保安資訊--本周(台灣時間2022/08/19)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 95 萬 3,400 個受保護端點上總共阻止了1.552億次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2022/08/14)**

- 在**19萬4,200**台端點上，阻止了**7,290**萬次嘗試掃描**Web**服務器的漏洞。
- 在**35萬4,000**台端點上，阻止了**3,160**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬3,300**台**Windows**伺服主機上，阻止了**1,850**萬次攻擊。
- 在**14萬1,800**端點上，阻止了**710**萬次嘗試掃描伺服器漏洞。
- 在**6萬3,900**台端點上，阻止了**300**萬次嘗試掃描在**CMS**漏洞。
- 在**10萬1,700**台端點上，阻止了**310**萬次嘗試利用的應用程式漏洞。
- 在**29萬9,400**台端點上，阻止了**680**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5萬3,000**台端點上，阻止了**370**萬次加密貨幣挖礦攻擊。
- 在**36萬7,000**台端點上，阻止了**540**萬次向惡意軟體**C&C**連線的嘗試。
- 在**5,800**台端點上，阻止了**18萬4,700**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。

2022/08/19

Lazarus APT 用 macOS 惡意軟體瞄準求職者

本月期間，觀察到了歸咎於惡名昭彰的 Lazarus APT 集團的一個新的惡意活動實例。攻擊者再次利用 .pdf 檔案為誘餌，偽裝成知名公司的求職職缺。最近觀察到的一個例子是聲稱來自 Coinbase 的虛假職缺。由 Lazarus 散佈的惡意軟體已被編譯為同時支援 Intel 和 Apple 晶片架構，但在功能上非常相似。一旦執行，惡意軟體將連接到預先設定好的 C&C 伺服器，並等待接收威脅者的命令。

這個最新的攻擊行動與 Lazarus APT 集團的過往行動相似，這些行動也涉及虛假的求職職缺，並且可以與一個被稱為 "Dream Job *夢想工作" 行動有更多的關聯性。有關這一行動的更多資訊，請參閱我們早先的部落格文章：北韓駭客組織 Lazarus，針對化工行業進行間諜活動

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Nukesped
- OSX.Trojan.Gen
- Trojan Horse
- Trojan.Gen.MBT
- 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。

2022/08/18

新型 MasterFred 變種透過 Gymdropper 植入程式來安裝 Xenomorph 網路銀行木馬

MasterFred（又名Brox）是一個新變種的惡意程式，歸咎於被稱為 Hadoken Security 的威脅者，是最近在 Google Play 商店已經上架的應用程式 (App)。這個惡意應用程式使用 Gymdrop 植入程式來下載安卓平台上的 Xenomorph 銀行木馬，以感染受害者的設備。這個新的變種是一個惡意的植入程式，而不是可直接執行的木馬。植入程式通常被用來繞過 Google Play 商店實施的安全檢查機制，用於示警惡意或流氓應用程式。

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：

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
- AppRisk:Generisk

2022/08/17

假冒為知名加密貨幣交易機器人的惡意軟體不斷增加

加密貨幣交易機器人並非新鮮事，但在社交媒體上被有影響力的人不斷地宣傳後，越來越受歡迎了。大致說來，這些機器人是根據預定的規則自動執行特定交易的程式。有許多像 CryptoHopper 這樣的公司提供交易機器人服務，可以連上不同的經紀商。由於這些機器人被吹捧為不需要金融技能就能賺錢，許多加密貨幣愛好者都會嘗試一下，有些人最終會從不可靠的來源下載這些機器人。網路犯罪分子注意到這一趨勢，賽門鐵克看到越來越多的虛假加密貨幣交易機器人透過社交媒體、論壇、虛假網站和網路語音平臺（如Discord）傳遞。在過去的幾個月裡，這種社交工程手法被用來傳遞竊密程式、遠端存取特洛伊木馬和加密貨幣剪貼簿竊密器（Clipper）等威脅。最近，賽門鐵克觀察到一個經由瀏覽網頁時發動的順道下載攻擊行動來下載 RedLine 竊密程式，就是偽裝成已被破解的 CryptoHopper 加密貨幣交易機器人。

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 Horse

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。

2022/08/17

在傳遞各種遠端存取木馬 (RAT) 的攻擊行動都有 DarkTortilla 惡意軟體的痕跡

DarkTortilla 是一個基於 .NET 的惡意加密程式，自 2015 年以來在各種攻擊行動中被濫用。它已被用來提供各種惡意軟體的有效籌載，例如：AgentTesla、 AsyncRAT、 NanoCore 或 Redline 竊密程式。該惡意軟體主要是透過含有各種格式檔案（包括 .iso、.zip、.img 等）的惡意郵件攻擊行動來傳播。DarkTortilla 由運行最終有效籌載所需的兩個獨立元件組成--基於 .NET 的載入程式可執行檔和一個 DLL 核心處理器模組。DarkTortilla 的功能是確保目的機器上的持續性，進行反沙箱和反虛擬機器檢查，並交付和執行附加的有效籌載包。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Packed.Generic.619
- Trojan Horse
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/08/16

Typhon竊密程式透過釣魚網站傳播

Typhon 竊密程式惡意軟體的變種已被發現，由一個冒充 Lindesbergs Kommun（瑞典的一個市鎮）釣魚網站傳播。該惡意軟體透過一個執行惡意 PowerShell命令 的 .lnk 檔傳遞，並從攻擊者伺服器下載 Typhon 竊密程式的有效籌載。該惡意軟體一旦執行，就會試圖收集和外送各種機密資料，如社會安全碼、用戶憑證、銀行資訊、cookies、一鍵自動填入的資料、VPN 憑證和加密錢包等。收集到的資料被轉移到由攻擊者控制 Telegram 頻道或是匿名的 AnonFiles 檔案代管服務。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan.Gen.MBT
- 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。

2022/08/15

LogoKit：網路釣魚攻擊行動

每天都有無數的網路釣魚刺探，多由各種網路釣魚工具包所產生。最近，有一個工具包隨著它的熱門程度而聲名大噪，它利用開放的重定向漏洞，意圖躲避惡意郵件的檢測機制。開放式重定向漏洞允許遠端攻擊者將用戶重定向到任意網站，並透過帶有適當功能參數的 URL 進行網路釣魚攻擊。它被稱為 LogoKit，主要用於對大型的、熱門服務的憑證，如 Office 365、GoDaddy 和各種網路銀行的釣魚。

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。

2022/08/15

Zeppelin 勒索軟體在真實網路環境到處亂竄

賽門鐵克安全機制應變中心團隊瞭解到最近美國國土安全部網路安全暨基礎設施安全局 (CISA) 和聯邦調查局 (FBI) 觀察到的一些針對Zeppelin勒索軟體活動的警報。Zeppelin 是一個源自Buran勒索軟體的變種，在地下論壇以勒索軟體即服務（RaaS）的商業模式進行銷售。根據發佈的報告，在某些案例中，威脅者在目標網路中多次執行該勒索軟體，導致受害者需要獲得幾個不同的解密金鑰。眾所周知，Zeppelin勒索軟體背後的攻擊者還採用了先竊取機敏資料，勒索不成會公開機敏資料的雙重勒索手法。

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：

- AGR.Terminate!g2
- SONAR.SuspBeh!gen25
- SONAR.SuspDrop!gen1
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g193

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Buran
- Ransom.LetsGo
- Ransom.Zeppelin!g1
- 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：

- 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。

2022/08/15

最近針對烏克蘭的Shuckworm 攻擊行動中部署了竊密程式

博通 (Broadcom) 軟體事業部的企業安全部門--賽門鐵克觀察到針對烏克蘭的 Shuckworm 活動，似乎正在向目標網路散佈竊密惡意軟體。這項活動最近於 2022 年 8 月 8 日還持續進行中，在該行動中觀察到的大部分行為與 CERT-UA 在 7 月 26 日強調的活動一致。Shuckworm（又名 Gamaredon、Armageddon）是一個與俄羅斯有關聯的駭客組織，自 2014 年首次出現以來，它的行動幾乎完全集中在烏克蘭。一般認為是有政府資助的間諜行動。

在我們的部落格文章中有更多資訊可供參考：Shuckworm：與俄羅斯有關聯的駭客集團持續針對烏克蘭組織攻擊

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(Snoar)的防護：

- SONAR.SuspBeh!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Ratenjay
- SMG.Heur!gen
- Trojan Horse
- Trojan.Gamaredon
- Trojan.Gen.MBT
- 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／IP位址已於第一時間收錄於不安全分類列表中。

2022/08/15

SOVA：安卓行動平台上的銀行木馬

早在 2021 年 9 月，SOVA 背後的威脅者宣稱，該軟體仍處於開發階段。現在，隨著一個較新的版本被偽裝成帶有如 Chrome、亞馬遜和 NFT 的標誌的的安卓應用程式。威脅者捲土重來，主要針對銀行應用程式和加密貨幣交易所／錢包。

在當前版本中觀察到的一些改進。

- 重構並改進了cookie 竊取機制
- 允許惡意軟體透過攔截和迴避受害者試圖卸載應用程式來保護自己
- 攻擊者可以透過命令和控制（C&C）介面控制特定目標
- 允許攻擊者進行螢幕截圖，並記錄和執行命令
- VNC 的遠端連線能力

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

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

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。

2022/08/14

可同時針對Windows、Linux和macOS用戶的 "MiMi "的木馬化跨平臺通訊軟體

Lucky Mouse（又稱APT27、Bronze Union、Emissary Panda和Iron Tiger）是一個自 2013 年以來活躍的中國駭客組織，最近被發現發動新一波的攻擊行動，利用一個名為 "MiMi" 的木馬化的跨平臺通訊軟體，提供一個被稱為 "rshell" 的後門樣本。被下毒的通訊軟體將下載並安裝用於 Windows 作業系統的 HyperBro 樣本和用於 Linux 和 macOS 的 rshell 物件。

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
- Trojan Horse
- Trojan.Gen.MBT
- 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。

2022/08/12

ROMCOM RAT 與古巴勒索軟體同時使用

ROMCOM RAT 是一個正在積極開發中的客製化遠端存取木馬，今年年初首次出現。最新的版本被認為是由一個新的威脅者與古巴勒索軟體 (Cuba Ransomware) 一起部署。ROMCOM 具有遠端存取木馬的典型功能：與 C&C 通信、檢索系統資訊、刪除檔案、螢幕截圖、下載檔案、啟動程序等。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Exp.CVE-2020-1472
- Hacktool
- Ransom.Cuba
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Nvcertleak!g1
- WS.Malware.1
- WS.Malware.2

基於行為偵測技術(Snoar)的防護：

- SONAR.TCP!gen1

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已於第一時間收錄於不安全分類列表中。