Infected: Trojan.Backdoor Activity 634

2023/06/06

HelloTeacher安卓手機上惡意軟體針對越南銀行用戶

HelloTeacher 是一種安卓智慧型手機上的惡意軟體，偽裝成熱門的通訊 APP (例如：Viber 或 Kik Messenger)，針對越南銀行用戶進行散佈。安裝後，HelloTeacher 將提示受害者啟用輔助功能服務，該服務一旦啟用，惡意軟體便可以從帳戶餘額、聯繫人、照片和已安裝的應用程序中竊取資訊，並具有螢幕擷取、竊取簡訊內容等附加功能。

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。

- AdLibrary:Generisk
- Android.Malapp
- Android.Reputation.2

2023/06/06

留意即將出現的新一波NoEscape勒索軟體攻擊

另一個被稱為“NoEscape”勒索軟體即服務 (RaaS) 的專案正在暗網上做廣告招兵買馬。NoEscape 是用 C++ 撰寫，並使用高度可定制的勒索軟體即服務 (RaaS) 營運模式。該惡意軟體具有禁用 UAC、停止系統服務和程序以及刪除系統備份和磁碟區陰影複製的功能。被 NoEscape 加密後的檔案會被新增“.CCBDFHCHFD”等副檔名，並留置 .txt 文字檔的勒索贖金支付說明檔。其營運模式正不斷推陳出新，因此一旦找到更多合作夥伴，很可能會觀察到更多相關活動。

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(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g189

- SONAR.SuspLaunch!g193

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- 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：

- Attack: Ransom.Gen Activity 46

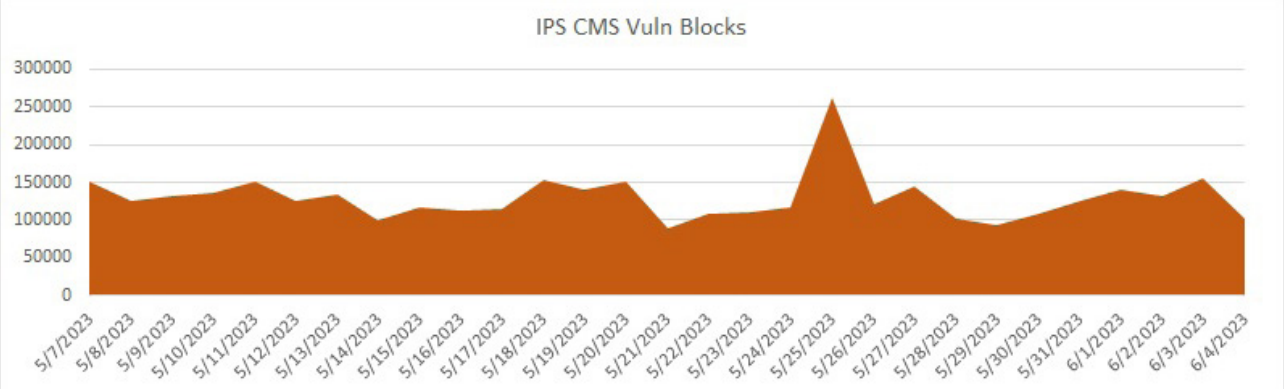
2023/06/05

防護亮點：IPS～補強內容管理系統(CMS，Content Management System)漏洞的安全網

WordPress、Joomla、Drupal……等內容管理系統 (CMS，Content Management System) 被廣泛用於建立和管理網站。它們的受歡迎程度意味著大量網站建立在這些平台上，使它們成為攻擊者覬覦的目標。這些平台是複雜的軟體系統，具有各種元件、佈景主題 (Themes)、外掛 (Plugins) 和多元的模組，通常由不同的開發人員所建立。這種複雜性可能會引入可被威脅者濫用的漏洞。隨著大量可用的第三方主題和外掛的出現，確保每個元件的安全變得非常具有挑戰性。

不幸的是，許多網站所有者並沒有保持他們的 CMS 及其組件是最新，這可能會使漏洞得不到修補，從而使攻擊者更容易利用已知的安全漏洞。通常 CMS 漏洞都有詳細記錄，攻擊者會主動搜索運行老舊版本的網站。大多數攻擊者會利用自動化工具來開採利用這些漏洞，從而更容易發動廣泛的攻擊。他們可以在網際網路上掃描運行特定 CMS 版本的網站、識別漏洞並大規模發起自動化攻擊。

賽門鐵克入侵防禦系統(IPS) 無時不刻一直在主動攔阻試圖利用這些 CMS 漏洞利用的威脅。



駭客最喜歡攻擊伺服器，特別是面向網際網路的公眾服務主機的先天脆弱性。在我們“上個月 IPS 做了什麼來保護伺服器？”5 月份的公告中，我們 IPS 網路層防護成功攔阻在 12.2K 伺服器上共 140 萬次的 CMS 漏洞利用嘗試。攻擊者從未鬆懈，一直樂此不疲。

多年來，CMS 漏洞與各種威脅和惡意活動有關。已經出現的一些常見威脅包括：

- 未經授權的存取：利用 CMS 漏洞可以為攻擊者提供對網站後端的未經授權存取，從而使他們能夠控制內容管理系統。此存取可用於操縱網站內容、竊取資料或執行其他惡意活動。
- 篡改：可利用 CMS 漏洞透過注入未經授權內容或修改現有內容來篡改網站。攻擊者可能會用惡意或仇視內容置換網站的原始內容，從而對網站所有者或組織的聲譽造成損害。
- 資料外洩：CMS 漏洞可能導致資料外洩，攻擊者可以存取存儲在網站上的敏感資訊。這可能包括用戶憑證、個人資料、財務數據或專有業務訊息。被盜資訊可用於身份盜用、金融欺詐或在黑市上出售。
- 散播惡意軟體：利用 CMS 漏洞可以讓攻擊者將惡意程式碼注入網站。此程式碼可用於將惡意軟體散播給毫無戒心的造訪者，駭入他們的電腦並可能將感染鏈傳播到其他系統。
- 網路釣魚攻擊：可以開採利用 CMS 漏洞來發動網路釣魚行動。攻擊者可以建立看似合法但目的是竊取用戶憑證／帳密或機敏資訊的虛假登錄頁面或表單。網路釣魚攻擊可能導致身份盜用、財務損失或未經授權存取其他帳戶。
- SEO (搜尋引擎最佳化) 垃圾郵件：可以利用 CMS 漏洞將隱藏鏈接或關鍵字注入網站內容。這通常是為了 SEO (搜索引擎最佳化) 垃圾郵件目的，攻擊者操縱搜索引擎排名來推廣他們自己的網站或產品。
- 分散式阻斷服務 (DDoS)：可利用 CMS 漏洞對網站發起 DDoS 攻擊。透過利用 CMS 或相關外掛程式中的弱點，攻擊者可以用大量請求使網站伺服器過載，從而使合法用戶無法造訪該網站。

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 **零時差**防護技術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: WordPress Plugin XSS Attempt
- Web Attack: WordPress XMLRPC Malicious Pingback Request
- Web Attack: Wordpress Arbitrary File Download 4
- Web Attack: Sourcecodester System CVE-2020-29227
- Web Attack: Joomla Component Local File Inclusion
- Attack: Web CMS Multiple Sql Injection
- Web Attack: Drupal Core RCE CVE-2018-7602
- Web Attack: WordPress Plugin Path Traversal Attempt
- Web Attack: Wordpress Arbitrary File Download CVE-2003-1599
- Attack: Wordpress Duplicator Plugin Unauthenticated Arbitrary File Download

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。

2023/06/04

EdgeGuard竊密程式

另一個竊密程式的程式碼最近被分享在開發網站 GitHub，賽門鐵克已經觀察到測試活動。EdgeGuard 竊密程式具有常見的功能，並很可能會被駭客組織和個人利用，因為它是免費提供。但是，由於存在許多其他類似的威脅，因此不能保證達到高流行率。目前鎖定的目標主要包括瀏覽器暫存的密碼、歷史記錄和下載，以及像是 Atomic、Exodus 和 MetaMask 等加密貨幣錢包。

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

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/06/02

專釣大魚～SharpPanda進階持續威脅(APT)駭客組織發動的大規模魚叉式網路釣魚行動

有人在真實網路情境發現到 SharpPanda 進階持續威脅 (APT) 駭客組織針對 G20 國家的政府組織所發動的網路攻擊行動。攻擊者發動客製化的魚叉式網路釣魚行動，讓收件者信以為真地開啟夾帶惡意酬載的檔案並落入其圈套。這些檔案是使用 RoyalRoad 的駭客工具產出的惡意程式，該工具濫用微軟 Office 的預設工具：Equation Editor的CVE-2018-0802、CVE-2018-0798 和 CVE-2017-11882 等漏洞。開啟檔案會引發後續的攻擊鏈，攻擊者試圖透過這些攻擊鏈從受害者那裡收集資料。如果受害者的電腦有繼續深掘的價值，下一階段的攻擊鏈將繼續進行，包含執行惡意酬載的核心主導程式，與 C&C 伺服器連線並執行後門程式。

該後門具有以下能力：

- 螢幕截圖
- 收集受害者電腦的資訊（例如：程序和服務資訊、Win 作業系統版本、登錄檔機碼等）
- 控制關機
- 使用命令列執行讀／寫命令
- 控制檔案的權限與屬性
- 控制程序 (Process) 的建立與終止

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：

- Bloodhound.RTF.12
- Trojan Horse
- W97M.Downloader

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。

2023/06/02

DBatLoader惡意垃圾郵件攻擊行動大肆散播，助長Remcos遠端存取木馬(RAT)感染率

DBatLoader 惡意酬載主導核心程式，最近被用於散播 Remcos 遠端存取木馬 (RAT) 惡意軟體。DBatLoader (又名 ModiLoader) 過去曾被視為提供各種惡意籌載的主導程式，例如：Remcos、Formbook 或 Warzone RAT。在最近觀察到的這次惡意行動中，受害者被帶有 iso 附件的採購訂單垃圾郵件所引誘，該 iso 檔包含可偽裝成 Excel 電子試算表的 ModiLoader 嵌入式可執行檔。然後，此 ModiLoader exe 將使用 Remcos 遠端存取木馬 (RAT) 來操弄受感染的電腦。

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.SuspBeh!gen530
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan Horse
- 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：

- System Infected: Netweird.B Activity 2
- System Infected: RemcosRAT Trojan Activity
- 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。