保安資訊--本周(台灣時間2024/10/11)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 45 萬 9,100 台受保護端點上總共阻止了 4,770 萬次攻擊。這些攻擊中有 81.9% 在感染階段前就被有效阻止：**(2024/10/07)**

- 在**8萬7,600**台端點上，阻止了**1,430**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**11萬2,200**台端點上，阻止了**840**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬9,800**台**Windows**伺服主機上，阻止了**7萬5,000**次攻擊。
- 在**5萬3,500**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬300**台端點上，阻止了**76萬1,600**次嘗試掃描在**CMS**漏洞。
- 在**4萬6,100**台端點上，阻止了**270**萬次嘗試利用的應用程式漏洞。
- 在**13萬2,100**台端點上，阻止了**280**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5,000**台端點上，阻止了**110**萬次加密貨幣挖礦攻擊。
- 在**9萬2,400**台端點上，阻止了**760**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**468**台端點上，阻止了**4萬3,000**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 18 萬 3,700 個受保護端點上阻止了總計 720 萬次攻擊。**(2024/10/07)**

- 使用網頁信譽情資，在 **174.3K** 個端點上阻止 **680** 萬次攻擊。
- 攔截 **22.4K** 個端點上 **285.6K** 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 **9K** 個端點上攔截 **116.7K** 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 **354** 個端點上攔截 **8.3K** 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。

2024/10/10
Havoc框架

研究人員發現，網路罪犯日益增加採用 Havoc 框架等滲透測試工具來規避安全系統。相較於 Cobalt Strike 或 Metasploit 等其他工具，此工具較少被宣傳與吹捧，因此較難被察覺。Mysterious Werewolf 駭客組織正在使用類似 Mythic 框架的戰略，而模仿冒用合法組織的網路釣魚電子郵件仍是取得未經授權存取的常見策略。

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-Sc!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：

- Scr.Malcode!gen43
- Scr.Malcode!gen104
- Scr.Mallnk!gen3

- Scr.Mallnk!gen13
- Trojan.Gen.NPE.C
- Web.Reputation.3
- 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
- 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。

2024/10/10

借力於CleanUpLoader惡意程式載入器，Rhysida勒索軟體集團，勢如破竹

最近一份報告揭露一個名為「CleanUpLoader」的惡意程式載入器／後門，被以採用雙重勒索戰術而聞名的「Rhysida」勒索軟體集團用來作為初始感染媒介。它通常會偽裝成 Microsoft Teams 或 Google Chrome 等軟體的安裝程式。該惡意程式載入器能與多個命令與控制 (C&C) 伺服器進行通訊，讓 Rhysida 建立常駐能力並執行資料外洩。

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-Rgsvr!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.Gen.MBT
- Trojan Horse

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。

2024/10/10

Ivanti的雲端服務應用程式CSA(Cloud Services Application)有3個零時差漏洞，在真實網路情境已遭開採濫用於發動網路攻擊

Ivanti 已針對最近揭露的三個 Ivanti CSA (雲端服務應用程式) 漏洞發布新的安全公告。報告的漏洞如下：

- CVE-2024-9379--SQL 注入漏洞
- CVE-2024-9380--作業系統指令注入漏洞
- CVE-2024-9381--路徑遍歷漏洞

前兩個漏洞也已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。新漏洞與兩個早先 CSA 漏洞 CVE-2024-8963 及 CVE-2024-8190 一同被開採濫用。成功開採濫用這些漏洞可授予未經驗證的攻擊者管理員權限，可能導致安全措施失效、任意 SQL 語句執行或遠端程式碼執行 (RCE)。原廠已釋出 CSA 的更新版本 (5.0.2)，以修正上述漏洞。

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：

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，預設鎖定政策就可保護底層伺服器免受此漏洞影響，包括防止執行任意指令和限制讀取關鍵作業系統檔案。
- DCS 的網路規則政策可設定為，將應用程式限制為受信任的用戶端。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/10/10

以Lua撰寫的惡意軟體新變種鎖定教育界為攻擊目標

最近以 Lua 撰寫的惡意軟體新變種鎖定教育界為攻擊目標的案例有所激增，特別是針對正在搜尋「遊戲外掛」學生玩家社群中的熱門遊戲發動目標式攻擊。威脅者利用虛假的「遊戲外掛」，誘騙使用者下載此惡意軟體。基於 Lua 的惡意軟體能夠在受感染的系統上常駐，滲出已擷取的機敏憑證資訊，並傳送額外的有效酬載。

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：

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：

- Scr.Malcode!gdn21

- Trojan Horse
- 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.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C
- Heur.AdvML.L

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。

2024/10/09

Horus Protector：新崛起的惡意軟體傳遞服務商

初試啼聲的 Horus Protector 是一家新崛起惡意軟體傳遞服務商，該服務標榜是完全偵測不到 (FUD) 的加密程式，並散佈各種惡意軟體家族，包括 AgentTesla、Remcos、Snake 和 NjRat。該服務使用包含 VBE 指令碼的 .zip 檔散佈惡意軟體，並從使用者的機器收集資訊並傳送至其伺服器。

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：

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
- 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。

2024/10/09

與北韓有關連的威脅份子利用惡意軟體攻擊科技業求職者

2023 年開始《Contagious Interview*傳染性面試》網路攻擊行動是由與北韓有關連的威脅份子所發起。最近觀察到與該行動相關的活動，威脅份子偽裝成人才招募人員，引誘受害者參加設好圈套的的面試。先前使用過惡意軟體的新變種以科技業求職者為目標。BeaverTail 下載器和竊取器負責下載最終的 InvisibleFerret 後門程式的有效酬載。Palo Alto Networks Unit 42 的研究人員發表一份報告，其中包含這項活動的技術細節。

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：

- OSX.Trojan.Gen
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

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

2024/10/08

PhantomLoader惡意軟體載入器，盡其所涉入的網路攻擊行動

PhantomLoader 是一種惡意軟體載入器，會將自己偽裝成某款防毒軟體的合法 32 位元 DLL，最近被發現偽裝成該軟體的真正元件「PatchUp.exe」。據觀察，該惡意軟體載入器採用二進位修補和自我修改技術，將被稱為 SSLoad 採用 rust 程式語言開發的惡意軟體載入記憶體。

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
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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。

2024/10/08

惡意廣告散播行動，同時傳遞Windows和Mac平台上惡意程式的有效酬載

最近發表一份報告指出，廣告商正在推送與 Slack--團隊溝通平台或 Notion--數位管家等實用軟體的相關廣告，引誘下載惡意軟體的有效酬載。廣告商註冊在現有企業名下，並發佈針對 Windows 和 Mac 使用者的廣告。經過多次重導向後，使用者會下載偽裝成廣告軟體的惡意竊密軟體。

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：

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
- 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。

2024/10/08

防護亮點：惡意程式載入器來來去去，唯有GuLoader「屹立不倒」，也唯有賽門鐵克用戶可以「臨危不亂」

在網路犯罪的生態圈，惡意程式載入器已成為推動地下經濟的重要工具。這些惡意程式是傳送各種惡意軟體的切入點，從勒索軟體、木馬程式到惡意竊密程式，不一而足。網路罪犯利用對這些工具的需求，在暗網論壇上出售或出租這些工具，使大規模攻擊能夠同時感染數千個系統。隨著時間的推移，我們看到惡意程式載入器來來去去 (以下僅列出部分清單)，但 GuLoader 從一開始出現就具有獨特的持久性，可以說是當今威脅環境中最長壽的惡意程式載入器之一。

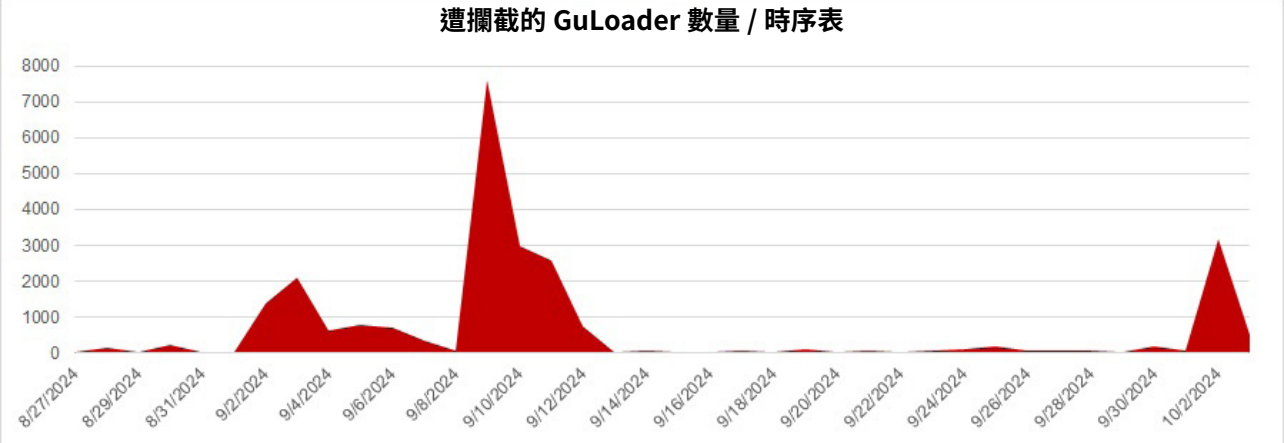
- GuLoader (2019年至今)

- Emotet (2014-2021 年，2022 年曾短暫重現)
- Dridex (2014 年至今)
- BazarLoader (2020 年至今)
- Zloader (2016-2022)
- TrickBot (2016-2020)
- Nemucod (2015-2016)
- Upatre (2013-2015)
- Andromeda/Gamarue (2011-2017)
- Pony (2013-2015)
- Smoke 惡意程式載入器 (2011 年至今)
- RIG 洞利用工具包 (2014-2018)
- Nymaim (2013-2017)

過去幾年來，GuLoader 的攻城掠地確實讓它躍居引領網路安全成為頭條新聞的要角。自 2019 年首次出現以來，這種精密複雜的惡意程式載入器已經成為網路罪犯最喜歡的工具，廣受駭客集團和單獨的攻擊者所採用。它有能力靈活應對各種情境和迴避技術使其成為傳送各種類型惡意軟體的多功能武器，幾乎可以滲透所有行業的組織。無論是在醫療保健、金融、政府或小型企業，GuLoader 已被部署到全球眾多領域，證明它有能力影響網路犯罪生態圈的市場的深度與廣度。

GuLoader 的主要攻擊媒介仍然是電子郵件，但隨著時間的推移，其作案手法已演變為各種傳送方式。最初它依賴惡意附件，現在已擴展到也使用惡意網址、內嵌惡意網址的 PDF、HTML 檔案，以及上架在 Google Drive 或 OneDrive 等雲端服務上的二進位檔案。

在過去幾週，賽門鐵克已經挫敗多起 GuLoader 所涉入的攻擊行動。GuLoader 活動的最高峰出現在 2024 年 9 月 9 日，超過 7,000 起封鎖數量。在這個高峰之前，9 月 5 日和 6 日出現較小幅的增加，顯示在 9 月 9 日高峰之前活動逐漸增加。高峰之後，活動水準仍然很高，但逐漸下降。在 9 月 10 日和 12 日前後出現明顯的激增。2024 年 10 月初再次復甦，再次在 10 月 2 日達到高峰，封鎖數量約為 3200 個。



這些攻擊同時被賽門鐵克多種解決方案的多層次防護技術所攔阻，包括郵件安全雲端服務 -- Email Security.cloud (ESS)、賽門鐵克端點安全完整版--Symantec Endpoint Security Complete (SESC)

以及賽門鐵克端點偵測與回應--Symantec Endpoint Detection & Response (EDR)。Cynic 是賽門鐵克的雲端沙箱解決方案，它透過分析行為而非依賴靜態簽章，在識別 GuLoader 等進階威脅方面扮演重要角色。其不斷強化的動態能力，例如：偵測不斷改變特徵的多形惡意軟體和零時差攻擊，可大幅強化賽門鐵克的電子郵件和端點安全產品。

賽門鐵克端點偵測與回應--Symantec Endpoint Detection & Response (EDR)，使用機器學習和行為分析來偵測和揭露可疑的網路活動，包括 PowerShell 執行和程序注入，同時也與 AMSI 整合以偵測混淆的腳本。EDR 會針對潛在的有害活動發出警示，排定事件的優先順序以進行快速分級事件，並允許事件回應人員執行查詢、撰寫自訂偵測規則，以及瀏覽裝置活動記錄，以便對潛在攻擊進行鑑識分析。當 SES 與 EDR 搭配使用時，結合的技術可提供多層防禦。兩者結合後，可針對已知與未知的威脅提供全面的防護，確保能在攻擊鏈的早期就能攔截，避免不斷演進的威脅，例如 GuLoader。。

賽門鐵克對 GuLoader 的防護措施包括以下幾項：

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!g*
- SONAR.SuspLaunch!g*

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。

端點偵測與回應(EDR)：

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多訊息，請參閱此 GitHub 儲存庫：https://github.com/Symantec/threathunters/tree/main/Trojan/Remcos

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.Guloader!gen*
- Trojan.Guloader

欲深入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。
欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲深入瞭解 Carbon Black，請點擊此處。

2024/10/08

Yunit Stealer--具備地理圍欄(geofencing)功能的惡意竊密程式

Yunit Stealer 是最近在真實網路情境到處肆虐的惡意軟體新變種。Yunit 具備廣泛的資訊竊取功能，包括竊取和外洩憑證、信用卡資料、加密貨幣錢包、cookie、自動填入資料 (autofill data) 等。收集到的資訊會透過 Discord 或 Telegram webhooks 傳送給攻擊者。Yunit 採用各種常駐技術、混淆、防禦迴避以及一些適地性服務 (Location Based Service) 的地理圍欄 (geofencing) 技術，確保只有來自目標地理位置的受害者才會感染惡意軟體。

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：

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

基於機器學習的防禦技術：

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

2024/10/08

全新惡意竊密程式：Vilsa Stealer

在真實網路情境發現全新的惡意竊密程式：Vilsa Stealer。該惡意軟體具有從受感染的機器中滲出各種機密資料的功能，包括：瀏覽器資料、憑證、自動填入資料 (autofill data)、cookie、銀行資訊、加密貨幣錢包、「Discord Token」(建立帳戶時產生的 Discord 使用者名稱和密碼的加密) 和 Telegram 資料等等。擷取的資訊會透過 GoFile API 上傳回遠端攻擊者。Vilsa Stealer 還採用一些反分析 (anti-analysis) 和偵測虛擬環境 (anti-VM) 的功能，來增加偵測和防禦的難度。

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

基於行為偵測技術(SONAR)的防護：

- 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：

- Infostealer
- Trojan.Gen.MBT
- 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。

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求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。