保安資訊--本周(台灣時間2024/07/12)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 49 萬 1,000 台受保護端點上總共阻止了 5,200 萬次攻擊。這些攻擊中有 82.4% 在感染階段前就被有效阻止：**(2024/07/08)**

- 在**10萬400**台端點上，阻止了**1,190**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**12萬4,200**台端點上，阻止了**950**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬5,400**台**Windows**伺服主機上，阻止了**107**萬次攻擊。
- 在**5萬9,300**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,800**台端點上，阻止了**69萬3,700**次嘗試掃描在**CMS**漏洞。
- 在**5萬5,800**台端點上，阻止了**690**萬次嘗試利用的應用程式漏洞。
- 在**16萬3,000**台端點上，阻止了**400**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6,000**台端點上，阻止了**110**萬次加密貨幣挖礦攻擊。
- 在**10萬4,200**台端點上，阻止了**820**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**1,100**台端點上，阻止了**8萬9,800**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。

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 10 萬 8,300 個受保護端點上阻止了總計 470 萬次攻擊。**(2024/07/08)**

- 使用網頁信譽情資，在 **99K** 個端點上阻止 **430** 萬次攻擊。
- 攔截 **20.9K** 個端點上 **363.4K** 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 **6.6K** 個端點上攔截 **76.3K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **211** 個端點上攔截 **8.6K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

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。

2024/07/11

儘管受到執法單位圍剿，勒索軟體組織涉入的惡意活動並未減少

賽門鐵克的威脅獵手團隊在最新發佈報告中分享對觀察到的勒索軟體活動，可供洞察未來。資料顯示，儘管 Lockbit 和 Noberus 勒索軟體組織遭到執法單位圍剿，而且 2023 年最後一個季度到 2024 年第一季度之間出現下降趨勢，但勒索軟體活動仍在上升。報告中的其他分析涉及哪些組織最活躍 (仍然是 LockBit) 和攻擊的途徑、媒介與手法 (漏洞利用使用最多)。

在我們部落格文章有更詳細內容：2024年第一季勒索軟體活動報告：儘管遭到執法單位圍剿，但仍然維持很高的活動水準。

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：

自適應防護技術(包含於SESC)：

- ACM.Mshta-Cmd!g1
- ACM.Mshta-Net!g1
- ACM.Ps-Mshta!g1
- ACM.Ps-Net!g1
- ACM.Ps-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen14

- SONAR.Ransomware!g8
- SONAR.SuspLaunch!g18
- SONAR.SuspScript!g7
- SONAR.TCP!gen1
- SONAR.TCP!gen6

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen67
- Infostealer.Bancos
- Ransom.Cl0p
- Ransom.Cl0p!gen1
- Ransom.Gen
- Ransom.Zombie
- 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.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：

- Audit: EFSRPC Bind Attempt

2024/07/10

不斷演變並增強其戰略和戰術，誘餌從盜版軟體到電子書，ViperSoftX惡意竊密程式總是透過「P2P點對點傳輸」的torrent網站傳播

ViperSoftX 是一種惡意竊密程式，它不斷演變並增強其戰略和戰術。最初，攻擊者利用熱門軟體的盜版來引誘用戶，通常是透過「P2P 點對點傳輸」的 torrent 網站傳播。不過，在最近的行動中，惡意軟體專門偽裝成電子書，也是透過「P2P 點對點傳輸」的 torrent 網站傳播。它還開始利用 CLR 在 AutoIt 環境中加入 PowerShell 操作。ViperSoftX 專注於竊取加密貨幣、系統資訊、剪貼簿置換、主機的指紋圖譜以及在遭感染系統上下載和執行其他惡意有效酬載。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g11

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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。

2024/07/10

安卓平台上的間諜軟體：GuardZoo～鎖定中東的國防相關機構

據觀察，一款名為 GuardZoo 安卓平台上的間諜軟體，以中東地區的國防相關機構為目標。據信，它與葉門的胡塞叛軍黨羽有關。該惡意軟體能夠從行動裝置中擷取個人資訊，包括照片、錄影、文件檔以及裝置詳情和設置。GuardZoo 主要透過以軍事和宗教為主題的誘餌在 WhatsApp 和行動裝置上的瀏覽器等平臺上傳播。

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

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。

2024/07/10

Linux中經常使用的Ghostscript 工具，存在嚴重等級的遠端程式碼執行(RCE)漏洞(CVE-2024-29510)

賽門鐵克發現 Linux 系統上常用『Ghostscript』文件轉換工具／編譯器，存在遠端程式碼執行漏洞 (CVE-2024-29510)。該漏洞影響 Ghostscript 10.03.0 及更早的版本。攻擊者可利用此漏洞繞過 -dSAFER 沙箱，進而執行命令和竄改檔案。解決方法是更新至 Ghostscript 的最新安裝版本 (v10.03.1)。

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)：

賽門鐵克的重要主機防護系統：DCS～Data Center Security 其出廠就預設的強化可針對此 CVE 提供零時差保護。DCS 的入侵防護系統 (IPS) 預設政策攔截 %pipe% 執行 I/O 操作。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/07/10

駭客組織：Water Sigbin，開採濫用漏洞散播挖礦程式

駭客組織：Water Sigbin(又名 8220 Gang) 開採濫用 Oracle WebLogic Server 中的漏洞(CVE-2017-3506 和 CVE-2023-21839) 向遭入侵系統傳遞 XMRing 的加密貨幣挖礦程式。該駭客組織採用多種規避伎倆，例如：程式碼混淆、無檔案執行技術以及將貨幣挖礦程式偽裝成合法程序。

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

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。

2024/07/09
防護亮點：賽門鐵克端點防護技術，有效應對近期遽增的側載攻擊

側載

Wikipediade 將側載定義為『在兩台本地裝置之間進行檔案傳輸的過程，尤其是指在一台電腦和一台行動裝置，例如：行動電話、智慧型手機、個人數位助理、平板電腦、可攜式媒體播放器或電子閱讀器』。

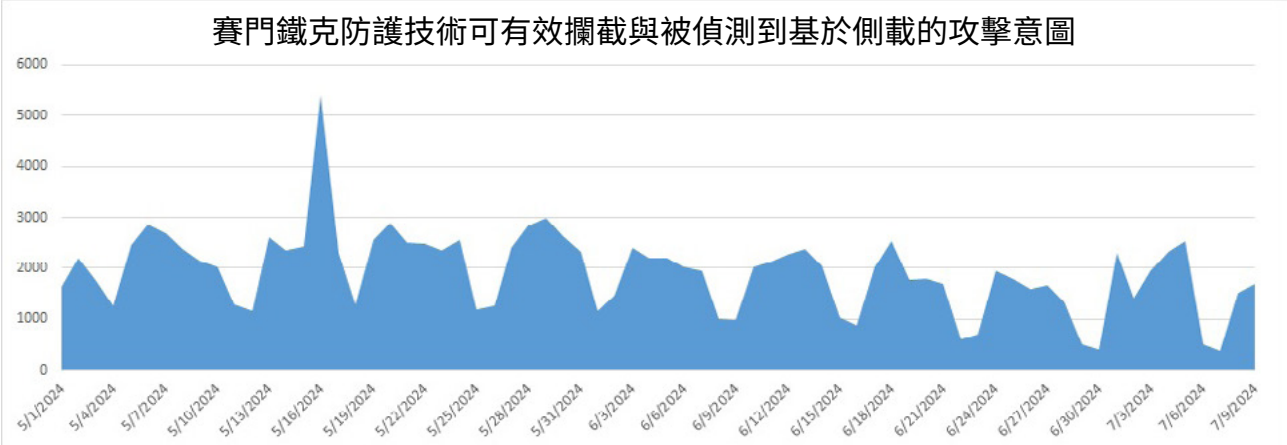
在本公告中，我們將討論與網路安全領域相關的側載問題。MITRE 在 T1574.002 中將側載攻擊定義為一種 (搜尋順序) 劫持執行流程，它利用 Windows 應用程式載入 DLL 的伎倆。攻擊者將惡意 DLL 存放在他們知道作業系統會搜尋的位置，以便將合法檔案載入到記憶體中執行。但是，當與該檔案相關的應用程式運行時，它會載入攻擊者的 DLL，而不是合法的 DLL，進而執行惡意程式碼。由於採用這種技術，如果有人在遭入侵的電腦上尋找惡意程序，很可能找不到。惡意 DLL 會有效地隱藏在合法名稱的檔案程序中，以執行攻擊者的預期的操作。這不僅使惡意程序難以被發現，也讓惡意軟體在系統重啟後依然存在。它也可用來協助權限升級。這種有效的攻擊技術已經使用很長時間，目前仍在使用。

惡意程式載入器和 DLL

下面列出一些試圖使用 DLL 側載技術惡名昭彰的惡意軟體檔名

合法可執行檔	可執行檔發佈者	側載 DLL 檔案
vlc.exe	VideoLAN	libvlc.dll
iTunesHelper.exe	Apple	CoreFoundation.dll
kinit.exe	Oracle Corporation	jli.dll
ccsvchst.exe	Symantec	cci80u.dll
vmtoolsd.exe	VMware, Inc.	glib-2.0.dll
atkexComSvc.exe	ASUSTeK Computer, Inc.	AsIO.dll
notepad++.exe	Don Ho	mimeTools.dll
DTShellHlp.exe	Disc Soft Ltd.	DTCommonRes.dll
KeyScrambler.exe	QFX Software Corporation	KeyScramblerIE.dll

最近的側載攻擊趨勢



請注意，圖表中包括被攔截與被偵測到。已偵測是否會產生如上區塊取決於產品的特定配置／設定，因為它與 Adaptive 和 EDR 等防護技術有關。

我們最近撰寫多份關於利用側載的威脅公告，可參考包括以下內容：

- Trojan.Darkgate，一種同時具有惡意竊密和檔案加密功能的惡意軟體。
  - 每周防護公告第十四頁--2024/05/03 最近傳播 DarkGate 惡意程式的垃圾郵件行動
  - 每周防護公告第四頁--2024/04/29 DarkGate惡意程式載入器仍在大肆傳播
- Trojan.Casbaneiro 一種銀行金融木馬惡意軟體，透過惡意垃圾郵件行動傳播，誘騙使用者點擊 HTML 附件。
  - 每周防護公告第四頁--2024/05/29 Metamorfo 銀行木馬
- Trojan.Wikiloader 一種惡意程式下載器，可將單獨的惡意軟體有效酬載注入到目標電腦上。
  - 原廠防護亮點分享--又見 WikiLoader 惡意程式載入器強勢回歸

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.Darkgate
- Trojan.Darkgate!gen7
- Trojan.Casbaneiro!gen1
- Trojan.Wikiloader!gen2
- Trojan.Sysilod!gen1
- Trojan.Sysilod!gen2
- Trojan.Dllhijack!gen2
- Trojan.Dllhijack!gen3
- Trojan.Dllhijack!gen4

基於行為偵測技術(SONAR)的防護：

- SONAR.DllHijack!gen2
- SONAR.DllHijack!gen3
- SONAR.DllHijack!gen4
- SONAR.DllHijack!gen5
- SONAR.SuspLoad!g55
- SONAR.SuspLaunch!g373
- SONAR.SuspLaunch!g374
- SONAR.SuspLaunch!g375
- SONAR.SuspLaunch!g376
- SONAR.SuspLaunch!g377
- SONAR.SuspLaunch!g378
- SONAR.SuspLaunch!g379
- SONAR.SuspLaunch!g380
- SONAR.SuspLaunch!g381
- SONAR.SuspLaunch!g382
- SONAR.SuspLaunch!g383
- SONAR.SuspLaunch!g384
- SONAR.SuspLaunch!g385

自適應防護技術(包含於SESC)：

- ACM.Lsass-LoadDll!g1

基於端點偵測與回應(EDR)：

- IF.HijackExecFlow!g4

欲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。
欲瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
賽門鐵克的端點安全企業版 (SESE)／端點安全完整版(SESC)內含防護 IOS／Android 的最先進防護技術，請點擊此處瀏覽更完整的資訊。
欲瞭解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

2024/07/08

熱門的自黏便箋方便小工具安裝程式，被植入木馬以大肆散播惡意軟體

網路威脅聯盟 (Cyber Threat Alliance，CTA) 成員：Rapid7 最近的一份報告披露，熱門的自黏便箋方便小工具『Notezilla』安裝程式已被植入木馬，以傳播惡意軟體。攻擊者對安裝程式進行重新封裝，以便暗度惡意竊密程式以竊取瀏覽器憑證、加密錢包、剪貼簿內容和按鍵記錄，以及下載和執行附加有效酬載的能力。

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：

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 Horse
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.C

2024/07/08

進階持續威脅(APT)駭客集團：Water Hydra近期發動開採濫用CVE-2024-21412漏洞的網路攻擊行動

2024 年初，威脅研究人員揭露透過偽造軟體安裝程式開採濫用 CVE-2024-21412 漏洞散播 DarkGate 惡意軟體的行動。之後，進階持續威脅 (APT) 駭客集團：Water Hydra 也開採濫用相同的漏洞，繞過 SmartScreen，使用 DarkMe RAT 針對金融交易商。

最近報告發現一起開採濫用 CVE-2024-21412 漏洞的新行動。它始於包含指向符合 WebDAV 網頁檔案管理標準的捷徑檔之釣魚郵件。點擊這些鏈結會觸發 PowerShell 和 JavaScript 等腳本，進而部署 Lumma 和 Meduza Stealer 等惡意有效酬載，以擷取受害者的敏感資訊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-CPE!g2
- ACM.Mshta-Cmd!g1
- ACM.Mshta-CPE!g1
- ACM.Mshta-Http!g1
- ACM.Mshta-Ps!g1
- ACM.Ps-Http!g2
- ACM.Ps-Mshta!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MSHta!g1
- SONAR.SuspScript!g5

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen111
- Trojan Horse
- Trojan.Gen.MBT
- WS.SecurityRisk.4

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：

- Audit: Suspicious Process Accessing Lets Encrypt Certified Site
- Web Attack: Webpulse Bad Reputation Domain Request

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克的重要主機防護系統：DCS～Data Center Security 其出廠就內建的系統鎖定政策，可以防止在相關程序的伺服器上被部署可疑的 web shell。
- DCS 強化政策主要在防範此漏洞。該政策將攔截與 webdev 伺服器的對外連接，以防止下載 LNK 檔。即使將 LNK 檔下載或複製到機器上也無法啟動 PowerShell，進而在初始階段有效阻止這種攻擊。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/07/08

異軍突起～採用Golang語言所撰寫的新型殭屍網路：Zergeca

在真實網路情境上觀察到一個採用 Golang 語言所撰寫、被稱為 Zergeca 的新殭屍網路。除了發動分散式阻斷服務攻擊 (DDoS) 外，該殭屍網路還具有其他一些功能，例如：基於代理的混淆。它掃描網路，查找存在未修補漏洞的系統，以便進行遠端駭客攻擊，它還具有反向 shell 功能，使攻擊者能夠繞過網路安全，收集敏感的系統資料。值得注意的是，Zergeca 利用 DNS-over-HTTPS (DoH) 對其 C&C 伺服器進行網域名稱系統 (DNS) 解析，並利用鮮為人知的 Smux 程式庫進行 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Linux.Mirai
- Linux.Trojan
- Trojan.Gen.NPE
- WS.Malware.1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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。

2024/07/07

謹防Orcinius木馬透過Dropbox和Google文件發起的多階段攻擊

謹防 Orcinius 木馬惡意軟體！據報導，這是一種多階段木馬，利用 Dropbox 和 Google Docs 作為其攻擊媒介的一部分，下載二階有效酬載。攻擊媒介始於一個 Excel 試算表，其中包含一個使用『VBA stomping』技術修改過的 VBA 巨集。執行後，該巨集就會運行，掛接到 Windows 作業系統以監控和截取按鍵和使用中視窗。

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.Downloader!gen60
- ISB.Downloader!gen68
- X97M.Zorex
- Web.Reputation.1
- WS.Malware.1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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。

2024/07/07

Neptune(*海王星)惡意竊密程式

研究人員發現一種名為 Neptune(*海王星) 的惡意竊密程式。這種惡意軟體會無聲無息地潛入系統，擷取密碼和財務資料，並謹慎地運行和自我定制，以逃避檢測。據觀察，該惡意軟體透過 GitHub 公開發佈，允許攻擊者自由修改和傳播。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Enc!g1
- ACM.Ps-Reg!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Malscript!gen9
- Scr.Malcode!gen129
- SMG.Heur!gen
- WS.Malware.1

基於機器學習的防禦技術：

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

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的好用資源。

保安資訊連絡電話：**0800-381-500**。