保安資訊--本周(台灣時間2023/11/03)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 62 萬 6,100 台受保護端點上總共阻止了 7,660 萬次攻擊。這些攻擊中有 86.1% 在感染階段前就被有效阻止：**(2023/10/30)**

- 在**11萬700**台端點上，阻止了**3,020**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**19萬400**台端點上，阻止了**1,510**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬2,600**台**Windows**伺服主機上，阻止了**1,490**萬次攻擊。
- 在**6萬5,200**台端點上，阻止了**240**萬次嘗試掃描伺服器漏洞。
- 在**1萬3,300**台端點上，阻止了**110**萬次嘗試掃描在**CMS**漏洞。
- 在**5萬100**台端點上，阻止了**160**萬次嘗試利用的應用程式漏洞。
- 在**23萬6,600**台端點上，阻止了**480**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6,900**台端點上，阻止了**210**萬次加密貨幣挖礦攻擊。
- 在**11萬4,700**台端點上，阻止了**870**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**857**台端點上，阻止了**6萬200**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。

2023/11/02

新版Sayler遠端存取木馬(RAT)

Sayler 遠端存取木馬 (RAT) 已被證實推出新版本。該版的惡意功能強大，包括鍵盤側錄、竊密程式、螢幕截圖／錄影和勒索軟體等等。Sayler RAT 透過垃圾郵件或欺騙性網站來入侵使用者系統，其主要的特色的是授予隱蔽不容易被發現的遠端存取權限，進而神不知鬼不覺地將蒐集到的資訊洩露出去。

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.Maljava

2023/11/02

由DoNot(又名APT-C-35)頑強駭客組織(APT)傳播的智慧型手機上的新型惡意軟體

據觀察，DoNot(又名 APT-C-35) 頑強駭客組織 (APT) 正在傳播一種智慧型手機上的新型惡意軟體。據瞭解，該駭客組織以南亞的政府組織為目標，其最新攻擊行動主要針對印度喀什米爾地區的安卓使用者。這種廣為散布的惡意軟體偽裝成通訊類別的 APP，具有從社交媒體 APP 中收集對話資訊、截圖和拍照以及錄製 VoIP 通話的功能。該惡意軟體也利用 Firebase Cloud Messaging (FCM) 來進行 C&C 通訊。

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。

2023/11/02

Phobos勒索軟體繼續透過濫用RDP服務，攻城掠地

Phobos 是一個較早的勒索軟體家族，早在 2018 年前後首次出現，至今仍在威脅環境中不時出現。據報導，最近觀察到的攻擊行動仍在濫用易受攻擊的遠端桌面協定 (RDP：Remote Desktop Protocol) 連現來傳播這種勒索軟體。Phobos 會加密用戶檔案，並冠上隨機副檔名。勒索 (贖金支付) 說明是以文字檔 (如：『info.txt』或『info.hta』) 的形式提供，建議受害者透過提供的電子郵寄地址聯繫攻擊者，以獲取如何解密鎖定文件的進一步說明。該惡意軟體具有刪除受感染端點上磁卷陰影複製 (volume shadow copies) 的功能。

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(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspDataRun

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Phobos
- Ransom.Phobos!gm1

基於機器學習的防禦技術：

- 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：

- Attack: Ransom.Crysis Activity 3

2023/11/02

BlackHatUP勒索軟體

BlackHatUP 是最近在網路威脅環境中發現的另一個 Chaos 勒索軟體新變種。該惡意軟體會加密使用者檔案，並冠上 .BlackHatUP 副檔名。勒索 (贖金支付) 說明會以檔名為『read_it.txt』的文字檔格式來提供，威脅者要求受害者透過電報與他們聯繫，以獲得如何解鎖檔案的進一步說明。BlackHatUP 具有刪除受感染電腦上的磁卷陰影複製 (volume shadow copies) 和備份索引 (backup catalogs) 的功能。

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(SONAR)的防護：

- SONAR.SuspDrop!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2023/11/01

戲劇性的宣傳，Mint(*薄荷)Stealer惡意竊密程式，讓人眼睛為之一亮

最近幾個星期，一名駭客在網站、Telegram 和論壇上積極宣傳一款名為 Mint Stealer 的惡意竊密程式。然而，在論壇上卻發生一些戲劇性的事情，因為據稱原作者貼文表示，有人試圖把自己裝扮成 Mint Stealer 的賣家來騙人。至於這究竟是一場騙局，還是真的有人取得他們的原始碼，目前還無法證實。

雖然廣告上說它比許多竊取程式要強得多，但其實都是一些個很常見的功能，賽門鐵克也見過 Python 和 JS 版本。下面是它的一些竊取功能：

- 電腦資訊
- 各種遊戲 APP 連線 (session)
- Discord 和 Telegram 權杖／連線 (session)
- Metamask 救援密碼 (Recovery Key) 和其他任何已知的加密貨幣冷錢包。
- 網頁瀏覽器密碼、cookies、自動填寫 (autofills) 機制的帳密等、歷史記錄和信用卡。

被盜資料先被壓縮並上傳到其命令與控制 (C&C) 伺服器，然後 Mint Stealer 會刪除該壓縮檔。

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：

- AGR.Terminate!g2
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/11/01

假冒巴拉圭政府機構的Formbook惡意電子郵件攻擊行動

假冒政府機構和知名企業的電子郵件攻擊行動屢見不鮮，在某些情況下，這可能是一種精心打造的社交工程伎倆。在最近一個案例中，賽門鐵克發現一個夾帶惡名昭彰的 Formbook 惡意程式網路壞蛋，假冒巴拉圭政府環境與永續發展部 (MADES) 發送的電子郵件。這些電子郵件 (主旨：Statement sept 22 ocean ltd) 包含一個惡意 .RAR 壓縮檔 (Statement20233010.rar)，內含中的 Formbook 二進位檔案偽裝成一份虛假聲明 (Statement20233010.exe)。該行動似乎不針對特定國家或行業，但已在多個國家觀察到，包括英國、美國、香港、越南、比利時、丹麥、日本、南非、澳大利亞等。

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!gdn32
- Scr.Malcode!gdn14

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/11/01

Ghostpulse(*幽靈脈衝)惡意軟體載入器

根據報導，一個全新網路攻擊行動利用虛假的 MSIX Windows APP 封裝格式檔傳播一種名為 Ghostpulse 新型惡意軟體載入器。幕後的威脅分子一直在使用惡意廣告和購買搜尋引擎排名 (SEO) 的手法，引誘用戶下載谷歌 Chrome、微軟 Edge 和 Brave 等主流網路瀏覽器的免費安裝程式。Ghostpulse 採用一種稱為 process doppelgänging (*程序二重化) 技術來呼叫各種類型的惡意軟體，包括 SectopRAT、Rhadamanthys、Vidar、Lumma 和 NetSupport RAT。

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：

- JS.Malscript!gen3
- Trojan.Gen.NPE
- Web.Reputation.1
- 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。

2023/11/01

駭客組織：Arid Viper(*乾旱毒蛇)將安卓平台手機惡意軟體偽裝成約會交友類別的APP

根據觀察，頑強的駭客組織：Arid Viper 在最近的一次攻擊行動中將其定制的行動手機惡意軟體偽裝成約會交友類別的 APP 更新檔。這些惡意軟體以 .APK 封裝格式檔包裝，一旦進入遭感染的裝置，就會被用來竊取裝置資訊、使用者資料、通話記錄、簡訊內容、憑證和其他機密資訊，還可能部署其他惡意有效籌載。一個名為『Skipped_Messenger』惡意套裝軟體被指稱為一款名為『Skipped』約會 APP，它利用谷歌 Firebase 系統作為攻擊者的命令和控制 (C&C) 管道。

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.1
- 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。

2023/11/01

駭客集團：Scarred Manticore利用LIONTAIL惡意軟體框架

在真實網路情境觀察到一個駭客集團：Scarred Manticore 所發起全新網路攻擊行動。攻擊者利用一個名為 LIONTAIL 惡意軟體框架來攻擊中東地區的金融、政府和電信等各個領域。LIONTAIL 由一組 shellcode 惡意程式載入器和有效籌載所組成，其中包括一個基於 C 語言的後門，允許通過 HTTP 執行遠端命令。據瞭解，Scarred Manticore 駭客集團還在其攻擊中使用大量自訂的 Web shell、DLL 後門和植入程式。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Hacktool.Ace
- Hacktool.Proxy.A
- Hacktool.Rootkit
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

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
- Heur.AdvML.C

2023/11/01

紛至沓來～假冒Nedbank銀行的網路釣魚行動在南非猶如打不死的蟑螂

針對大型銀行使用者（包括個人零售客戶和企業）的網路釣魚行動並不少見。但在過去的幾個星期裡，賽門鐵克發現一種相當頑固的惡意電子郵件攻擊行動，網路壞蛋偽裝成南非一家非常知名的銀行，也是南非最大的金融機構之一，不斷試圖竊取南非 Nedbank 用戶的憑證／帳密。這些惡意電子郵件的主旨為『Nedbank 信用卡每月費用電子結算單』，並包含一個惡意 HTML 檔（NedBank Statement.html），可導引到釣魚網頁。如果用戶被誘騙並輸入他們的憑據／帳密，該憑據將被收集並轉發到壞蛋所操控的網域。

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)。

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。

2023/10/31

Chaos勒索軟體新變種宣稱握有被害人非法證據的詭計威脅受害者乖乖就範

賽門鐵克最近觀察到一個 Chaos 勒索軟體的新變種，這個版本的變種以單機電腦為目標，雖然也是採用雙重勒索伎倆，但又與近來常見的手法不太一樣。除了加密檔案之外，勒索軟體還更改電腦的桌面背景圖案並帶有聯邦調查局 (FBI) 的標誌，指出在使用者的電腦上發現露骨和非法的兒童內容。根據勒索贖金支付說明文件，他們要求價值 1000 美元的比特幣來解密檔案件。為了增加額外的壓力，如果受害者不遵守，攻擊者威脅將他們聲稱收集的所有非法內容轉交給聯邦調查局。

雖然這是一種較罕見的手法，但它並不全然是新的，實際上是一種早期恐嚇勒索病毒的社交工程伎倆。不幸的是，某些勒索軟體攻擊者採用這種令人厭惡的手段來向受害者施壓。這種做法利用面臨法律後果和聲譽可能受到損害的恐懼，顯然是為了造成額外的痛苦甚至恐慌，希望能讓受害人更有可能乖乖就範。

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.SuspDrop!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/10/31

Akira竊密惡意程式

Akira 勒索軟體讓人印象最深的是對 Linux 平台的危害，但根據最近報告，居然也有一個名為 Akira 的竊密惡意程式正在廣為吹捧與散播，無論是用於測試還是實際的惡意活動。這是一個普通的竊密惡意程式 (用 Python 編寫)，能夠從基於 Chromium 得瀏覽器竊取 PC 資料、加密錢包、2FA 擴充功能轉儲、登入憑證、cookie、信用卡和自動填表資訊。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan.Gen.MBT

2023/10/31

防護亮點：DarkGate惡意程式已轉向濫用PDF附件檔

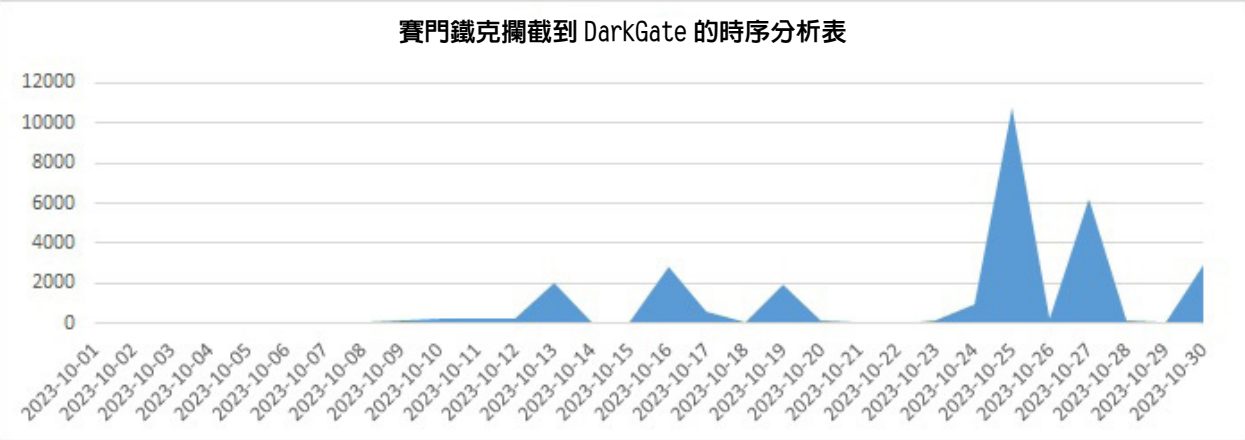
我們在今年 8 月發布了有關 DarkGate 惡意程式的最新資訊，這是一種基於 Windows 的惡意軟體，具有廣泛的功能，兼具竊密惡意程式和遠端存取木馬的功能，透過惡意廣告和購買搜尋引擎廣告排名 (SEO) 進行傳播，上個月被稱為 TA577 的駭客組織，同時也是前 Qakbot 的聯盟夥伴公司被發現透過其惡意電子郵件行動傳播 DarkGate，深入拆解其攻擊鏈發現其是複雜精密的工具與手法的組合。

最近，DarkGate 已轉向濫用 PDF 附件檔。在某些情況下，檔案名稱僅包含一兩個字母長度，以及在檔案內容中掃描的惡意連結。在這些情況下，該連結會下載一個 ZIP 壓縮檔，其內容包含惡意 VBS 或 MSI 檔案，第二階段的有效籌載是包含實際 DarkGate 惡意軟體程式碼的 AutoIT 腳本。

也觀察到第三種與 PDF 相關的感染事件。透過這些附加的 PDF 檔案內 (大多數檔名較長) 的連結會下載一個網頁 (URL) 捷徑，該捷徑連接到攻擊者控制的 WebDav 伺服器，以便執行惡意 VBS、JS 或 MSI 檔案。

- PDF > URL > .URL 捷徑 > MSI/JS/VBS > AutoIT > DarkGate

我們的情資大數據遙測系統報告，這項最新攻擊行動於 10 月 13 日正式開始，並在 10 月 25 日出現高峰，隨後在 10 月 27 日出現較少的回報。



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 多重防護技術能在第一時間就偵測到該惡意程式及有效對應**零時差**攻擊的防護機制及其威脅名稱：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.DLHeur!gen1
- Scr.DLHeur!gen6
- Scr.DLHeur!gen7
- Trojan.DLHeur!gen5

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)。

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。

欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲深入瞭解有關賽門鐵克基於雲的網絡安全服務 (WebPulse) 的更多訊息，請點擊此處。

2023/10/31

刀不留人～Knight (*騎士)勒索軟體

最近發布的一份報告詳細介紹與 Knight 勒索軟體相關的一些活動。該勒索軟體集團主要鎖定美國並在多個行業傳出災情。報導指出，雖然零售業的相關活動最多，但該駭客集團並不迴避攻擊醫療保健產業內的實體，可能對需要醫療照護的病患產生嚴重衝擊。

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：

- AGR.Terminate!g2

- SONAR.RansomGen!gen3
- SONAR.Ransomware!g1
- SONAR.Ransomware!g38
- SONAR.Ransomware!g7
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Knight
- Trojan Horse
- Trojan.Gen.MBT
- W32.Silly!gen
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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：

- Attack: Ransom.Gen Activity 29
- 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。

2023/10/31

BiBi-Linux資料刪除惡意軟體

BiBi-Linux 是一種新發現的 Linux 平台上的資料刪除惡意軟體。該惡意軟體出現在最近針對以色列企業的攻擊中。BiBi-Linux 用無用的資料覆蓋目標檔案以破壞它們。它將透過附加包含名稱『BiBi』的隨機字串來重新命名被刪除過的檔案。該惡意軟體不會滲出任何檔案，不會留下任何勒索資訊或留下任何有關如何聯繫攻擊者的說明。如果惡意軟體在沒有指定任何目標資料夾的情況下執行，它將從根目錄啟動，從而有效地使受感染的作業系統無法使用。

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：

- Trojan Horse
- WS.Malware.1

2023/10/31

Hunters International(*獵人國際)勒索軟體

一種名為「Hunters International」的全新勒索軟體已經在真實網路上流竄。該惡意軟體被認為是源於惡名昭彰的 Hive 勒索軟體的程式碼，因為它與該惡意軟體家族有許多相似之處。該惡意軟體會加密使用者檔案並冠上 .LOCKED 副檔名。勒索贖金支付等說明資訊檔案會存放在磁碟機上每個加密目錄中的「Contact Us.txt」檔案。該勒索軟體背後的威脅者還建立一個公開洩密網站，他們在該網站上公開了攻擊的受害者。

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
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2023/10/31

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 1.837 萬個受保護端點上阻止了總計 730 萬次攻擊。

- 使用網頁信譽情資，在 1.635 萬個端點上阻止了 620 萬次攻擊。
- 攔截了 37.2K 個端點上的 769.2K 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 16.1K 個端點上攔截了 197.5K 次瀏覽器通知詐騙攻擊。
- 在 813 個端點上攔截了 74.2K 次攻擊，這些攻擊利用了被入侵操控的網站上的惡意腳本注入。
- 在 2.1K 個端點上阻止了 3.7K 次技術支援詐騙攻擊。
- 在 280 個端點上阻止了 985 次加密劫持嘗試。

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。

2023/10/31

Hook(*掛鉤)安卓手機惡意程式災情不斷

該 Android 惡意軟體首次出現於 2023 年初，並在各種地下論壇上積極銷售。在過去的幾個月裡，零星出現這種具有遠端存取木馬 (RAT) 戰力的銀行惡意軟體偽裝成 APP。在最近一個案例中，一名攻擊者將他的惡意二進位檔案偽裝成娛樂類別的 APP，希望吸引土耳其手機用戶。該惡意 APP 透過 Discord 進行傳播，最有可能利用瀏覽網頁時的順道下載的社交工程伎倆。Hook 具有典型的覆疊 (overlay) 技術對網路金融更是具有殺傷力。

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。

- AppRisk:Generisk

2023/10/30

Chaos勒索軟體偽裝成《要塞英雄--Fortnite》線上遊戲安裝檔

眾所周知，《要塞英雄--Fortnite》是一款非常受歡迎的線上遊戲，全世界有很多人都在玩。不幸的是，不懷好意的人也意識到這一點，可悲的是，這種成功往往會招來惡意。在最近一個案例中，一個名為「LRD KMG」的勒索軟體攻擊者透過將其 Chaos 勒索軟體偽裝成 Fortnite 安裝程式來瞄準法國遊戲玩家。受害者會發現他們的檔案被加密，並收到一封簡短的勒索信，要脅他們支付價值 1000 歐元的比特幣來解鎖他們的檔案。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDrop!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/10/30

簡訊釣魚攻擊行動鎖定Costco會員系統

賽門鐵克最近觀察到，攻擊者試圖透過惡意簡訊服務 (SMS) 竊取 Costco 會員登入資訊。該伎倆涉及以金回饋的承諾來吸引用戶，目的在引誘他們連線到網路釣魚網站。

Costco 是一家會員制零售巨頭，以其倉庫式商店而聞名，業務遍及全球多個國家。

觀察到的惡意簡訊內容：

- COSTCO 您的會員年度現金回饋已結算完成，現在總共可以領取 58.88 美元。請參閱：CostcomemberLogin [.] com

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。

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。

2023/10/30

Higaisa ATP駭客組織，引誘受害者從品牌盜用網站下載惡意程式

名為「Higaisa」的進階持續性威脅 (Advanced Persistent Threat，APT) 駭客組織被證實發起一項新行動，誘使受害者造訪假冒 OpenVPN 的欺騙性網站。該假冒網站名為『open-vpn [.] 頂級域名』，專為中國用戶量身定制，目的是傳播惡意軟體。該威脅發動者發動品牌盜用的網路釣魚行動來吸引經常使用 VPN 接收者放下戒心不加思索網站的真偽，進而順利誘騙用戶使用欺詐性 OpenVPN 網站。該假冒網站可下載惡意的 OpenVPN 安裝程式檔案，該檔案一旦執行，就會在系統上運行基於 Rust 的惡意軟體，隨後觸發後續 shellcode 和 C&C 通訊。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan horse

基於機器學習的防禦技術：

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

2023/10/30

Remcos惡意木馬攻擊行動～冒名波蘭空調工程公司和匈牙利油漆和五金連鎖超市

Remcos 是名聲響亮的老牌遠端存取木馬 (RAT)，並且在全球範圍內不斷被發現，被多個駭客集團和個人戶所濫用。在最近的一個案例中，一名攻擊者目前正在瞄準歐洲公司，重點是波蘭和匈牙利，冒充知名的波蘭空調工程公司和另一家匈牙利油漆和五金連鎖超市。惡意電子郵件包含一個 Word 文件檔（UPIT.doc 或 Zapytanie ofertowe.doc），其精心製作成具有開採利用已知漏洞 (CVE-2017-11882) 的能力，如果執行，就可以取得該文件擋進而植入 Remcos。

觀察電子郵件主旨如下：

- Upit za ponudom 531996790090
- Prośba o ofertę N° 48723

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：

- Exp.CVE-2017-11882!g5
- Scr.Malcode!gdn34

2023/10/29

Poverty(*窮人)竊密程式～加密貨幣錢包被竊真的會變窮

Poverty(*窮人) 竊密程式最近嶄露頭角的另一個竊密程式。它透過惡意電子郵件和偷渡式下載傳播，後者是最受歡迎的感染媒介。這是一個普通的竊密程式，因為它不包含任何使它與其他更活躍的竊密程式相比脫穎而出的特色。它的功能包括：

- 收集系統資訊(作業系統、顯卡、硬體識別碼以及CPU、系統和鍵盤配置、顯示設定）
- 從 %APPDATA%、%LOCALAPPDATA% 和 %DESKTOP% 擷取檔案
- 竊取加密貨幣錢包、Telegram 對話、雙因素身份驗證 (2FA) 認證碼、cookie 等
- 螢幕截圖

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：

- AGR.Terminate!g5

- SONAR.Trafic2.RGC!g10

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/10/29

打不死的蟑螂～Android簡訊詐騙／收費詐騙惡意程式(Joker)

時隔多年，隨著 Google Play 上不斷檢驗 APP 的安全性，Android 簡訊詐騙／收費詐騙惡意程式 (Joker) 仍然沒有任何停止的跡象。Joker 惡意程式偽裝成應用程式商店中的正版 APP (操作方式也一樣)，一旦下載並安裝到使用者裝置上，就可以參與各種惡意活動。這些活動包括向付費號碼發送簡訊、未經用戶同意為用戶註冊付費服務以及竊取敏感資訊。

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。

- AppRisk:Generisk

2023/10/27

Jarjets勒索軟體～還是用加密後的副檔名來命名

Jarjets 是上週浮上檯面的另一個全新的勒索軟體。該惡意軟體會對使用者檔案進行加密，並冠上 .Jarjets 的副檔名。勒索贖金支付說明以名為「Jarjets_ReadMe.txt」文字檔存放在受感染的電腦上，內文要求受害者透過所提供的電子郵件地址與他們聯繫，以獲取如何解密檔案的進一步說明。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Generic.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/10/27

TA558駭客集團近期針對拉丁美洲的進階持續性威脅(APT)攻擊

眾所周知，TA558 駭客集團目標就是鎖定拉丁美洲的各個產業。在最近攻擊行動中，這些威脅者一直在利用帶有惡意附件的垃圾郵件來傳遞各種有效籌載，例如：AsyncRAT、NjRAT、Vjw0rm 或 RevengeRAT 等。據觀察，TA558 自 2017 年以來不斷利用年代久遠的微軟 MS Office 的預設工具，可於文件中插入及編輯方程式的 Equation Editor 漏洞（CVE-2017-8570、CVE-2017-11882），可能主要針對舊版或未修補的系統。

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：

- Exp.CVE-2017-8570!g*
- Exp.CVE-2017-11882!g*
- Scr.Malcode!gen
- Scr.Malcode!gen59
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Trojan.Malscript
- Web.Reputation.1
- WS.Malware.1

*這表示存在多個類似名稱的檢測，例如：Exp.CVE-2017-11882!g2、Exp.CVE-2017-11882!g3等。

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。

2023/10/27

最新的Xorist勒索軟體家族變種

Xorist 勒索軟體 (又稱 EnCiPhErEd) 是一個老牌惡意軟體家族。儘管它相對較老，但它在駭客威脅圈仍然相當活躍，每個月我們都會觀察到新的變種在真實網路情境流竄。Xorist 主要透過破解軟體的安裝程式、偷渡式下載或惡意垃圾郵件行動來傳播。該惡意軟體的最新版本會加密使用者檔案並將其冠上 .hjutm 或 .th 副檔名。勒索贖金支付說明是以 .txt 檔案的形式提供，但也以彈跳視窗的形式向受害者顯示。

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.CryptoTorLocker
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/10/26

逃竄在阿拉伯半島的BatCloak的惡意程式--自稱來自沙迦酋長國(Emirate of Sharjah)的網路攻擊行動

賽門鐵克最近觀察到另一起針對阿拉伯半島各產業 (本地公司和跨國企業) 和政府機構的 BatCloak 惡意程式的網路攻擊行動。這次攻擊背後的攻擊者把自己塑造成沙迦大學，並採用社交工程技倆。如果使用者成功被電子郵件 (主旨：GOVT OF SHARJAH - UNIVERSITY OF SHARJAH - QUOTATION View) 引誘並開啟惡意壓縮檔（UNIVERSITY OF SHARJAH_Project.rar），他們會發現偽裝成的 BatCloak 二進位檔案 (UNIVERSITY OF SHARJAH_Project.bat) 的專案報價。

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)。

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen82

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.C