保安資訊--本周(台灣時間2024/05/17)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 7,700 台受保護端點上總共阻止了 5,460 萬次攻擊。這些攻擊中有 82.7% 在感染階段前就被有效阻止：**(2024/05/13)**

- 在**10萬4,400**台端點上，阻止了**1,830**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**13萬8,100**台端點上，阻止了**1,160**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬4,300**台**Windows**伺服主機上，阻止了**820**萬次攻擊。
- 在**6萬3,900**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,600**台端點上，阻止了**79萬9,200**次嘗試掃描在**CMS**漏洞。
- 在**4萬5,300**台端點上，阻止了**140**萬次嘗試利用的應用程式漏洞。
- 在**18萬2,800**台端點上，阻止了**420**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬1,100**台端點上，阻止了**130**萬次加密貨幣挖礦攻擊。
- 在**9萬8,500**台端點上，阻止了**820**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**417**台端點上，阻止了**6萬4,800**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 15 萬 3,000 個受保護端點上阻止了總計 580 萬次攻擊。**(2024/05/13)**

- 使用網頁信譽情資，在 **139.6K** 個端點上阻止 **520** 萬次攻擊。
- 攔截 **30.3K** 個端點上 **513.1K** 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 **10.4K** 個端點上攔截 **112.9K** 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 **362** 個端點上攔截 **15.8K** 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。

2024/05/16
Synapse勒索軟體

Synapse 是一款用 C 語言撰寫的勒索軟體，可以加密本機、抽取式硬碟和網路分享所有的檔案，並能傳播到網路上的其他系統。被加密檔案的副檔名為 .Synapse。此外，還會留下檔名為 [random_string].README.txt 的贖金支付說明。該勒索軟體能夠收集系統資訊和加密統計資料，並將資料滲出到遠端 C&C 伺服器。受害者會得到一個網址 (託管在 Tor 網路上) 作為聯繫方式。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen14
- SONAR.Ransomware!g38
- SONAR.SuspWrite!g6
- SONAR.TCP!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：

- Trojan Horse

- 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

2024/05/16
駭客組織Storm-1811發動語音網路釣魚攻擊，透過微軟的遠端協助工具「快速助手(Quick Assist)」進行技術支持詐騙

據報告，駭客組織 Storm-1811 發動語音網路釣魚攻擊，濫用微軟的用戶端管理工具：「快速助手 (Quick Assist)」來進行網路釣魚 (語音釣魚)，這也算是技術支持詐騙的社交工程攻擊。Quick Assist 可讓人員透過遠端連線與另一個人共用其 Windows 或 macOS 裝置的應用程式。您的支持人員可以使用它從遠端連線到使用者的裝置，然後檢視其顯示、建立批注或完全控制。如此一來，他們可以針對技術問題進行疑難解答、診斷，並直接在其裝置上提供指示給使用者。一旦用戶授予完全控制權，威脅者就會執行腳本下載批次檔，目的是在整個網路中部署 Black Basta 勒索軟體作為最終有效酬載。

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：

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。

2024/05/16
Springtail威脅組織在攻擊中引入全新Linux後門程式

在最新發佈的報告中，賽門鐵克的威脅獵手資安團隊揭示最近發現由北韓國家級駭客間諜組織：Springtail (也稱 Kimsuky) 所開發的全新 Linux 後門程式。該組織與最近一次針對南韓某機構的網路攻擊行動所引用的惡意軟體有所關連。該行動利用木馬程式工具偷渡全新 Linux 後門。

在我們部落格系列的專家文章中有更詳細資訊可供參考：Springtail：在工具包中新增Linux後門。

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-Rd32!g1
- ACM.Ps-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g13
- SONAR.SuspLaunch!g266

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：

- Infostealer
- Linux.Gomir
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

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

2024/05/15
全新Cuttlefish(*墨魚)的惡意程式

據報導，一種名為 Cuttlefish 全新惡意軟體幾乎為感染小型辦公室／居家工作室(SOHO)和企業級的網路路由器而設計，其目的是監控其網路的進出流量，並會以一種不引人注意的方式滲出與身份驗證相關的資訊，例如：用戶名、密碼和權杖等。它還能引進更多有效酬載。

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：

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.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: Malicious Shell Script 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。

2024/05/15
Remcos遠端存取木馬(RAT)借力PrivateLoader來提升威脅力道

Remcos 是一種遠端存取木馬 (RAT)，可對遭入侵系統進行未經授權的遠端控制和監視。最近發現 Remcos RAT 搭配 PrivateLoader (一種模組化多功能的惡意程式下載器) 來增強其功能，並能在受害者機器上常駐。利用透過 VB 腳本、登錄檔 (registry) 和建立服務，以不定期重新啟動惡意軟體，該惡意軟體可以徹底滲透系統、逃避檢測並向其 C&C 伺服器回報統計資料。

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：

自適應防護技術(包含於SESC)：

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

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDataRun

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- 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。

2024/05/15
惡意的Minecraft遊戲模組，正從Windows玩家的電腦收集資料

許多遊戲玩家喜歡使用自訂模組來增強遊戲體驗，例如：那些提供 Windows 無邊界的自訂模組。該功能可實現多工處理和應用程式之間的無縫切換，簡化遊戲錄製等任務。

然而，據報導，一個分享 Minecraft 內容的開源平臺上上架一個惡意遊戲模組。該遊戲模組內藏惡意軟體，用意在獲取各種源於 Chromium 類型的瀏覽器和其他應用程式所儲存的資料。獲取的資料可能包括帳戶權杖、儲存的密碼、銀行資訊、位址等。此外，惡意軟體還會將使用者機器的識別資訊發送到 Discord webhook。值得注意該惡意軟體專門針對 Windows 系統，目前已從該平臺上被移除。

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：

- Infostealer
- WS.Malware.1

2024/05/15
GitCaught網路攻擊行動中，傳播的惡意軟體有macOS平台上常見 Atomic 惡意竊密程式(AMOS)的蹤影

據報導，最近一個命名為 GitCaught 的網路攻擊行動，針對包括 macOS 在內的各種平臺傳播多個惡意竊密程式的有效酬載。傳播的惡意軟體包括 Atomic Stealer(AMOS)、Vidar Stealer、Lumma 和 Octo 銀行木馬。攻擊者一直利用上傳在 Github 上假冒的設定檔和資源庫，提供偽裝成各種流行應用程式的軟體二進位檔案。此行動幕後的威脅者也一直在濫用基礎的網路設施，包括 Filezilla FTP 伺服器來傳輸惡意軟體。

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(SONAR)的防護：

- SONAR.TCP!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：

- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- Trojan Horse
- 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。

2024/05/15
借重PureCrypter惡意程式載入器，Mallox勒索軟體傳播行動勢如破竹

PureCrypter 惡意程式載入器最近涉入一起惡意行動，被用於傳播 Mallox 勒索軟體的有效酬載。據報導，在攻擊的初始階段，攻擊者會對易受攻擊或配置錯誤的 MS-SQL 伺服器進行暴力攻擊。PureCrypter 惡意程式載入器是一種惡意軟體即服務 (MaaS)，可以同時服務許多駭客圈的客戶。據瞭解，Mallox 勒索軟體的營運商在過去攻擊中採用雙重勒索戰術，因此遞送有效酬載也可能具有在加密前先滲出使用者資料的能力。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Untrst-FlPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g230
- SONAR.SuspLaunch!g341

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.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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：

- System Infected: Bad Reputation Process Request 4
- System Infected: Trojan.Backdoor Activity 634
- 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。

2024/05/15

夾帶被下毒Word文件檔，惡意郵件散播行動正在大肆傳染DanaBot惡意程式

據觀察，最近一次傳播 Danabot 惡意程式的垃圾郵件散播行動，是夾帶被下毒的 Word 文件檔散播，該附件檔內含惡意的外部鏈結，如果點擊該鏈結，就會啟動攻擊鏈的序曲，下載其他可執行檔，包括命令提示字元和 PowerShell。此過程最終會導致 iu4t4.exe(Danabot) 和 rundll32.exe 等有效酬載的下載，這些有效酬載的作用是收集敏感的使用者和系統資訊。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1
- ACM.Ps-Rd32!g1
- ACM.Rd32-RLsass!g1
- ACM.Untrst-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1
- SONAR.TCP!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：

- CL.Downloader!gen20
- ISB.Downloader!gen69
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- 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：

- System Infected: Trojan.Danabot Activity 3

2024/05/14
防護亮點：SONAR同時採用多重先進技術防護「就地取材(LOTL)」程序和兩用工具的威脅

何謂 Symantec Endpoint Protection 中的行為分析 (SONAR)？

行為分析這種即時防護，可在電腦上執行應用程式時偵測潛在惡意的行為。行為分析使用啟發式技術及信譽資料來偵測新出現和不明威脅。行為分析提供「零時差」防護，因為它會在傳統病毒和間諜軟體偵測定義檔建立前偵測惡意行為，從而解決威脅。行為分析可為您的用戶端電腦提供額外的防護等級，並能與您現有的病毒和間諜軟體防護、入侵預防、記憶體攻擊緩和以及防火牆防護相輔相成。行為分析使用啟發式系統，該系統會運用賽門鐵克的線上威脅情資網路，並且對用戶端電腦進行主動型本機監視，以偵測新出現的威脅。行為分析也會偵測您應監視之用戶端電腦上的變更或行為。

SONAR

賽門鐵克的行為分析技術被稱為「SONAR」，我們將在本防護公報中使用這個專用術語。SONAR 可透過追蹤跨檔案譜系、登錄檔、程序譜系、服務、執行緒插入、DLL 側載和程序空白技術等複雜攻擊鏈。它還能追蹤攻擊鏈中合法程序的使用情況。其中包括「就地取材 (LOTL)」程序和兩用工具。一旦識別出惡意向量 (方法／途徑／酬載)，SONAR 就會刪除惡意檔案、登錄項目和程序，並終止攻擊中使用任何 LOTL 和兩用工具的程序，進而瓦解整個攻擊鏈。

AutoIt：凸顯「就地取材(LOTL)」程序和兩用工具的資安風險

AutoIt 是使用於 Windows 平台的自動腳本語言，可用來建立自動化執行腳本的免費自動化工具。一些惡意軟體家族 (例如：Darkgate 和 Astaroth) 在攻擊鏈中安裝並濫用 AutoIt，從可信任的協力廠商程式中執行惡意腳本。這些基於腳本的有效酬載通常都經過混淆化 (Obfuscation)，以逃避靜態偵測技術的偵測，但無法輕易躲過行為偵測技術的檢測。

SONAR 採用多重技術防護「就地取材 (LOTL)」程序和兩用工具的威脅：

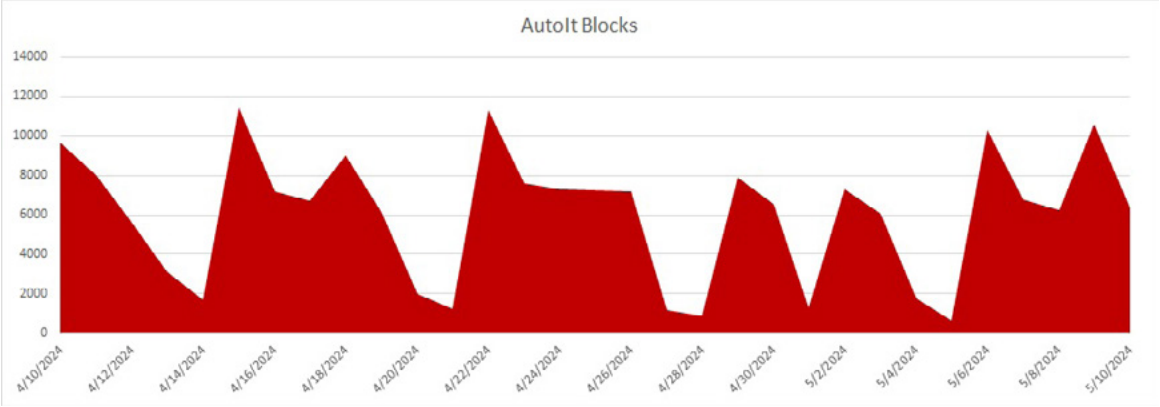
1. 我們追蹤程序的起源，例如二進位檔案是如何被導入以及程序是如何啟動的。它可觸

發對可疑程序起源的行為檢測，例如：AutoIt 由不尋常的父系程序啟動 (例如：SONAR.SuspBeh!gen804)，或 AutoIt 被掏空 (例如：SONAR.SuspStart!gen18)。

2. 我們監控攻擊鏈中所有程序的所有行為。AutoIt 可被運用於多種惡意情境，包括下載額外的有效酬載 (例如：SONAR.Dropper!gen2) 和啟動程序，以進一步實施攻擊 (例如：SONAR.SuspLaunch!g220)。
3. 我們確保終止所有涉入攻擊的 LOTL 和兩用程序。遭濫用的 AutoIt 程序往往就是攻擊鏈中的關鍵。若僅刪除其他被檢測到的程序／元件而不刪除 AutoIt 程序，會使系統受到進一步攻擊和再次感染。

無論我們是直接從行為偵測技術檢測到遭濫用的 AutoIt 程序，還是檢測到攻擊的其他元件 (例如：賽門鐵克靜態資料掃描檢測到的惡意檔注入，或賽門鐵克網路層入侵防禦技術 IPS 檢測到 C&C 流量)，SONAR 都會追蹤遭濫用的 AutoIt 實例，可以避免攻擊鏈初始階段的星星之火，延燒成重大資安事件的燎原大災難。(例如：AGR.Terminate!g2)。

SONAR 每天攔截數千次源於 AutoIt 遭濫用的攻擊



SONAR 有效防護 AutoIt 遭濫用的實例，只是我們全球資安專家團隊日以繼夜分析的無數威脅向量 (方法／途徑／酬載) 和惡意軟體家族中的其一例子。最新 SONAR 行為保護技術透過每日數次的持續更新。

要了解更多有關 Symantec Endpoint Protection 行為分析技術 SONAR 的資訊，請點擊此處。
要了解有關啟用 SONAR 的更多資訊，請點擊此處。
SONAR 還與 Symantec Cloud Sandbox 整合。要了解 SONAR 和 Symantec Cloud Sandbox 如何協同工作來檢測 Monster Stealer，請點擊此處。

2024/05/14
借力於Phorpiex殭屍網路，駭客組織散播大量的LockBit Black勒索軟體

據報導，借力於 Phorpiex 殭屍網路大規模傳播能力，駭客組織可以短時間內發動散播大量 LockBit Black 勒索軟體的網路攻擊行動。Phorpiex 營運模式屬於惡意軟體即服務平臺，十多年來在駭客圈已佔有一席之地，更積累大量客戶群。自 2018 年以來，Phorpiex 一直參與資料滲透和勒索軟體傳播等行動。儘管多年來有人試圖破壞其運作，但該殭屍網路架構依舊持續存在。

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.Untrst-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen82
- SONAR.Ransom!gen113
- SONAR.SuspBeh!gen821

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：

- Ransom.Lockbit!g6
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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。

2024/05/14

Dracula*德古拉(又稱Samurai*武士)惡意竊密程式

Dracula (又稱 Samurai) 惡意竊密程式，歸屬於 Amnesia Team(又名 Cerberus) 駭客組織所有。該駭客組織以使用其他各種惡意竊密程式而聞名，包括 Aurora、Lumma、Redline 和 Rhadamanthys 等。攻擊者利用 Dracula 從受害者機器中竊取大量機密資訊，包括憑證、銀行資訊等。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.Stealer!gen1
- SONAR.TCP!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：

- Backdoor.Ratenjay
- Trojan Horse
- 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.A!400
- Heur.AdvML.A!500
- 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：

- System Infected: Trojan.Backdoor Activity 568
- 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。

2024/05/14
WaveStealer：透過訊息平台傳播的全新惡意竊密程式

WaveStealer 是一種新出現的高度精密惡意軟體，正透過 Telegram 和 Discord 等平臺上傳播，讓用戶低價購買。該惡意軟體偽裝成電玩遊戲安裝程式，主要在從遭入侵系統中擷取各類敏感性資料。它的目標是網路瀏覽器、加密貨幣錢包、信用卡號以及與 Telegram 和 Discord 等訊息平台相關的資料。此外，WaveStealer 還能截取螢幕截圖，進而增強其資料滲透能力。

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 Horse
- Trojan.Gen.MBT
- Trojan.Malscript!inf
- 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：

- Audit: Connection to file.io
- 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。

2024/05/14
借力Google廣告， FIN7惡意軟體傳播行動，如虎添翼

據報導，一個由威脅者 FIN7 發起利用 Google 廣告的惡意軟體活動已在網路上出現。攻擊者利用欺騙性網站偽裝成 AnyDesk、WinSCP、BlackRock、Asana、Concur 和 Google Meet 等知名品牌。這些網站的瀏覽者通常是透過贊助商 Google 廣告來瀏覽，他們會遇到假的快顯視窗，讓他們下載看似瀏覽器擴展的內容。然而，下載的有效載荷實際上是一個 MSIX 檔，這是一種 Windows 應用程式的封裝格式，它為感染鏈的後續階段提供 NetSupport RAT 和 DiceLoader。

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：

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
- 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。

2024/05/13
Beast(*野獸)勒索軟體和Vidar惡意竊密程式偽裝成文件檔傳遞

在最近網路攻擊行動中，有人利用侵犯版權警告和求職履歷等檔案傳播勒索軟體和惡意竊密程式。最初感染源自一封帶有外部惡意連結的釣魚郵件，點擊後會下載一個壓縮檔。解壓縮後，會出現兩個可執行檔，這些檔案被證實就是 Beast(*野獸) 勒索軟體和 Vidar 惡意竊密程式。

Beast 勒索軟體是 Monster 勒索軟體的進化版本，有兩種類型：一種會加密檔案後再加以壓縮，並且內含勒索 (贖金支付) 說明『[遭入侵電腦 ID].BEAST.zip』壓縮檔。另一種只是添加『[遭入侵電腦 ID].BEAST』。

Vidar 惡意竊密程式的目標是擷取 cookie、瀏覽器歷史記錄或儲存憑證等瀏覽器資料，但它也可以擷取加密貨幣錢包、FTP、電子郵件或聊天應用程式中的資訊。

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：

- 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

2024/05/13
菲律賓最大的電子支付系統：GCash的用戶正遭受簡訊釣魚之苦

行動錢包／手機錢包的便利性和易用性，改變金融業的樣貌，同時也為網路犯罪分子提供有利可圖的目標，因為賽門鐵克繼續觀察到世界各地出現的大量網路釣魚行為。

最近一個例子中，一名駭客以菲律賓的行動／手機使用者為目標，覬覦透過引誘來騙取他們 GCash 帳戶 (菲律賓最大電子支付系統) 相關的敏感資訊。這些資訊可能會導致詐騙和後續潛在的經濟損失。

觀察到惡意簡訊內容樣本：

- Good day from GCash, Your account will be restricted due to unrecognized login attempts, we request you to verify your account to avoid account deactivation within 24 hours. Verify here: [malicious URL].
(中文意思：您好，這是來自 GCash 的通知，您的帳戶將因登錄失敗次數過多而無法使用，請您在 24 小時內驗證您的帳戶以避免帳戶停用。點此驗證：[惡意的網址]。

這種社交工程伎倆，即警告用戶他們 GCash 帳戶因登錄失敗次數過多而無法使用，是網路犯罪分子使用的一種巧妙而有效方法。它利用用戶對失去財務資源存取權的恐懼和緊迫感。用戶在恐慌中為了避免帳戶受到限制，更有可能匆忙行事，忘記平時的謹慎。

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。WebPulse 已知道此次活動中使用假冒的 GCash 域名。

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。

2024/05/13
Trinity勒索軟體

根據資安公司 Cyble 發佈最新研究報告，Trinity 是新發現的勒索軟體，極可能是『2023Lock』勒索軟體的後繼升級版本。該惡意軟體會加密使用者檔案，並冠上『.trinitylock』副檔名。據報導，Trinity 勒索軟體還與另一個名為 Venus 勒索軟體共用部份程式碼。Trinity 背後的威脅者採用雙重勒索手段，他們會先行竊取機密檔檔，並威脅要公開發佈這些檔案。

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(SONAR)的防護：

- SONAR.Ransomware!g1
- SONAR.Ransomware!g3

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：

- Ransom.Generic.1
- Web.Reputation.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- Heur.AdvML.C

2024/05/13
惡意郵件散播行動採用多重腳本來傳播ASyncRAT惡意程式

最近觀察到的網路攻擊行動中，有多個腳本被用於傳播 ASyncRAT 惡意程式的有效酬載。透過 HTML 電子郵件附件啟動，受害者會受到各種非 PE 檔案的攻擊，以傳播和建立 ASyncRAT 的常駐功能。攻擊會下載一個 Windows 指令檔 (WSF)，然後啟動一個 VBS 檔，負責進一步執行。攻擊的後期部分由 JS、PowerShell 和批次腳本元件執行。

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-Rd32!g1
- ACM.Ps-Wscr!g1

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.Dropper
- Trojan.Gen.MBT
- 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。

2024/05/13
Black Basta勒索軟體攻擊醫療保健行業

賽門鐵克安全回應中心 (Symantec Security Response) 瞭解到網路安全暨基礎設施安全局 (Cybersecurity & Infrastructure Security Agency，CISA)、聯邦調查局 (Federal Bereau of Investigation，FBI) 與跨州資訊共享分析中心 (Multi-State Information Sharing and Analysis Center，MS-ISAC) 等多個美國政府單位。最近聯合發出警報，稱觀察到多起 Black Basta 勒索軟體涉入的目標式攻擊行動。該惡意軟體至少在 2022 年就已被發現，並被利用針對關鍵基礎設施 (包括醫療保健和公共衛生(HPH)部門) 的一系列攻擊行動。Black Basta 是一種勒索軟體即服務 (RaaS)，主要透過網路釣魚或利用已揭露的漏洞傳播。這種惡意軟體幕後的攻擊者通常採用雙重勒索戰術，不僅加密使用者檔案，還竊取用戶檔案並威脅不支付贖金就會公開被盜資料。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-TskReg!g1
- ACM.Rcln-Lnch!g1

- ACM.Untrst-RunSys!g1
- ACM.Vss-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.RansomBasta!g3
- SONAR.Ransomware!g19
- SONAR.Ransomware!g30
- SONAR.SuspBeh!gen6
- SONAR.SuspBeh.C!gen1
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g138
- SONAR.SuspLaunch!g250
- 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：

- Downloader
- Ransom.Basta
- Ransom.Basta!g2
- Ransom.Basta!g3
- Ransom.Basta!gm
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.6
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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：

- System Infected: Trojan.Backdoor Activity 634
- 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。

2024/05/13
全新挖礦木馬被命名為：Hidden Shovel

研究人員透過網路安全監測發現一種名為『Hidden Shovel』的新型挖礦木馬。該木馬最初發現於 2023 年 11 月，經過多次升級，目前版本為 3.0。Hidden Shovel 主要特徵包括強大的隱蔽性、反分析機制、DLL 劫持後門和 shellcode 注入功能。

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：

- ISB.Downloader!gen173
- ISB.Heuristic!gen5
- ISB.Heuristic!gen39
- ISB.Heuristic!gen50
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.Malware.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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 (29565)

2024/05/10
CVE-2024-24506--線上問卷平台LimeSurvey的社群／自建版存在跨網站腳本(XSS)漏洞

CVE-2024-24506 是一個最近披露的跨網站腳本 (XSS) 漏洞，影響線上問卷平台 LimeSurvey 的社群／自建版的 5.3.32 版本。該漏洞是由於管理員電子郵位址欄位的用戶輸入資料驗證瑕疵所引起。該漏洞如果被成功開採濫用，遠端攻擊者可透過管理員電子郵位址參數來插入及執行任意程式碼。

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: LimeSurvey Community 5.3.32 Stored XSS CVE-2024-24506

2024/05/10
CVE-2024-1313--開源的分析暨視覺化應用Grafana，存在不安全的物件授權漏洞(Broken Object Level Authorization，BOLA)

CVE-2024-1313 是最近被揭露影響開源的分析暨視覺化應用 Grafana 的不安全物件授權漏洞(Broken Object Level Authorization，BOLA)。該漏洞如果被成功開採濫用，可能會導致未經授權的存取和儀表板資料被洩漏。沒有權限的攻擊者可能會繞過授權並刪除 Grafana 儀表板快照。原廠已經釋出該漏洞的修程式。

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：

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: Grafana BOLA Vulnerability CVE-2024-1313

2024/05/10
Ivanti的Pulse Secure SSL VPN系統存在的漏洞遭開採濫用，散播Mirai殭屍網路

今年 1 月，Ivanti 報告影響 Ivanti Connect Secure SSL VPN 和 Ivanti Policy Secure Gateway 基礎設施防護閘道的兩個漏洞：CVE-2023-46805(身份驗證繞過) 和 CVE-2024-21887(命令注入)。在真實網路情境已有開採濫用，這些具有遠端程式碼執行功能的 Ivanti Pulse Secure 漏洞，透過 shell 腳本來傳播 Mirai 殭屍網路的案例。這種漏洞利用能夠傳遞惡意軟體，輕而易舉就入侵整個網路，構成重大威脅。

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：

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：

- Linux.Mirai!g2
- 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：

- [34495] Web Attack: Ivanti ICS CVE-2023-46805
- [34496] Web Attack: Ivanti ICS CVE-2024-21887

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。

2024/05/10

網路上撿到破解版軟體是災難的開始～Windows和MS Office的破解版／序號產生器傳播惡意軟體

據觀察，有一種惡意軟體散播行動正透過流行軟體的破解版來傳播遠端存取木馬 (RAT) 和挖礦劫持軟體，特別針對 Windows 作業系統和 MS Office 軟體的使用者。惡意軟體一旦安裝，通常會在工作排程程式中建立常駐目的的工作，即使在刪除後也能繼續安裝新的惡意軟體。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Http!g2
- ACM.Ps-Masq!g1
- ACM.Ps-Reg!g1
- ACM.Untrst-RunSys!g1

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：

- Downloader
- ISB.Downloader!gen221
- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Gen.MBT

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。

2024/05/09

惡意軟體Coper遭偽裝成假冒Android平台的Chrome APP，並濫用LiveChat CDN來大肆散播

賽門鐵克每天都會發現 Coper 惡意軟體，偽裝成假冒 Android 平台的 Chrome APP 來散播。這種手法並不新鮮，已經行之多年了。攻擊鏈的初始步驟仍不確定，但最近觀察到 Coper 樣本上架在客戶服務平臺 LiveChat 使用的內容交付網路 (CDN) 上。與 LiveChat 服務相關的檔案保存在該 CDN 傳播，像是客戶和代理在即時聊天會話中共用的圖片、文件和其他多媒體內容。Coper 的功能包括收集敏感資訊、顯示假視窗、欺騙使用者，使其在不知情的情況下洩漏出憑證等。

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：

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

2024/05/09

惡意垃圾郵件行動：上傳到GitHub上受密碼保護的壓縮檔會感染AsyncRAT惡意程式

在過去兩周中，賽門鐵克觀察到一個威脅者利用一種奇特的攻擊鏈向遭入侵系統發送高度混淆的有效酬載。攻擊以包含惡意 PDF、DOCX 或 SVG 檔 (檔名：REMITIRA A TRAVES DEL SERVICIO POSTAL AUTORIZADO.docx、Radicado juridico 23156484.svg 和 99-DEMANDA .docx) 的惡意電子郵件開始。

如果用戶不疑有他被誘騙開啟這些檔案，就會被提示點擊下載連結，以獲取保存在 GitHub 專案上受密碼保護的 ZIP 壓縮檔 (CITACION_DEMANDA.zip)，其中包含假訴訟文件。壓縮檔中包含一個乾淨的 EXE、一個 .AI 和 .EPS 檔，以及一個惡意 DLL，該 DLL 會側載已證實為 AsyncRAT 的最終有效籌載。

在這次行動中，該駭客似乎以哥倫比亞和其鄰國西班牙語系的企業組織為目標。該機構是哥倫比亞司法系統的一個重要機構，負責調查犯罪、起訴罪犯並確保正義得到伸張。

以下是觀察到一些 GitHub 上的惡意網址：

- hxxps[:]//github[.]com/jair1212/codigos/raw/main/CITACION%20DEMANDA[.]zip
- hxxps[:]//github[.]com/brianaf2024/publicidad-abrirl/raw/main/CITACION%20DEMANDA[.]zip
- hxxps[:]//github[.]com/santiagonasar/PUBLICIDAD2/raw/main/CITACION%20DEMANDA[.]zip
- hxxps[:]//github[.]com/Dios1525301/CAMILOEFRQ3R/raw/main/CITACION%20DEMANDA%20JUDICIAL.zip

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)。

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RLsass!g1
- ACM.Untrst-RunSys!g1

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.Gen.MBT
- Trojan Horse
- Trojan.Piedef

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2024/05/03

最近傳播Darkgate惡意程式的垃圾郵件行動

該攻擊行動的初始感染鏈是從一個帶有 HTML 附件的電子郵件開始。該 HTML 檔使用的背景圖片看起來像一個空白的 Microsoft 文件，在該檔案中可以看到如何修復離線檢視的檔案說明。這是企圖誘騙受害者將惡意 PowerShell 程式碼貼到 Windows 終端機。程式碼執行後，將下載一個 HTA 檔案並繼續執行，最終下載一個後續的 ZIP 檔。解壓縮後，它會啟動 AutoIt 的開源自動化引擎，執行 script.a3x 的惡意 AutoIt 腳本，最終載入 Darkgate 木馬。

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-Ps!g1
- ACM.Ps-CNPE!g1
- ACM.Ps-CPE!g2
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AONAR.SuspBeh!gen804

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：

- ISB.Downloader!gen48
- ISB.Heuristic!gen106
- Trojan.Darkgate
- WS.Malware.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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。

2024/02/21

Astaroth、Mekotio和Ousaban？三支金融木馬亂奔駭帳號

最近發現有三種銀行木馬在針對拉丁美洲使用者的資訊中利用惡意 run.app 連結。這些連結會將使用者重導向到一個 MSI，該 MSI 會發送 Astaroth(之後會發送 Ousaban) 或 Mekotio。

觀察到惡意垃圾郵件中出現的主旨內容：

- Advertencia AFIP：Datos de registro desactualizados - Riesgo de bloqueo.
- Aviso de Factura：Pendiente de Autorización
- Factura de Servicios：Detalles Adjuntos
- Factura Mensual：Resumen de Cargos

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(SONAR)的防護：

- SONAR.SuspPE!gen32

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan.Dropper
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

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)。

基於機器學習的防禦技術：

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