保安資訊--本周(台灣時間2022/10/07)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 100 萬受保護端點上總共阻止了1.537億次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2022/10/03)**

- 在**18萬9,700**台端點上，阻止了**7,730**萬次嘗試掃描**Web**服務器的漏洞。
- 在**34萬4,800**台端點上，阻止了**2,580**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬1,300**台**Windows**伺服主機上，阻止了**1,940**萬次攻擊。
- 在**12萬8,400**端點上，阻止了**680**萬次嘗試掃描伺服器漏洞。
- 在**5萬1,400**台端點上，阻止了**290**萬次嘗試掃描在**CMS**漏洞。
- 在**8萬9,700**台端點上，阻止了**320**萬次嘗試利用的應用程式漏洞。
- 在**33萬5,200**台端點上，阻止了**760**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7萬2,000**台端點上，阻止了**280**萬次加密貨幣挖礦攻擊。
- 在**4萬9,300**台端點上，阻止了**520**萬次向惡意軟體**C&C**連線的嘗試。
- 在**5,100**台端點上，阻止了**18萬2,100**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。

2022/10/06

LilithBot--新型態的殭屍電腦(bot)惡意軟體，還內建其他功能

該惡意軟體歸屬於 Eternity 駭客組織，並以惡意軟體即服務 (Malware-as-a-Service) 營運模式來銷售。該惡意軟體不斷推陳出新，也開放自訂功能。它不但可由操作者自行配置與設定，更可以像任何其他殭屍電腦 (bot) 惡意軟體一樣用於下載和執行其他惡意軟體，特別令人膽戰心驚是它新增的內建功能，例如：竊密程式、剪貼簿竊密器和挖礦綁架功能。

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：

- Trojan.Gen.MBT
- 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已於第一時間收錄於不安全分類列表中。

2022/10/06

RatMilad手機行動裝置間諜軟體

RatMilad 是一種針對企業裝置的新型手機行動裝置惡意軟體，最近才在真實網路環境被發現。該惡意軟體具有間諜軟體和遠端存取木馬 (RAT) 功能。根據從攻擊者收到的命令，它可以從受感染設備中收集廣泛的資料，對其進行過濾並執行其他惡意操作，例如：寫入和刪除檔案等。RatMilad 被認為是透過 Telegram 頻道上偽裝成 VPN 應用 App 來進行散播，它依靠社交工程伎倆來說服用戶在他們的行動裝置上側載虛假的 App。

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.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。

2022/10/06

OneDrive中的側載漏洞被用於挖礦綁架行動

根據最近一份報告，在真實網路環境發現一種利用 Microsoft OneDrive 中已知 DLL 側載漏洞的新形挖礦綁架行動有增多的趨勢。攻擊者利用惡意的 secur32.dll 二進位檔案，這些二進位檔案被植入到目標電腦上，然後由合法的 OneDrive 可執行檔載入。根據特定攻擊行動中鑑識分析的檔案，發現的有效籌載是 Lolminer 或 XMRig 挖礦程式。

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：

- Scr.Malcode!gdn32
- SMG.Heur!gen
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B

2022/10/05

MafiaWare666勒索軟體

MafiaWare666 是另一個用 C# 語言撰寫的普通勒索軟體變種。雖然已經有一些網路攻擊行動在散播這種勒索軟體的不同版本，但這種惡意軟體仍然相對簡單，沒有內建任何混淆或反分析技術。一旦用戶的檔案被加密，MafiaWare666 就會在檔案上附加額外的副檔名。該惡意軟體使用的一些已知副檔名包括。.MafiaWare666、.jcrypt、.brutusptCrypt 或 .bmcrypt。投放的勒索與贖金說明會要求向指定的加密錢包位址支付比特幣。

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：

- Ransom.Gen
- Scr.Malcode!gdn14
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/10/05

Doenerium竊密程式

在真實網路環境發現多起散播 Doenerium 竊密程式的網路攻擊行動。該惡意軟體已可透過從特定網站下載取得的偽裝成 Windows 惡意軟體移除工具進行散播。Doenerium 是一支可在 Github 上取得的開放原始碼竊密程式。該惡意軟體的資訊竊取功能針對的是瀏覽器的資料、憑證、剪貼簿資料、加密錢包和 Discord 權杖等。該惡意軟體還可能停用與虛擬化軟體和惡意軟體分析有關的各種程序。

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
- Trojan.Gen.NPE
- WS.Malware.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已於第一時間收錄於不安全分類列表中。

2022/10/04

ChromeLoader在最近針對企業的攻擊行動中，嶄露頭角

最近活動中，我們觀察到 ChromeLoader 惡意軟體工具的使用情況發生變化。至少從 2022 年初開始，該工具就很活躍，主要用於針對一般消費者的憑證竊取。我們的資料顯示，最近的攻擊開始改弦易轍轉且針對企業目標，目的是散播勒索軟體、資料盜竊和造成系統的不穩定。

攻擊者利用各種方法來散播 ChromeLoader。攻擊活動利用惡意廣告、社交媒體網站、破解或盜版軟體以及冒充合法軟體等方法來傳播這種惡意軟體。

ChromeLoader 通常透過下載到受害者機器上的 ISO 檔來安裝。ISO 檔被掛載在被攻擊的系統上，其中的內容負責將惡意的可執行程式傳送到電腦上。

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.Chromesten
- Downloader.Chromst!g1
- Trojan.Chromeloader

- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

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：

- Malicious Site: Malicious Domain Request 21
- Malicious Site: Malicious Domain Request 22
- Web Attack: Malicious Website Request 10
- Web Attack: Malicious Website Request 11

2022/10/03

Discord平台充斥RedLine惡意竊密程式陷阱

RedLine 竊密程式自 2020 年首次被發現以來，其受歡迎的程度持續在緩步上升。這種威脅被多個團體和個人採用，他們不斷透過瀏覽網頁時順道下載 (drive-by-download) 伎倆和發動惡意郵件攻擊行動，是消費者和企業市場遭遇災難之一。在許多情況下，威脅者利用這種惡意軟體從組織中洩漏出敏感性資料，這通常會衍生更嚴重的網路、線上詐騙，機敏資料和快速入侵內部網路的帳密憑證等被賣到地下市場。

最近，有報導稱，有一個惡意組織試圖用含有 PDF 附件的惡意郵件引誘受害者。如果受害者被 PDF 內嵌的鏈結 (URL) 成功引誘，它將下載寄生在 Discord 平台上的 RedLine 二進位檔案。

以下節錄自維基百科：Discord 是一款專為社群設計的免費網路即時通話軟體與數位發行平台，主要針對遊戲玩家、教育人士、朋友及商業人士，使用者之間可以在軟體的聊天頻道透過訊息、圖片 、影片和音訊進行交流。這款軟體可以在 Microsoft Windows、macOS、Android、iOS、Linux和網頁上執行。

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：

- Trojan Horse

2022/10/03

來自中東的DeftTorero駭客威脅組織

DeftTorero 駭客威脅組織 (Lebanese Cedar(*黎巴嫩雪鬆) 或 Volatile Cedar(*揮發性雪松))，據信來自中東，至少自 2015 年以來一直活躍於威脅領域。眾所周知，DeftTorero 發動的進階持續威脅 (APT) 常採用無檔案技術以及常用的攻擊工具。Explosive 遠端存取木馬 (RAT) 也是 DeftTorero 攻擊行動中常見的有效籌載之一，攻擊者在攻擊的初始階段也一直在使用 Caterpillar 和 ASPXSpy webshell。

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(Snoar)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：

- Backdoor.Trojan
- Hacktool
- Hacktool.Ace
- HackTool.LaZagne!gen1
- Hacktool.Mimikatz
- Infostealer!im
- ISB.Downloader!gen210
- ISB.Heuristic!gen23
- ISB.Heuristic!gen27
- NetCat
- SecurityRisk.LaZagne
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於機器學習的防禦技術：

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

2022/10/03

ZINC/Lazarus進階持續威脅(APT)駭客組織利用武器化的開放原始碼軟體

據報導，Zinc 也稱為 Lazarus 進階持續威脅 (APT) 駭客組織在領英 (LinkedIn) 上冒充招聘人員，以引誘鎖定對象來安裝木馬化的開放原始碼安裝套件包。該攻擊行動一直鎖定多個領域的個人和組織，包括媒體、國防和航太以及 IT 服務。威脅者散播的木馬化惡意軟體隱藏在已知的開放原始碼軟體中，例如：PuTTY、KiTTY、TightVNC Viewer 和 Sumatra PDF Reader。已經確定攻擊行動一直在傳播來自 ZetaNile 和 EventHorizon 家族等的惡意軟體。

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.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

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已於第一時間收錄於不安全分類列表中。

2022/10/03

Royal(*皇家)勒索軟體出現變種

在最近針對組織的攻擊中，觀察到一個被稱為 Royal 的全新勒索軟體家族。Royal 背後攻擊者使用「回呼函式」(callback) 網路釣魚攻擊來散播惡意軟體。攻擊者還利用 Cobalt Strike 在後續攻擊階段執行惡意操作。Royal 勒索軟體會將檔案加密後帶有 .royal 副檔名，然後再刪除 README.TXT 檔案，將受害者引導至基於 Tor 的支付網站。據報導，勒索軟體可能會針對虛擬主機並加密其虛擬硬碟檔 (VMDK)。

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(Snoar)的防護：

- SONAR.SuspLaunch!gen4

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Royal
- Trojan Horse
- WS.Malware.2

2022/10/02

RecordBreaker(*破紀錄)惡意程式大流行

Raccoon 2.0，也稱為 RecordBreaker，隨著賽門鐵克觀察到越來越多透過瀏覽網頁時的順道下載 (drive-by-download) 伎倆來作為感染媒介而繼續大流行。在大多數此類型的攻擊行動中，攻擊者將惡意二進位檔案偽裝成破解軟體、偽造的更新和驅動程式安裝檔／前導下載程式。時至今日，它主要影響是消費者，但企業也無法倖免。越來越多的團體和個人正在利用普通的資訊竊密程式從組織中竊取敏感資料。他們採取勒索手段或在地下市場出售竊得的資料和可以入侵企業內部網路的憑證與權限。

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：

- Trojan.Gen.2
- Trojan.Gen.MBT
- Suspicious: Reputation

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/09/30

利用未修補的Microsoft Exchange漏洞的目標式攻擊還是時有耳聞

賽門鐵克獲悉有特定目標式攻擊的報告，這些攻擊是利用 Microsoft Exchange 中未修補漏洞的破口。這些漏洞已被確認歸屬於編號 CVE-2022-41040 偽造伺服器端請求 (SSRF)、CVE-2022-41082 等漏洞。這些被利用來允許經過身份驗證的用戶，以惡意 webshell 的形式來遠端執行程式碼。

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

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: AntSword Scan Attempt

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) 能為最近發現 Microsoft Exchange 漏洞提供最佳的零時差保護。DCS 內建的安全政策，即能阻止任意在有漏洞 Microsoft Exchange 伺服器上的惡意程式植入或進一步執行惡意程式。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2022/09/30

全新的Lazarus進階持續威脅(APT)攻擊行動，現在鎖定：macOS 用戶

本月發現一個新的惡意活動實例，稱為“Operation In(ter)ception”或“Operation Dream Job”。該活動歸因於 Lazarus 進階持續威脅 (APT) 駭客組織。就在上個月，一項類似的行動正在利用加密貨幣交易平台 Coinbase 的職缺誘餌，意圖用惡意軟體感染 macOS 用戶。新的攻擊行動不再與 Coinbase 有所關聯，現在在另一個交易所 Crypto.com 使用吸引人的職缺來當誘餌。Lazarus 傳播的惡意軟體有特別針對 Intel 和 M1 Apple Silicon 架構編譯，但在功能方面差異不大。一旦被執行，惡意軟體將連接到預先定義的 C&C 伺服器並等待來自攻擊者的命令。

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.Nukesped
- 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已於第一時間收錄於不安全分類列表中。