Network Security
Consulting Services
Information Security
Identity Security
Endpoint Security
Recon
Weaponize
Deliver
Exploit
Install
Command & Control (C&C)
Action

保安資訊--今日最新(台灣時間2021/11/26)
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 140 萬個受保護端點上總共阻止了 1.782 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2021/11/22)**

- **在23萬9,600台端點上，阻止了6,370萬次嘗試掃描Web服務器的漏洞。**
- **在58萬5,800台端點上，阻止了5,270萬次嘗試利用的Windows作業系統漏洞的攻擊。**
- **在9萬1,100台Windows伺服主機上，阻止了2,100萬次攻擊。**
- **在19萬1,400端點上，阻止了1,320萬次嘗試掃描伺服器漏洞。**
- **在11萬0,600台端點上，阻止了590萬次嘗試掃描在CMS漏洞。**
- **在14萬4,300台端點上，阻止了400萬次嘗試利用的應用程式漏洞。**
- **在48萬8,800台端點上，阻止了1,370萬次試圖將用戶重定向到攻擊者控制的網站攻擊。**
- **在2,800台端點上，阻止了360萬次加密貨幣挖礦攻擊。**
- **在5萬8,100台端點上，阻止了490萬次向惡意軟體C&C連線的嘗試。**
- **在9,200台端點上，阻止了30萬1,500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。

2021/11/25
全世界波斯語系的 Windows 使用者，成為伊朗威脅行為者的鎖定目標

新的伊朗威脅行動者利用惡意 Word 文件，作為附件的魚叉式網路釣魚活動，瞄準講波斯語的 Windows 使用者。這些附加的 Word 文件經拆解分析後，證實是利用了編號：CVE-2021-40444 的 Microsoft MSHTML 遠端代碼執行(RCE)漏洞。

一旦使用者開啟惡意的 word 附件，就會利用多階段攻擊執行基於 PowerShell 具資訊竊取功能的有效籌載，最終從受感染系統（包括 Google 和 Instagram 憑證）中竊取系統資訊。

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：
- Exp.CVE-2021-40444
- Exp.CVE-2021-40444!*
- Trojan.Gen.MBT
- Trojan.Gen.NPE

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: Microsoft MSHTML RCE CVE-2021-40444
- 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已於第一時間收錄於不安全分類列表中。

2021/11/24
基於 JavaScript(Java描述語言)的惡意程式載入器：「RATDispenser」

惡意軟體攻擊者正重新詮釋他們的舊技術以進行全新改造，最近在一個名為「RATDispenser」基於 JavaScript 之惡意程式載入器的幫助下，可以提供隱蔽的惡意軟體。報告顯示，分發了八個惡意軟體家族系列，目的是竊取用戶資訊並獲得對受感染設備的存取權限。

攻擊始於帶有文本形式的 JS 文件的惡意電子郵件。簡單地雙擊該文件，就會啟動初始感染，接著執行第二階段的惡意軟體以建立對受害者電腦的控制。在此之後，經過混淆處理的 JavaScript 文件，會對自身進行解碼並寫入一個 VBScript 文件。然後 VBscript 將嘗試下載外部酬載，如果成功，隨後將自行刪除。

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!gen10
- Infostealer!im
- ISB.Downloader!gen52
- ISB.Downloader!gen54
- ISB.Downloader!gen68
- ISB.Downloader!gen69
- ISB.Downloader!gen81
- ISB.Downloader!gen223
- ISB.Downloader!gen341
- ISB.Dropper!gen1
- ISB.Dropper!gen35
- ISB.Houdini!gen7
- Packed.Generic.575
- Packed.Generic.603
- Trojan Horse
- Trojan.Maljava
- WS.Malware.1
- W32.Spyrat

基於機器學習的防禦技術：
- Heur.AdvML.B
- Heur.AdvML.C

2021/11/24
駭客把華為AppGallery當跳板來散布木馬程式

木馬化行動應用程式是一種已經存在多年的技術，被多個團體和個人採用。在官方應用商店列出的應用程式中，隱藏惡意軟體不僅是一種強大的感染媒介，而且是一種持續成功的感染媒介。近日，大量在華為 AppGallery 上架的安卓應用（遊戲）被舉報被木馬化。這些行動應用程式所隱藏威脅能夠從受感染的手機中收集敏感資訊。超過 900 萬台裝置安裝了這些行動應用程式。

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
- AdLibrary:Generisk
- Android.Reputation.2

2021/11/24
C-23 APT (*進階持續威脅)集團，散布安卓平台惡意程式的新變種

根據最近發布的一份報告，已經發現了先前歸因於 C-23 的 APT 組織的 Android 惡意軟體的新變種。該惡意軟體偽裝成軟體更新應用程式，並可能利用包含下載鏈接的簡訊訊息傳送給用戶。威脅行為者為新變種添加了一些新功能，以提高威脅的規避性。由 C-23 威脅組織散布的 android 惡意軟體能夠從受感染裝置收集各種資訊，包括：日誌、聯絡人、相片和文件，還可以啟動錄音／錄影並截取螢幕畫面。

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

- AdLibrary:Generisk
- Android.Reputation.2
- Android.Reputation.3
- AppRisk:Generisk

2021/11/23

持續潛伏伺機而動的的Raccoon(*浣熊)資訊竊取程式

Raccoon(*浣熊)資訊竊取程式仍然活躍在影響全球消費者和企業的威脅環境中。多個意圖竊取憑證和加密錢包的團體和個人正在使用這種資訊竊取即服務 (stealer-as-a-service)。多年來，人們看到它利用惡意電子郵件、漏洞利用工具包進行散布，並且在最近幾個月越來越多地偽裝成破解軟體。

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
- Heur.AdvML.C

2021/11/22

惡意攻擊行動，利用 Excel 二進位活頁簿格式檔 (xlsb) 文件傳送 Dridex 銀行木馬

Dridex 是一種銀行木馬，它已經活躍了近十年。該惡意軟體能夠竊取受感染機器上的敏感資訊。最近，觀察到惡意軟體行動利用 Excel 二進位活頁簿格式檔 (xlsb) 文件傳送 Dridex。攻擊者在分發時加密 ZIP 文件，以此繞過電子郵件安全軟體的檢查。

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.MalMacro!gen3
- Trojan Horse
- Trojan.Gen.MBT

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。

2021/11/19

藝高人膽大：SquirrelWaffle 也開始利用 Microsoft Exchange 漏洞

最近幾個月，SquirrelWaffle 載入程式在威脅領域赫赫有名，並持續利用定期發送惡意垃圾郵件的攻擊行動來維持熱度。此惡意軟體幕後的主謀採用了各種技巧來傳播他們的惡意軟體，其中之一是使用 Microsoft Exchange 中最近的漏洞，例如：ProxyLogon 和 Proxyshell。據報導，SquirrelWaffle 一直在利用這些漏洞來修改內部往返的郵件內容，並利用這個漏洞來發送惡意軟體。被修改過的回覆電郵內容被加入了惡意的網頁鏈結 URL，將受害者誘導到攻擊鏈的其餘階段上。

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
- Trojan Horse
- Trojan.Mdropper

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: Microsoft Exchange Server CVE-2021-26855
- Web Attack: Microsoft Exchange Server RCE CVE-2021-34473
- Web Attack: Microsoft Exchange Server CVE-2021-34473
- Web Attack: Microsoft Exchange Server Elevation of Privilege CVE-2021-34523

基於安全強化政策(適用於使用DCS)：

賽門鐵克的 DCS (Symantec Data Center Security) 出廠即已包含 Microsoft Exchange 伺服器和 Windows 網域控制器的安全強化政策，可有效防止 ProxyLogon 和 ProxyShell 漏洞。

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。

2021/11/19

新的水坑式攻擊活動被利用於散布 Macma 後門程式

發現一個針對多個香港網站訪問者的新水坑式攻擊行動。本次攻擊行動的主使者一直在利用最近的 XNU 權限提升漏洞 (CVE-2021-30869) 來投放 MacOS 後門的新變種。這個被稱為 Macma 或 OSX.CDDS 的惡意軟體具備識別目標裝置、上傳或下載任意檔案以及鍵盤側錄等功能。

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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- Trojan.Malscript
- WS.Malware.1

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。

2021/11/18

Spectre 殭屍網路修改他們的C&C 網域

Spectre 殭屍網路於 2020 年 9 月首次被發現。該殭屍網路是一種適用於 Linux 平台的遠端存取木馬 (RAT)。

最近，觀察到他們修改了他們的 C&C 網域域配置文件，並看到利用頂級域名 “api[.]github[.]com” 和 “www[.]ibm[.]com” 。沒有發生駭客攻擊或錯誤配置，只是攻擊者能夠利用 ClouDNS 服務中的漏洞。

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.NPE
- Trojan Horse
- Linux.Mirai

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。

2021/11/18

Muhstik 殭屍網路把目光轉到 Kubernetes (K8s) pod

正如最近報導所表明的那樣，Muhstik 殭屍網路幕後主謀在他們的加密貨幣行動中將目光投向了 Kubernetes pods，這是利用受感染的 Kubernetes pods Wordpress 進行的。這種威脅已經存在幾年了，發動分佈式拒絕服務 (DDoS) 攻擊和下載挖礦程式。主要鎖定 Web 應用程式和物聯網裝置並將其收編為殭屍網路中的成員。

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：

- Linux.Kaiten
- Trojan Hors

2021/11/18

使用全新的戰術--新的勒索軟體組織「 Memento Team」(*紀念品團隊)

新的勒索軟體組織「 Memento Team」(*紀念品團隊)，採用了不同的伎倆來劫持受害者的檔案。與常用的加密檔案不同--為了避開安全軟體的偵測(安全軟體已大大提升商品化加密勒索軟體的偵測能力)--Memento Team 跳過加密並將檔案移動到受密碼保護的檔案中(如Winrar)。該團隊使用強密碼將檔案移動到檔案中，並加密密鑰，然後刪除原始檔案。這種戰術是為了克服安全軟體的檢測，並能夠鎖定檔案並留下勒索訊息檔案。*使用常用合法工具軟體來做壞事的，都可以統稱為就地取材攻擊。

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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.Mimikatz
- Hacktool.Mimikatz!g4
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Seaduke
- W32.Beapy
- 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：

- Ransomware C2 connectivity
- System Infected: Coinminer Activity 2
- System Infected: Trojan.Coinminer Activity 26
- System Infected: VBS CoinMiner Download

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。

2021/11/18

域前置(Domain Fronting)技術，被利用於散布 Cobalt Strike 的攻擊中

近期一個新的惡意行動，攻擊者利用域前置 (Domain Fronting) 技術來瞄準緬甸用戶。據報導，威脅發動者使用帶有 Meterpreter stager 的片段式有效籌載荷提供 Cobalt Strike。Cobalt Strike 仍然是各種威脅組織中功能強大且非常流行的工具，可用於分發各種最終有效籌載，包括商品化惡意軟體和勒索軟體。

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!gen1
- Backdoor.Rozena
- 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：

- 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。

2021/11/17

BrazKing 行動惡意軟體針對巴西的銀行用戶

根據最近發布的一份報告，名為 BrazKing 的行動平台惡意軟體繼續針對巴西的銀行用戶。據報導，該惡意軟體利用社交工程的誘因發布惡意網址的網路釣魚信件。BrazKing 可以顯示假冒的互動視窗，誘使用戶輸入他們的銀行憑證。該惡意軟體還包括一些功能，允許它擷取已感染設備的螢幕畫面並記錄用戶的鍵盤記錄。收集到的資料被發送到攻擊者的 C&C 伺服器。

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

- AdLibrary:Generisk
- Android.Reputation.2
- AppRisk:Generisk

2021/11/17

Krane：近期部署了 XMRig 加密貨幣挖礦程式的惡意軟體攻擊行動

一種使用暴力攻擊嘗試傳播的新惡意軟體被發現並被稱為 Krane。該變種能夠下載第二階段的有效酬載或在受感染的機器上投放 Monero XMRig 加密貨幣挖礦程式。Krane 有趣地結合了 bash 和 python 腳本，用於傳播和橫向移動。

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：

- Downloader
- Downloader.Trojan
- Hacktool
- Hacktool.Rootkit
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2

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。

2021/11/16

GravityRAT 遠端存取木馬 (RAT)，繼續監視 Android 用戶

一種名為 GravityRAT 的多平台遠端存取木馬 (RAT)，自 2015 年以來經常在威脅環境中被觀察到，並且直到今天仍然活躍。該惡意軟體的活動範圍主要出現在南亞，最近發現有攻擊者將此威脅偽裝成與聊天相關的 Android 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

- AdLibrary:Generisk

2021/11/15

“Moses Staff ” 的新興勒索軟體組織對以色列國防部發動網路攻擊

一個名為“Moses Staff”的新興勒索軟體組織，聲稱已成功入侵以色列國防部的服務器和網站。該團體報告說，他們現在擁有國家機密資料，例如：報告、作戰地圖、士兵和部隊的資訊以及信件與往來通訊。他們威脅要洩露更敏感的資訊，以作為對以色列當局工作方式的警告。

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
- Trojan.Gen.NPE
- Trojan Horse

- Ransom.Gen
- WS.Malware.2

基於機器學習的防禦技術：

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

2021/11/15

Emotet 死灰復燃，並使用了 Trickbot

儘管執法部門在 2021 年 4 月關閉了 Emotet 的命令和控制 (C&C) 伺服主機，但專家們觀察到最近 Trickbot 活動會注入一個標識為 Emotet 的 DLL。眾所周知，Emotet 利用帶有惡意附件的垃圾郵件行動作為其主要傳送機制，因此使用 Trickbot 作為下載方法是一種新行為，可能是 Emotet 有死灰復燃捲土重來的徵兆。

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：

- WS.Malware.2
- Trojan.Gen.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已於第一時間收錄於不安全分類列表中。

2021/11/15

行動平台惡意軟體 Joker 出現最新變種，使用混淆技術並俱備下載多階段有效籌載的能力

在真實環境中觀察到了 Joker 行動平台惡意軟體的新變種。Joker 最初於 2017 年發現的惡意軟體家族，眾所周知，它以 Android 設備為目標，並以竊取資訊為目的。新變種具有先進的混淆和規避技術，並俱備下載多階段有效籌載的能力。

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。

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

- AdLibrary:Generisk
- Android.Reputation.2
- AppRisk:Generisk

2021/11/14

充斥著 Cobalt Strike 的多階段 PowerShell 攻擊

最近一組研究人員，發現了利用偽裝成哈薩克共和國衛生部的惡意 PDF 文件，進行多階段 PowerShell 攻擊。去年 11 月 8 日，一個名為“DangerSklif”的人利用 Github 上傳了攻擊的第一部分。

攻擊將從 LNK 檔案開始，並在執行時打開一個 PDF 文件作為誘餌，同時執行 PowerShell ，以利用自動執行登錄檔／註冊表的機碼來運行多種技術，例如：權限提升和持久性。精心設計的攻擊將採取更多其他步驟以躲避偵測，來增加將 Cobalt Strike 部署到其目標的可能性。

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!gen4
- ISB.Heuristic!gen58
- ISB.Downloader!gen446
- ISB.Downloader!gen77
- Trojan Horse

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。

2021/11/14

SharkBot，一種橫跨金融與加密貨幣的銀行惡意軟體

另一種被稱為 SharkBot 的 Android 行動平台上的銀行惡意軟體，已經出現在行動威脅領域。它不僅使用經典的螢幕覆蓋技術，而且還使用 Android 輔助功能 (Accessibility Services) 來執行自動傳輸攻擊。類提款機 (ATS) 攻擊允許攻擊者在合法的銀行行動應用程式 (App) 和加密貨幣錢包的用戶介面欄位輸入數據。根據最近報導，該惡意軟體一直針對英國、美國和意大利的銀行和加密貨幣的 (交換) 服務商。

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

- AdLibrary:Generisk

2021/11/12

IE 的漏洞最近被利用於散布 Magniber 勒索軟體的攻擊行動

據報導，Magniber 勒索軟體集團在其最新攻擊中利用了兩個 Internet Explorer (IE) 漏洞以及惡意廣告。這兩個被利用的 IE 漏洞被追踪為 CVE-2021-26411 和 CVE-2021-40444，並且分別在 3 月和 9 月已由微軟發布修補。

Magniber 作為 Cerber 勒索軟體的接班人是於 2017 年首次出現，主要針對亞洲的組織。該勒索軟體沒有採用最近常見的雙重勒索戰術 (檔案加密及勒索不成則公佈竊取的機密資訊)，而是僅依靠檔案加密。

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-2021-26411
- Exp.CVE-2021-40444*
- ISB.CVE-2021-26411!g1
- Ransom.Magniber
- Ransom.Magniber!gen1
- Ransom.Magniber!gen2
- Trojan.Gen.MBT

基於行為偵測技術(Snoar)的防護：

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

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
- Web Attack: Internet Explorer RCE CVE-2021-26411
- Web Attack: Microsoft MSHTML RCE CVE-2021-40444

2021/11/12

攻擊者濫用 Windows 10 應用程式安裝程式 (Apps Installer) 進行 BazarLoader 後門程式傳遞

據報導，一項散布 BazarLoader 後門程式的新網路攻擊行動，攻擊者濫用 Windows 10 應用安裝程序進行惡意軟體傳送。初始感染媒介是垃圾郵件，其中包含指向帶有 ms-appinstaller：前綴 (prefix) 的網址鏈接。單擊此鏈接會觸發 MS App 安裝程序下載包含最終籌載的惡意 .appxbundle 檔案。

BazarLoader 惡意軟體過去曾在多起針對企業的攻擊行動中使用過，並且還經常被用來提供額外的有效載荷，步步進逼並危害目標環境。

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

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：

- Malicious Site: Malicious Domain Request 15

- Malicious Site: Malicious Domain Request 16
- Malicious Site: Malicious Domain Request 21
- Malicious Site: Malicious Domain Request 22
- 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。

2021/11/10

在印度發動網路釣魚和間諜軟體的:Smishing 攻擊行動

印度的銀行用戶已成為網路釣魚和間諜軟體的詐騙行動的攻擊目標。攻擊者發送惡意簡訊，其中包含指向假冒印度國家銀行 (SBI) 網站的鏈接，以試圖釣魚他們的銀行帳密。如果受害者被釣魚網站成功引誘，他們還會被提示安裝偽裝成 SBI 縮發行的安卓版之銀行APP間諜軟體。

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

- AppRisk:Generisk

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) 重要來源之一的 Symantec WebPulse 中威脅情報，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。WebPulse 知道此行動中使用假冒的 DHL 域名。

2021/11/10

MasterFred，Android平台上使用螢幕覆蓋層技倆的惡意程式

螢幕覆蓋層 (Overlay) 是行動裝置平台上的銀行惡意軟體和竊密應用程式中最常用的技倆之一。 最近，在威脅環境中發現了一種名為“MasterFred”的新威脅。MasterFred 利用覆蓋受害者手機螢幕以掩蔽自己的行動 (也可能會關閉手機挑出的通知訊息)，以試圖獲取財務憑證和信用卡資訊。

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

- AdLibrary:Generisk
- AppRisk:Generisk

2021/11/10

Void Balaur，受僱的駭客組織

最近，一個名為“Void Balaur”的網路犯罪分子被曝光，它已經活躍多年，在地下論壇上提供入侵服務。該組織專門竊取電子郵件和社交媒體帳戶，多年來一直參與針對各個行業、組織、新聞工作者和倡議人士的一系列有針對性的攻擊。他們主要使用網路釣魚網站作為竊取登錄憑證的手段，但也使用 Z*stealer 和 DroidWatcher 等惡意軟體。

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.M

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

- 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。

2021/11/10

PhoneSpy 行動惡意軟體，操控你的手機，側錄你的通話、簡訊、錄影

根據最近的一份報告，正在進行的利用名為 PhoneSpy 的行動惡意軟體的攻擊行動針對韓國的用戶。該惡意軟體偽裝成各種合法應用程式，能夠從受感染裝置竊取資料和憑證，安裝從攻擊者 C&2 伺服器下載的任意 APK 套裝，從設備錄製聲音／影片並發送簡訊。

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

- AdLibrary:Generisk
- AppRisk:Generisk
- Android.Reputation.2

2021/11/09

AbstractEmu：一支Android 平台的惡意程式

AbstractEmu 是一支 Android 平台上的惡意軟體，具有間諜和遠端存取功能，以及獲得 root 存取權限的能力。10 月下旬，在 Google Play 商店和第三方商店中都觀察到了多個實例。為了引誘受害者，攻擊者將他們的惡意軟體偽裝成可以幫助管理密碼、資料使用和金錢的 Android 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

- AdLibrary:Generisk
- AppRisk:Generisk
- Android.Reputation.2

2021/11/09

Abcbot 殭屍網路，也新增DDOS攻擊能力

Abcbot 是一種惡意軟體變種，最早於 2021 年 7 月被發現。該殭屍網路以鎖定資料庫和網頁伺服主機等為目標，並利用漏洞和弱密碼進行傳播。根據最近的一份報告，Abcbot 的創作者在過去幾個月中不斷改版，目前結合了幾種不同的 DDoS 攻擊方法以及自我更新功能。

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：

- Downloader
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.2

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。

2021/11/08

發現惡意 coa 和 rc NPM 套件組

最近修改了兩個流行的 NPM 套件組“coa”和“rc”，以包含將在安裝包時執行的惡意腳本。 這些腳本會嘗試下載並執行 Danabot 木馬，這是一種竊取密碼的惡意軟體。

npm 全名為 Node Package Manager，是 Node.js 的套件 (package) 管理工具，類似 Perl 的 ppm 或 PHP 的 PEAR 等。安裝 npm 後，使用 npm install module_name 指令即可安裝新套件，維護管理套件的工作會更加輕鬆。

npm 可以讓 Node.js 的開發者，直接利用、擴充線上的套件庫 (packages registry)，加速軟體專案的開發。npm 提供很友善的搜尋功能，可以快速找到、安裝需要的套件，當這些套件發行新版本時，npm 也可以協助開發者自動更新這些套件。

npm 不僅可用於安裝新的套件，它也支援搜尋、列出已安裝模組及更新的功能。

以上NPM說明參考自 NPM 套件管理工具 | Node.js Taiwan 社群協作中文電子書 (gitbooks.io)

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 Horse
- Trojan.Danabot
- Trojan.Gen.MBT
- Trojan.Malscript

- WS.Malware.1

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：

- Malicious Site: Malicious Domains Request
- System Infected: Trojan.Danabot Activity 3

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。

2021/11/07

WatchDog 組織，採用新的挖礦綁架行動

最近，共享的證據證實 WatchDog 組織已將 TeamTNT 挖礦綁架組織至少一些行為、工具和策略納入其運營中。它似乎按預期工作，因為這些工具的使用，顯著增加了他們加挖礦綁架的營運績效。相比之下，他們似乎沒有使用 TeamTNT 常用的某些其他技術，包括憑証抓取、橫向移動和谷歌的 Go 語言 (GoLang) 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：

- Downloader
- Linux.Coinminer
- Linux.Kaiten
- Linux.Lightaidra
- Linux.Trojan
- Trojan Horse
- 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已於第一時間收錄於不安全分類列表中。

2021/11/05

MirCop 老牌勒索軟體，也玩嚇人遊戲

MirCop 是一種古老的勒索軟體，其最近的變種顯示出一種以恐怖殭屍為主題的新花樣。感染始於新的網路釣魚行動，該行動表明之前有關訂單供應清單安排的通聯已遺失。該誘餌用於讓受害者點擊 Google Drive 的鏈接，從而將 MHT 檔案下載到受害者的電腦上。當 MHT 檔案打開時，它會下載一個內含 EXE 執行檔的 RAR 壓縮檔，該檔案使用 VBS 腳本來刪除和執行 MirCop 籌載。勒索軟體立即將背景更改為殭屍主題圖像並加密檔案。

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(Snoar)的防護：

- SONAR.SuspDataRun

基於行為偵測技術(Snoar)的防護：

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

基於機器學習的防禦技術

- 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。

2021/11/05

Underminer 漏洞利用工具包，開始提供 Amadey 惡意軟體

Underminer 漏洞利用工具包已經存在好幾年，但最近有人看到它提供了 Amadey 惡意軟體。為了獲得持久性，Underminer 建立了一個每天只運行一次的排程，可以下載各種攻擊工具，包括資料竊取程式 (infostrealers)。然後，被盜的憑證可用於存取其他資源，作為其他攻擊（包括勒索軟體）的第一階段，以便在網路中取得立足之地。

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：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT

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。

2021/11/04

勇往向前的竊密惡意軟體：Agent Tesla 攻擊行動

Agent Tesla 是一個長期躋身頂級排名的資訊竊取（竊密）程式，並且沒有任何緩和的跡象。這種具有資訊竊取和遠端存取功能的流行威脅被多個團體和個人用於網路犯罪和針對性攻擊。賽門鐵克24小時全天候監控 Agent Tesla 的行動，包括最近偽造兩家知名公司的電子郵件：一個是國際級的工程服務公司。另一個則是銷售聲音和振動測量儀器給工程界的公司。

這個還在發動中的惡意垃圾郵件攻擊行動使用“報價”和“散貨運輸”等社交工程主題，目標針對全球的各種公司和機構。電子郵件主題包括：“New Quote Request(*請重新報價)”和“[Removed] - Cargo Crane[*已刪除] - *貨運起重機”。

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(Snoar)的防護：

- Infostealer.Atesla
- MSIL.Packed.19
- Scr.Malcode!gdn30
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan Horse

基於機器學習的防禦技術：

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