保安資訊--本周(台灣時間2022/01/28)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 130 萬個受保護端點上總共阻止了 2.187 億次攻擊。這些攻擊中有 96% 在感染階段前就被有效阻止：**(2022/01/24)**

- 在**25萬3,000**台端點上，阻止了**1.167億**次嘗試掃描**Web**服務器的漏洞。
- 在**51萬400**台端點上，阻止了**4,100萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬9,800**台**Windows**伺服主機上，阻止了**2,640萬**次攻擊。
- 在**19萬1,100**端點上，阻止了**1,140萬**次嘗試掃描伺服器漏洞。
- 在**10萬9,100**台端點上，阻止了**540萬**次嘗試掃描在**CMS**漏洞。
- 在**15萬1,900**台端點上，阻止了**420萬**次嘗試利用的應用程式漏洞。
- 在**49萬8,800**台端點上，阻止了**1,400萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5,200**台端點上，阻止了**410萬**次加密貨幣挖礦攻擊。
- 在**4萬7,700**台端點上，阻止了**520萬**次向惡意軟體**C&C**連線的嘗試。
- 在**8,300**台端點上，阻止了**21萬7,200**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。

2022/01/27

使用 Excel 巨集的新變種 Emotet 攻擊被發現

在過去的幾周中，我們觀察到使用惡意巨集散佈 Emotet 的 Excle 檔案。惡意檔案透過電子郵件傳遞，並誘使收件人在打開附件時啟用巨集。執行時，巨集會向命令和控制伺服器 (C&C) 報到以下載其他惡意軟體。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.Module!gen3

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：

- MScr.Malcode!gen
- Scr.MalMacro!gen2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/01/27

CVE-2021-4034 (PwnKit)，Linux的 Polkit 工具裡的 pkexec（類Unix 作業系統上的權限管理工具）執行漏洞

Polkit（以前稱為 PolicyKit）是一個用在 Linux (類 Unix) 作業系統中控制系統權限的元件。鎖定 CVE-2021-4034 (PwnKit) 的漏洞將使攻擊者能夠利用 Polkit 的 pkexec 工具，進而允許任何本地用戶在易受攻擊 (有漏洞) 的系統上獲得 root 權限並繞過任何身份驗證。

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：

基於安全強化政策(適用於使用DCS)：

Symantec DCS 內建的強化和檢測政策已預先提供針對此 Linux 權限提升漏洞的零日保護。

2022/01/26

Linux 平台也出現，Lockbit 勒索軟體變種，VMware ESXi 虛擬機請特別留意

Lockbit 是另一個勒索軟駭客集團，他們已經開枝散葉並在他們的武器庫中新增了一個 Linux 變種，這個最新的變種針對 VMware ESXi 虛擬機。一個 ESXi 伺服器託管多個虛擬機，如果成功加密，對受害組織的影響可能很大。

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

2022/01/26

在真實世界觀察到一種名為 DTPacker 的新型惡意軟體

已觀察到一種用 .NET 撰寫的新惡意軟體，研究人員將其命名為 DTPacker。目前看來，它的獨特之處在於使用美國前總統唐納・川普的名字作為固定密碼進行解碼。以前的變種使用基於利物浦足球俱樂部主題下載位置的密碼。一個惡意軟體既是打包工具又是下載程式也是獨一無二。該惡意軟體安裝了遠端存取木馬和資訊竊盜程式，包括 Agent Tesla、Ave Maria、AsyncRAT 和 FormBook 以及其他有效籌載，然後再安裝勒索軟體。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.Heur.RGC!g510
- SONAR.SuspBeh!gen66

檔案型(基於回應式樣本的病毒定義檔)防護：

- MSIL.Packed.1
- MSIL.Packed.18
- Scr.Malcode!gdn30
- Scr.Malcode!gdn40
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

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

2022/01/26

DazzleSpy---一種全新的 MacOS 惡意軟體

根據最近發布的一份報告，一種名為 DazzleSpy 全新 MacOS 惡意軟體已在一系列水坑攻擊中擴散。惡意行動涉及假冒或合法但受感染的網站，這些網站提供 Webkit 漏洞利用，而該漏洞又被用來做為 DazzleSpy 有效籌載來感染 Mac 用戶。該惡意軟體本身具有後門功能，包括收集有關受感染主機的資訊、資料滲透、各種檔案操作和啟用RDP 連線。

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.Malscript
- 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。

2022/01/26

APT28發起的多階段間諜攻擊行動

最近發表關於針對政府高官的多階段間諜活動的研究，並歸咎於 APT28 組織。感染鏈中的第一個鏈接是附加在電子郵件中的惡意 Excel 文件，該文件將用於利用 MSHTML 遠端程式碼執行 (remote code execution，RCE）漏洞 (CVE-2021-40444)。成功利用後，它將會執行一個惡意二進位檔案，該二進位檔案將用作名為“Graphite”的第三階段惡意軟體的下載程式。Graphite 將利用微軟的 OneDrive 作為 C&C 伺服器，多階段攻擊的其餘部分最終將下載並執行“Empire”，這是一個基於 PowerShell 的開放原始碼後滲透攻擊框架。

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：

- MSIL.Downloader!gen7
- Trojan.Dropper
- Trojan.Gen.2
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

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

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。

2022/01/25

改良的安卓平台惡意軟體：BRATA(巴西遠端存取工具安卓版)

12 月發現了一個新的 BRATA（巴西遠端存取工具安卓版）變種，據報導它是具有新危險功能的改進版本。一旦不知情的受害者安裝惡意應用程式，GET 請求連接將被發送到專用 C&C 伺服器，隨後取得惡意 .apk 檔案。BRATA 主要分佈在 Google Play 上。

下面列出了 BRATA 現在包括的新功能：

- 執行設備恢復出廠設置的能力：在未經授權的電匯嘗試之後，攻擊者（Threat Actors ） 似乎正在利用此功能擦除任何不法痕跡。
- GPS定位能力。
- 能夠在設備和 C&C 伺服器之間使用多個通信通道（HTTP和TCP）來保持持續連線能力。
- 能夠透過VNC和鍵盤側錄技術持續監控受害者的銀行應用程式。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- WS.Malware.1
- WS.Malware.2

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已於第一時間收錄於不安全分類列表中。

2022/01/25

APT36 又名 Earth Karkaddan(*地球卡卡丹)，利用 CapraRAT 安卓惡意軟體

APT36 也被稱為 Earth Karkaddan (*地球卡卡丹) 或 Mythic Leopard (*神話豹)，是一個針對印度軍事和外交組織的 APT 駭客集團。有人已經發現該駭客集團在其行動中利用魚叉式網路釣魚電子郵件，同時提供各種惡意軟體有效籌載，例如：ObliqueRAT。據報導，在2021年，APT36利用了名為 CapraRAT 的 Android 平台惡意軟體。這種行動惡意軟體與其 Windows 的同類 Crimson RAT 惡意軟體極為相似，後者過去也被該威脅組織使用過。

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.Dropper!gen25
- Trojan Horse
- Trojan.Gen
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- W97M.Downloader

基於機器學習的防禦技術：

- Heur.AdvML.C

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。

- TAndroid.Reputation.1
- Android.Reputation.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。

2022/01/25

與 TrickBot 威脅集團相關的 Diavol 勒索軟體

根據最近發佈的一份報告，Diavol 勒索軟體變種已與惡名昭彰的 Trickbot 銀行木馬幕後威脅集團有關。自 2021 年 7 月左右以來，Diavol 一直在散佈行動中出現，並且與 Conti 勒索軟體變種顯示出某些相似之處。Diavol 加密資料並向加密檔案新增 .lock64 副檔名。勒索說明包括如果不付款，則威脅要公布被盜資料。

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
- Ransom.Diavol
- Ransom.Diavol!g1
- Ransom.Diavol!gm1
- Trojan Horse
- Trojan.Gen.MBT

基於行為偵測技術(Snoar)的防護：

- SONAR.Cryptlck!g171

基於機器學習的防禦技術：

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

2022/01/24

新一波的 FakeCop 間諜軟體簡訊釣魚浪潮，正在襲擊日本行動使用者

2021年，一種名為 FakeCop 的 Android 間諜軟體被觀察到透過惡意簡訊在日本傳播，該攻擊者假裝代表 KDDI 並試圖引誘受害者安裝偽裝成 Android 安全應用程式的 FakeCop。

賽門鐵克一直在觀察這類行動，但本月早些時候出現新一波的感染嘗試。這次的攻擊者假裝來自 KDDI 和 Docomo，這兩家公司都是日本的大型行動電信服務商。惡意攻擊者繼續使用免費「duckdns.org」動態DNS服務來協助傳遞，僅在過去 4 天中，我們就觀察到與此特定行動相關的 1000 多個網址 (URL)。

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

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。

2022/01/24

使用惡意 PowerPoint 檔案，部署遠端存取木馬 (RAT) 以替換加密錢包地址的行動

出現一個網路釣魚活動，它使用惡意 PowerPoint 檔案來部署惡意遠端存取木馬 (RAT)，如 AveMaria 和 AgentTesla。這些資訊竊取程式針對許多應用程式，並具有一長串功能。透過使用 Windows 內建工具（PowerShell 和 MSHTA），將執行惡意 PowerPoint 檔中經過混淆處理的巨集。除了洩露受害者資訊和有關受感染電腦的資訊外，惡意軟體還會查找任何加密貨幣錢包樣式，並將資訊替換為攻擊者的錢包位址。

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!gen12
- Downloader
- ISB.Downloader!gen80
- ISB.Downloader!gen398
- ISB.Downloader!gen433
- ISB.Downloader!gen510
- 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／IP位址已於第一時間收錄於不安全分類列表中。

2022/01/23

MarsStealer 資訊竊取程式，對密碼和加密貨幣虎視眈眈！

最近幾個月，一種名為 MarsStealer 惡意軟體越來越流行，並且已經透過惡意電子郵件和偷渡式下載進行散布。在這些偷渡式下載的行動中，我們觀察到常用的的社交工程戰術，例如：假冒的原始遊戲提供改善模組、破解軟體、序號產生器、假冒的修補程式等。

自從該惡意軟體被破解並免費分享以來，越來越多的團體和個人一直在測試這個資訊竊取程式，有些人顯然已將其添加到他們的武器庫中。這是一個相當普通的資訊竊取程式，針對瀏覽器密碼、加密貨幣瀏覽器擴展和加密錢包，它當然有足夠的功能來吸引更多意圖不軌的人。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.Heur.RGC!g556

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：

- Trojan.Gen.2
- Trojan horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/01/21

最近的電子郵件行動中觀察到拉丁美洲銀行木馬 Guildma，也稱為 Astaroth

Guildma，也稱為 Astaroth，是一種先進的拉丁美洲銀行木馬，專門針對巴西。它用 Delphi 設計，由各種模組、創新的執行方法和其他複雜的攻擊技術所組成。除了針對金融機構，Guildma 還試圖竊取電子郵件帳號、電子商店和串流影音服務的憑證。此外，它還具有後門的能力，包括螢幕擷取、鍵盤側錄、下載檔案和重開機。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.Module!gen3

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：

- Heur.AdvML.B
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

2022/01/21

STRAT：藏身在垃圾郵件攻擊行動的遠端存取木馬(RAT)

STRRAT 遠端存取木馬 (RAT)，最近被發現透過假冒主要航運公司的惡意詐騙垃圾郵件行動來散布。這些訊息誘騙使用者開啟實際上是惡意壓縮檔的運輸發票。一旦被感染，RAT 就會開始作鍵盤側錄、安裝遠端控制功能並洩露儲存在瀏覽器和電子郵件用戶端的密碼。

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.Adwind!gen22

郵件安全防護機制：

- Coverage is in place for Symantec's email security products

檔案型(基於回應式樣本的病毒定義檔)防護：

- 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: 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。

2022/01/21

駭客組織 Donot Team，持續發動間諜行動

根據最近發布的報告，被稱為Donot Team(又名APT-C-35)駭客組織持續針對南亞的組織和個人展開間諜行動。威脅參與者在最近的行動中，利用各種惡意軟體變種--其中包括 DarkMusical、Gedit 和 Henos。惡意軟體的傳播媒介主要包含惡意附件的魚叉式網路釣魚電子郵件。

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：

- Bloodhound.RTF.10
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Mdropper
- WS.Malware.2

基於行為偵測技術(Snoar)的防護：

- SONAR.Module!gen3

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／IP位址已於第一時間收錄於不安全分類列表中。

2022/01/21

帶著 BHUNT 竊取程式的加密錢包

在真實世界發現了一種名為 BHUNT 新型資訊竊取惡意軟體。以 .NET 設計二進位惡意軟體針對加密錢包檔案、剪貼簿資訊和暫存在瀏覽器中的憑證。BHUNT 已使用 Themida 和 VMProtect 等商業打包程式加密。BHUNT 資訊竊取惡意軟體一種可能的可疑交付技術是透過破解軟體安裝程式。

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：

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

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：

- 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。

2022/01/21

Vulturi 資訊竊密程式的活動激增

在過去幾個月裡，被稱為 Vulturi Stealer 資訊竊密程式越來越流行 (儘管它名氣還沒有大到像 Agent Tesla、RedLine、Lokibot、AZORult 等)。賽門鐵克認為這種增加的活動與論壇、網站和社交媒體網站上出現各種破解軟體版本有關。目前為止，它已透過惡意電子郵件和順道下載散布。

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.SuspLoad!g35
- SONAR.Trafic2.RGC!g13

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：

- Packed.Generic.548
- Packed.NSISPacker!g10
- Scr.Malcode!gdn34
- Trojan.Gen.MBT
- Trojan Horse

基於機器學習的防禦技術：

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

2022/01/21

WebHard 上託管的成人遊戲，導致 DDoS IRC 機器人

早在去年 10 月，就有一個惡意人士利用 WebHard（韓國線上儲存服務）作為 UDP RAT 交付傳送平台的活動。

根據最近報導，還有另一個活動共用相似處，包括傳送平台、社交工程和下載程式。然而這一次，它是一個偽裝成成人遊戲的 DDoS IRC 機器人。這個機器人被稱為“Simple-IRC-botnet”（用 Golang 編寫），也可以在知名的代管平台上使用，用於軟體開發和版本控制。如果成功引誘，受害者的機器將被用於執行拒絕服務 (DoS) 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.Dropper!gen2

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

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: Malicious Website Activity 47

2022/01/20

注意Remcos 遠端存取木馬 (RAT)活動

Remcos 是一種普通的遠端存取木馬 (RAT)，被多個團體和個人用來進行科技犯罪和有針對性的攻擊。由於可透過網際網路免費存取，且已被破解（即修改，通常是為了不用啟動授權或停用其他限制），威脅的流行度繼續增長。持續不斷觀察到 Remcos 相關的行動，主要透過惡意電子郵件散布，但也包括其他媒介，如順道下載。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspBeh!gen24
- SONAR.SuspBeh!gen530
- SONAR.SuspDataRun

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!gdn30
- Scr.Malpbs!gen1
- Trojan.Gen.MBT

2022/01/20

Cypher 遠端存取木馬(RAT)，跟踪 Android 用戶

心懷不軌的團體和個人現在有許多針對 Android 行動用戶的遠端存取木馬可供選擇，但大多數人傾向於使用可免費存取或已破解的遠端存取木馬 (RAT)，而 Cypher 遠端存取木馬 (RAT) 就是當紅炸子雞。這種普通的惡意軟體原本就不貴，以每月約 100 美元或終身 400 美元的價格出租--已被破解的更是無本生意，並使許多人趨之若鶩。

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