保安資訊--本周(台灣時間2023/09/01)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 66 萬 2,900 台受保護端點上總共阻止了 7,850 萬次攻擊。這些攻擊中有 86.3% 在感染階段前就被有效阻止：**(2023/08/28)**

- 在**13萬4,300**台端點上，阻止了**3,070**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**21萬2,000**台端點上，阻止了**1,660**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬7,600**台**Windows**伺服主機上，阻止了**1,240**萬次攻擊。
- 在**8萬7,500**台端點上，阻止了**240**萬次嘗試掃描伺服器漏洞。
- 在**1萬3,900**台端點上，阻止了**89萬3,300**次嘗試掃描在**CMS**漏洞。
- 在**6萬5,900**台端點上，阻止了**130**萬次嘗試利用的應用程式漏洞。
- 在**23萬2,200**台端點上，阻止了**550**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬2,800**台端點上，阻止了**200**萬次加密貨幣挖礦攻擊。
- 在**14萬3,200**台端點上，阻止了**890**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**2,000**台端點上，阻止了**8萬1,700**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。

2023/08/31

SapphireStealer惡意竊密軟體

SapphireStealer 是一種基於 .NET 的開源惡意竊密軟體，自 2022 年12 月前後公開發布以來，在真實網路情境回報的案例越來越多。該惡意軟體的目標是對各種資料進行竊取外洩，包括遭入侵主機的資訊、瀏覽器中存儲的憑證、螢幕截圖以及存在磁碟中符合預定義標準的檔案和圖像檔。拆解最近 SapphireStealer 相關行動的攻擊鏈發現，名為 FUD-Loader 的惡意軟體載入程式一直用來向受害者傳送有效籌載。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Infostealer.Eynice
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.2

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

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。

2023/08/31

中了#勒索軟體怎會是『Good day～美好的一天』

感染勒索軟體的當下，肯定不會是美好的一天 (Good Day)，但是居然有自稱 Good Day 的勒索軟體，大概只有它們自己是美好的一天。Good Day 是 ARCrypter 勒索軟體的變種，它的名字源於其贖金支付網站上的問候語。該勒索軟體最近被假冒成 Microsoft Windows Update 的更新檔案進行散布。成功啟動後，它將加密檔案並冠上 .crYpX 的副檔名，其中 X 是大寫字母，通常以 A 開頭，直到 E。

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.Gen
- WS.Malware.1

基於機器學習的防禦技術：

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

2023/08/31

BadBazaar惡意軟體透過被植入木馬的Signal和Telegram APP傳播給Android 用戶

在網路上有人回報已經感染 BadBazaar 惡意軟體，該惡意軟體是透過被植入木馬的熱門 APP：Signal 和 Telegram 來散播給安卓平台的用戶。名為 Signal Plus Messenger 和 FlyGram 的惡意 APP 最初出現在 Google Play 商店和三星 Galaxy 商店中，但後來被下架。由名為 GREF 的威脅組織發起的 BadBazaar 惡意軟體攻擊行動此前曾被用於針對維吾爾族和突厥等其他少數民族。被加料的 APP 功能正常，毫無異狀，但是在背景默默執行，用戶毫無察覺。BadBazaar 木馬的功能主要專注在間諜活動和資料竊取。該惡意軟體能夠收集有關受感染裝置的各種資訊，包括 IMEI 號碼、MAC 位址、位置資訊和 Wi-Fi 網路資訊等。

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：

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

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。

2023/08/31

MMRat：安卓平台上的惡意軟體

MMRat 是新發現的安卓／Android 平台上的惡意軟體，在針對東南亞的網路攻擊行動中被利用。該惡意軟體使用自定義 Protobuf 通訊協定從遭入侵的裝置中竊取資料。MMRat 一直以來偽裝成官方應用商店網路釣魚網站進行傳播。惡意軟體的功能包括裝置資訊收集、鍵盤側錄、啟動錄影、擷取螢幕解鎖畫面和資料外洩等。透過濫用輔助功能服務，惡意軟體允許攻擊者遠端控制裝置，從而執行其他惡意活動，例如：銀行欺詐。

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.Malapp
- 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。

2023/09/30

免費的永遠最貴～貪圖免費Robux遊戲幣未成，反而感染加密勒索軟體

Robux 是 Roblox 平台上的虛擬貨幣，Roblox 是近來很受歡迎的線上遊戲平臺，也是元宇宙概念的遊戲平台，允許用戶建立、分享和玩其他用戶建立的遊戲。Robux 作為其遊戲幣，玩家可以用來購買虛擬物品、配件、自訂虛擬人偶選項和其他遊戲素材。這些素材可以增強遊戲體驗，也可以讓玩家在 Roblox 宇宙中展現出自己的特色。

Robux 可以經由多種管道獲得，包括用現實世界的貨幣購買、透過 Roblox 聯盟計畫賺取、參與開發者交換計畫等。許多玩家試圖使用遊戲外掛來從事不當的行為，希望免費獲得 Robux，但這往往要付出高昂的代價，因為惡意團體和個人會對這些玩家下手。

在最近的一個例子中，賽門鐵克發現一個透過瀏覽網頁的順道下載攻擊行動，歹徒將勒索軟體偽裝成假冒的 Robux 印鈔機程式。如果成功執行，它就會加密檔案，並要求受害者使用 Element 加密型群組通訊軟體 APP 與他們聯繫並支付價值 50 美元的比特幣。

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.SuspBeh!gen625

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/08/30

Openfire 上的CVE-2023-32315漏洞，被開採利用來傳播Kinsing惡意軟體

CVE-2023-32315 是Openfire的一個身份驗證繞過漏洞，早在 2023 年 5 月就被披露。未經身分驗證的攻擊者可建立新的管理員帳號而接管這些系統，影響 Openfire 管理主控台(Openfire是熱門的開源即時通訊系統)。如果該漏洞被利用，未經身份驗證的用戶就可以存取 Openfire 管理主控台中的受限部分，並上傳惡意外掛程式，進而可能導致受影響應用程式的全面崩潰。根據最近的一份報告，在真實網路情境發現了利用這個漏洞傳播 Kinsing 惡意軟體的新攻擊行動。攻擊者一直在使用上傳到 Openfire 控制台的惡意外掛程式來部署 Kinsing 有效籌載，這反過來又會導致在受感染主機上下載和執行挖礦惡意軟體。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Maljava
- 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：

- Attack: Openfire Authentication Bypass Vulnerability CVE-2023-32315

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。

2023/08/29

5月初披露的CVE-2023-33246 RocketMQ漏洞，已經被DreamBus殭屍網路開採利用

CVE-2023-33246 是一個歸屬於簡訊傳送和串流媒體平台：Apache RocketMQ 的遠端程式碼執行 (RCE) 漏洞。該漏洞早在今年 5 月初就已經被披露，如果被成功開採利用，遠端攻擊者可以執行任意程式碼。根據最新的報告，名為 DreamBus 的模組化殭屍網路在新觀察到的攻擊行動中重新出現，該攻擊行動開採利用 RocketMQ 漏洞，進行初始存取和惡意軟體派送。DreamBus 功能包括執行 bash 腳本、其他模組功能和下載以及執行XMRig挖礦軟體的有效籌載。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Linux.Mirai
- Trojan Horse
- 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: 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)：

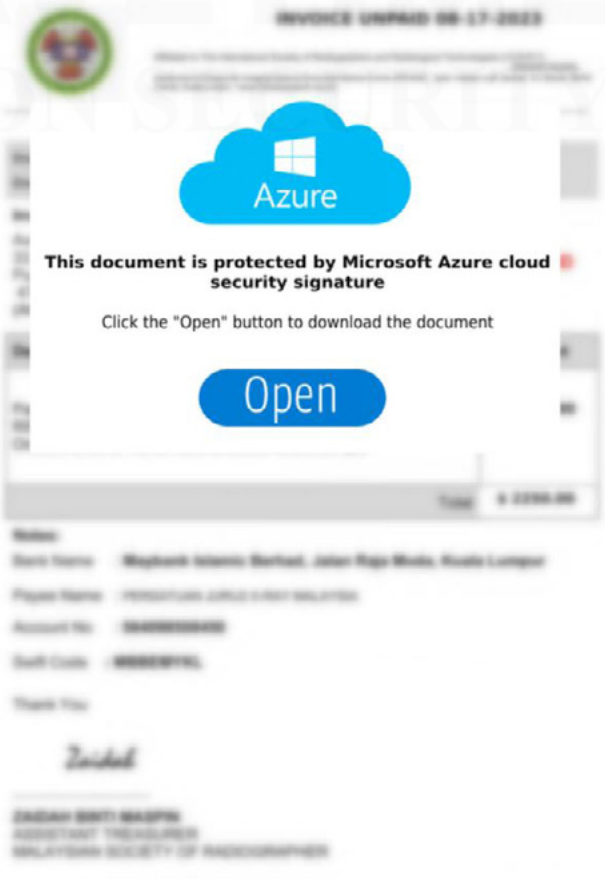
被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2023/08/29

防護亮點：7月和8月的IcedID惡意攻擊行動

IcedID（也稱為Bokbot）是一種眾所周知的模組化銀行金融木馬惡意軟體，最初出現在 2017 年左右的威脅環境中。它與時俱進並不斷發展，如今更常被用作其他惡意模組和有效負載（包括勒索軟體）的載入器。IcedID 透過魚叉式網路釣魚行動廣泛散布。過去，它還經常在其他惡意軟體 (例如：Emotet) 的攻擊鏈中散布附帶負載。

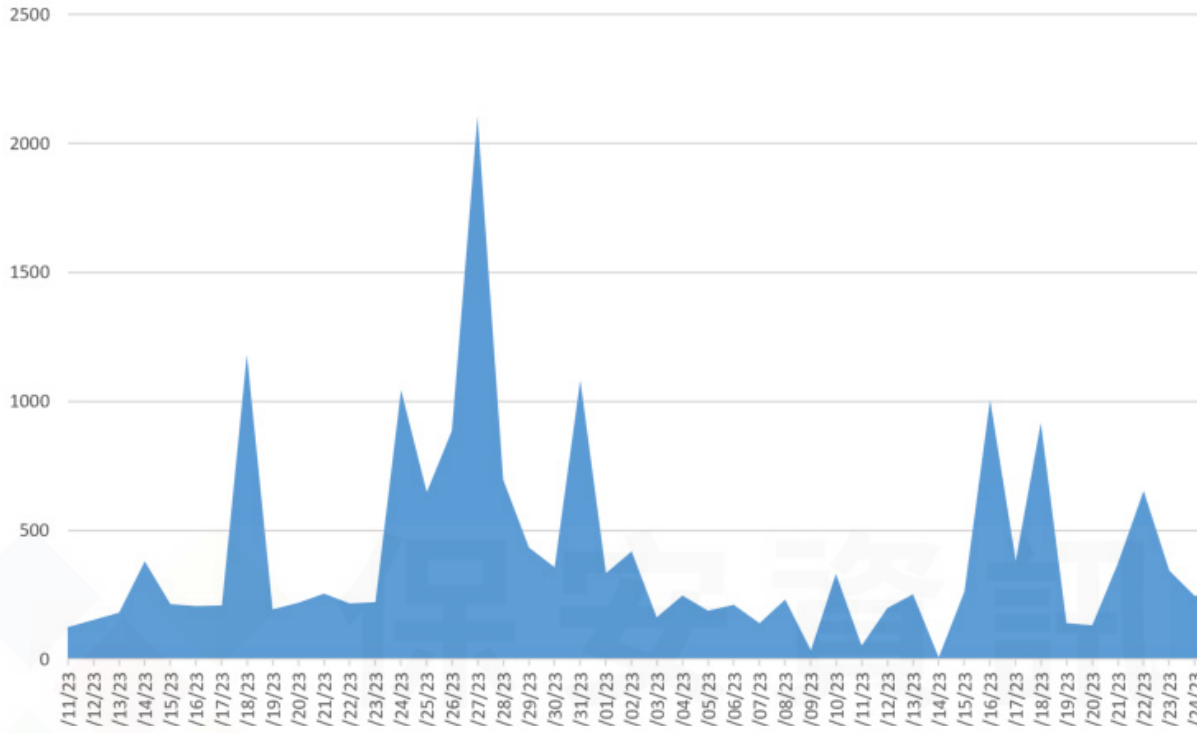
賽門鐵克觀察到，由於惡意垃圾郵件活動依舊節節攀升，7 月和 8 月 IcedID 相關活動也明顯增加。8 月份的最新攻擊樣貌以多階段的攻擊鏈為主，其中涉及由惡意垃圾郵件傳遞的檔名，例如：『Doc_Scan_08_18』或『Document_08_22』的 PDF 檔。惡意 PDF 檔聲稱已經過安全軟體檢查的發票檔案，誘騙受害者放下戒心直接點擊『下載』或『打開』按鈕來下載所需的檔案，如右圖所示。



單擊該鏈接後，受害者會被重定向到包含惡意 JavaScript 的網址，該網址一旦執行，就會將 IcedID 有效籌載以 .dll 二進位檔案件的形式傳遞到受感染的電腦上。

下圖顯示過去兩個月攔截到的 IcedID 的次數，以每日細分：

過去兩個月攔截到的 IcedID 的次數，以每日細分



賽門鐵克提供的解決方案內建多層級防護技術，個別技術多能在第一時間就具備**零時差**防護的能力並有明確的定義，僅就不同防護技術說明如下：

基於行為偵測技術(SONAR)的防護：

- SONAR.IcedID!g4
- SONAR.IcedID!g5
- SONAR.SuspLaunch!g235
- SONAR.TCP!gen1

基於端點偵測與回應(EDR)：

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics, Techniques, and Procedures, TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多資訊，請參閱此鏈接：https://github.com/Symantec/threathunters/tree/main/Trojan/IcedID
- 賽門鐵克的端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

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.DLHeur!gen1
- Scr.IcedID!gen1
- Scr.IcedID!gen3
- Scr.Malcode!gdn28
- Scr.Malcode!gen46
- Scr.Malpdf!gen2
- Trojan.IcedID
- Trojan.IcedID!g16
- Trojan.IcedID!g17
- Trojan.IcedID!g18
- Trojan.IcedID!gm
- Trojan.Gen.MBT
- Trojan Horse
- 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
- 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 592
- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 764
- System Infected: Trojan.Backdoor Activity 765
- 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。

欲深入瞭解更多有關於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。
欲深入瞭解有關賽門鐵克基於雲的網絡安全服務 (WebPulse) 的更多訊息，請點擊此處。
欲瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
欲深入瞭解更多有關於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。
欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲瞭解更多有關於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。

2023/08/28

Linux系統上的Desktop Bus(D-Bus)API被LaZagne駭客工具濫用於進行資訊擷取

LaZagne 是源於開放原始碼的熱門密碼復原工具，已知被多個網路上的歹徒用於竊取憑證／帳密。隨著許多駭客組織對 Linux 系統的覬覦與投入，LaZagne 的 Linux 版本也在真實網路情境裡日益被廣泛的使用。據觀察，LaZagne Linux 模組利用 D-Bus API 竊取包括憑證在內的機敏資料。D-Bus (『Desktop Bus』的縮寫) 是類 Unix 系統 (Unix-like) 中常用的一種機制，允許多個組件和應用程序之間進行通訊。最近利用 D-Bus API 的 LaZagne 攻擊行動一直致力於從 Pidgin 或 KWallet 等應用程序中擷取資訊。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Hacktool.LaZagne
- Hacktool.LaZagne!gen1
- Infostealer
- SecurityRisk.LaZagne
- 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。

2023/08/25

CollectionRAT--被北韓國家級APT駭客組織Lazarus拿來發動網路攻擊的全新惡意軟體

CollectionRAT 是北韓國家級 APT 駭客組織 Lazarus 最近在網路攻擊行動所利用的另一個惡意軟體。該惡意軟體與另一個稱為 EarlyRAT 的惡意軟體家族表現出某些相似之處，該惡意軟體家族之前被認為是 Andariel 駭客組織所為。CollectionRAT 具有收集有關遭入侵系統的資訊並執行遠端命令的功能。它還能夠運行從遠端 C&C 伺服器下載的附加有效籌載。據報導，Lazarus 在攻擊的初始階段越來越依賴開放原始碼工具的使用。此類工具的一些示例包括 DeimosC2 或 Malicious Plink。

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
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- 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
- Heur.AdvML.A!300
- 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。

2023/08/25

開採利用IT管理軟體ManageEngine的CVE-2022-47966漏洞，北韓國家級APT駭客組織Lazarus 散播QuiteRAT木馬程式

據報導，北韓國家級 APT 駭客組織 Lazarus，在最新的攻擊行動中開採利用 ManageEngine 的 CVE-2022-47966 漏洞。該漏洞是一個未經身份驗證的遠端程式碼執行 (RCE) 漏洞，影響二十多個 Zoho 公司的 ManageEngine IT 管理軟體，如果該漏洞被成功開採利用，遠端攻擊者可以在易受攻擊的伺服器上執行任意命令。最近 Lazarus 活動中發現的惡意有效籌載之一是遠端存取木馬 (RAT)，稱為 QuiteRAT。該惡意軟體基於 Qt 框架，屬於 MagicRAT 惡意軟體家族。在功能方面，它能夠收集有關遭入侵系統的基本資訊、執行遠端命令以及下載和運行其他有效籌載。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen6

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.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: Zoho Manageengine RCE Vulnerability CVE-2022-47966

基於安全強化政策(適用於使用DCS)：

Windows 版本上的賽門鐵克的重要主機防護系統：DCS(Data Center Security) 內建的強化政策就能夠針對開採利用 CVE-2022-47966 漏洞的威脅提供零時差保護。預設最小權限與最低資源機制的沙箱運行環境，可完全防止安裝 webshell 和惡意軟體工具、並可完全阻絕任意應用程式、系統命令的執行。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。

2023/08/25

也會竊取加密貨幣錢包的Hakuna Matata勒索軟體

Hakuna Matata 是最近在真實網路情境所發現到的另一種全新勒索軟體。該勒索軟體採用 AES-256 加密演算法，並具有停用與備份軟體相關的程序和服務的功能，以及刪除受感染端點上的陰影複製 (shadow copies) 等功能。據觀察，Hakuna Matata 的某些版本還包含加密貨幣錢包地址剪貼簿置換偷竊模組，允許攻擊者將受害者的加密貨幣錢包地址與惡意軟體攻擊者擁有的地址交換。

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.RansomGen!gen3

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Hakuna
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B