保安資訊--本周(台灣時間2024/06/14)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 52 萬 5,700 台受保護端點上總共阻止了 4,860 萬次攻擊。這些攻擊中有 80.7% 在感染階段前就被有效阻止：**(2024/06/10)**

- 在**10萬8,800**台端點上，阻止了**1,690**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**13萬7,600**台端點上，阻止了**1,060**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬5,300**台**Windows**伺服主機上，阻止了**780**萬次攻擊。
- 在**6萬800**台端點上，阻止了**200**萬次嘗試掃描伺服器漏洞。
- 在**1萬3,600**台端點上，阻止了**84萬3,900**次嘗試掃描在**CMS**漏洞。
- 在**4萬4,700**台端點上，阻止了**150**萬次嘗試利用的應用程式漏洞。
- 在**17萬3,300**台端點上，阻止了**440**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6,300**台端點上，阻止了**140**萬次加密貨幣挖礦攻擊。
- 在**11萬2,500**台端點上，阻止了**780**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**701**台端點上，阻止了**8萬8,300**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 17 萬 4,700 個受保護端點上阻止了總計 810 萬次攻擊。**(2024/06/10)**

- 使用網頁信譽情資，在 **162.8K** 個端點上阻止 **760** 萬次攻擊。
- 攔截 **27.7K** 個端點上 **411.1K** 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 **82.3K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **369** 個端點上攔截 **12.3K** 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。

2024/06/13

El Dorado勒索軟體：攻擊增多

El Dorado 是典型的雙重勒索軟體，最近在其網站上聲稱有多名受害者。一旦他們取得一家公司的存取權，就會搜尋帶有有價值資料的機器進行外滲和加密，並在加密檔中增加 .00000001。他們的勒索贖金支付說明 (HOW_RETURN_YOUR_DATA.TXT) 檔案被放置在不同的資料夾中。在該說明中，他們聲稱自己曾是『白帽駭客』，但因收入微薄而開始此一非法行為。他們還告知受害者如何透過 TOR 網路和使用其網站上的即時聊天工具與他們聯繫，並威脅說如果受害者在 7 天內不與他們聯繫並支付贖金，他們就會出售或洩露被竊取的資料。此外，他們還威脅對受害者的公司、合作夥伴和客戶進行持續攻擊，進一步向受害者施壓。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransomware!g6
- SONAR.Ransomware!g16
- SONAR.Ransomware!g27

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.C

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。

2024/06/13

Celestial Force攻擊行動

思科資安部門 (Cisco Talos) 的研究人員報告一個名為『Celestial Force行動』(Operation Celestial Force) 的新惡意活動。該行動至少從 2018 年開始活躍，目標是印度國防、政府和技術部門的組織。根據發佈的研究報告，『Celestial Force 行動』是由一個名為 Cosmic Leopard 的威脅組織發起。攻擊者一直在利用安卓惡意軟體 GravityRAT 以及名為 HeavyLift 的Electron 框架的 Windows 惡意程式載入器。該 APT 駭客組織實施的攻擊由一個名為 GravityAdmin 獨立定制工具管理，該工具可集中執行被攻擊系統上的惡意操作。

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：

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

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
- 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。

2024/06/13

CVE-2024-30080--Microsoft 訊息佇列(Message Queuing)中介軟體服務的遠端程式碼執行弱點

微軟發布 6 月例行更新，微軟修補一個關鍵等級 (CVSS 風險評分：9.8) 的訊息佇列 (Message Queuing) 中介軟體服務中的漏洞：CVE-2024-30080。透過向受攻擊的伺服器發送特製的惡意 MSMQ 資料封包並利用該漏洞，攻擊者可實現遠端程式碼執行並接管未做修補的伺服器。此報告的漏洞影響 Windows Server 2008 到 Windows 10 的多個 Windows 作業系統。

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: Microsoft Message Queue CVE-2024-30080

2024/06/13

CVE-2024-4701--Netflix Genie作業編排引擎漏洞

CVE-2024-4701 是一個最近披露的嚴重 (CVSS 得分 9.9) 路徑遍歷漏洞，影響 Netflix 用於大資料應用程式的 Genie 工作業編排引擎。如果成功開採濫用該漏洞，遠端攻擊者可在受影響的應用程式中執行任意程式碼，並暴露敏感資訊。Genie OSS 4.3.18 版已修補該漏洞。

網路知識：Genie 是 Netflix 開發的開源分散式作業編排引擎，提供 REST-ful API 來運行各種大資料作業，例如：Hadoop、Pig、Hive、Spark、Presto、Sqoop 等。它還提供 API 用於管理許多分散式處理集群的中繼資料、在集群上運行的命令和應用程式。

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：

- Web Attack: Netflix Genie CVE-2024-4701

2024/06/13

CVE-2024-2194--WP Statistics外掛程式存在跨網站腳本(XSS)漏洞

CVE-2024-2194 是一個最近披露的存儲跨網站腳本 (XSS) 攻擊漏洞，這些漏洞存在 WordPress 的 WP Statistics 外掛程式 14.5 以下版本。如果成功開採濫用該漏洞，未經身份驗證的攻擊者可在頁面中注入任意 Web 腳本。當使用者存取被注入的頁面時，這些任意腳本就會被執行。據報告，該漏洞已在網路上被大肆開採濫用。

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：

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: WP Statistics Plugin XSS CVE-2024-2194

2024/06/12

Noodle遠端存取木馬(RAT)可同時支援Windows和Linux平台的部署

Noodle 遠端存取木馬 (RAT) 是趨勢科技研究人員最近發現一種惡意軟體。據報告，該遠端存取木馬 (RAT) 涉入亞太地區的目標式攻擊行動。Noodle 遠端存取木馬 (RAT) 是一種模組化惡意軟體，功能相對簡單，與 Gh0st 遠端存取木馬 (RAT) 和 Rekoobe 惡意軟體系列有多處程式碼雷同。它讓攻擊者下載／上傳任何檔案、在記憶體中執行模組以及 TCP 代理。Noodle 遠端存取木馬 (RAT) 幕後的主使者在最終部署有效酬載之前，還利用 MultiDrop 和 MicroLoad 惡意軟體。除了該惡意軟體的 Windows 版本，還發展 Linux 版本。它具有下載／上傳任意檔案、反向執行 shell 以及 SOCKS 通道的功能。

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：

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.Trojan
- Trojan Horse
- Trojan.Gen.NPE

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。

2024/06/12

Adwind(又名 jRAT)在最近針對義大利用戶的網路攻擊行動中傳播

在最近針對義大利用戶的網路攻擊行動中發現 Adwind 惡意軟體 (也稱為 jRAT 或 njRAT)。攻擊鏈包括含 .zip 附件的惡意郵件。解壓縮後，用戶會收到 .HTML 檔案，諸如 INVOICE.html 或 DOCUMENT.html，這些檔案會指向惡意 .jar 檔案。最後注入有效酬載是 Adwind 遠端存取木馬 (RAT)，可讓攻擊者控制遭入侵的端點並收集和外洩機密資料。

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：

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：

- Scr.Maljava!gen1
- Trojan Horse
- Trojan.Maljava
- Trojan.Malscript
- Trojan.Pidief
- 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。

2024/06/12

WarmCookie後門

WarmCookie 是一種全新發現的後門惡意程式，以求職詐騙為幌子的廣告藉由網路釣魚行動來傳播。攻擊鏈利用惡意 JS 腳本執行 PowerShell 命令，最終結果會導致下載 WarmCookie 的 DLL 有效負載。攻擊者濫用背景智慧型傳送服務 (BITS) 下載惡意有效酬載。WarmCookie 後門具有廣泛的功能，包括端點指紋辨識 (fingerprinting)、螢幕截圖、任意命令執行、檔案內容讀取／滲出和部署附加有效酬載等。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-TskReg!g1
- ACM.Rd32-TskReg!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。

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.Gen.MBT
- 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

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。

2024/06/12

Black Basta攻擊者開採濫用CVE-2024-26169漏洞發動零時差攻擊

賽門鐵克的威脅獵手團隊在最新發佈的報告中指出，有證據顯示與 Black Basta 勒索軟體有關聯的攻擊者，已經編譯 CVE-2024-26169 漏洞利用攻擊程式碼來瞄準未及時上修補的目標。CVE-2024-26169 漏洞是 Windows 錯誤報告服務中一個權限提高漏洞，可讓攻擊者提升權限。分析顯示，最近 Black Basta 所涉入攻擊中部署的一個漏洞利用工具一直在利用這個零時差漏洞。

在我們的部落格文章中有更詳細的內容：勒索軟體攻擊者可能利用權限提升漏洞作為零時差漏洞。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!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
- Exp.CVE-2024-26169!g1
- Trojan.Gen.9
- Trojan.Gen.NPE
- Scr.Malcode!gen49
- Web.Reputation.1
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2024/06/12

全新的惡意Valley遠端存取木馬(RAT)涉入網攻擊行動

據觀察，一起網路攻擊行動將最新版本的 Valley遠端存取木馬 (RAT) 作為最終有效酬載。攻擊載體包括一個帶有注入式 shellcode 的惡意程式下載器，該 shellcode 可動態解析 API 並與 C&C 伺服器建立連接，以下載攻擊鏈下一階段的惡意軟體。這樣遠端攻擊者就可以在未經授權的情況下，存取和控制受感染的機器。Valley 遠端存取木馬 (RAT) 的新變種具有螢幕截圖、程序過濾、強制關機和清除 Windows 事件日誌等功能。

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：

自適應防護技術(包含於SESC)：

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

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
- Heur.AdvML.C

VMware Carbon Black 產品的防護機制：

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

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2024/06/11

透過UUEncoding (UUE)檔案傳輸的Remcos遠端存取木馬(RAT)

最近一個傳播 Remcos 遠端存取木馬 (RAT) 的網路釣魚行動，使用與航運或報價相關的主題文件檔為誘餌。初始攻擊源於一個 UUE 編碼的 VBS 腳本開始，解碼後會出現另一個混淆的 VBS 腳本。該腳本會儲存並執行 PowerShell 腳本，而 PowerShell 腳本又會連接到一個網址連結，以下載另個混淆的 PowerShell 腳本。這個混淆化的攻擊鏈目的是逃避檢測。一旦啟動，Remcos 遠端存取木馬 (RAT) 最終有效酬載將收集系統資訊和按鍵，並將其傳輸到多個命令和控制伺服器。

網路知識：Uuencoded File 檔案最初是由 Apple Archive Utility 軟體應用程式的 Apple 所開發。根據網站訪客分析指出，UUE 檔案通常現身於 Windows 10 使用者電腦，且最受 Colombia 歡迎。就統計上而言，這些使用者最有可能執行 Google Chrome 網際網路瀏覽器。

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：

自適應防護技術(包含於SESC)：

- 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。

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.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。

2024/06/11
防護亮點：網路釣客加大對Telegram聊天機器「應用程式介面」(API)的惡意濫用

Telegram 服務

Telegram 是一種安全的雲端訊息服務平台，以其「高度隱私性」、「豐富的跨平台支援」、「免費且極大的開發彈性」三大特色和自毀訊息而聞名。它支援大規模群組、廣播頻道和廣泛的媒體／檔案共用。該服務在全球擁有數億活躍用戶。

濫用行為呈上升趨勢

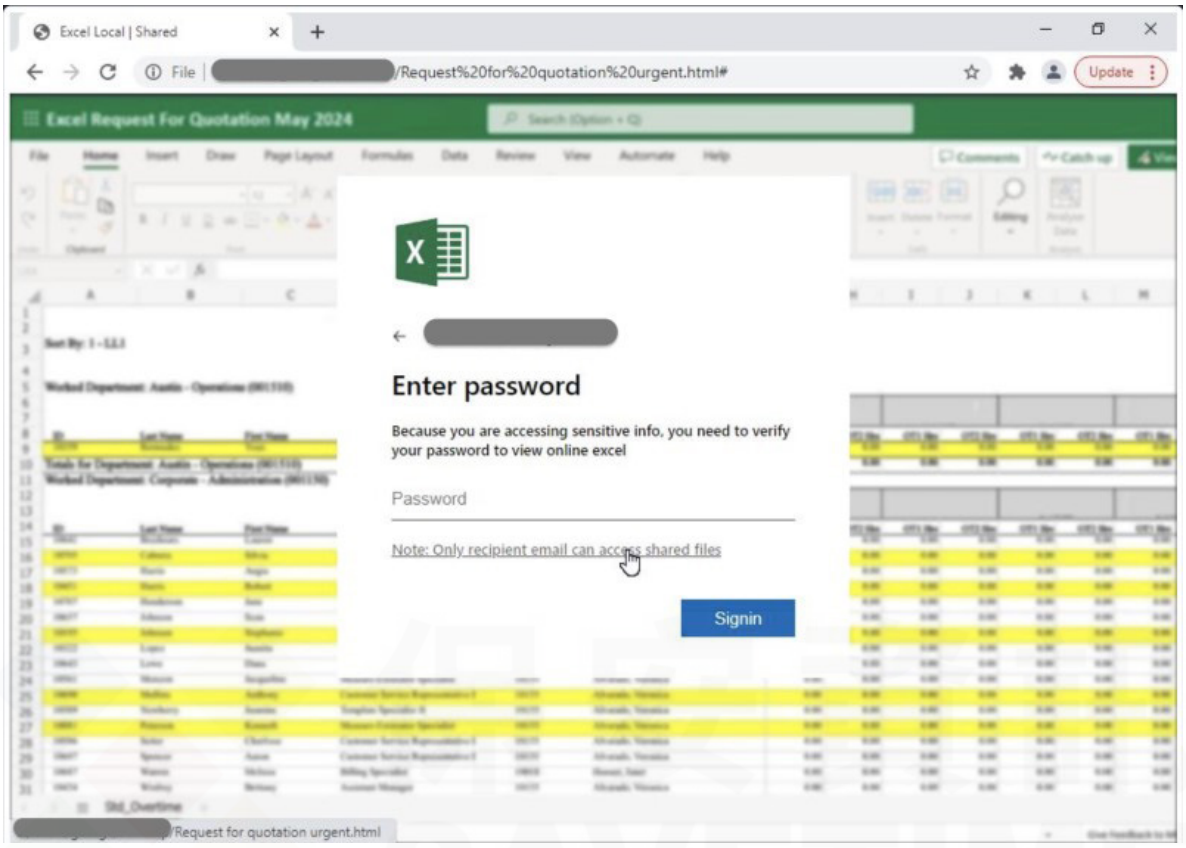
在過去幾個月裡，越來越多的網路釣客透過惡意 HTML 檔案，效仿惡意竊密程式和遠端存取木馬 (RAT)，現在還濫用 Telegram Bot API 來竊取用戶的憑證和其他敏感資訊，例如：信用卡詳細資訊。這些活動遍佈全球，它們可能給企業帶來重大的財務損失、運營中斷和信譽受損。攻擊者使用竊得的憑證進行帳戶劫持、身份／財務盜竊和其他攻擊，並經常在暗網上出售竊取的資料。

此增長原因有幾個關鍵因素。從威脅行為者角度來看，Telegram 提供的易用性和匿名性使其成為一個極具吸引力的選擇。Telegram Bot API 直接明瞭，只需最低限度的程式設計技能，並提供一種高效率、可擴展的方式來處理大量被盜資料。Telegram 的即時性使攻擊者能夠立即接收憑據和其他敏感資訊，使其能夠在受害者做出反應之前迅速採取行動 (例如：更改密碼、通知他們 IT 部門等)。此外，從傳統的網路釣魚滲透方法轉向新技術可以暫時規避現有類型的監控和保護。

攻擊工作流程

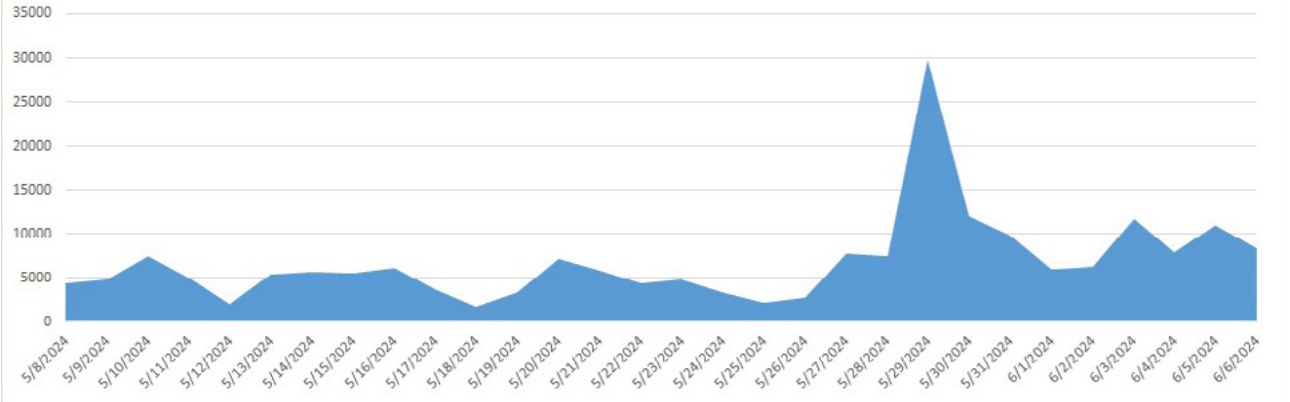
1. 攻擊者通常會先建立一個 Telegram 機器人，獲取允許機器人與 Telegram 伺服器通訊的 API 權杖。接著，攻擊者建立一個 Telegram 公開或私人頻道，機器人將在該頻道中發送竊取的憑證。
2. 發送給受害者的釣魚郵件包含 HTML 檔，其中大部分都偽裝成合法的辦公室文件 (PDF、Excel、Word 等)。被開啟後，這些檔會顯示一個偽造的登錄頁面，仿造安全文件登錄畫面的外觀。用戶被提示輸入憑證以『檢視』文件，但輸入的憑證不會瀏覽任何真實檔案，而是直接發送給攻擊者。
3. 被截取的憑證會透過 Telegram Bot API 發送給 Telegram 機器人。HTML 檔案中的 JavaScript 代碼會使用竊取來的憑證向 Telegram Bot API 發送 HTTP GET 或 POST 請求。腳本會防止表單以傳統方式提交，收集用戶名和密碼，並透過機器人將這些資訊發送到指定的 Telegram 頻道。
4. 最後，一旦憑證被發送給機器人，它們就會被發佈到 Telegram 頻道中。攻擊者可以即時監控該頻道，收集竊取的資訊。這種方法可以讓網路釣魚者以最小的代價有效率且匿名地收集憑證。

一份典型的偽造檔案，要求輸入使用者密碼



觀察到的惡意 HTML 表現出不同程度之混淆，並採用不同的腳本技術。下圖反映近期的攻擊趨勢。

濫用 Telegram 聊天機器「應用程式介面」(API) 的網路釣魚活動時序表



要在不斷變化的威脅環境中保持領先地位，就需要全天候監控、持續創新、自適應的安全政策以及跨技術的威脅情報共享。賽門鐵克整合所有功能且更強大威脅情資，以促進對本公告所述威脅的強大防禦，確保提供全面保護，最終讓用戶高枕無憂。

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：

- Phish.Html*
- Phish.TGhtml
- Scr.Phish!gen7

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。

2024/06/11

TellYouThePass 勒索軟體開採濫用存在PHP 程式語言中的 CVE-2024-4577 引數注入(Argument Injection)漏洞

CVE-2024-4577 是存在 PHP(一種流行的腳本工具) 中的高嚴重性 (CVSS風險評分：9.8) 引數注入 (Argument Injection) 漏洞。當 PHP 以 CGI 模式執行時，此漏洞會影響 PHP。如果成功開採濫用該漏洞，未經認證攻擊者可在受影響的 PHP 伺服器上執行任意程式碼，導致系統完全崩潰，並傳播包括勒索軟體在內的惡意軟體。TellYouThePass 勒索軟體組織就是利用這個最近修補過的漏洞。賽門鐵克的網路防護技術入侵防護系統 (IPS) 可阻止這些漏洞利用嘗試，防止系統受到進一步感染／破壞。

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.suspscript!g7
- Sonar.susplaunch!g18

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.Gen
- Ransom.Zombie

- 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: PHP-CGI Argument Injection Vulnerability CVE-2024-4577

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。

2024/06/11

Fog(*霧)勒索軟體

最近一種名為 Fog 的全新勒索軟體在真實網路情境中大肆傳播。該惡意軟體背後的攻擊者，一直在利用被洩露的 VPN 憑證攻擊美國教育和娛樂部門組織的脆弱網路。據報導，攻擊者還使用多種網路和通訊埠掃描程式，以及一種名為 SharpShares 的開源工具，讓他們搜尋並列出可存取的網路分享。Fog 勒索軟體會加密使用者檔案，並冠上『.fog』或『.flocked』副檔名。勒索 (贖金支付) 說明以檔名為『readme.txt』的文字檔形式發佈，其中包含受害者如何聯繫攻擊者來交涉贖金的說明。

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.Psxsv-Masq!g1
- ACM.Ps-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.PsExeSvc!gen2
- SONAR.SharpShares!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.Sharpshare
- 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。

2024/06/11

AZStealer--基於Python的惡意竊密程式

AZStealer 是最近發現一種基於 Python 的惡意竊密程式。它具有從遭入侵端點竊取各種資訊的功能，包括：瀏覽器中儲存的資料 (cookie、歷史記錄、書簽、密碼、已保存的信用卡資訊和自動填入的資料)、Discord 權杖、Steam、Uplay、Tiktok、Telegram、Twitch、Spotify、Reddit 或 Roblox 等其他應用程式的登錄對話。所有被竊取的資訊都會被壓縮，並根據壓縮檔大小直接透過 Discord webhooks 外洩出去，或先上傳到 Gofile 線上檔案儲存空間，再透過 Discord 外洩。AZStealer 還嘗試竊取帶有預定義目標副檔名或檔名中包含密碼、錢包、備份等特定關鍵字的檔案。

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：

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.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
- 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。

2024/06/11

Fireant進階持續威脅(APT)駭客組織鎖定越南企業，發動LNK捷徑檔的網路攻擊行動

據報導，Fireant(又稱 Mustang Panda) 進階持續威脅 (APT) 駭客組織，利用 Windows 捷徑 (.LNK) 檔發起一場惡意軟體攻勢。該威脅行為者以越南企業為目標，引誘它們遵守與教育部門和稅務法規相關的規定。攻擊載體是帶有惡意 .LNK 捷徑檔的壓縮檔 (zip、rar) 附件的網路釣魚電子郵件。最終的有效載荷據了解是 PlugX 遠端存取木馬 (RAT)，可以讓攻擊者在遭入侵的系統上遠端執行各種命令。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!gen5

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。

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: PHP-CGI Argument Injection Vulnerability CVE-2024-4577

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。

2024/06/11

小心Python套件索引(PyPI：Python Package Index)的軟體儲存庫中惡意Python套件(Package)

在 Python 套件索引 (PyPI：Python Package Index) 的軟體儲存庫中發現許多惡意 Python 套件 (Package)，其目的是利用輸入錯誤來攻擊合法套裝軟體的用戶。例如：一個名為『crytic-compilers』的套件偽裝成合法函式庫『crytic-compile』，目的在傳播 Lumma 惡意竊密程式。另一個惡意 PyPI 套件『pytoileur』能夠下載和安裝木馬化的 Windows 二進位檔案，用於監視、常駐和竊取加密貨幣等目的。

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：

- Downloader
- Infostealer
- Trojan Horse
- Trojan.Gen.2
- 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。

2024/06/11

DERO針對Kubernetes基礎設施的加密劫持行動

經常被形容為「雲端的作業系統」的 Kubernetes 是一個開源平台，可用於管理容器化應用程式和服務的叢集。根據 2023 年 3 月的一份報告，加密貨幣 Dero比Monero 具有更好的隱私性、匿名性和更快的回報速度，經常被用於加密劫持。威脅研究人員最近一份報告討論加密劫持攻擊行動的演變過程，其中攻擊載體包括利用外部可存取且啟用匿名身份驗證的 Kubernetes API 伺服器。獲得存取權限後，攻擊者使用和善的名稱在各種 Kubernetes 命名空間中部署加密工作負載，以逃避檢測。

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：

- OSX.Trojan.Gen.2
- Trojan Horse
- 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!300
- Heur.AdvML.A!400
- 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。

2024/06/10

狼狽為奸：使用PhantomLoader的SSLoader惡意軟體

SSLoader 惡意軟體使用 PhantomLoader(一種部署惡意軟體的有效工具) 來增強其難以捉摸的隱秘行為。這種惡意軟體透過釣魚郵件攻擊行動進行滲透，在躲避檢測的同時執行偵查，並在透過各種技術交付有效載荷的同時將資料滲回給威脅行為者。

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

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.Gen.MBT
- PUA.Gen.2
- WS.Malware.1
- WS.SecurityRisk.3

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

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。

2024/06/10

又見JScript類型的遠端存取木馬(RAT)，透過網路釣魚行動傳播

承如大家所熟悉 JScript 類型的遠端存取木馬 (RAT) 通常透過網路釣魚傳播，最近發現一次攻擊使用與以前相同的技術，即初始載入器腳本連接到 C&C 伺服器，觸發新惡意腳本 (稱為第二階段載入器) 的傳輸。然後，該載入器會從伺服器獲取一個 JScript RAT 元件，進而達成常駐並執行從伺服器接收到的命令。

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.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：

- ISB.Downloader!gen40
- Web.Reputation.1
- WS.SecurityRisk.4

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。

2024/06/10

濫用Google廣告傳播偽裝成進階IP掃描器的後門惡意軟體

在真實網路情境中觀察到一個偽裝成進階 IP 掃描軟體的惡意後門軟體。Advanced IP Scanner 是一款適用於 Windows 的免費網路掃描程式，主要提供 IT 管理人員用於分析區域網路 (LAN) 和收集有關連接設備的資訊。然而，在過去一年中，該工具已成為水坑式攻擊的目標。威脅行動者一直在模仿合法網站並濫用 Google 廣告，以確保其惡意網站在搜索結果中排名優先。作為攻擊鏈的一部分，偽裝安裝程式被用來部署和載入 CobaltStrike beacon。

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

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。

2024/06/10

透過魚叉式網路釣魚偽裝成政府機構的新型Grandoreiro銀行木馬攻擊行動

在真實網路情境中發現 Grandoreiro 銀行木馬涉入的新行動。威脅行動者利用偽裝成政府機構信函的魚叉式網路釣魚電子郵件，誘使收件人下載暗藏惡意軟體的 ZIP 壓縮檔。Grandoreiro 是一種高度複雜、更能適應變化的 Windows 銀行木馬，首次在 2016 年被發現。它能夠劫持瀏覽器對話、搜索電子郵件帳戶、從網路瀏覽器中竊取憑證、收集作業系統和已安裝軟體的詳細資訊，並將收集到的資料外洩到其 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：

自適應防護技術(包含於SESC)：

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

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!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。

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!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。

2024/06/10

Agent Tesla發送惡意XLA文件

Agent Tesla 是一款基於 .Net 的資訊竊取型遠端存取木馬 (RAT)，最近被觀察到發送西班牙語系的惡意垃圾郵件，並附帶 XLA 文件。這些檔案利用 Office 文檔中多個舊漏洞 (CVE-2017-11882 和 CVE-2017-0199)，導致 Excel 自動下載並打開遠端存放的惡意 RTF 和 JS 檔，最終導致 Agent Tesla 感染。

賽門鐵克博通公司感謝網路威脅聯盟 (CTA) 成員 Fortinet 分享有關該惡意軟體的初始樣本。CTA 成員利用這些情報為客戶快速部署保護措施，並有系統地瓦解惡意網路行為者。瞭解有關網路威脅聯盟的更多資訊。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

基於行為偵測技術(SONAR)的防護：

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

VMware Carbon Black 產品的防護機制：

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

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：

- Bloodhound.RTF.12

- Bloodhound.RTF.20
- Exp.CVE-2017-11882!g2
- Exp.CVE-2017-11882!g3
- Scr.Malcode!gen59
- Trojan.Gen.2
- Trojan Horse

基於機器學習的防禦技術：

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

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: Malicious RTF File CVE-2017-0199
- Audit: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity 568

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。

2024/06/09

偽造的『Windows、Office註冊機 KMSpico啟動工具』被用來發送Vidar惡意竊密程式

研究人員最近發現另一個偷渡式下載惡意行動，用戶被受騙下載一個名為『Windows、Office 註冊機 KMSpico 啟動工具』的惡意軟體。該工具在市場上被稱為 Windows 的 『通用啟動程式』，但已不再維護。該攻擊利用 Java 依賴性和惡意 AutoIt 腳本來禁用 Windows Defender，最終透過 shellcode 解密 Vidar 有效載荷。Vidar 的主要功能是從瀏覽器和數位錢包中竊取敏感的使用者資料。不過，這種惡意竊密程式也可以作為勒索軟體的下載器。

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：

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：

- Trojan.Gen.MBT

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。

2024/06/07

有利可圖的地方就有江湖～Sticky Werewolf 新興APT駭客集團

Sticky Werewolf 駭客集團，最初發現於一年多以前。據瞭解，該鎖定各種組織機構為目標，最近的目標是製藥和航空部門。在他們的攻擊手法中，發現利用惡意捷徑檔 .lnk 文件檔來偽裝成 .docx 檔案、.pdf 文件檔來當誘餌、惡意批次檔和 AutoIT 腳本等。Sticky Werewolf 在行動中傳播最終有效載荷包括各種遠端存取木馬 (RAT) 和惡意竊密程式。以前攻擊中傳播的惡意軟體系列包括 Rhadamanthys 惡意竊密程式、Ozone 遠端存取木馬 (RAT)、MetaStealer 惡意竊密程式、DarkTrack 和 NetWire。

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-Reg!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-TJs!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen804
- SONAR.SuspLaunch!g221
- SONAR.SuspPE!gen32
- SONAR.SuspStart!gen18
- 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

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。

2024/06/07

Seidr惡意竊密程式

Seidr 是最近在真實網路情境中發現並透過非法市場銷售的另一個惡意竊密程式。該惡意軟體基於 C++，採用模組化架構。從功能上看，Seidr 可從遭入侵的端點竊取各種資訊，包括作業系統相關資訊、透過鍵盤側錄從系統瀏覽器收集到的資料、加密貨幣錢包等。Seidr 利用 Telegram 實現資料外滲和指揮控制 (C&C) 目的。

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.MalTraffic!gen1
- SONAR.Stealer!gen1

VMware Carbon Black 產品的防護機制：

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- 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!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。

2024/06/07
DORRA勒索軟體

DORRA 是最近發現的 Makop 惡意軟體家族的勒索軟體後繼新變種。該惡意軟體會加密使用者檔案，並冠上『.DORRA』副檔名、唯一 ID 和開發者的電子郵件位址。該勒索軟體會以名為『README-WARNING.txt』的文字檔形式發送勒索 (贖金支付) 說明，要求受害者透過提供的電子郵件與攻擊者聯繫，以獲取有關資料解密的進一步說明。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Makop!g1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.B

2024/06/07
Apache RocketMQ成為Muhstik殭屍網路攻擊行動的目標

據觀察，最近發生一起針對 Apache RocketMQ 平臺的攻擊行動，利用一個已知漏洞 (CVE-2023-33246) 執行遠端代碼。作為行動一部分，威脅行動者正在部署以分散式阻斷服務攻擊(DDoS)攻擊著稱的 Muhstik 殭屍網路。Muhstik 可提供常駐能力、逃避檢測、執行橫向移動，並透過 IRC 命令和控制伺服器進行通訊。該惡意軟體可用於加密貨幣挖礦和發起分散式阻斷服務攻擊。

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.Kaiten
- 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: RocketMQ RCE CVE-2023-33246

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。

2024/06/06

增強版『Vidar 惡意竊密程式』問世

在真實網路情境中觀察到一種更新版的 Vidar 惡意竊密程式。這種可定制的惡意軟體以惡意軟體即服務 (malware-as-a-service) 的形式在暗網和 Telegram 頻道上銷售，利用社交媒體平臺作為其命令和控制基礎設施的一部分，並與 STOP／Djvu 勒索軟體和 SmokeLoader 後門等其他惡意軟體進行合作。該惡意軟體採用 C++ 語言開發，目標是受害者的個人資訊、網路瀏覽器資料、加密貨幣錢包、金融資訊、通訊應用程式等。它能躲避檢測，並將敏感性資料從遭入侵系統外洩到其 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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-Rgasm!g1
- ACM.Rgasm-Lnch!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer.Vidar
- 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

VMware Carbon Black 產品的防護機制：

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

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。