保安資訊--本周(台灣時間2022/09/16)
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1.451億次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2022/09/12)**

- 在**18萬7,600**台端點上，阻止了**6,880萬**次嘗試掃描**Web**服務器的漏洞。
- 在**36萬6,500**台端點上，阻止了**2,780萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬**台**Windows**伺服主機上，阻止了**1,820萬**次攻擊。
- 在**11萬9,500**端點上，阻止了**550萬**次嘗試掃描伺服器漏洞。
- 在**4萬9,200**台端點上，阻止了**250萬**次嘗試掃描在**CMS**漏洞。
- 在**8萬6,700**台端點上，阻止了**280萬**次嘗試利用的應用程式漏洞。
- 在**33萬4,700**台端點上，阻止了**800萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬2,400**台端點上，阻止了**310萬**次加密貨幣挖礦攻擊。
- 在**4萬7,000**台端點上，阻止了**520萬**次向惡意軟體**C&C**連線的嘗試。
- 在**5,900**台端點上，阻止了**15萬5,200**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。

2022/09/15

與 ArkeiStealer 竊密程式有關的活動日益增加

ArkeiStealer 是一種普通的竊密程式，能夠竊取敏感資訊、憑證和加密貨幣錢包。它至少從 2018 年開始出現，其熱門程度多年來一直是時冷時熱。在過去幾週，賽門鐵克觀察到有關活動有所增加，這很可能是由於駭客論壇和網站上發佈破解版本的關係。威脅者主要透過瀏覽網頁時的順道下載 (drive-by-download) 伎倆來作為感染媒介，將惡意二進位檔案偽裝成虛假的軟體安裝程式和更新檔案。

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：

- Trojan.Gen.MBT
- Suspicious: Reputation

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2022/09/15

Gamaredon 進階持續威脅(APT)駭客組織向烏克蘭民眾傳播惡意竊密程式

據報導，一個由 Gamaredon 進階持續威脅 (APT) 駭客組織 (又名 Shuckworm) 發起的新行動，向烏克蘭民眾傳播惡意竊密程式。攻擊者利用惡意郵件中含有惡意 VBS 巨集的 MS Office 檔案。一旦執行，這些巨集就會下載內含 Windows 快捷鍵 .lnk 的 .rar 壓縮檔案。透過執行 PowerShell 腳本，該惡意竊密程式被部署到目標主機上。該惡意軟體有能力從受感染的機器中竊取資料，並傳播額外的任意有效籌載。竊密程式還可以從隨身碟等抽取式儲存裝置預先搜尋特定副檔名的檔案類型以利精準竊取、快速得手。

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：

- CL.Downloader!gen203
- Scr.Malcode!gen
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- W97M.Downloader
- 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: 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。

2022/09/15

Webworm 進階持續威脅(APT)駭客組織的最新活動

賽門鐵克--Symantec 目前是博通--Broadcom 企業安全部門，深入瞭解一個我們稱為Webworm的駭客組織最新活動。該駭客組織已經依特定功能改造了三個問世很久的知名遠端存取木馬 (RAT) 客製化版本，包括 Trochilus、Gh0st RAT 和 9002 RAT。賽門鐵克觀察到的入侵指標 (IOCs) 至少有一個被用於攻擊亞洲多個國家運營的 IT 服務商，而其他指標似乎處於部署前或測試階段。據瞭解，至少自 2017 年以來，Webworm 一直活躍在俄羅斯、喬治亞、蒙古和其他一些亞洲國家的政府機構和 IT 服務、航太和電力行業相關的企業。

在我們的部落格文章中有更多資訊可供參考：間諜攻擊者持續測試和使用依特定功能改造問世很久的知名遠端存取木馬 (RAT) 的客製化版本

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.TCP!gen6

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.B
- Heur.AdvML.C

2022/09/14

威脅日益高漲的 Linux SideWalk 變種後門

據報導，被稱為 SideWalk 的 Linux 模組化變種後門已被 SparklingGoblin 進階持續威脅 (APT) 駭客組織使用。據報導，雖然這種惡意軟體 Linux 變種早在 2021 年針對香港一所大學的行動中被利用，但它最初與 SparklingGoblin 活動沒有關聯，並被命名為 StageClient。該 Linux 變種在惡意軟體架構和 C&C 通信方面都與 Windows 變種有許多相似之處。

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
- Trojan.Gen.NPE
- 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。

2022/09/13

具有隱藏虛擬網路連線 (hVNC) 能力的 Icarus 竊密程式

Icarus 是一支普通的竊密程式（電腦資訊、密碼和加密錢包竊取），具有透過隱藏的虛擬網路連線（hVNC）進行遠端存取的能力--這種技術允許威脅者建立被攻擊機器的隱藏桌面。它最近在各種駭客論壇和網站上做廣告，但也有免費的破解版在散播。賽門鐵克預測，隨著團體和個人購買這個產品或取得破解版的增加，相關活動也會日益增長。

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：

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/09/13

TA505 的 TeslaGun 控制台被用於散播 ServHelper 惡意軟體

據報導，被稱為 TA505 (又名 EvilCorp) 進階持續威脅 (APT) 駭客組織利用一個名為 TeslaGun 全新軟體控制台來操控其被稱為 ServHelper 惡意軟體攻擊行動。TA505 威脅者是一個以獲取金錢利益為動機的駭客組織，幾年來一直為人所知，ServHelper 惡意軟體也被用於該 APT 駭客組織以前的各種攻擊。TeslaGun 控制面板允許攻擊者向選定的目標散播後門惡意軟體，管理從受害者那裡收集的攻擊資料和資訊，並向受感染的主機發送遠端命令。

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：

- Packed.Generic.525
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

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：

- 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。

2022/09/13

與 ShadowPad 有關的進階持續威脅 (APT) 駭客組織發起新一輪的間諜攻擊

原本就與 ShadowPad 遠端存取木馬有關聯的獨特間諜行動組織，採用一個全新、多樣化的工具集，針對某些亞洲國家政府和國有組織發動一系列的持續攻擊。這些攻擊至少從 2021 年初就開始，似乎以收集情報為主要目標。這些攻擊值得注意的特點，是攻擊者利用各式各樣的合法套裝軟體，以使用一種被稱為 DLL 側載技術載入其惡意軟體的有效籌載。

在我們的部落格文章中有更多資訊可供參考：新一波鎖定亞洲政府的間諜攻擊活動

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(Snoar)的防護：

- SONAR.ProcHijack!gen5

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Hacktool.Mimikatz
- Infostealer.Logdatter
- ISB.Heuristic!gen11
- ISB.Heuristic!gen71
- PUA.Gen.6
- 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
- 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。

2022/09/12

Bronze President 進階持續威脅(APT)駭客組織在最新攻擊行動中散播 PlugX 惡意軟體

據報導，與中國有關聯的 Bronze President 進階持續威脅 (APT) 駭客組織，在最近一系列攻擊行動中針對政府官員散播 PlugX 惡意軟體。攻擊者以政治相關主旨為幌子的釣魚郵件來散播該惡意軟體，這些郵件含有嵌入惡意 .lnk 檔案的 .rar 壓縮檔。PlugX 是一個模組化 RAT 變種，早在 2008 年就已經被用於各種惡意攻擊。該惡意軟體被認為是用來收集資訊，由於它的模組化結構，功能可以根據從攻擊者的命令和控制伺服器 (C&C) 收到的指令集而有許多不同功能。

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

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：

- 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。

2022/09/11

觀察到全新 Qakbot 惡意垃圾郵件攻擊行動，惡意 HTML 檔案引爆攻擊鏈

Qakbot 是網路威脅生態中最普遍的金融惡意軟體之一，已經觀察到一個全新的攻擊行動。多年來，Malspam（基本上兼具惡意電子郵件和竊密的行為）繼續被用作感染的初始感染媒介，然而攻擊鏈本身不斷翻新，有時包括新的技術。在這個新的攻擊行動中，惡意垃圾郵件威脅者利用惡意的 HTML 附件（例如：Document[4 random numbers].html和Infos[4 random numbers].html），導引下載一個包含惡意 LNK 檔的密碼保護 ZIP。如果受害者被成功引誘，LNK 將觸發攻擊鏈的其餘部分，包括 CURL 和 WSCRIPT 進而下載 Qakbot。

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：

- ISB.Downloader!gen520
- ISB.Downloader!gen523
- Scr.Mallnk!gen3
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/09/09

StormKitty 竊密程式透過瀏覽網頁時的順道下載 (drive-by-download) 以及惡意垃圾郵件攻擊行動來散播

StormKitty 竊密程式是一種威脅，在一個用於軟體開發和版本控制的知名雲端服務站台，可公開取得其程式碼。這不是一個全新的竊密程式，其熱門程度隨社交媒體、駭客論壇和網站上對討論與關注程度而有所波動。在過去的幾週裡，賽門鐵克看到利用瀏覽網頁時的順道下載 (drive-by-download)（例如：破解軟體和虛假的更新程式）和惡意郵件（SWIFT 跨國匯款系統社交工程攻擊）行動有關的活動略有增加。這種惡意軟體功能說不上有特別的突出，就跟一般的竊密程式大致相同，主要是竊取密碼、discord 權杖和加密錢包。

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：

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!gdn34
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B