保安資訊--本周(台灣時間2024/05/10)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 49 萬 800 台受保護端點上總共阻止了 5,610 萬次攻擊。這些攻擊中有 84.1% 在感染階段前就被有效阻止：**(2024/05/06)**

- 在**10萬7,600**台端點上，阻止了**2,040**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**14萬6,900**台端點上，阻止了**1,080**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬5,200**台**Windows**伺服主機上，阻止了**850**萬次攻擊。
- 在**6萬6,800**台端點上，阻止了**200**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,300**台端點上，阻止了**81萬5,100**次嘗試掃描在**CMS**漏洞。
- 在**5萬7,900**台端點上，阻止了**160**萬次嘗試利用的應用程式漏洞。
- 在**17萬9,100**台端點上，阻止了**410**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2萬3,300**台端點上，阻止了**150**萬次加密貨幣挖礦攻擊。
- 在**9萬9,000**台端點上，阻止了**750**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**430**台端點上，阻止了**6萬3,100**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。

有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點(桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在 13 萬 9,500 個受保護端點上阻止了總計 510 萬次攻擊。**(2024/05/06)**

- 使用網頁信譽情資，在 **126.6K** 個端點上阻止 **450** 萬次攻擊。
- 攔截 **29K** 個端點上 **509.8K** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在 **9.6K** 個端點上攔截 **102.5K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **329** 個端點上攔截 **18.7K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

2024/05/09

助紂為虐：俄羅斯的網際網路基礎架構服務商：Bulletproof，提供駭客發動SocGholish網路攻擊行動所需的基礎架構服務

據報導，俄羅斯的網際網路基礎架構服務商：Bulletproof，提供駭客發動網路攻擊所需與惡意程式上架與傳播網路攻擊行動的基礎架構服務，包括命令與控制 (C&C) 伺服器和傳遞 SocGholish 惡意軟體的網路釣魚頁面。最近幾個月多個惡意軟體行動都使用 Matanbuchus 惡意程式載入器，其 C&C 基礎設施上架在『Proton66 OOO』等 Bulletproof 所提供的代管服務上。此外，還觀察到威脅者利用該基礎設施上架採用由 Plesk 服務創立的釣魚網頁，假冒 UPS、Chronopost 和法國衛生系統等機構的包裹追蹤服務。這些行動通常透過垃圾簡訊進行傳播，而這些攻擊背後的組織通常透過 Telegram 提供的服務為非作歹。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-Wscr!g1
- ACM.Wscr-Rd32!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中現有政策已經阻止並檢測到相關的惡意指標。建議最低策略是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- JS.Downloader
- JS.Redirector
- Scr.Malcode!gen
- Trojan.Mdropper
- Trojan.Gen.MBT
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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。

2024/05/08

惡意的Minecraft遊戲模組：鎖定遊戲玩家散播zEus惡意竊密程式

據報導，一個針對微軟的 Minecraft 遊戲玩家所發動惡意軟體散播行動，以提供增強遊戲外觀自訂的套裝軟體為幌子，實際上卻是在傳播 zEus 惡意竊密程式。該惡意竊密程式主要的特色是具有躲避檢測的能力，同時竊取敏感性資料並注入額外的有效酬載 (通常以批次檔的形式)，以便與命令與控制 (C&C) 伺服器建立通訊，以獲取進一步指令。這種惡意軟體能夠進行螢幕截圖，並將資料滲出到攻擊者操控的 webhook 伺服器。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Reg!g1
- ACM.Ps-RgPst!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中現有政策已經阻止並檢測到相關的惡意指標。建議最低策略是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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：

- Audit: CURL Process Accessing Lets Encrypt Certified Site
- 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。

2024/05/08

RokRAT遠端存取木馬持續到處流竄

APT37 駭客組織 (也稱 ScarCruft) 繼續透過 .LNK 捷徑檔散播RokRAT 遠端存取木馬，尤其針對韓國使用者。該惡意軟體偽裝成實際檔案，啟動後會執行 PowerShell 命令。隨後，這些命令將執行其他檔案，使攻擊者能夠收集使用者資訊並將資料傳輸回其 C&C 伺服器。

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.Powershell!g20

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Scr.Heuristic!gen20
- Scr.Mallnk!gen13
- WS.Malware.2
- WS.SecurityRisk.4

2024/05/08

不堪其擾～Gadfly駭客組織所傳播的網路釣魚信件多到爆匣

賽門鐵克最近發現，由 Gadfly 駭客組織 (也稱 TA577) 所發動的網路釣魚攻擊行動日益增加。該行動引誘使用者開啟以拉丁文命名的 PDF 附件，其內容包含利用容易信以為真的相似／錯別字之微軟服務類型網域的網址連結，其最終目的是竊取憑證以供日後使用。

附件檔案名稱示例：

- DOLOREMQUEQ.pdf
- INCIDUNTRH.pdf
- SUNTP.pdf
- DESERUNTE.pdf
- EIUSHW.pdf

相似／錯別字的微軟服務類型網域之網址連結域示例：

- loginmlcrosoftonline
- ioqinmlcrosotfonilna。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中現有政策已經阻止並檢測到相關的惡意指標。建議最低策略是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 信譽服務中獲得最大收益。

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：

- Scr.Malcode!gen
- Trojan.Gen.NPE

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。

2024/05/08

Hunt 勒索軟體--Dharma／Crysis的全新變種

Hunt 是最近在真實網路情境上發現的另一個源於 Dharma/Crysis 勒索軟體的新變種。該惡意軟體會加密使用者檔案，並冠上 .hunt 副檔名以及唯一的受害者 ID 和威脅者的電子郵件位址。以文字檔形式留下的勒索(贖金支付)說明要求受害者透過提示的電子郵件位址聯繫攻擊者，以獲取如何恢復被鎖定檔案的進一步說明。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中現有政策已經阻止並檢測到相關的惡意指標。建議最低策略是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Crysis
- Ransom.Crysis!gm
- SMG.Heur!gen

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

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.Crysis Activity 3

2024/05/08

WordPress架站軟體的Automatic外掛程式(Plugin)存在SQL注入(SQLi)漏洞：CVE-2024-27956，已真實網路情境上被大肆開採濫用

WordPress 是全世界最受歡迎的架站軟體，根據維基百科的資料顯示 (2022.06.10)，全球約有 42.9% 網站是使用 WordPress 架設而成。CVE-2024-27956 正是最近被公開存在 Automatic 外掛程式 (Plugin) 版本 3.92.1 之前發現的嚴重 (CVSS 風險評分：9.8) 的 SQL 注入 (SQLi) 漏洞。成功開採濫用該漏洞可讓攻擊者執行任意 SQL 查詢、建立新的管理帳戶或上傳惡意檔案至受影響伺服器。此漏洞已被報告在真實網路情境上被大肆開採濫用。

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：

- PHP.Backdoor.Trojan

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: WP-Automatic Plugin SQL Injection Vulnerability CVE-2024-27956

2024/05/08

Shinra勒索軟體

最近發現 Shinra 勒索軟體是源於 Proton 惡意軟體家族的新變種，它會加密檔案並冠上『.SHINRA3』副檔名，同時將檔案主檔名重新命名為隨機字串。它會以檔名為『#SHINRA-Recovery.txt』文字檔形式發送勒索 (贖金支付) 說明，其中包含聯繫方式，通常是攻擊者的電子郵件位址。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-FlPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g250

- SONAR.SuspLaunch!g340
- SONAR.SuspLaunch!gen4

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中現有政策已經阻止並檢測到相關的惡意指標。建議最低策略是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 信譽服務中獲得最大收益。

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.C

2024/05/08

CVE-2024-2389--Progress公司的Flowmon網路效能監控工具存在重大等級之命令注入漏洞

CVE-2024-2389 是最近披露一個 CVSS 風險評分為 10 的重大漏洞，它影響 Progress 公司的 Flowmon一種市場深受歡迎的網路效能監控工具)。如果被成功開採濫用，該漏洞允許未經認證的攻擊者透過偽造 API 請求存取 Flowmon 網路介面。此漏洞會進一步導致在易受攻擊的系統上執行任意程式碼。該漏洞的概念驗證 (POC) 程式碼已經公開發佈，供應商已經發佈該應用程式的修補版本。

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: Progress Flowmon CVE-2024-2389

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克的重要主機防護系統：DCS～Data Center Security其出廠就內建的系統鎖定政策，可以防止在相關程序伺服器上被部署可疑的 web shell。
- DCS 預設的鎖定政策可保護底層 UNIX 伺服器免受此漏洞的影響，包括防止執行任意命令和限制讀取主要的作業系統檔案。
- 可對政策中的 DCS 網路規則進行配置，以限制受信任用戶端的暴露。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/05/07

防護亮點：賽門鐵克入侵預防技術～以防護GuLoader的實例來驗證IPS的實績

賽門鐵克的入侵預防技術讓威脅不能越雷池一步，並在初始階段就阻斷以防患未然。賽門鐵克的 IPS 是行業中最佳深度資料封包檢查引擎，可保護數以億計的端點 (桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。對於大型企業，SEP 端點防護擁有多層次防護技術，僅單一項 IPS 技術就能涵蓋 90% 以上威脅防護和事的可視性。

多年來一直支援 Windows 和 MacOS 上 SEP 的 IPS 網路防護技術也為賽門鐵克的瀏覽器保護解決方案提供支援。瀏覽器防護將賽門鐵克 IPS 網路保護導入谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器。

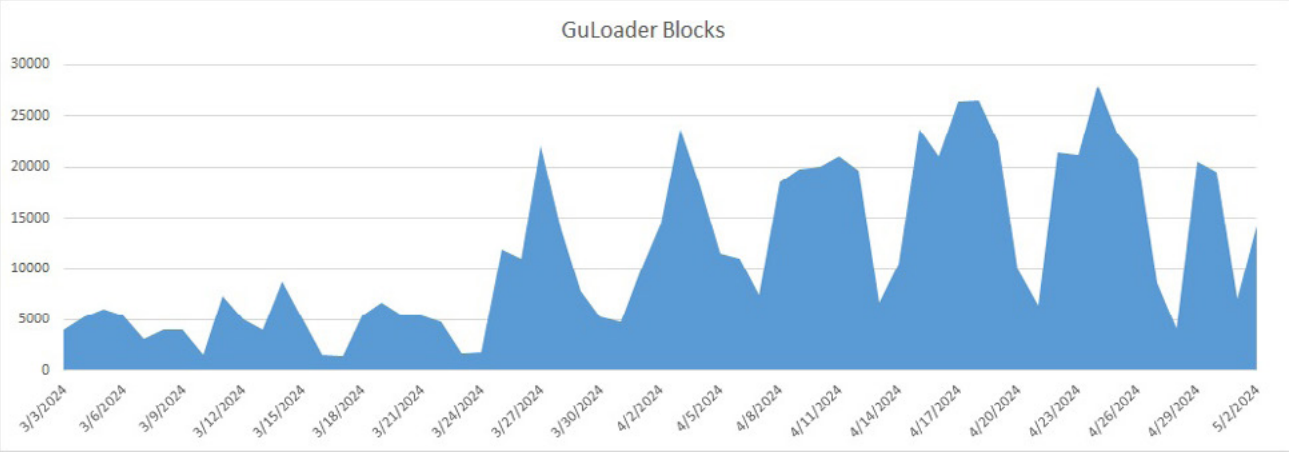
賽門鐵克 IPS 主要功能包括：

- IPS 引擎可以在該端點的網路層、檔案層和更深入的程序層等不同階層，精準檢測和攔截網路威脅活動。
- 遍佈全球的賽門鐵克威脅情資團隊，對當今影響企業網路威脅提供無與倫比的分析，並透過特徵碼資料更新來增強賽門鐵克 IPS。
- IPS 特徵碼集每週 5 天、每天透過 LiveUpdate 更新。這些特徵碼通常會主動阻止威脅的傳播，特徵碼每天都會更新，以改進目標式攻擊類型的 IPS 防護。
- IPS 利用 WebPulse 網頁脈衝專利技術，基於網址／網域／IP 分類來阻止已知釣魚網站和惡意軟體網域。賽門鐵克 WebPulse 服務依靠全球智慧型網路來識別威脅、威脅工件和惡意網路活動。
- 入侵預防的稽核特徵 (IPS Audit Signatures) 提供客戶自行微調 IPS 防護的自訂靈活性。
- 端點 IPS 為賽門鐵克 EDR 提供網路可見性，使威脅獵手團隊和事件回應人員能夠獲得豐富的網路資訊。

以防護 GuLoader 實例來驗證 IPS 實績

GuLoader 是近年非常氾濫的一種惡名昭章的惡意軟體下載器，因其在全球各地傳播各種不同的惡意軟體而聞名。某些情況下，它會載入 Agent Tesla 惡意竊密程式，而在其他情況下，它可能會下載 Remcos 遠端存取木馬。在我們最近的防護公報中了解有關 GuLoader 的更多資訊。

防護 GuLoader 的實績，是賽門鐵克 IPS 保護價值的常態而非特例。阻止 GuLoader 相關網路流量可防止下載和執行攻擊鏈後期階段的酬載。IPS 每天能檢測並阻止成千上萬 GuLoader 活動。



IPS攔截到GuLoader的數量/時序表

我們再看看每週活躍的其他威脅類別，以及它們被 IPS 阻擋的次數。在過去 7 天裡，SEP 的網路防護引擎 (IPS) 總共攔截了 5.57 萬次攻擊，涵蓋 51.06 萬個受保護端點。其中 82.8% 的攻擊是在執行有效載荷之前的感染前階段就被攔截的。

- 在 1.103 萬個端點上阻止了 1890 萬次掃描 Web 伺服器漏洞的嘗試
- 在 1.423 萬個端點上阻止了 1160 萬次利用 Windows 作業系統漏洞的嘗試
- 在 3.67 萬台 Windows 伺服器上阻止了 920 萬次攻擊
- 在 67.5K 個端點上阻止了 190 萬次掃描伺服器漏洞的嘗試
- 在 14.6K 個端點上阻止了 818.1K 次掃描 CMS 漏洞的嘗試
- 在 48.7 千個端點上阻止了 150 萬次利用應用程式漏洞的嘗試
- 阻止了 186.1K 個端點上 420 萬次攻擊，這些攻擊試圖將用戶重導向到攻擊者控制的網站
- 透過 11.3K 個端點阻止了 150 萬次挖礦嘗試
- 在 107.4K 個端點上阻止了 810 萬次惡意軟體 C&C 嘗試
- 在 538 個端點上阻止了 56.5K 次加密劫持嘗試

按一下此處了解有關在桌上型電腦和伺服器上啟用 IPS 的更多資訊。
按一下此處了解有關整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站。
別家都沒有的功能？試試使用賽門鐵克瀏覽器保護功能保護您的瀏覽器。

2024/05/07

死灰復燃～Lockbit 勒索軟體的攻擊還在增長

今年 2 月初，Lockbit 勒索軟體家族在一次名為『克羅諾斯攻擊行動』(Operation Cronos) 的多國執法單位聯手圍剿行動中，逮捕該勒索軟體集團的多名成員，沒收他們的基礎設施，並公開發佈解密工具。儘管遭受重擊，Lockbit 仍然活躍在威脅環境中，我們最近觀察到與該勒索軟體新變種相關的檢測量有激增趨勢。賽門鐵克的進階機器學習 (AML) 技術在攻擊鏈的初始階段就檢測到惡意電子郵件，在阻止這次攻擊中發揮非常重要的作用。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen113
- SONAR.Ransom!gen82
- SONAR.SuspBeh!gen821
- SONAR.Uacbypass!gen30

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中現有政策已經阻止並檢測到相關的惡意指標。建議最低策略是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 信譽服務中獲得最大收益。

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：

- Ransom.Lockbit
- Ransom.Lockbit!g6
- Scr.Malcode!gen19
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2024/05/07

檔案伺服器軟體CrushFTP存在零時差漏洞：CVE-2024-4040，已在真實網路情境被開採濫用

CVE-2024-1852 是最近被披露的一個注入漏洞，影響檔案伺服器軟體 CrushFTP 10.7.1 和 11.1.0 之前的版本。被成功開採濫用此漏洞會讓未經認證的遠端攻擊者，在受影響的伺服器上跳脫使用者虛擬檔案系統 (Virtual File System，VFS) 範圍，繞過認證、獲取管理權限及可能執行任意遠端程式碼。據報告，該漏洞已在真實網路情境被開採濫用，原廠已發佈該應用程式的修補版本。

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: CrushFTP CVE-2024-4040

2024/05/06

報稅季節必出現的社交工程伎倆：假冒稅務機關網頁傳播VBlogger惡意軟體

一起涉及偽造義大利網域名稱的假冒稅務局網頁的惡意軟體散播行動已被通報。當用戶瀏覽該假冒網站時，會無意中下載一個包含惡意軟體下載器的壓縮檔案，該下載器隨後透過 FTP 到義大利境內最大網路服務站台：Altervista 下載最終的有效酬載。這款名為『vblogger』的惡意軟體是用 VB6 開發，具有鍵盤側錄和剪貼簿擷取功能。收集到的資訊被存儲在文字檔中，用發送到架構在 Altervista 上的指揮與控制伺服器 (C&C)。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1
- ACM.Ps-Net!g1
- ACM.Ps-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper

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。

2024/05/06

免費的最貴又一例～一款針對macOS平台出現的全新惡意軟體：Cuckoo～透過音樂翻錄／轉檔應用程式的下載網站散播

據報導，有一種名為 Cuckoo 的新型 macOS 惡意軟體。該惡意軟體透過一些網站傳播，這些網站提供從串流媒體服務中翻錄／轉檔音樂的應用程式。Cuckoo 擁有廣泛的功能，包括收集瀏覽器儲存的資訊，例如：密碼、cookie 和其他憑證。此外，它還會收集與已安裝的加密貨幣錢包和擴展相關的系統資訊和資料。

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
- 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。

2024/05/06

印度國軍正遭受針對式的安卓平台上的惡意軟體肆虐

據報導，一款新型安卓惡意軟體以社交工程伎倆，透過 WhatsApp (一種智慧型手機的跨平台加密即時通訊應用程式) 進行傳播，將自己偽裝成與國防部相關的 APP，以印度國軍部隊為目標。成功發送後，該 APP 會以聯絡人應用程式 (Contacts) 的名義進行安裝。執行後，該應用程式會請求存取簡訊、通訊錄、儲存和電話的許可權，隨後將自己隱藏。

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.2
- 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。

2024/05/06

偽裝成合法APP圖示的安卓平台的遠端存取木馬(RAT)

一種偽裝成知名安卓平台 APP 圖示的遠端存取木馬 (RAT) 已被偵測到。在誘騙使用者安裝到他們的手機／平板上之後，該惡意軟體會請求管理員憑證。隨後，它會進行資料收集活動，例如：收集電話號碼、搜索已安裝應用程式的詳細資訊、更改設備桌布，甚至根據從命令與控制 (C&C) 伺服器收到的指令向指定號碼發送資訊。

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：

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

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。

2024/05/03

進階持續威脅(APT)攻擊組織：Damselfly，濫用NiceCurl和TameCat自訂後門程式

NiceCurl 和 TameCat 是最近涉入進階持續威脅 (APT) 攻擊組織：Damselfly(又稱 APT42) 網路攻擊行動的兩個自訂後門程式。據報導，這些後門主要是透過魚叉式網路釣魚行動散播，被攻擊團體用於初始存取階段。NiceCurl 是一款基於 VBScript 的惡意軟體，具有下載和執行附加模組的功能，而 TameCat 後門則用於執行 PowerShell 和 C# 腳本以及下載附加的任意內容。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g332

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Mallnk!gen3
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Web.Reputation.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：

- 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。

2024/05/03

TesseractStealer惡意竊密程式濫用OCR引擎擷取資訊

TesseractStealer 是最近由 ViperSoftX 惡意軟體傳播的惡意竊密程式。該惡意軟體濫用 Tesseract(一種開源 OCR 引擎) 從使用者影像檔中擷取文字。該惡意軟體關注的重點在與憑證和加密貨幣錢包資訊相關的特定資料。除 TesseractStealer 外，最近還觀察到一些 ViperSoftX 運行時會注入 QuasarRAT 惡意軟體家族的另一個有效酬載。

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：

自適應防護技術(包含於SESC)：

- CM.Untrst-RunSys!g1
- ACM.Untrst-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.MalTraffic!gen1
- SONAR.SuspBeh!gen6

- SONAR.SuspBeh!gen25
- SONAR.SuspBeh!gen667
- SONAR.SuspLaunch!g13
- SONAR.SuspLaunch!g266
- SONAR.TCP!gen1

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.MBT
- Trojan.Gen.NPE
- Trojan.Malscript
- Web.Reputation.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: Bad Reputation Application Network Activity
- System Infected: Bad Reputation Process Request
- System Infected: Backdoor.Trojan Activity 406
- System Infected: Trojan.Backdoor Activity 568

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。

2024/05/03

最近傳播Darkgate惡意程式的垃圾郵件行動

該攻擊行動的初始感染鏈是從一個帶有 HTML 附件的電子郵件開始。該 HTML 檔使用的背景圖片看起來像一個空白的 Microsoft 文件，在該檔案中可以看到如何修復離線檢視的檔案說明。這是企圖誘騙受害者將惡意 PowerShell 程式碼貼到 Windows 終端機。程式碼執行後，將下載一個 HTA 檔案並繼續執行，最終下載一個後續的 ZIP 檔。解壓縮後，它會啟動 AutoIt 的開源自動化引擎，執行 script.a3x 的惡意 AutoIt 腳本，最終載入 Darkgate 木馬。

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：

自適應防護技術(包含於SESC)：

- ACM.Mshta-Ps!g1
- ACM.Ps-CNPE!g1
- ACM.Ps-CPE!g2
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AONAR.SuspBeh!gen804

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：

- ISB.Downloader!gen48
- ISB.Heuristic!gen106
- Trojan.Darkgate
- WS.Malware.1
- WS.SecurityRisk.4

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

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。

2024/05/03

macOS平台的惡意程式Adload最新變種的新亮點：檢測躲避

SentinelOne 一份報告陳述最近觀察到一種 macOS 平台的惡意程式 Adload 變化。該惡意軟體家族最新變種具有躲避最新蘋果 XProtect 簽章的功能。Adload 惡意軟體出現在 macOS 系統中已有數年時間，已知它是透過瀏覽網頁時的偷渡式下載傳播，通常用於劫持瀏覽器搜索結果、向網頁注入廣告或向受害者發送各種有效酬載。

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：

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
- Trojan Horse
- 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。

2024/04/30

GuLoader惡意軟體下載器，涉入針對俄語系國家的網路攻擊

已觀察到一名威脅者利用不同的社交工程手法發動兩起電子郵件攻擊行動，這些行動都有 Guloader 涉入的跡象。這兩起電子郵件攻擊行動都針對俄語系國家，例如：俄羅斯、白俄羅斯、吉爾吉斯和哈薩克的產業。

在一封電子郵件 (主旨：СПЦ №130 подписанная Belarus) 中，他們冒充一家從事製藥和保健行業的俄羅斯大型公司。該公司有多個業務部門，包括藥品行銷、零售連鎖藥店和醫藥產品製造。攻擊者使用類似銷售的社交工程手法，夾帶一個壓縮附件檔 (СПЦ №130 от 12.04.2024 подпис.7z)，並誘使受害者執行其中偽裝成產品特性摘要的惡意二進位檔案 (СПЦ №130 от 12.04.2024 подпис..exe)。

在分析上述攻擊情境時，賽門鐵克在公開來源中發現另一個惡意壓縮檔 (Доверенность Транзит Хоргос.7z)，其中包含完全相同的 GuLoader 有效酬載。因此，作者似乎也在使用不同的電子郵件方案開展並行活動 (儘管目前還無法獲得該電子郵件)。根據其名稱，威脅者試圖用與霍爾果斯貨物過境相關的法律檔案引誘受害者。霍爾果斯是哈薩克和中國邊境上的一個重要地點，因其作為主要陸港和新絲綢之路經濟帶上的樞紐而聞名，促進中國、中亞和歐洲之間的大量貿易和物流業務。

GuLoader 是一種惡名昭章的惡意軟體下載器，因其經常涉入世界各地的攻擊行動被用於傳播各種惡意軟體而聞名。在本案例中，它正在載入 Agent Tesla 惡意竊密程式，但也可能下載 Remcos 遠端存取木馬。

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)。

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse