保安資訊--本周(台灣時間2022/10/14)
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 98 萬 600 台受保護端點上總共阻止了 1.337億次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2022/10/17)**

- 在**18萬1,400**台端點上，阻止了**6,260**萬次嘗試掃描**Web**服務器的漏洞。
- 在**33萬7,500**台端點上，阻止了**2,460**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬9,800**台**Windows**伺服主機上，阻止了**1,990**萬次攻擊。
- 在**12萬2,400**端點上，阻止了**530**萬次嘗試掃描伺服器漏洞。
- 在**4萬3,500**台端點上，阻止了**220**萬次嘗試掃描在**CMS**漏洞。
- 在**8萬3,000**台端點上，阻止了**260**萬次嘗試利用的應用程式漏洞。
- 在**32萬9,200**台端點上，阻止了**750**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,500**台端點上，阻止了**330**萬次加密貨幣挖礦攻擊。
- 在**5萬400**台端點上，阻止了**510**萬次向惡意軟體**C&C**連線的嘗試。
- 在**5,200**台端點上，阻止了**19萬9,900**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。

2022/10/14

日益增多的活動讓Magniber勒索軟體備受矚目

根據最新的報告，近幾個月來，Magniber勒索軟體的感染率明顯增加。Magniber二進位檔經常以假冒的軟體更新，或利用誤植相似域名的伎倆散播，這些詭計利用使用者不小心輸入錯誤的類似網頁名稱而被騙導引至攻擊者所操控的網頁上。幾個最新的Magniber活動顯示，感染鏈正在不斷變化，採用各種不同的檔案格式，例如：jse、js、msi或wsf。勒索軟體背後的攻擊者似乎也相當定期地提升其規避技術的功能，因為最新的惡意軟體變種具有多重功能，包含在記憶體中執行或繞過Windows中UAC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(Snoar)的防護：

- SONAR.RansomMgnibr!g1
- SONAR.RansomMgnibr!g2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- ISB.Downloader!gen67
- JS.Downloader
- Ransom.Magniber
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.4

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。

2022/10/14

Alchimist攻擊框架被利用來傳播Insekt 遠端存取木馬(RAT)

一個被稱為Alchimist的全新攻擊框架在真實網路世界異軍突起，據說在針對Windows、Linux和MacOS端點的攻擊中都已經有被利用的案例。該框架允許攻擊者自行建立與配置有效籌載，並提供可自訂的感染機制。Alchimist已經被用來傳播Golang撰寫的惡意軟體，即Insekt 遠端存取木馬(RAT)，它擁有遠端存取和shellcode執行功能。除了Insekt，在觀察到的攻擊行動中還散播了一些其他工具，其中包括MacOS特權利用工具、Fscan工具和反向代理。

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：

- Hacktool
- ISB.Downloader!gen48
- JS.Downloader
- OSX.Trojan.Gen
- Trojan Horse
- Trojan.Gen.MBT
- 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。

2022/10/13

全新駭客集團：Water Labbu，所發動的進階持續威脅(APT)活動

一個被稱為Water Labbu的全新駭客集團，在接二連三的針對加密貨幣盜竊的攻擊中被發現。攻擊者一直透過惡意的JavaScript程式碼注入來入侵加密貨幣詐騙網站。據報導，Water Labbu攻擊者還藉助Cobalt Strike stagers來利用已知編號CVE-2021-21220的Chromium的漏洞，利用Electron的應用程式，大肆部署後門。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt!gm1
- Backdoor.Cobalt!gm5
- Backdoor.Rozena
- Meterpreter
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.6
- 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: 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。

2022/10/13

Budworm(*芽蟲)駭客集團恢復了對美國組織的攻擊

最近與Budworm駭客集團有關的活動顯示，他們又開始針對美國的組織了。透過針對美國州的立法機構，這是該駭客集團多年來第一次針對美國的機構。該組織的其他目標包括一個中東政府、一家電子製造商和一家東南亞醫院。

Budworm已被觀察到利用CVE-2021-44228和CVE-2021-45105的Log4j漏洞，以提供有效籌載，通常是一個被稱為HyperBro的惡意軟體家族。該惡意軟體主要是透過DLL側載的方式啟動。Budworm使用的其他有效籌載和工具包括PlugX／Korplug木馬、Cobalt Strike和LaZagne……等等。

在我們的部落格文章中有更多資訊可供參考：Budworm：間諜組織重新將目標對準了美國的機構。

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：

- Backdoor.Korplug
- Hacktool.Fscan
- Hacktool.Iox
- HackTool.LaZagne!gen1
- SecurityRisk.LaZagne
- Spyware.Gen
- Trojan Horse
- Trojan.Dropper
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.3

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: Log4j CVE-2021-45105
- Attack: Log4j2 RCE CVE-2021-44228 2
- Attack: Log4j2 RCE CVE-2021-44228 3
- Attack: Log4j2 RCE CVE-2021-44228 4
- Attack: Log4j2 RCE CVE-2021-44228 5
- Attack: Log4j2 RCE CVE-2021-44228 7

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。

2022/10/12

GlobeImposter勒索軟體重新出現在最近的攻擊行動中

據報導，GlobeImposter是2017年發現的一個舊的勒索軟體變種，在最近一些針對MS-SQL伺服器的攻擊行動中出盡鋒頭。攻擊背後的威脅者似乎是透過已知的漏洞或透過一系列暴力猜解和字典攻擊來入侵低安全性的伺服器。一旦獲得對伺服器的存取權限，就會部署勒索軟體二進位檔案。GlobeImposter可以停用選定的資料庫服務，並在加密受害者的資料之前刪除陰影複製(shadow copies)。

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.SuspBeh!gen54
- SONAR.SuspDrop!gen7

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Cryptolocker
- Ransom.GlobeImposter
- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- 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

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。

2022/10/11

Snake(*蛇形)鍵盤側錄程式有竄升的趨勢

自從2020年首次被發現以來，Snake 鍵盤側錄程式的熱門程度起起伏伏，但它仍然是當今世界上最受歡迎的竊密程式之一。在最近幾周，我們觀察到，隨著團體和個人所發動的惡意的垃圾郵件攻擊行動，Snake 鍵盤側錄程式的流行率略有上升。當涉及到這些活動時，大多數時候都採用了常見的報價、付款、SWIFT匯款和航運等社交工程伎倆，附件的惡意二進位檔案往往被偽裝成PDF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：

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：

- Msil.Packed.20
- Scr.Malcode!gdn30
- Scr.Malcode!gdn34
- Trojan.Gen.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/10/07

針對微軟SQL Server而來的後門程式Maggie

Maggie是一個專門針對MS SQL伺服器的新後門。該惡意軟體將自己偽裝成一個「擴充預存程序（Extended Stored Procedure）」的DLL檔。「擴充預存程序」是透過以動態連結程式庫（DLL）檔案形式編譯的額外功能來擴展SQL伺服器的功能。攻擊者只能透過MS SQL查詢來控制Maggie，以下指令給後門執行具體的行動或執行命令。該後門支援51個指令，包括下載和刪除檔案，執行SOCKS5代理，執行程式，對其他SQL伺服器進行暴力掃描，安裝和執行終端服務與其他許多作業。

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：

- Backdoor.Maggie
- 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

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。