保安資訊--本周(台灣時間2022/09/30)
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1.459億次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2022/09/26)**

- 在**19萬7,200**台端點上，阻止了**6,880**萬次嘗試掃描**Web**服務器的漏洞。
- 在**37萬3,100**台端點上，阻止了**2,710**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬1,900**台**Windows**伺服主機上，阻止了**1,900**萬次攻擊。
- 在**12萬5,300**端點上，阻止了**590**萬次嘗試掃描伺服器漏洞。
- 在**5萬2,000**台端點上，阻止了**250**萬次嘗試掃描在**CMS**漏洞。
- 在**8萬9,700**台端點上，阻止了**290**萬次嘗試利用的應用程式漏洞。
- 在**33萬5,100**台端點上，阻止了**770**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2萬4,100**台端點上，阻止了**330**萬次加密貨幣挖礦攻擊。
- 在**5萬1,700**台端點上，阻止了**540**萬次向惡意軟體**C&C**連線的嘗試。
- 在**5,600**台端點上，阻止了**18萬9,400**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。

2022/09/29

Chaos -- Go 語言設計的 Kaiji 惡意軟體的後繼版本

Chaos 是一種採用 Go 語言設計的的惡意軟體，被認為是舊版 Kaiji 殭屍網路的後繼變種。該惡意軟體支持各種架構，包括 Windows、Linux、ARM、Intel (i386)、MIPS 和 PowerPC。Chaos 惡意軟體的主要散播方法之一是利用已知漏洞。惡意軟體的功能取決於從 C&C 伺服器接收到的命令集，它可能包括擴散到其他目標、DDoS 攻擊或加密貨幣挖礦等惡意行為。

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!gen25

檔案型(基於回應式樣本的病毒定義檔)防護：

- Linux.Kaiji!gen
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

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

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: Zyxel Firewall Unauthenticated Command Injection CVE-2022-30525
- Web Attack: f5 Big-IP iControl Rest RCE CVE-2022-1388
- Web Attack: Huawei Router RCE CVE-2017-17215

基於安全強化政策(適用於使用DCS)：

- DCS 內建的安全政策即能阻止Chaos 惡意軟體的零時差攻擊。
- DCS 能防止從C&C Server或特別的位置，使用FTP、HTTP、P2P等方式下載並安裝相關 Malicious Binary寫入磁碟、建立 cron 作業、建立和啟動服務或任何系統組態列舉嘗試

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。

2022/09/29

Prilex ：銷售點管理系統 (POS) 惡意軟體以新功能強勢回歸

最近觀察到新版本 Prilex 銷售點管理系統 (POS) 惡意軟體。這個新版本的一個關鍵特性是能夠在擷取交易後生成新的 EMV 密碼，這使他們能夠繞過 CHIP 和 PIN 等反欺詐安全措施執行幽靈或回復交易。為了感染 PoS，攻擊者在電話或電子郵件中冒充 PoS 供應商的技術人員，假裝 PoS 需要軟體更新。然後，惡意威脅者會派“技術人員”到現場進行安裝或指導目標安裝 AnyDesk 以進行遠端安裝。

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
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan Horse
- W32.Cambot
- WS.Malware.*

基於機器學習的防禦技術：

- Heur.AdvML.*

2022/09/29

近期多起攻擊行動，大量散播 Cobalt Strike 信標

在真實網路環境發現多起散播 Cobalt Strike 有效酬載的新惡意攻擊行動。攻擊者一直在利用與政府組織的職務描述或職缺敘述相關誘餌主題的網路釣魚附件。散播的惡意檔案附件試圖利用一個相對較舊的 CVE-2017-0199 MS Office RCE 漏洞。如果成功利用，攻擊鏈將繼續透過一系列 VB 和 PowerShell 腳本，直到下載最終的有效酬載。除了 Cobalt Strike 信標之外，Redline Stealer 和 Amadey 二進位惡意檔案也屬於下載的有效酬載。Cobalt Strike 可以幫助攻擊者在後續攻擊中執行惡意操作或散播額外的任意二進位檔案。

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：

- Backdoor.Cobalt
- Backdoor.Cobalt!gm1
- CL.Downloader!gen173
- ISB.Downloader!gen48

- ISB.Downloader!gen63
- Scr.Malcode!gen
- Scr.Malcode.T!ge
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- W97M.Downloader

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：

- Attack: Malicious RTF File CVE-2017-0199
- System Infected: Infostealer.Amadeybot Activity

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。

2022/09/29

Witchetty (*詭計多端) 間諜組織的最新活動狀態

Witchetty 間諜組織（又名 LookFrog）一直在逐步更新其工具集，使用新的惡意軟體攻擊中東和非洲的目標。該組織使用的新工具包括採用隱寫術的後門木馬 (Backdoor.Stegmap)，這是一種罕見的技術，惡意代碼隱藏在圖像中。在 2022 年 2 月至 2022 年 9 月的襲擊中，Witchetty 以兩個中東國家的政府和一個非洲國家的證券交易所為目標。攻擊者利用 ProxyShell（CVE-2021-34473、CVE-2021-34523 和 CVE-2021-31207）和 ProxyLogon（CVE-2021-26855 和 CVE-2021-27065）等漏洞在直接提供公眾服務的伺服器上安裝 Web Shell以竊取憑證、在網路中橫向移動以及在其他電腦系統上安裝惡意軟體。

在我們的部落格文章中有更多資訊可供參考：Witchetty間諜組織在攻擊中東政府時使用更新的工具集。

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.Lookback
- Backdoor.Stegmap

- Hacktool
- Hacktool.Fscan
- Hacktool.Gen
- Hacktool.Mimikatz
- Spyware.Keylogger
- Trojan Horse
- Trojan.Chinchop
- Trojan.Gen.NPE
- 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。

2022/09/28

Roshtyak -- 一種經嚴重混淆的惡意軟體

Roshtyak 屬於 Raspberry Robin 威脅組織的後門有效籌載。該惡意軟體經過大量混淆處理，並採用許多不同的反沙箱和反虛擬機技術。如果惡意軟體檢測到假的有效負載駐留在 VM 或除錯工具環境中，則使用的規避機制之一是丟棄該有效負載。觀察到的虛假有效籌載屬於 BroAssist 廣告軟體系列，其目的是讓研究人員相信所調查的威脅並不那麼有趣。Roshtyak 功能包括對受害者資訊進行滲透外洩以及下載其他任意有效籌載。

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：

- Packed.Generic.553
- 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／IP位址已於第一時間收錄於不安全分類列表中。

2022/09/27

Erbium -- 惡意軟體即服務 (MaaS) 的竊密程式

Erbium 是一種相對較新的竊密程式，以惡意軟體即服務（MaaS）軟體包形式出售。該惡意軟體含有竊取機密用戶資料的功能，包括密碼、信用卡資料、瀏覽器 cookie 和自動化表單填寫資料的內容以及各種加密錢包。收集到的訊息透過內建 API 系統滲出到攻擊者的 C&C 伺服器。Erbium 還可以建立與 Discord 內容遞交網路（CDN）的連接，並下載其他任意有效籌載。在網路上，已經觀察到惡意軟體透過偷渡式下載和各種破解軟體進行散播。

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.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／IP位址已於第一時間收錄於不安全分類列表中。

2022/09/26

Bundlore 沒有停止的跡象

Bundlore 是一個眾所周知的廣告捆綁軟體， 多年來一直影響 Windows 和 MacOS 環境，那段時間，許多變化被曝光。賽門鐵克繼續看到 Bundlore 的活動，因為它沒有顯示出停止的跡象，特別是在 MacOS 環境。它的運作方式在這段時間內沒有改變--它繼續透過惡意廣告的偷渡式下載作為其感染媒介，偽裝成假的更新、破解檔和序號產生程式。

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：

- OSX.Trojan.Gen

2022/09/26

SystemBC 代理機器人，繼續被利用於惡意攻擊行動中

SystemBC (也被稱為 Coroxy) 是一個眾所周知的代理機器人，多年來被各種威脅者利用來下載和執行包括勒索軟體在內的惡意有效籌載。SystemBC 有一個獨特的功能，允許它在受感染的用戶端上建立 SOCKS5 代理，以達到惡意流量加密通道的目的。據瞭解，SystemBC 在地下論壇上被出售，至今仍是一個活躍的威脅。據報導，一些利用這種惡意軟體的最新攻擊行動也將 CobaltStrike 作為其有效籌載。

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：

- Backdoor.Cobalt
- Backdoor.SystemBC
- Backdoor.SystemBC!g1
- Backdoor.SystemBC!g2
- Backdoor.SystemBC!g3
- 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

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 Process Request 4
- 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。

2022/09/26

NullMixer 惡意軟體的植入程式

NullMixer 是一款常被用於散播各種惡意軟體家族有效籌載的植入程式。攻擊鏈通常經由惡意網站散播各種包含惡意軟體植入程式的破解版熱門軟體的安裝程式或熱門軟體金鑰產生器程式。據報導，NullMixer 可以植入包含以下惡意軟體系列的有效籌載：SmokeLoader、RedLine Stealer、PseudoManuscrypt、FormatLoader、ColdStealer。

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：

- MSIL.Downloader!gen6
- Packed.Generic.525

- PUA.Gen.2
- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- W32.XiaobaMiner
- 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：

- 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。

2022/09/25

Harly 為安卓使用者訂閱付費服務

又一個安卓訂閱木馬--被稱為 Harly--最近被揭發。根據報告，它自 2020 年以來一直很活躍，並且在 Google Play 上觀察到多個受感染的安卓應用程式 APP。這種類型威脅並不新鮮，事實上已經困擾安卓用戶許多年，名列前茅是 Joker，而 Harly 行為方式也基本相同。如果受害者被成功欺騙，下載並安裝偽裝成合法應用程式的 Harly 木馬，它將偷偷地為他們做訂閱付費服務。

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
- AppRisk:Generisk

2022/09/23

利用 SocGholish 框架散播 NetSupport 遠端存木馬 (RAT)

根據最新報告，SocGholish 惡意軟體框架已在最近一次散播 NetSupport 遠端存取木馬 (RAT) 的攻擊行動中大顯身手。SocGholish 透過入侵受感染網站來注入惡意 HTML 程式碼以進行社交工程。注入的程式碼會將用戶重導向到偽造的瀏覽器更新頁面，從中下載包含惡意腳本的壓縮檔案，然後在受害者的機器上執行。該攻擊鏈最終導致 NetSupport RAT 有效籌載下載。

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：

- ISB.Downloader!gen542
- Trojan Horse
- WS.Malware.2
- 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。

2022/09/23

最近有流行～Fargo 也稱為 Mallox 的勒索軟體

據報導，Fargo 勒索軟體 (又名 Mallox) 在最近針對 MS-SQL 伺服器的攻擊中被大量散播。一旦寄生在目標伺服器上，勒索軟體將嘗試停用特定程序和服務以繼續進行加密。惡意軟體會在加密檔案中附加一個額外的副檔名。副檔名可能會因惡意軟體版本而略有不同--這包括以下副檔名：.FARGO、.FARGO2、.FARGO3 或 .FARGO4 是最新變種的副檔名。

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：

於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.Cryptlocker!g42
- SONAR.RansomGen!gen4

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Scr.Malcode!gdn14
- Scr.Malcode!gdn30
- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

基於安全強化政策(適用於使用DCS)：

適用於 Microsoft SQL Server 的 DCS 安全強化政策提供零時差攻擊保護，可以抵禦 Fargo 勒索軟體。適用於 Microsoft Windows 和 SQL Server 的進階 DCS 沙箱控制可防止將惡意程式碼散播到伺服器。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2022/09/22

不要掉入陷阱，留意利用 Formbook 惡意程式的人資招聘社交工程攻擊伎倆!

Formbook 不是一種新的惡意軟體，我們經常發布有關其活動的訊息。賽門鐵克的顧客包含多元的不同規模企業、團體與個人，我們得以定期觀察各種規模和目標的攻擊活動。攻擊者繼續將惡意電子郵件作為主要的感染媒介，並在其攻擊鏈中使用許多伎倆。大多數利用常見的報價、SWIFT 匯款和航運等社交工程策略，但我們偶爾也會遇到一個特立獨行。

最近有一個這類型的變種範例，其中一個威脅者試圖透過冒充 IT 經理應徵者來引誘受害者。電子郵件附有一個 ISO 檔案附件檔，內容包含偽裝成個人簡歷的惡意二進制文件檔。人資招聘社交工程伎倆具有強大的誘惑，尤其是在科技行業裁員相當普遍的今天。

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

基於機器學習的防禦技術：

- Heur.AdvML.B