保安資訊--本周(台灣時間2023/01/20)
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 79 萬 5,900 台受保護端點上總共阻止了 9,990 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/01/15)**

- 在**14萬6,900**台端點上，阻止了**4,190**萬次嘗試掃描**Web**服務器的漏洞。
- 在**29萬5,400**台端點上，阻止了**2,170**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬400**台**Windows**伺服主機上，阻止了**1,810**萬次攻擊。
- 在**8萬7,800**台端點上，阻止了**290**萬次嘗試掃描伺服器漏洞。
- 在**1萬9,900**台端點上，阻止了**130**萬次嘗試掃描在**CMS**漏洞。
- 在**5萬6,300**台端點上，阻止了**200**萬次嘗試利用的應用程式漏洞。
- 在**28萬700**台端點上，阻止了**670**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,500**台端點上，阻止了**260**萬次加密貨幣挖礦攻擊。
- 在**14萬2,500**台端點上，阻止了**1,180**萬次向惡意軟體**C&C**連線的嘗試。
- 在**3,900**台端點上，阻止了**15萬1,600**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。

2023/01/20

Dharma／Crysis勒索軟體最新變種

Dharma 也稱為 Crysis，是過去幾年出現在威脅領域的勒索軟體家族。雖不像過去那麼盛行，它仍然會定期重新出現，並在真實網路環境上出現新的變種。眾所周知，Crysis 是透過包含惡意附件的垃圾郵件或透過直接開採利用有漏洞的 RDP 伺服器來傳播。雖然這種勒索軟體以勒索軟體即服務 (RaaS) 模式運行而廣為人知，但 Crysis 原始碼早在 2020 年就被洩露，導致多年來出現原生惡意軟體的大量變種和分支。

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.RansomCrys!g1
- SONAR.RansomCrys!g2
- SONAR.SuspDataRun

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Crysis
- Ransom.Crysis!gm
- SMG.Heur!gen
- WS.Malware.1

基於機器學習的防禦技術：

- 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：

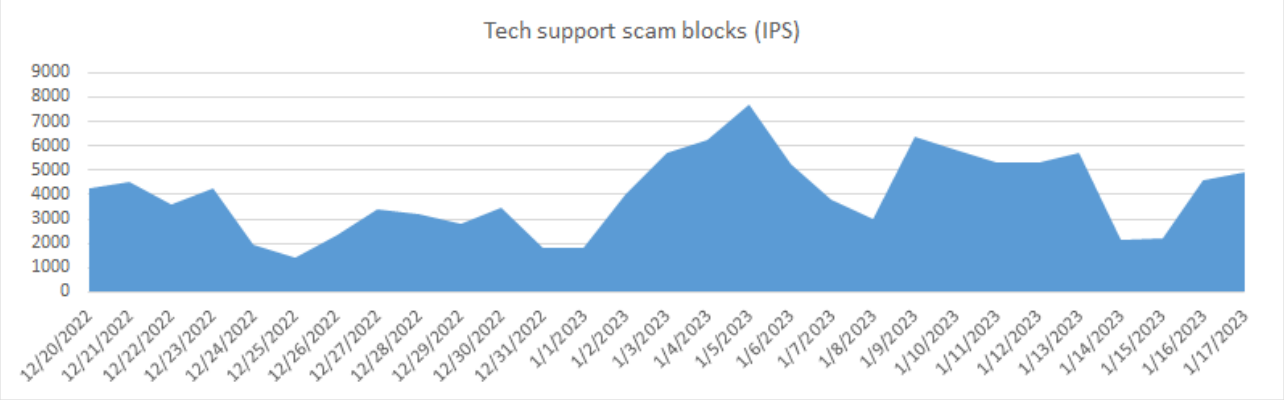
- Attack: Ransom.Crysis Activity 3

2023/01/20

防護亮點：賽門鐵克的端點IPS入侵防護技術，有效攔截日新月異的技術支援詐騙

～防護亮點～

技術支援詐騙是已久的老梗，許多人不相信這個年代還會有受害者。可悲的是，事實並非如此。我們的網路流量監控系統顯示這些詐騙仍然非常活躍。賽門鐵克每天都會繼續偵測到全新的假冒技術支援網站和惡意流量重導向到詐騙者控制的站台。



技術支援詐騙會影響消費者和企業，但由於可能會竊取與公司相關的機敏資訊，因此它們對組織和企業的影響可能更大。雖然經濟利益通常是主要目標，但冒充技術支援代表並說服員工允許遠端連線遙控他們的電腦或暴露敏感訊息可能會導致資料外洩和嚴重的經濟損失。技術支援詐騙並會收集並洩漏被盜憑證，再將這些憑證在黑市上出售，進而提高詐騙得逞的機會。

賽門鐵克擁有領先業界的 **零時差** 保護技術，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：

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: Fake Scan Webpage*
- Malicious Site: Malicious Domain Request*
- Web Attack: Fake Tech Support Domains*
- Web Attack: Fake Tech Support Website*

* 這表示存在多個名稱相似的檢測，例如：Web 攻擊--假的技術支援網站 295、Web 攻擊--假技術支援網站 374 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。

欲瞭解更多有關於賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。

欲瞭解更多有關於賽門鐵克網頁完整防護組合--Symantec Web Protection 的更多訊息，請點擊此處。

欲瞭解更多有關於賽門鐵克雲端網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

2023/01/20

Nitro不只是勒索軟體，還會竊取Discord權杖

Nitro 是一種普通的勒索軟體變種，最初於 2021 年發現，據報導僅用於教育目的。這種惡意軟體的新變種偶爾會在真實網路環境上被發現，這顯示它仍被使用。它的影響雖然似乎非常有限。在贖金方面，Nitro 要求提供 Discord Nitro 訂閱禮品程式碼，而不是任何付款。除了通常的勒索軟體功能外，Nitro 還能夠從受感染的機器上竊取 Discord 權杖。

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
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/01/20

Hook--Ermac 行動惡意軟體的進化版本

Hook 是一種源於 Ermac 變種的行動惡意軟體。除了典型的間諜軟體特徵和已知的 Ermac 惡意軟體相似的功能外，Hook 還展示一些遠端存取工具 (RAT) 功能。這種惡意軟體變種可以操控裝置系統、建立遠端通訊、截取螢幕截圖、模擬點擊或按下特定介面上的事件等。Hook 幕後的攻擊者除了使用普通的 HTTP 通訊之外，並在 Ermac 中與 C&C 服務的 WebSocket 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。

- AdLibrary:Generisk
- Android.Reputation.1
- 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。

2023/01/20

Trigona勒索軟體活動呈上升趨勢

Trigona 勒索軟體，自 2022 年初以來就一直活躍，並在 2022 年底其活動明顯增加。它採用雙重勒索手段，這是現在幾個惡名昭章的勒索軟體集團常用的方法。加密後，檔案將附加“._locked”副檔名，並留下與 Lockbit 類似格式的贖金說明。沒有指定贖金金額，但警告受害者，如果不付款，他們的資料將被公開拍賣。

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.Cryptlck!g171
- SONAR.PsDownloader!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.C

2023/01/20

VectorStealer竊密程式，嶄露頭角

VectorStealer 是一種竊密程式，於 2022 年底在地下論壇上刊登廣告。最近幾個月，有發現真實的使用案例。儘管其功能與其他惡意軟體相似，但它在駭客組織和個人中越來越受歡迎。它已被用於以運輸和報價為主題的垃圾郵件和偷渡式下載活動。攻擊者使用的控制面板帶有深紅色背景，登錄框上面寫有 VectorStealer。

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：

- Trojan.Gen.2
- Scr.Malcode!gdn34

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/01/19

觀察到Gomorrah 4.0新版竊密程式活動

Gomorrah 竊取程式意軟體於 2020 年初首次為人所知，此後斷斷續續地出現在網路威脅領域。它不像 Formbook、Agent Tesla 或 RedLine 等其他惡意軟體那樣常見。最初需購買，後來被破解，現在任何人都可以免費使用。Gomorrah 通常透過偷渡式下載傳播，它的命令和控制伺服器偶爾會被偵測到。

最近，賽門鐵克觀察到另一個行動，其中 Gomorrah 偽裝成常用軟體的安裝程式，這是一種常見的社交工程手法。在功能方面，它可以竊取儲存在 Chromium 類型瀏覽器中的密碼、來自 Discord 和 Telegram 的通訊、加密錢包、VPN 密碼、竊取檔案和螢幕截圖等。

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：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.C

2023/01/19

Wroba 安卓手機行動惡意軟體具有修改DNS設定的功能

Wroba 安卓手機行動惡意軟體與稱為 Roaming Mantis 的駭客組織有所關聯。據報導，此惡意軟體的最新變種具有修改 DNS 設定的功能。這個新功能讓攻擊者為了 DNS 劫持攻擊而入侵 Wi-Fi 路由器。任何存取此類受感染路由器的用戶都將被重導向到提供惡意籌載的登錄頁面。這種傳播方法不同於可追溯到 2019-2022 年的一些較早的 Roaming Mantis 攻擊行動，在當時，簡訊釣魚攻擊是首選的感染方法。

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：

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。

2023/01/19

Cacti遠端程式碼執行(RCE)漏洞(CVE-2022-46169)在真實網路環境上被開採利用

Cacti 是一種開放原始碼網路監控工具，為流量圖工具：RRDtool 的前端應用程式。去年 12 月，一個影響 Cacti 1.2.22 及其舊版本的命令注入漏洞 (CVE-2022-46169) 被揭露。雖然該漏洞在揭露後不久就得到修補，但新的報告顯示遠端程式碼執行 (RCE) 漏洞目前正在被廣泛開採利用。該漏洞可能允許未經身份驗證的攻擊者在運行 Cacti 的伺服器上執行任意程式碼。

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：

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: Cacti Unauthenticated Command Injection Vulnerability CVE-2022-46169

2023/01/19

寶刀未老～Phobos勒索軟體仍在流通

Phobos 是一個較舊的勒索軟體家族，於 2018 年左右首次出現在威脅領域，與更舊的 Dharma (Crysis) 勒索軟體有一些相似之處。儘管已經流通好幾年，但這種勒索軟體的一些新變種和更新版本至今仍在真實網路環境上出現。本月觀察到的最新 Phobos 變種會加密用戶的檔案並附加如下的副檔名：

- .duck
- .eight
- .elbie
- .elbow
- .faust
- .steel
- .win

眾所周知，Phobos 勒索軟體在被加密檔案上採用多種副檔名手法，最近觀察到的變種在這方面也沒有多大變化。

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.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
- WS.SecurityRisk.4

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.Crysis Activity 3

2023/01/19

觀察到Loda和Warzone遠端存取木馬(RAT)涉及的目標式攻擊行動

多個駭客集團正在全球採用 Loda 和 Warzone 遠端存取木馬 (RAT) 發動目標式攻擊行動，包括最近在俄羅斯使用政府內部文件當誘餌的惡意行動報告。這些攻擊從一封包含 VHDX 附件的惡意電子郵件開始，該附件又包含兩個誘餌檔案和一個惡意 LNK。執行時，LNK會部署名為 Warzone 或 Loda 遠端存取木馬 (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：

- Scr.Malcode!gdn32
- Trojan.Gen.MBT
- Trojan.Gen.2
- Trojan Horse

基於機器學習的防禦技術：

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

2023/01/18

EyeSpy間諜軟體透過VPN安裝程式傳播

在稱為 20Speed 的伊朗 VPN 服務的木馬化安裝程式中發現 EyeSpy 惡意軟體。這個竊密程式能夠從瀏覽器和加密錢包中竊取各種類型的資訊，例如：按鍵、檔案和密碼。據報導，該行動於 2022 年 5 月開始，並於 2022 年底情勢升高。VPN 軟體通常用於繞過網際網路審查並存取被阻止的內容，使其成為許多人追捧的工具。這使得 VPN 軟體成為向大量潛在受害者傳播惡意軟體的良好媒介。

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.Reputation.1

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。

2023/01/18

CentOS Web Panel(CWP) 7存在遠端程式碼執行(RCE)漏洞(CVE-2022-44877)，建議即刻進行更新修補

CentOS Web Panel (CWP) 是 Linux 伺服器的網頁管理介面元件。它允許用戶透過網頁管理介面管理其伺服器的各種組態配置，包括 Web伺服器、電子郵件、DNS 和資料庫。

最近 Centos 釋出 Centos Web Panel 7 中存在的遠端程式碼執行 (RCE) 漏洞 (CVE-2022-44877) 更新修補，如果該漏洞被成功利用，遠端攻擊者可以透過登錄參數中的 shell 指令執行任意作業

系統命令。

更新修補釋出後，報告此漏洞的安全研究人員分享一個概念驗證。不幸的是，當指導和概念驗證程式碼公開可用時，它通常會隨著攻擊者的研究並消化其程式碼而助長惡意活動。在過去的一週中，已多次嘗試使用 CVE-2022-44877 漏洞，來入侵尚未修補的 CWP 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：

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: Centos Web Panel 7 RCE CVE-2022-44877

2023/01/18

NjRAT遠端存取木馬(RAT)利用地緣政治當誘餌在中東和北非傳播

在中東和北非地區發現一個利用中東地緣政治主題的誘餌來傳播NjRAT的攻擊行動。阿拉伯語系的使用者被引誘下載受感染的 Cab 類型檔案，這些檔案上架在不嚴謹的代管伺服器上。開啟誘餌檔案後，受害者的機器就會感染 PowerShell 腳本類型的植入程式，該腳本負責將 NjRAT 二進元檔案載入到記憶體。

NjRAT 允許攻擊者在受感染系統上進行惡意活動，例如：點擊與鍵盤側錄、掌控受害者的鏡頭、竊取暫存在瀏覽器中的憑證、開啟反向 Shell、上傳／下載檔案、執行程序、修改檔案和登錄機碼等惡意行為。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen11
- ISB.Downloader!gen80
- ISB.Heuristic!gen5
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.NPE
- VBS.Downloader.Trojan

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。

2023/01/18

APT15所操控的Turian後門

Turian 後門被公認是 APT15 駭客組織所操控的惡意軟體（也被稱為 Playful Taurus 或 Vixen Panda）。該後門最初在 2021 年被發現，據說正在不斷優化改版中。Turian 已被發現用於多起 2022 年所發生的攻擊行動，並與歹徒所操控的全新或改良後的 C&C 基礎設施協作。Turian 的功能包括執行從 C&C 伺服器收到的命令，並在受感染的端點上建立反向連線 Shell。

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：

- Backdoor.Trojan
- Trojan Horse
- Trojan.Gen.2
- 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。

2023/01/18

在真實網路環境偵測到多起Batloader惡意軟體活動

Batloader 是一支常被用於攻擊鏈初始階段的惡意軟體，突破之後會導引更進階的惡意軟體組合和有效載荷。該惡意軟體通常透過惡意廣告和搜尋引擎最佳化中毒 (SEO Poisoning) 手法進行傳播，隨後利用偽裝成合法軟體安裝程式的惡意.MSI安裝檔。就在最近幾個月，Batloader在真實網路環境的活動顯示，這種惡意軟體提供各種有效籌載，包括 Cobalt Strike、Royal Ransomware、Qakbot、Vidar 和 RacoonStealer……等等。

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：

- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.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。

2023/01/17

VagusRAT遠端存取木馬(RAT)採用誤植／輸入錯誤域名攻擊(typosquatting)和搜尋引擎最佳化中毒(SEO Poisoning)的手法傳播

VagusRAT 遠端存取木馬 (RAT) 是另一個採用誤植/輸入錯誤域名攻擊(typosquatting)和Google Ads 搜尋引擎最佳化中毒(SEO Poisoning)手法，向毫無戒心的受害者傳播的惡意軟體。VagusRAT是以惡意軟體即服務（MaaS）的形式出售的，它與一個惡意軟體產生器緊密相關，允許額外定制惡意套裝軟體。該惡意軟體具有廣泛的遠端存取能力，包括對HRDP（隱藏遠端桌面協定）的支援，該協定允許攻擊者在合法使用者存取受感染系統的同時，不會在機器上觸發任何警報。

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 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：

- Scr.Malcode!gdn14
- 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

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。

2023/01/17

DDOSIA殭屍網路惡意軟體被用於對烏克蘭發動DDoS攻擊

DDOSIA 是一個被稱為 NoName057(16) 的駭客集團，在過去幾個月的一系列分散式阻斷服務 (DDoS) 攻擊中利用的殭屍網路惡意軟體。DDOSIA 正在開發各種版本，適用於 Windows、Linux 和macOS 平臺。據瞭解，威脅組織 NoName057(16) 的目標是銀行、教育和政府部門，以及其他單位。這個歹徒過去發動的幾次攻擊都是針對烏克蘭或支持烏克蘭的國家和組織。

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：

- DDoS.Trojan
- Trojan Horse
- 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。