保安資訊--本周(台灣時間2024/02/23)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 53 萬 500 台受保護端點上總共阻止了 5,570 萬次攻擊。這些攻擊中有 85.9% 在感染階段前就被有效阻止：**(2024/02/19)**

- 在**11萬3,100**台端點上，阻止了**1,950**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**12萬9,100**台端點上，阻止了**1,090**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬8,000**台**Windows**伺服主機上，阻止了**9,300**萬次攻擊。
- 在**6萬7,800**台端點上，阻止了**210**萬次嘗試掃描伺服器漏洞。
- 在**1萬6,300**台端點上，阻止了**92萬6,100**次嘗試掃描在**CMS**漏洞。
- 在**4萬7,200**台端點上，阻止了**140**萬次嘗試利用的應用程式漏洞。
- 在**21萬600**台端點上，阻止了**450**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**9,400**台端點上，阻止了**130**萬次加密貨幣挖礦攻擊。
- 在**11萬1,300**台端點上，阻止了**660**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**564**台端點上，阻止了**9萬9,900**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 14.49 萬個受保護端點上阻止了總計 620 萬次攻擊。**(2024/02/19)**

- 使用網頁信譽情資，在 **129.9K** 個端點上阻止 **540** 萬次攻擊。
- 攔截 **32K** 個端點上 **602.3K** 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 **11.9K** 個端點上攔截 **131.5K** 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 **460** 個端點上攔截 **30.7K** 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。

2024/02/23
防護亮點：名為ApateWeb惡意轉導向網路攻擊行動

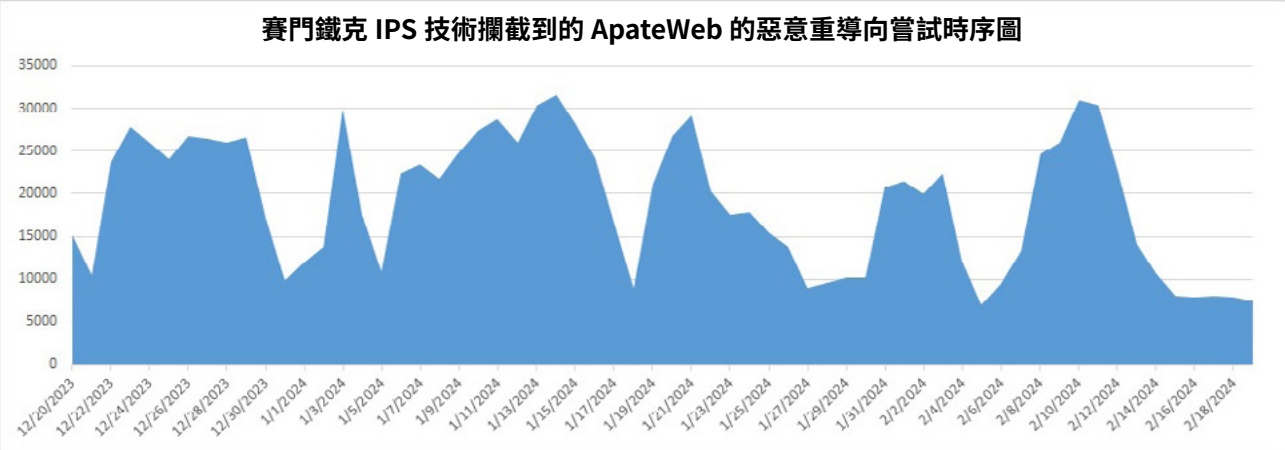
名為 ApateWeb 是一種惡意轉導向網路攻擊行動，會將毫無戒心的使用者帶到內藏惡意內容的網站。該行動透過欺騙性垃圾郵件或受害者瀏覽遭入侵的網站時啟動。受害者首先會收到一個 javascript 惡意有效籌載，該惡意籌載會使用一個獨特的架構對受害者進行跟蹤。

初始有效酬載收集受害者所使用的應用程式、框架、作業系統類型、版本……等指紋資訊。然後發送到攻擊者的伺服器，再利用這些資訊確定下一步的轉導向。下一步的轉導向使用隨機網域，然後再發送惡意有效酬載。最後觀察到的惡意有效酬載是潛在不受歡迎的應用程式／程式 (PUA 或 PUP)、恐嚇軟體或通知詐騙。

ApateWeb 採用多種伎倆來躲避安全研究人員的檢測和分析：

- 只有當受害者的瀏覽器檢索到帶有特定參數的網頁時，該行動才會將流量轉發到下一層。任何直接瀏覽 ApateWeb 控制網域網站的人都會被重導向到一個熱門的搜尋引擎或收到一個空頁面。這一策略有助於保護其功能變數名稱不被定期掃描網站的安全爬蟲攔截。
- 如果安全爬蟲存取了入門網頁，ApateWeb 會顯示一個錯誤頁面來隱藏自己。該行動透過檢查使用者代理來檢測爬蟲和機器人。
- ApateWeb 控制著 10,000 多個已註冊的域名，並濫用萬用字元 DNS 紀錄，這使得該行動幾乎可以透過無限多的子網域來傳播惡意內容。

賽門鐵克的網路層防護技術--入侵預防系統 (IPS) 會阻止 ApateWeb 的重導向嘗試，以防止系統受到感染／入侵。攻擊在初始階段就會被阻止，進而確保沒有惡意有效酬載被植入系統。



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: Malicious Redirection 44
- Malicious Site: Malicious Domain Request 143
- Malicious Site: Malicious Domain Request 142
- Malicious Site: Malicious Domain Request 164
- Web Attack: Malicious JavaScript Download 55

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。
欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

2024/02/23

釣魚郵件中出現偽造的英國關稅總署(HM Revenue & Customs)郵件通知

英國關稅總署 (HMRC：HM Revenue & Customs 是英國的稅務和海關機構，負責徵收所得稅、公司稅和資本利得稅……等稅種。最近，賽門鐵克發現有人假冒英國關稅總署進行網路釣魚，誘使使用者開啟假的通知郵件。郵件中提到使用者設定檔沒有更新。使用者需要更新個人資料，如果不更新，個人資料將被 HMRC 刪除。這些詐騙性的電子郵件主要在誘騙使用者點擊釣魚網頁。受害者點擊電子郵件內容中顯示的釣魚網頁後，就會看到登入憑證的網頁。

- 電子郵件主旨：Action Needed: Important Government Gateway Online Account Verification
- 電子郵件寄件者： Government Gateway <偽造的電子郵寄地址>

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)。

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。

2024/02/23

Ivanti旗下產品存有XML外部實體(XXE)注入漏洞：CVE-2024-22024

CVE-2024-22024 是最近被披露的一個 XML 外部實體 (XXE) 注入漏洞，會影響 Ivanti Connect Secure 和 Ivanti Policy Secure 產品的 SAML 元件。若被成功開採利用此漏洞可讓攻擊者在未進行必要身份驗證的情況下存取某些受限資源。據報告，該漏洞已在真實網路情境被開採利用。供應商已經發佈了存在漏洞的產品的修補版本。

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: Ivanti XXE Vulnerability CVE-2024-22024

2024/02/23

攻擊者以聯邦快遞(FedEx)服務為幌子來竊取憑證／帳密

賽門鐵克發現，冒充聯邦快遞 (FedEx) 服務以竊取憑證的網路釣魚攻擊有新的發展。在此一行動中，網路釣魚電子郵件偽裝成重新安排送貨時間或檢查包裹細節的送貨通知。電子郵件內容簡短，提醒收件人點擊釣魚網址。一旦點擊，受害者就會看到用於竊取憑證的網頁。

電子郵件主旨：

- Reschedule your package delivery
- Confirm Delivery: Your parcel will be delivered by David
- Confirm Delivery: Your parcel will be delivered by David

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)。

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。

2024/02/23

Sticky Werewolf(*難纏狼人)駭客組織鎖定波蘭公部門為目標

Sticky Werewolf 駭客組織上一次出現是在 2023 年 10 月，目標是俄羅斯和白俄羅斯的機構組織，最近又在涉入以波蘭公部門為目標的攻擊行動中被觀察到。這些攻擊利用魚叉式網路釣魚技術，釣魚郵件包含指向偽裝成 PDF 副檔名的惡意.exe 執行檔的連結。點擊這些惡意連結就會下載 Darktrack 遠端存取木馬 (RAT) 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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-FlPst!g1

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
- 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。

2024/02/22

假冒瀏覽器更新來散播Async遠端存取木馬(RAT)

據報導，一個遭入侵的合法網站被操弄篡改，並與一個指向虛假瀏覽器更新的基於惡意 JavaScript 框架的 SocGholish 惡意網址相連結。SocGolish 有效酬載最終會安裝遠端存取木馬 (RAT)，這是一個已知的憑證竊取程式和其他惡意軟體的惡意載入程式。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- JS.Downloader
- Trojan Horse
- 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。

2024/02/22

網路釣魚郵件以語音訊息為障眼法誘騙使用者下載惡意PDF

在最近的一次網路釣魚案例中，攻擊者向收件人發送包含冒充語音訊息通知的 PDF 附件之電子郵件。PDF 檔包含『收到新語音訊息』範本格式，其標準概述來電者 ID、訊息長度和語音郵件預覽，預覽預設是『不幸的是，目前無法取得此訊息的文字部份』。要求收件人點擊釣魚網頁來『收聽語音訊息』。

電子郵件信件標頭(mail header)：
主旨：新語音資訊，來自 <電話號碼> --無線來電者
附件檔名：Voicemail(1).pdf

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.Pidief

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。

2024/02/22

Lucifer分散式服務阻斷(DDoS)殭屍網路活動

在真實網路情境上發現一起新的網路攻擊行動，它利用名為 Lucifer 的 Linux DDoS 殭屍網路。該惡意軟體以 Apache Hadoop YARN 和 Apache Druid 基礎設施實例為目標。它利用任何潛在存在的設定錯誤或已知漏洞來入侵目標系統。一旦惡意軟體成功感染系統，它就會下載並執行主要有效酬載，即一個名為 XMRig coinminer 的木馬。該木馬用於挖掘門羅幣 (Monero)。

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：

- Backdoor.Trojan
- PUA.Gen.2
- Trojan.Gen.NPE
- 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: Apache Druid RCE CVE-2021-25646

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

偽裝成銀行行動APP的Octo(*八爪魚)安卓惡意軟體

在最近的一次網路攻擊行動中，有人發現 Octo 這一支在安卓平台上的惡意軟體，偽裝成一家信譽良好的希臘銀行 APP。Octo 是一種具有遠端存取功能的安卓平台手機惡意軟體，以全球金融機構為目標，最早出現在 2022 年初。該惡意軟體的功能包括停用推送通知、攔截簡訊、停用聲音、鎖定裝置畫面、啟動遠端存取連線……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
- WS.Malware.1

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

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

2024/02/21

RustDoor和GateDoor惡意軟體

RustDoor 是一款後門功能特別顯眼的 macOS 平台上的惡意軟體，而 GateDoor 則是一款具有惡意軟體載入功能的 Windows 平台上之惡意軟體。這兩種惡意軟體都是透過偽裝成正版官網的假網站，以蒙騙受害者下載工具程式或更新程式來傳播。RustDoor 和 GateDoor 會以常用安裝的程式更新／工具式為幌子，接收並執行來自 C&C 伺服器的命令以執行惡意操作。每個惡意軟體支援的命令不盡相同，但在基礎架構上有相似之處，這表示它們有共同的攻擊開發者。攻擊行動包括滲出收集的資訊、下載其他檔案和執行命令。

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.Stealer!gen1
- SONAR.MalTraffic!gen1

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
- Ransom.Zombie
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B!100
- 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。

2024/02/21

假冒人力資源部(HR)發送年度晉升通知的電子郵件成為網路釣魚的當季魚餌

駭客現在又給釣魚郵件增加一個新主題，這次是與員工晉升有關。在最近一次網路釣魚活動中，有人向收件人發送包含釣魚網頁並偽裝成年度員工晉升通知的電子郵件。郵件內文簡短，提到人力資源部發佈一份符合晉升條件的候選人名單。為了查看年度晉升名單，誘使用戶點擊企圖竊取憑證的網路釣魚網址。

電子郵件主旨：

- 主旨：年度晉升
- 寄件者：人力資源部 <被動過手腳的電子郵件位址>

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)。

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

VietCredCare惡意竊密程式

VietCredCare 是最近發現一種針對越南使用者的惡意竊密程式。該惡意軟體功能主要是竊取各種資訊，包括銀行詳細資訊、加密貨幣錢包憑證、瀏覽器歷史記錄和 cookie……等。得利於Telegram Bot API 的整合能力，收集到的資料會從遭入侵機器中轉出。該惡意軟體具有篩選與 Facebook 帳戶相關 Cookie 和憑證的特定功能，有助於幫助攻擊者接管企業 Facebook 帳戶。據了解，這種惡意竊密程式會以『惡意竊密程式即服務』(Stealer-as-a-Service) 形式出售給各種威脅組織。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.Stealer!gen1

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.Malware.2

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：

- System Infected: Trojan.Backdoor Activity 564
- System Infected: Trojan.Backdoor Activity 721

2024/02/21

HomuWitch勒索軟體

HomuWitch 是另一個普通的勒索軟體，去年首次在真實網路情境上被發現。該惡意軟體會加密使用者檔案，並冠上 .homuencrypted 的副檔名。勒索軟體攻擊者要求受害者用門羅幣 (Monero，XMR) 支付贖金，並要求他們透過電子郵件或即時通訊軟體與攻擊者聯繫。

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

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Ransomware!g34
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Zombie
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.2
- 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.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。

2024/02/21

日本Credit Saison持卡人成為新一波網路釣魚的目標

Credit Saison 是總部位於日本東京最大信用卡發行商之一。最近，賽門鐵克發現有釣魚網站假冒 Credit Saison 服務，誘使使用者打開假冒的通知郵件。電子郵件內文提到確認 Saison 卡的使用情況。這些釣魚郵件試圖誘使用戶打開並點擊釣魚網址。

- 電子郵件主旨：【最終確認】セゾンカード ご利用確認のお願い
- 翻譯電子郵件主旨：【最後確認】請求確認賽森卡的使用情況【Final confirmation】Request for confirmation of Saison card usage

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)。

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。

2024/02/20

專門針對遠端字典伺服器Redis(REmote DIctionary Server)的Migo惡意軟體

據報導，一款名為『Migo』全新惡意軟體針對 Linux 主機上的 Redis 伺服器，採用削弱技術停用 Redis 的安全功能，例如：設置保護模式、唯讀複製、增量同步和增量同步保存。Migo 是一款基於 Golang 的 ELF (可執行與可鏈結格式) 惡意軟體，主要在對目的電腦執行挖礦劫持攻擊。

保安網路知識補充：ELF 全名是 Executable and Linking Format，在 Linux 中是編譯後的 binary、object 檔規範，也就是說我們從 source code 編譯後產生的檔案格式就是 ELF。 ELF 的格式可以從兩種角度來看，第一種是 Link 的時候，第二種是執行的時候。

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

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。

2024/02/20
SpyNote針對西班牙數位銀行使用者

賽門鐵克在監控全球網路威脅情況時發現針對西班牙 Android 行動手機用戶的遠端存取木馬活動。這一活動幕後的組織或個人一直在試圖用一個假的安全應用程式 APP ([銀行名稱] security.apk) 引誘一家知名西班牙數位銀行的使用者，該假 APP 模仿官方版的 APP，允許使用者安全地存取他們的銀行帳戶、核准交易和管理他們的安全設置。

如果使用者被成功誘騙安裝該惡意程式，最終就會被 SpyNote 入侵。SpyNote 是一種惡名昭章的遠端存取特洛伊木馬程式，被全球多個攻擊者使用。

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

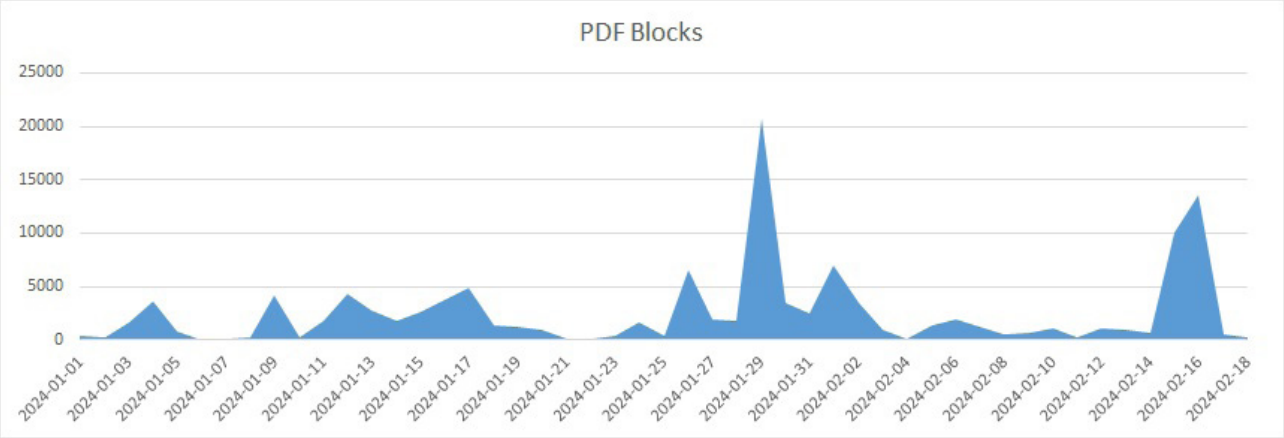
2024/02/20
防護亮點：濫用惡意PDF檔案的網路攻擊持續上升

在過去幾個月中，我們發現濫用惡意 PDF 檔案的郵件攻擊激增。為了應對這些攻擊，賽門鐵克創新的 PDF 啟發式解決方案利用先進的啟發式和機器學習技術。事實證明，這種主動式防護技術非常有效，成功阻止大量攻擊，包括由 TA544、TA577 和 RogueRadicate……等惡名昭章的駭客組織所策動的網路攻擊。

以下是我們的啟發式解決方案在 1 月和 2 月期間阻止的一些垃圾郵件攻擊行動，涉入的駭客正試圖在其攻擊鏈中濫用惡意 PDF 檔案：

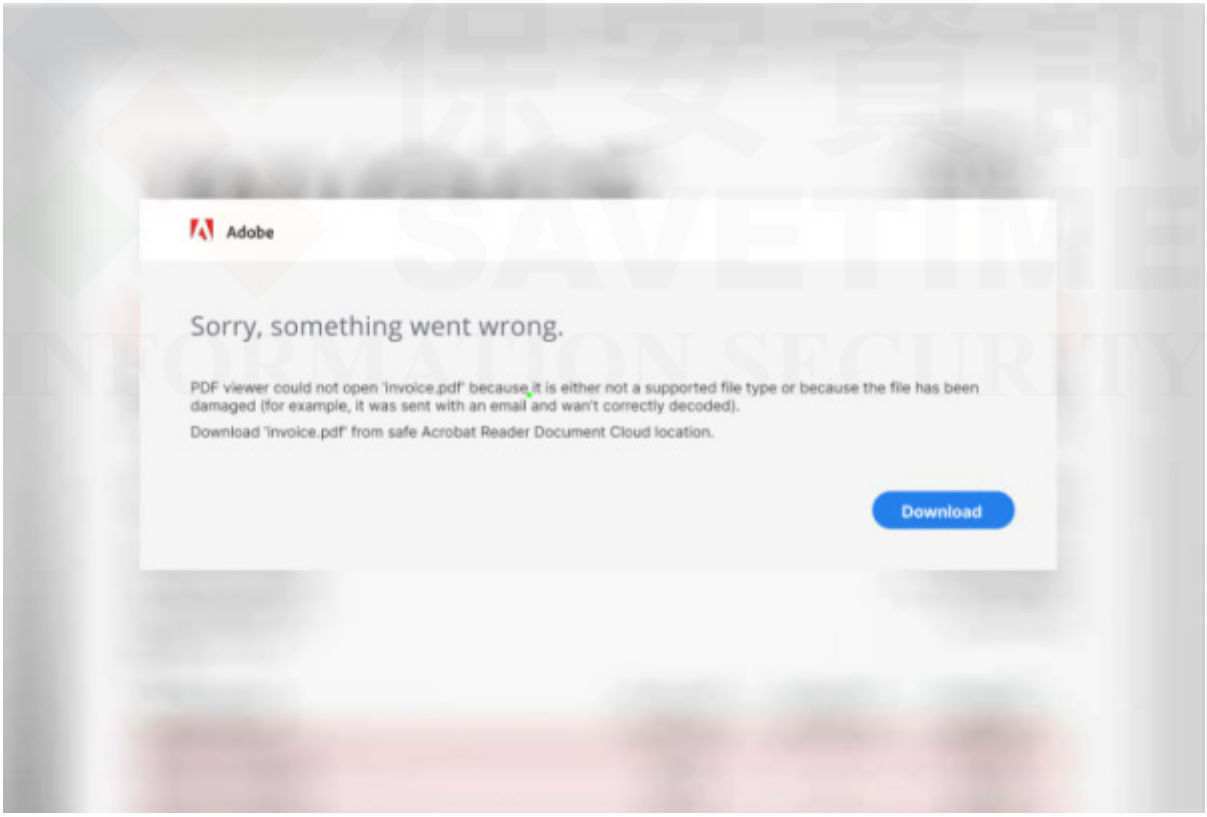
- 1 月 9 日～利用 PDF 附件傳遞 Netsupport 遠端存取木馬 (RAT) 最終有效酬載的垃圾郵件攻擊行動。
- 1 月 16 日～利用 PDF 附件傳遞 Lokibot 最終有效酬載的垃圾郵件攻擊行動。
- 1 月 16 日、24 日和 2 月 1 日、2 日～利用 PDF 附件傳遞 DBatLoader 和 Remcos 最終有效酬載的垃圾郵件攻擊行動。
- 1 月 17 日、31 日～利用 PDF 附件傳遞 Wikiloader 最終有效酬載的垃圾郵件攻擊行動。
- 1 月 24 日、25 日、26 日、29 日和 2 月 12 日、13 日～利用 PDF 附件傳遞 Darkgate 最終有效酬載的垃圾郵件攻擊行動。

暗藏惡意程式碼的 PDF 網路攻擊在 1 月下旬和 2 月中旬出現明顯的高峰。



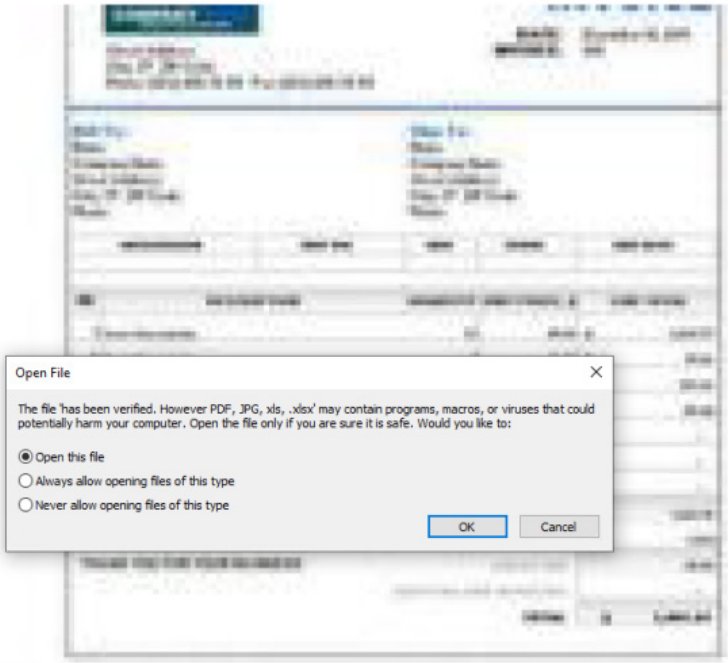
NetSupport 遠端存取木馬(RAT)

據觀察，最近傳遞 NetSupport 遠端存取木馬 (RAT) 網路攻擊行動與去年 11 月 Darkgate 行動使用類似的 PDF。因此，我們認為它們是由同一個攻擊者 RogueRadicate 所發送。當使用者點擊 PDF 中的下載連結時，會傳遞惡意有效酬載。



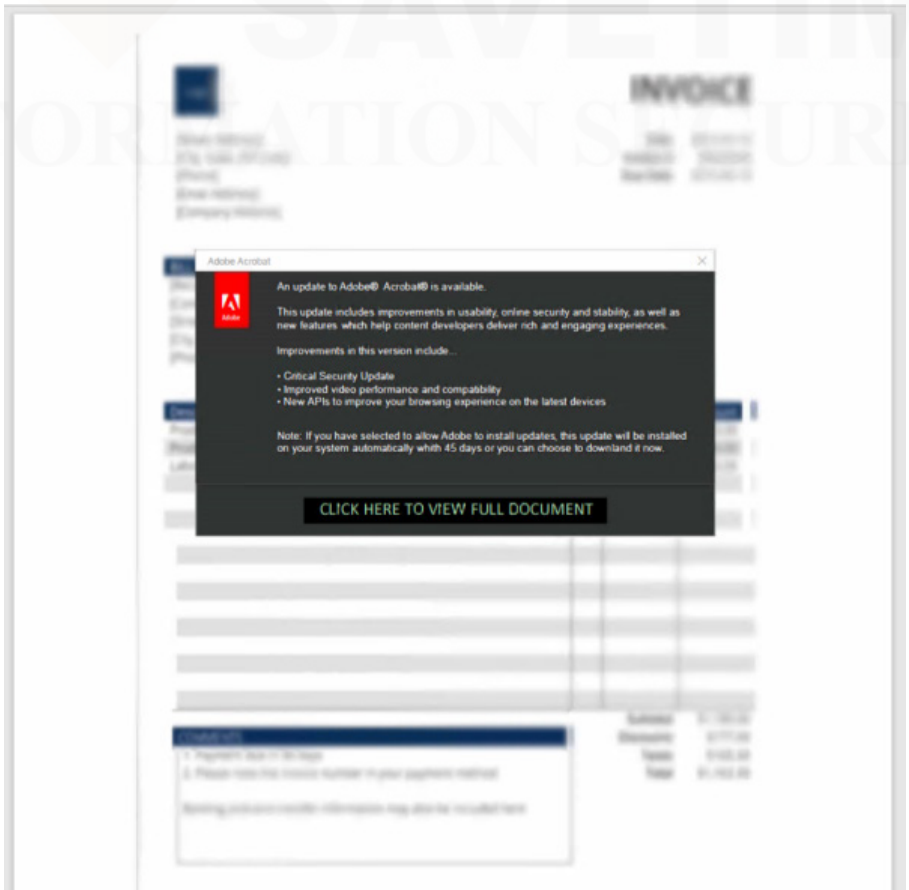
木馬程式LokiBot

值得關注的趨勢是，越來越多的惡意竊密程式選擇透過 PDF 垃圾郵件進行傳播。我們在今年 1 月破獲一波 Lokibot 寄生惡意 PDF 的網路攻擊行動，使用者打開 PDF 附件時會被注入一個 Office 檔案。最終的有效酬載通常會濫用眾所周知的陳年老漏洞 (例如：CVE-2017-11882 或 CVE-2017-0199) 下載並執行。



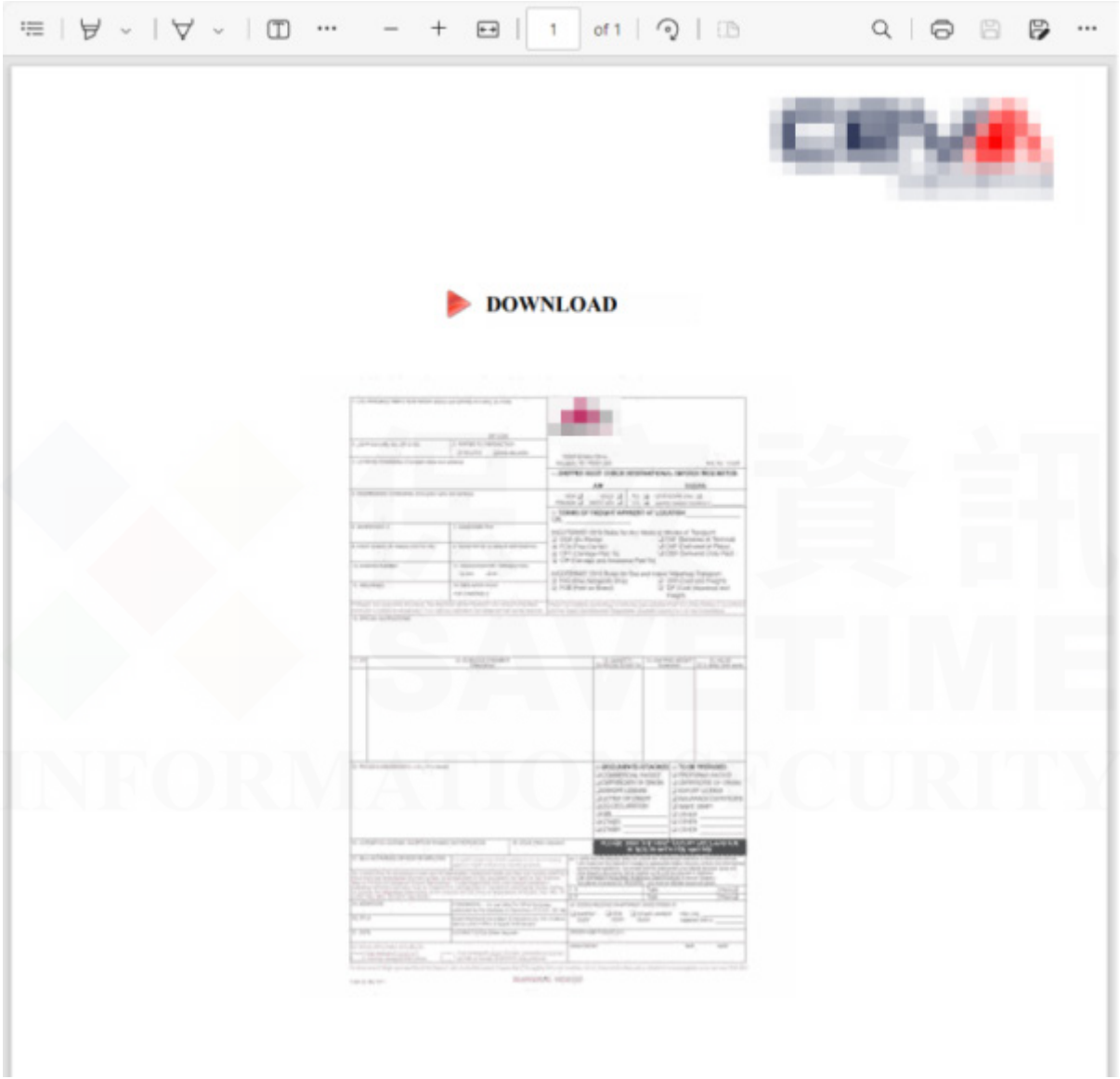
惡意軟體載入器DBatLoader和Remcos遠端存取木馬(RAT)

我們最近還觀察到某些 PDF 垃圾郵件攻擊行動間歇性地將 DBatLoader 和 Remcos 作為其最終有效酬載。該電子郵件偽裝成出貨單／發票，但要求使用者更新 Adobe Acrobat 軟體才能查看完整文件。如果使用者點擊更新連結，該威脅將下載惡意有效酬載，而不是軟體更新。



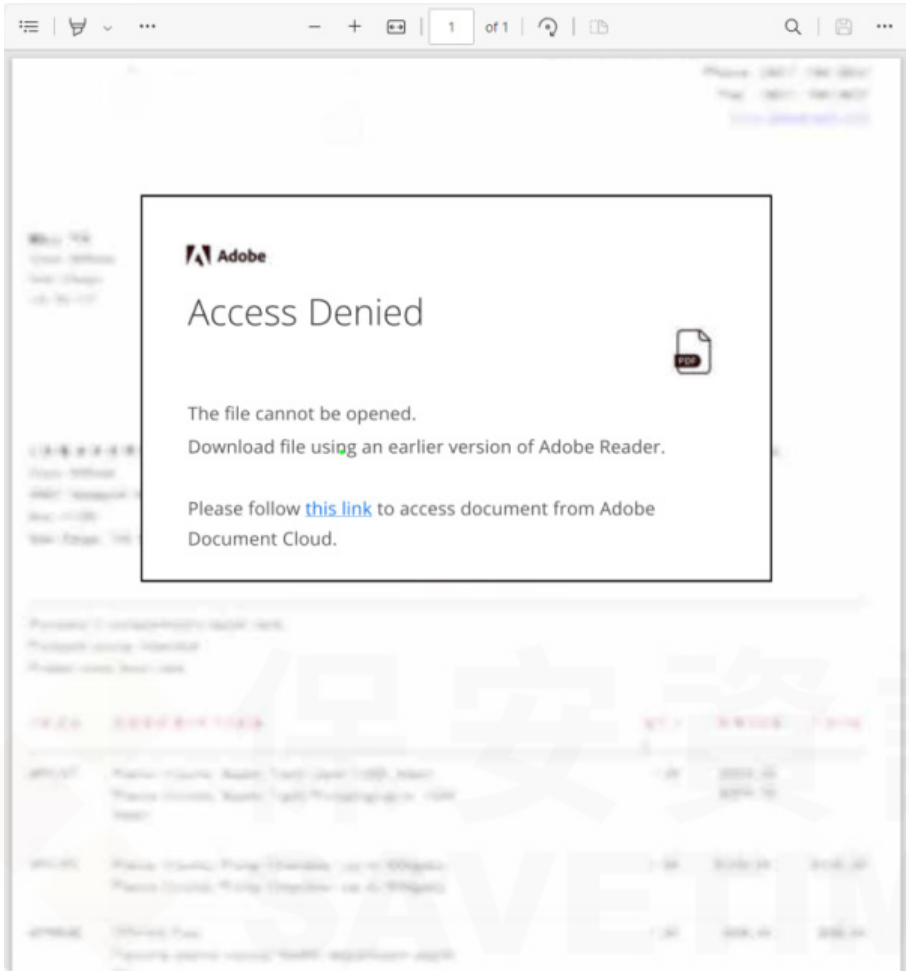
WikiLoader 惡意程式載入器

我們在之前的『防護亮點』中報導今年傳播 Wikiloader 垃圾郵件行動的強勢回歸。垃圾郵件中使用的 PDF 偽裝成一家物流公司的發票下載。點選連結後，用戶將被被重導向到一個網站，且會被注入惡意有效酬載。



惡意程式載入工具：DarkGate(*黑暗之門)

Darkgate 在去年 10 月至 11 月期間相當活躍。在 12 月份相對沉寂一段時間後，他們在 1 月份再次出現。他們在垃圾郵件中使用的 PDF 檔會顯示『存取拒絕』或『檔案顯示不正確』……等警告，目的是說服使用者點選連結進行所謂的 Adobe Reader 更新或下載檔案進行離線查看。與其他連結一樣，該連結會將使用者轉導向到另一個網站，並注入惡意有效酬載。有關 2024 年 1 月『Darkgate』活動更多資訊，請參閱先前的《防護公告：惡意程式載入工具DarkGate(*黑暗之門)涉入的網路攻擊行動中，藏身在PDF附件陷阱越來越多)》。



值得一提的還有……

除了減輕上述一波波垃圾郵件的攻擊，PDF 啟發式防護技術還能有效阻止透過電子郵件附件或連結傳送的網路釣魚 PDF，這些網路釣魚主要在竊取使用者的機密資訊，例如：信用卡詳細資訊、銀行帳戶憑證或電子郵件帳戶登錄資訊。

賽門鐵克可保護您免受這些 PDF 相關的威脅(**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.DLHeur!gen1
- Scr.DLHeur!gen2
- Scr.DLHeur!gen3
- Scr.DLHeur!gen5
- Scr.DLHeur!gen6
- Scr.DLHeur!gen7
- Scr.DLHeur!gen8
- Scr.DLHeur!gen9
- Scr.DLHeur!gen10

- Scr.DLHeur!gen13
- Scr.DLHeur!gen14
- Scr.DLHeur!gen15
- Trojan.DLHeur!gen2
- Trojan.DLHeur!gen3
- Trojan.DLHeur!gen4
- Trojan.DLHeur!gen5
- Phish.Pdf!gen2
- Phish.Pdf!gen3
- Phish.Pdf!gen4
- Phish.Pdf!gen5
- Phish.Pdf!gen6
- Phish.Pdf!gen7
- Phish.Pdf!gen8
- Scr.Qbot!gen12
- Scr.Qbot!gen14
- Scr.Qbot!gen19

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)。

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。

2024/02/20

DOPLUGS--一種可自訂且源於PlugX 惡意軟體家族

DOPLUGS 是一種可自訂且源於 PlugX 惡意軟體家族，在最近涉入由 Earth Preta(又名 Mustang Panda) APT 駭客組織所發起的網路攻擊行動而聲名大噪。攻擊者透過魚叉式網路釣魚行動向東亞和東南亞的受害者傳播該惡意軟體。DOPLUGS 惡意程式載器主要用於下載 PlugX 惡意軟體中更常見的有效酬載。此外，在真實網路情境上還發現一個整合 KillSomeOne 模組的 DOPLUGS 新變種。KillSomeOne 是一種 USB 蠕蟲病毒，主要用於傳播惡意軟體、竊取檔案和收集資料。

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-Http!g2
- ACM.Ps-Rd32!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!300
- 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。

2024/02/20

Water Hydra進階持續威脅(APT)駭客組織開採濫用CVE-2024-21412漏洞進行DarkMe惡意軟體傳播

據報導，Water Hydra 進階持續威脅 (APT) 駭客組織在其最新網路攻擊行動中，開採濫用了最近被披露的 CVE-2024-21412 漏洞。CVE-2024-21412 是一個網際網路捷徑檔安全機制功能繞過漏洞，CVSS 風險評分為 8.1。如果被成功開採濫用，未經認證的攻擊者可以繞過現有的安全檢查，向目標使用者發送特製檔案。Water Hydra APT 一直在利用這一漏洞繞過 Microsoft Defender SmartScreen 安全功能，向受害者發送 DarkMe 惡意軟體。DarkMe 是一款基於 Visual Basic 的惡意下載器，用於執行攻擊者命令並向被攻擊的端點發送任意有效酬載。

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

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Exp.CVE-2024-21412

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

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：

- System Infected: Trojan.Backdoor Activity 770
- Web Attack: Malicious Payload Download 29
- 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。

2024/02/19

Nood遠端存取木馬(RAT)惡意軟體

Nood RAT 是源於 Gh0st RAT 惡意軟體的 Linux 平台上的全新變種。該惡意軟體的功能包括遠端 shell 執行、資訊竊取、檔案管理、在遭入侵系統上設置 Socks 代理和通訊埠轉發……等。Nood RAT 可能會接收來自攻擊者 C&C 伺服器的其他指令，同時與這些伺服器的通訊保持加密，以試圖阻撓任何網路檢測工作。

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：

- Backdoor.Trojan
- Trojan Horse
- 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。

2024/02/19

BackMyData--源於Phobos勒索軟體的全新變種

BackMyData 是在真實網路情境上觀察到最新 Phobos 勒索軟體變種。該惡意軟體已被用於針對羅馬尼亞醫院和醫療設施的最新網路攻擊。該惡意軟體會加密檔案，並冠上 .backmydata 副檔名、受害者 ID 和開發者電子郵寄地址。勒索贖金支付說明以『info.hta』和『info.txt』文字檔的形式發佈，要求受害者與加害者聯繫，獲取有關資料復原的進一步說明。BackMyData 具備刪除受感染電腦上磁碟備份的功能。該勒索軟體還能透過在註冊表中建立機碼項目以及將惡意軟體可執行檔新增到遭入侵端點的開機檔案夾中來建立常駐能力。

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-RgPst!g1
- ACM.Ps-Wbadmin!g1
- ACM.Untrst-RunSys!g1
- ACM.Vss-DlShcp!g1
- ACM.Wbadmin-DlBckp!g1
- ACM.Wmic-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- Sonar.Ransom!gen105
- Sonar.SuspLaunch!gen4
- Sonar.SuspLaunch!g18
- Sonar.SuspLaunch!g21
- Sonar.SuspLaunch!g253

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Phobos!gm1

基於機器學習的防禦技術：

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

2024/02/19

Bumblebee重出江湖

最近觀察到的一次惡意垃圾郵件行動重新導入了Bumblebee惡意軟體。Bumblebee 是一種惡意載入器，在消失多個月前曾廣受許多個駭客組織採用。新一波攻擊行動試圖透過以語音信箱為主題的電子郵件連結到惡意檔案下載來傳播Bumblebee。該檔案反過來會啟動一個腳本，該腳本會執行 Powershell 指令，進而下載 Bumblebee。

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.Gen.NPE

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。

2024/02/18

以偽造的法國法院判決來詐騙微軟365憑證

惡意 PDF 涉入的網路釣魚攻擊屢見不鮮，但最近幾個月卻沒有停止的跡象。全球範圍內每天都有針對企業和消費者的網路釣魚行動，其中一些行動是根據地區和／或行業部門的不同來量身定制的目標式釣魚行動。

賽門鐵克在法國就發現這樣一個行動，攻擊者試圖以 PDF 檔名：([公司名稱] Convocation au Tribunal.pdf) 的形式偽造法院判決來引誘使用者。一旦惡意 PDF 檔被開啟，用戶就會收到一條訊息，顯示該檔案已在 OneDrive 上提供。網頁重導向到一個釣魚頁面，該頁面模仿 Microsoft 365 登錄，目的是騙取使用者的憑證／帳密。

利用偽造的法院判決作為網路釣魚的社交工程伎倆可能非常有效。透過利用與法律事務相關的緊迫感和恐懼感，網路犯罪分子會營造一種情境，讓收件者感到不得不迅速採取行動以避免不利後果。

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)。

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。

2024/02/16

iOS平台上的銀行木馬：GoldPickaxe

GoldDigger 是一款安卓平台 (Android) 上的銀行木馬惡意軟體，最初出現在 2023 年 10 月，目標使用者是越南的用戶。在網路上觀察到一種名為 GoldPickaxe 的全新變種，可同時適用於 Android 和 iOS 系統。攻擊者可利用 iOS 版本**收集臉部生物識別資訊**和其他身份資訊，以克服銀行生物身份驗證並非法存取帳戶。並濫用受感染設備上的可存取的服務，以便從加密貨幣應用程式和錢包中滲出個人資料、簡訊、雙因子認證 (2FA) 憑證、銀行憑證和資料。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.3

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
- OSX.Trojan.Gen

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。

2024/02/16

挖礦劫持惡意程式納入間接系統呼叫規避技術

間接系統呼叫是 Pikabot 等勒索軟體載入程式 (Loader) 經常使用的一種規避技術，最近也觀察到其他類型的惡意軟體也開始採用這種伎倆，最值得一提的是挖礦劫持惡意程式。XMrig 算是挖礦劫持惡意程式圈的老江湖，透過新增 run 註冊表和服務項目來建立常駐功能。然後，它在記憶體中執行，以逃避檢測並在受感染的系統中常駐。

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

基於機器學習的防禦技術：

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

2024/02/16

RansomHouse駭客組織利用MrAgent工具發動對ESXi平台的攻擊

據瞭解，RansomHouse 駭客組織，過往因利用 WhiteRabbit 或 MarioLocker (又名 Mario ESXi) 等惡意軟體針對 Linux 機器和 VMware ESXi 伺服器進行攻擊而聲名大噪。該駭客組織最近一直在利用一種名為 MrAgent 的工具，該工具允許在大型環境中自動傳遞勒索軟體，並同時透過多個虛擬機管理程式 (Hypervisor) 上部署。MrAgent 具有排程和記錄惡意二進位檔案部署、搜查目標基礎架構資訊以及在虛擬機管理程式 (Hypervisor) 上執行命令的功能。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Ransom.Gen
- Trojan Horse
- 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

2024/02/16

Alpha(*阿爾法)勒索軟體

Alpha 是一種全新的勒索軟體，於 2023 年 2 月首次出現，並在最近幾周動作頻繁。它與早已銷聲匿跡的 NetWalker 勒索軟體非常相似，後者在一次國際執法行動後於 2021 年 1 月被剷除。這兩種勒索軟體都採用類似的 PowerShell 載入器來傳遞有效籌載。除此之外，Alpha 和 NetWalker 的有效籌載之間，還存在大量雷同的程式碼。雖然 Alpha 於 2023 年 2 月首次出現，但它一直低調行事，直到最近幾周才似乎開始擴大營運規模並公開一個資料洩漏網站。

在我們的布落格文章中有更詳細的內容：從 NetWalker 死灰復燃的 Alpha 勒索軟體

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：

- AGR.Terminate!g2
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Alpha
- Ransom.Gen
- 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

2024/02/16

散播DanaBot銀行木馬的垃圾郵件攻擊行動

最近發現一個採用義大利文撰寫的惡意郵件攻擊行動，在散播 DanaBot 殭屍電腦程式。該電子郵件包含一個指向惡意 JS 檔的連結，該檔將會下載並執行 DanaBot DLL。DanaBot 是一種銀行木馬，具有竊取被害人財務資訊的功能。

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!gen60
- ISB.Downloader!gen68
- Scr.Malcode!gen60
- Scr.Malcode!gen120
- 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.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。

2024/02/16

Srry惡意竊密程式透過惡意JavaScript進行傳播

SrryStealer 是一款全新的惡意竊密程式，它透過惡意 JavaScript 檔，暗中入侵受害者系統。執行後，它會終止目標系統的多個程序，包括與瀏覽器和 Discord 相關的程序。然後，它會收集大量資料，包括系統資訊和個人保存的資料，例如：登錄憑證、瀏覽器歷史記錄、自動填入密碼、信用卡詳細資訊、加密貨幣錢包和 Discord 權杖。收集到的資料隨後會外傳到攻擊者所操控的指揮控制 (C&C) 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

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

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：

- 29565_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，針對此漏洞提供如下的多層級保護：

- 基於可疑程序執行的預防：預防政策可防止惡意軟體在系統中被注入或執行。
- 基於對外連線的預防：在這種情況下，預防政策會阻止網際網路 (mythic-slender[.]online) 的對外連線。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2024/01/25

惡意程式載入工具DarkGate(*黑暗之門)涉入的網路攻擊行動中，藏身在PDF附件陷阱越來越多

DarkGate 是一種惡意遠端存取木馬 (RAT)，自 2018 年以來一直到處傳播。這種『惡意軟體即服務』(MaaS) 類型的惡意軟體發展迅速，就在去年 10 月，我們曾撰文報導 DarkGate 將 PDF 附件納入其網路攻擊行動的武器，以此來提高其行動的成功率。

最近，發現一種 Darkgate 藏身在惡意 PDF 檔所涉入的網路攻擊行動，其感染鏈如下：

- 網址 > 短網址 1 > 短網址2 > ZIP壓縮檔 > MSI 安裝檔 > DLL 測載 > Autoit3.exe 以及 Autoit script > DarkGate

感染鏈的複雜性顯示作者為逃避檢測的本領 (**目前除賽門鐵克外，沒有其他供應商在 VirusTotal 上顯示檢測結果，因此他們在某種程度上是成功的**)，但我們的啟發式引擎還是偵測到它。

MSI 會安裝一個名為 ItuneHelper.exe 的合法 EXE 執行檔，攻擊者使用 DLL 側載的伎倆。這種技術結合合法應用程式和惡意 DLL，在本例中，惡意 DLL 被命名為『CoreFoundation.dll』。它冒用 EXE 檔中真正 DLL 元件的名稱。

在執行過程中，CoreFoundation.dll 會從 sqlite3.dll 檔案中呼叫 Autoit3.exe 和一個名為 script.au3 的惡意檔。Autoit3.exe 是合法的 EXE 檔，它會執行 script.au3 來解密和載入最終有效籌載--一個 DarkGate 二進位檔案。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.DLHeur!gen7

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)。