保安資訊--本周(台灣時間2023/12/29)
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 58 萬 300 台受保護端點上總共阻止了 5,740 萬次攻擊。這些攻擊中有 80.7% 在感染階段前就被有效阻止：**(2023/12/25)**

- 在**9萬6,800**台端點上，阻止了**1,650**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**16萬6,000**台端點上，阻止了**1,420**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬**台**Windows**伺服主機上，阻止了**1,060**萬次攻擊。
- 在**5萬8,300**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬7,600**台端點上，阻止了**74萬2,900**次嘗試掃描在**CMS**漏洞。
- 在**4萬1,700**台端點上，阻止了**120**萬次嘗試利用的應用程式漏洞。
- 在**22萬1,900**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**1,670**台端點上，阻止了**180**萬次加密貨幣挖礦攻擊。
- 在**11萬5,000**台端點上，阻止了**930**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**712**台端點上，阻止了**30萬8,300**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 1.35 萬個受保護端點上阻止了總計 590 萬次攻擊。**(2023/12/24)**

- 使用網頁信譽情資，在 **1.209** 萬個端點上阻止 **510** 萬次攻擊。
- 攔截 **28.5K** 個端點上 **570.3K** 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 **11.4K** 個端點上攔截 **175.8K** 次瀏覽器通知詐騙攻擊。
- 在 **498** 個端點上攔截 **39K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。
- 在 **915** 個端點上阻止 **2.6K** 次技術支援詐騙攻擊。
- 在 **184** 個端點上阻止 **511** 次加密劫持嘗試。

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。

2023/12/27

荷蘭International Card Services BV發行的Visa信用卡，持卡人正遭受網路釣魚之苦

賽門鐵克發現新一波網路釣魚行動專門針對荷蘭 International Card Services BV 發行的 Visa 信用卡持卡人，以竊取憑證／帳密。在這波網路釣魚行動中，奇怪是網路釣手並沒有附上網路釣魚網頁的超連結，而是將其與電子郵件內容一起以純文字形式包含在內。在這次網路釣魚行動中，電子郵件收件人被要求驗證他們的電子郵寄帳號。有趣的是，在這個所謂的電子郵件驗證過程中，受害者需要在瀏覽器中複製／貼上或手動輸入實際的網路釣魚網址。一旦開啟該釣魚網頁，受害者就會看到憑證/帳密登入的網頁。

電子郵件示例：

- 原文主旨：laaste herrinering uw aandacht is vereist.
- 翻譯後主旨意思：最後一次提醒您注意。
- 原文主旨：Heeft u een momentje voor ons?
- 翻譯後主旨意思： 您有空嗎？
- 原文主旨：Opnieuw identificeren bij Ics
- 翻譯後主旨意思：請重新確認身份
- 原文寄件者：Mijn ICS Alerts <redacted_email_address>
- 翻譯後寄件者：我的 ICS 警報 <redacted_email_address>

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。

2023/12/27

TISAK勒索軟體

TISAK 是在真實網路情境所發現的全新勒索軟體。它似乎是 Proxima／BlackShadow 勒索軟體家族的後繼新版本。它會加密使用者檔案，並冠上 .Tisak 的副檔名。加密完成後，一個檔名為 Tisak_Help.txt 的勒索 (贖金支付) 說明的文字檔會被存放在被加密檔案的相同目錄內。該惡意軟體會終止各種系統程序和服務以及刪除卷影副本的功能。該勒索軟體幕後的主使者還採取雙重勒索伎倆，如果不乖乖就範付贖金，就會公佈受害者遭竊的資料。

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：

基於行為偵測技術(SONAR)的防護：

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

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/12/27

Adobe用戶請小心～假冒Adobe Creative Cloud電子郵件通知的網路釣魚正流行

Adobe Creative Cloud 為平面設計、影片編輯、網頁開發、攝影……等，提供完整的專業應用程式組合。最近，賽門鐵克發現一些冒充 Adobe Creative Cloud 並誘使使用者打開虛假通知電子郵件的網路釣魚案件。電子郵件本文內容簡潔，藉故存儲在雲端的待處理的工作檔案。這些釣魚電子郵件試圖誘使使用者打開並點擊釣魚網頁。受害者點擊電子郵件內容中顯示的釣魚網址之後，就會被導引到誘使填寫憑證／帳密的釣魚網頁。

電子郵件示例：

- 主旨： 您從 AdobePDF 收到了一份文件檔
- 主旨 您收到了一份新文件檔

- 寄件者：AdobePDF AdobePDF<遭變造過的電子郵件位址>
- 寄件者：Adobe Adobe <遭變造過的電子郵件位址>

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。

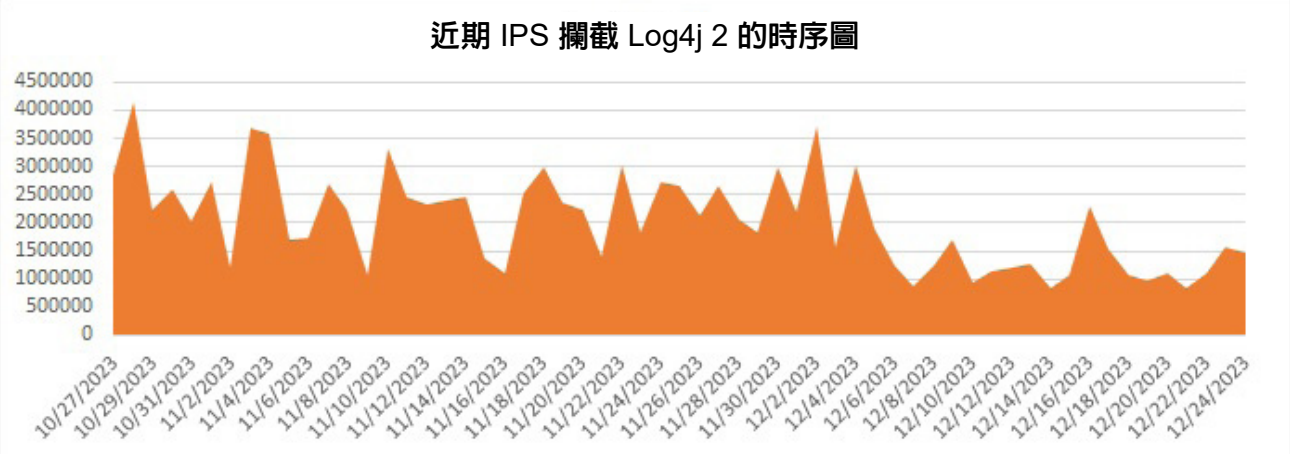
2023/12/26

防護亮點：IPS(入侵防禦系統)阻止了數百萬次Log4j攻擊

眾所周知，有許多漏洞早已被修補，但仍被世界各地的駭客組織和個體戶大肆開採濫用。雖然大多數漏洞在被披露的當年影響最大、破壞性最強，但有些漏洞在多年後仍然非常有效，例如：Log4j RCE CVE-2021-44228。

該漏洞於 2021 年被披露，被廣泛稱為『Log4Shell』，是 Apache Log4j 2 函式庫 (一種常見基於 Java 的日誌應用系統) 中出現一個嚴重等級的安全性漏洞。這個漏洞能導致應用程式被提權，讓遠端攻擊者得以有足夠的權限來執行任意程式碼，對尚未完全修補漏洞採用 Log4j 的日誌系統所有應用系統或程式構成重大風險。

賽門鐵克每天都能監控到世界各地的威脅行動者試圖開採濫用這個漏洞，您可以從下面 IPS(入侵防禦系統) 遙測圖表中看到這一點 (請注意，賽門鐵克將這些攻擊攔截為『Log4j2』)。雖然我們針對這一漏洞提供其他防護機制，包括標準的防毒技術和基於安全政策強制的 DCS 政策，但由於攻擊的性質 (網路層，無檔案行威脅) 我們的 IPS 技術能夠更好地防禦這一漏洞，本文章僅介紹我們基於網路的保護措施--IPS。



網路有許多探討關於陳年老舊或已經進行修補的漏洞持續遭受惡意行動者開採濫用資訊。其中一些主要原因如下：

- **老舊系統**：組織繼續使用老舊的系統是個棘手問題，這些系統難以升級，儘管有可用的修補程式，但仍暴露在風險中。
- **資訊落差**：並非每個人都能及時瞭解情況或採取行動。漏洞意識和進行修補之間的落差使攻擊者得開採濫用已知的弱點。
- **資源不足**：巧婦難為無米之炊 (尤其是中小型企業組織) 資源不足導致無法定期更新，使其容易遭開採濫用。
- **料敵如神**：攻擊者戰略性地瞄準眾所周知的漏洞，看準並非所有系統都會及時進行修補的心態。
- **拿捏平衡**：系統管理員在安全性和運行穩定性之間取捨掙扎，往往會延遲進行修補以避免重新開機或藍+底字的中斷。
- **人類的惰性**：拒絕改變是常見的人格特質，這也是為什麼儘管存在已知風險，但陳年漏洞仍持續被開採濫用的主因。

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 多重防護技術能在第一時間就偵測到該惡意程式及有效對應**零時差**攻擊的防護機制及其威脅名稱：

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: Log4j2 RCE CVE-2021-44228 2
- Attack: Log4j2 RCE CVE-2021-44228 4

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。

2023/12/26

資料分析系統Qlik Sense已知的CVE-2023-41266路徑遍歷漏洞正被大肆開採濫用

CVE-2023-41266 是一個影響資料分析系統 Qlik Sense 的路徑遍歷漏洞。如果成功開採濫用該漏洞，未經身份驗證的遠端攻擊者可建立匿名會話。這樣，他們就可以將 HTTP 請求傳輸到未經授權的端點。賽門鐵克的網路層防護技術：入侵預防技術 (IPS) 已根據威脅狀況監控結果進行了掃描，掃描結果顯示近期開採濫用該漏洞的情況有所上升。賽門鐵克的網路層防護技術：入侵預防技術 (IPS) 會阻止這些漏洞利用嘗試，以防止對系統造成進一步感染/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：

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: Qlik Sense Enterprise Path Traversal CVE-2023-41266

2023/12/26

Xamalicious安卓手機惡意軟體

Xamalicious 是一款針對安卓平臺的手機後門惡意軟體。該惡意軟體使用 Xamarin 框架構建，這是一個使用 .NET 和 C# 建立應用程式的開源／開放原始碼平臺。此前，該惡意軟體已透過寄生在 Google Play 和其他第三方平臺上的各種 APP 進行傳播。Xamalicious 具有收集受感染裝置資訊的功能，包括硬體資訊、已安裝 APP 清單、地理位置資訊和網路服務提供商資訊等。第二階段有效籌載可讓攻擊者完全控制受感染的設備，並執行其他欺詐任務。

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：

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

2023/12/25

恐懼下的直覺反應容易上當～幣安土耳其(Binance Turkey)用戶落入冒名的金融犯罪調查委員會(MASAK)的監管圈套

幣安 (Binance) 是全球最大的加密貨幣交易所。世界各地紛紛出現更多針對 Binance 用戶的網路釣魚行為，賽門鐵克最近發現一個針對土耳其 Binance 用戶的網路釣魚行動。這些資訊中，社交工程伎倆與其他更常見的手法有所不同。在這裡，他們假冒金融犯罪調查委員會 (MASAK)--土耳其負責打擊洗錢和恐怖主義融資的監管機構--進行的監管有關的帳戶問題 (阻止用戶購買、出售和轉移加密貨幣) 為幌子來誘騙用戶。

觀察到惡意簡訊：

- BN Turkiye hesabiniz Masak denetimi sebebiyle alim-satim ve transfer islemlerine kisitlanmisitr. hxxps://bitly[.]ae/verifty B002

如果用戶沒有警覺性上鉤並點擊簡訊中的惡意短網址，他們將被轉導向到一個虛假的幣安土耳其 (Binance Turkey) 登錄頁面。

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

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。WebPulse 已知道此次活動中使用假冒的 Binance 域名。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2023/12/25

就是要K你～駭客集團UAC-0099持續鎖定烏克蘭組織的網路砲火不曾中斷

『UAC-0099』是一個小有名氣的駭客集團，至少從 2022 年中就開始鎖定烏克蘭為目標。在最近一些攻擊行動中，攻擊者一直在利用 RAR .SFX 自解壓縮檔、偽裝成 WordPad 編寫的 .LNK 捷徑檔以及 PowerShell 腳本和 LoanPage VBS 惡意軟體有效籌載。據觀察，UAC-0099 還在其攻擊感染鏈中開採濫用已知的 WinRAR CVE-2023-38831 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：

基於行為偵測技術(SONAR)的防護：

- ACM.Ps-Base64!g1
- ACM.Ps-TVbs!g1
- ACM.Ps-Wscr!g1
- ACM.Schtsk-TVbs!g1
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen4
- CL.Downloader!gen241
- Exp.CVE-2023-38831
- ISB.Downloader!gen63
- ISB.Downloader!gen77
- Scr.Malcode!gen
- Scr.Mallnk!gen1
- Scr.Mallnk!gen6
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- 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。

2023/12/25

Bandook惡意軟體--老當益壯的威脅在真實網路情境依舊能興風作浪

Bandook 是一種遠端存取木馬，早在 2007 年就被發現。雖然這是一個相當古老的惡意軟體家族，但時至今日，Bandook 後繼新版本仍在真實網路情境依舊能興風作浪。拆解最近一次事件來分析，Bandook 寄生在惡意的 PDF 檔來進行傳播，後繼導致下載受密碼保護的 7z 壓縮檔，一旦解壓縮就會還原為 Bandook 有效籌載。感染後，惡意軟體將執行從攻擊者所操控的 C&C 伺服器接收到的命令。該有效籌載還具有更多的功能，可以下載其他任意模組和可執行檔。

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：

- ACM.Untrst-RunSys!g1
- SONAR.ProcHijack!gen9
- SONAR.SuspBeh!gen306
- SONAR.SuspBeh!gen397
- SONAR.TCP!gen1

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.Pidief
- Scr.Malcode!gen
- Web.Reputation.1
- 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

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。

2023/12/24

菲國最大銀行BDO UNIBANK用戶正遭受惡意簡訊為害之苦

Banco De Oro (BDO) Unibank 是菲律賓最大的銀行，也是東南亞排名前 20 的銀行之一。在過去幾個時期，賽門鐵克發現該銀行手機用戶經常收到惡意簡訊，攻擊者試圖誘使沒有警覺心的使用者提供敏感資訊，最終導致金融盜竊。雖然這一波攻擊行動主要還是影響消費者，但也發現有針對企業用戶。

惡意簡訊的社交工程利用帳號限制和時間緊迫感，設定 24 小時的最後期限。網路釣手利用短網址重新導向到釣魚／詐騙網站。短網址是模糊／掩蓋連結目的地的一種常見手法，這樣可以更容易地誘騙人們點擊網路釣魚連結或瀏覽有害的網站。

惡意簡訊和網址示例：

- [BANCO DE ORO] 您的帳戶因無法識別的嘗試而被限制，如不採取措施，您的帳戶將在 24 小時內被終止。在此更新 shorten[.]e/BDO_ONLINEPAY

- [BANCO DE ORO!] 您的帳戶因無法識別的嘗試而被限制，如不採取措施，帳戶將在 24 小時內被終止。更新 shorten[.]e/BDO-VerifyMyAccount
- [BANCO DE ORO] 您的帳戶因未識別的嘗試而被限制，如果不採取措施，帳戶將在 24 小時內被終止。在此更新 shorten[..]e/BDO-OnlineUpdate

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

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。WebPulse 已知道此次活動中使用假冒的 BDO 域名。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2023/12/24

竊密惡意軟體：Agent Tesla不放假，聖誕假期期間利雅德銀行(Riyad Bank)遭冒名發送大量垃圾郵件

通常在聖誕假期期間，惡意軟體活動會比較少，但這並不意味著沒有惡意軟體。各種不同媒介的攻擊 (例如：電子郵件、瀏覽網頁時的順道下載、漏洞開採濫用等) 仍在繼續。最近，一個知名的竊密惡意軟體：Agent Tesla 引起賽門鐵克的注意，該惡意軟體冒充沙烏地阿拉伯主要金融機構利雅德銀行 (Riyad Bank)，是該國資產規模最大的銀行之一。

惡意電子郵件 (主旨：Riyad Bank Trade Finance Transaction Notification--REF2023122047047) 同時發送給當地 (沙烏地阿拉伯) 和國際組織 (無論是否與當地有聯繫)。附件是一個冒充圖片檔的 7z 壓縮檔 (Payment_Advice.JPEG.7z)，內含的 Agent Tesla 二進位檔案也冒充付款說明檔，實則為執行檔 (Payment_Advice.exe)。

這種威脅是一種遠端存取木馬 (RAT) 和惡意竊密程式的多功能惡意程式，已經存在好幾年了，現在仍然非常猖獗。全球有多個駭客集團和個體戶還在使用它。它被用來進行財務和身份盜竊，以及資料洩露--可以外傳敏感的公司資訊或洩露機密檔案，有時還會轉為勒索。

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)。

基於機器學習的防禦技術：

- 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：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/12/22

儲億銀行(Truist Financial)儲戶成為新型網路釣魚郵件的攻擊目標

儲億銀行 (Truist Financial) 是美國排名前八的商業銀行，總部位於北卡羅來納州夏洛特市。最近，賽門鐵克發現新一波利用虛假帳戶通知欺騙 Truist Bank 服務的網路釣魚。電子郵件內容提到對您的帳戶進行了『待處理的交易』，在完成適當驗證後，這筆待處理交易金額就會消失，不必實際真的付費。它誘使用戶點擊『立即驗證 』的釣魚網址，準備竊取憑證。

電子郵件主旨：

- 主旨：關於您帳戶的重要更新
- 主旨：帳戶通知
- 主旨：驗證您的詳細資訊
- 主旨：緊急通知
- 寄件者：『儲億銀行』< 亂編的郵件帳號>

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。

2023/12/22

MetaStealer惡意竊密程式透過惡意廣告散播

MetaStealer 是一款早在 2022 年就被發現的竊密惡意程式。據瞭解，它透過惡意垃圾郵件散播行動以及與盜版軟體捆綁的方式傳播。最近，該惡意軟體還被發現透過惡意廣告傳播。點擊廣告後，受害者會被重導向到偽裝成 AnyDesk 或 Notepad++ 軟體下載入口網站登陸頁面。MetaStealer 具有從本地瀏覽器收集各種資訊、竊取憑證／帳密、加密貨幣錢包、從各種第三方應用程式中擷取資料等功能。

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：

基於行為偵測技術(SONAR)的防護：

- ACM.Ps-Rd32!g1
- ACM.Rd32-CPE!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!300
- 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。

2023/12/22

Chameleon(*變色龍)安卓惡意軟體後繼版本繞過生物識別身份／帳號驗證

Chameleon 是一種安卓網路銀行惡意軟體，於 2023 年初首次出現。該惡意軟體曾涉入早期針對澳洲和波蘭安卓用戶的攻擊行動中，並偽裝成銀行或加密貨幣 APP 進行傳播。Chameleon 的功能包括鍵盤側錄、簡訊內容收集、憑證竊取和 Cookie 竊取等。最近發現該後繼版本允許攻擊者繞過受感染裝置上的生物識別身份／帳號驗證，迫使其退回到標準身份驗證手段，例如：輸入 PIN 碼和解鎖設備。

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.1
- Android.Reputation.2

2023/12/22

F5用戶請留意～HamsaUpdate網路攻擊行動

HamsaUpdate 網路攻擊行動是最近發現針對使用 F5 網路設備的以色列客戶之攻擊行動。據報導，攻擊者利用檔案清除惡意軟體 (Wiper) 攻擊 Windows 伺服器 (採用 Hatef 惡意程式) 和 Linux 平臺 (採用 Hamsa 惡意程式)。初始攻擊鏈源於夾帶 .zip 壓縮檔的釣魚電子郵件所發起，壓縮檔中包含一個偽裝成 F5 更新工具的 .NET 應用程式。部署的惡意軟體載入器 (Loader) 具有執行檔案清除惡意軟體有效籌載的功能。在檔案清除過程中，惡意軟體會透過 Telegram 與攻擊者持續連線，提供受感染電腦的最新狀態以及運行中的清除任務的進度。

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：

基於行為偵測技術(SONAR)的防護：

- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1
- AGR.Terminate!g2
- SONAR.MalTraffic!gen1
- SONAR.SuspLaunch!g220
- SONAR.SuspLaunch!g221
- SONAR.SuspPE!gen32
- SONAR.SuspStart!gen18
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!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。