保安資訊--本周(台灣時間2024/02/02)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 57 萬 2,900 台受保護端點上總共阻止了 5,730 萬次攻擊。這些攻擊中有 83.5% 在感染階段前就被有效阻止：**(2024/01/30)**

- 在**10萬9,000**台端點上，阻止了**1,820萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**14萬9,000**台端點上，阻止了**1,330萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬1,200**台**Windows**伺服主機上，阻止了**1,050萬**次攻擊。
- 在**6萬7,000**台端點上，阻止了**190萬**次嘗試掃描伺服器漏洞。
- 在**1萬2,600**台端點上，阻止了**80萬4,600**次嘗試掃描在**CMS**漏洞。
- 在**4萬7,200**台端點上，阻止了**120萬**次嘗試利用的應用程式漏洞。
- 在**22萬7,200**台端點上，阻止了**490萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬2,700**台端點上，阻止了**150萬**次加密貨幣挖礦攻擊。
- 在**11萬500**台端點上，阻止了**800萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**707**台端點上，阻止了**13萬7,100**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 15.86 萬個受保護端點上阻止了總計 630 萬次攻擊。**(2024/01/30)**

- 使用網頁信譽情資，在 **142.5K** 個端點上阻止 **550** 萬次攻擊。
- 攔截 **33.3K** 個端點上 **620.7K** 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 **12.1K** 個端點上攔截 **154K** 次瀏覽器通知詐騙攻擊。
- 在 **512** 個端點上攔截 **40.6K** 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 **857** 個端點上阻止 **1.3K** 次技術支援詐騙攻擊。
- 在 **181** 個端點上阻止 **500** 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。

2024/02/01

Jenkins的CVE-2024-23897透過CLI的任意檔案讀取漏洞可能會導致遠端執行任意程式碼

CVE-2024-23897 是一個最近揭露的影響 Jenkins 的嚴重等級 (CVSS 風險評分：7.5) 任意檔案讀取漏洞，Jenkins 是由 java 所撰寫 CI(Continuous Integration--持續整合)／CD(Continuous Deployment--持續部署) 工具，可以透過網頁 UI 來設定編譯、佈署的參數，並觸發整個 CI／CD 流程。該漏洞是由受影響版本 Jenkins CLI 命令分析器中的錯誤引起。如果被成功開採濫用，未經認證的遠端攻擊者可讀取任意檔案，並可能洩漏儲存在 Jenkins 控制器檔案系統上的敏感資訊。賽門鐵克的網路層防護技術入侵預防系統 (IPS) 可攔截這些漏洞利用嘗試，以防止對系統造成進一步感染／入侵。

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: Jenkins Arbitrary File Read Vulnerability CVE-2024-23897

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，

可以保護底層的 UNIX 伺服主機免受此漏洞侵擾，包括防止執行任意命令和限制查看關鍵的作業系統檔案。

- DCS 的網路規則政策可設定為，將 Jenkins 應用程式限制為受信任的用戶端。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/02/01

在真實網路情境上發現全新的VileRAT遠端存取木馬變種的蹤跡

一種與 DeathStalker(Evilnum) 駭客組織有關的 VileRAT 遠端存取木馬全新變種，在真實網路情境上被發現。VileRAT 是採用 Python 所撰寫，具有遠端存取、鍵盤側錄、遠端命令執行和資訊收集……等功能。最近觀察到的網路攻擊行動利用 NSIS 安裝程式和 VileLoader 惡意軟體載入器來傳輸 VileRAT 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.Dropper!gen2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Dropper
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Reputation.1

基於機器學習的防禦技術：

- 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。

2024/01/31

勒索(贖金支付)說明居然有多語系可切換～Lockxx勒索軟體

據報導，又有一種勒索軟體在亞洲、歐洲和美國出現。這種威脅一旦入侵成功，就會進行檔案加密並冠上 .lockxx 的副檔名。此外，它還會以 HTML 應用程式檔 (lockxx.recovery_data.hta) 留下中英文內容的勒索 (贖金支付) 說明，受害者還可以透過頁面的頂部按鈕切換語系。

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.SuspLaunch!g193
- ACM.Wmic-DlShcp!g1
- SONAR.SuspLaunch!g189
- SONAR.SuspLaunch!g340
- SONAR.SuspLaunch!g341
- SONAR.SuspLaunch!g195
- SONAR.SuspLaunch!g250

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!100

2024/01/31

俄羅斯的進階持續性威脅(APT)駭客組織發起魚叉式網路釣魚行動

一個俄羅斯 APT 駭客組織利用各種主題的魚叉式網路釣魚行動 (主題例如： NASA、USAID……等) 來攻擊俄羅斯反對派組織。受害者被誘騙開啟一個偽裝成 PDF 的 LNK 檔案，該檔會執行一個屬於名為 HTTP-Shell 開源專案的 Powershell 腳本。該工具具有上傳／下載檔案功能、C&C 選項以及在目錄間輕鬆移動。

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：

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：

- CL.Downloader!gen12
- CL.Downloader!gen241
- CL.Downloader!gen263
- Scr.Malcode!gen
- WS.Malware.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。

2024/01/31

CVE-2023-22527--存在Atlassian Confluence的遠端程式碼執行(RCE)漏洞，正在被大肆開採濫用

CVE-2023-22527 是 Atlassian Confluence Data Center 和 Server 中的一個嚴重等級 (CVSS 分險評分：10) 的 OGNL(Object-Graph Navigation Language) 物件圖導航語言注入漏洞。如果成功開採濫用此漏洞，未認證的遠端攻擊者可在受影響的實例上實現遠端代碼執行 (RCE)。賽門鐵克的網路防護技術入侵預防系統 (IPS) 可阻止這些漏洞利用嘗試，防止對系統造成進一步感染／入侵。Confluence 是 Atlassian 強大的團隊協作和文件管理平台。

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: Atlassian Confluence RCE CVE-2023-22527

2024/01/31

Pawn Storm駭客集團(又名 APT28)的最新活動

Pawn Storm(又名 APT28 或 Fancy Bear*奇幻熊) 是一個在威脅領叱吒風雲約二十年的威脅組織(最有名的戰功是影響美國大選翻盤的網路釣魚行動)。在過去的一年中，該駭客集團鎖定政府機構、國防工業、金融、能源和運輸……等，不同行業的大量受害者發起有針對性的 NTLMv2 雜湊中繼攻擊。據瞭解，Pawn Storm 在其攻擊行動中利用魚叉式網路釣魚、暴力攻擊以及開採濫用已被公開揭露的漏洞。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen241
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1
- WS.Malware.2

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

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 721
- 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。

2024/01/31

Phobos勒索軟體家族又有新變種：FAUST

據報導，FAUST 勒索軟體是源於 Phobos 勒索軟體家族的新變種。FAUST 變種可利用 VBA 腳本為行動的一部分在 Office 文件檔中傳播。該勒索軟體會加密使用者檔案，並冠上『.faust』副檔名，並留下 info.hta 和 info.txt 的勒索贖金支付說明檔。這些檔案用在加密受害者檔案後與駭客的聯繫。受害者被提示透過電子郵件或 TOX 加密訊息與攻擊者聯繫，進行贖金交涉。

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：

- CL.Downloader!gen38
- CL.Downloader!gen205
- Ransom.Phobos!gm1
- Trojan.Malfilter
- Trojan.Maladd
- Trojan Horse
- Web.Reputation.1
- WS.Malware.1

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

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。

2024/01/31

偽裝成服飾品牌的Ducktail惡意軟體鎖定行銷專業人員

Ducktail是一個惡意軟體家族，自 2021 年年中開始活躍。該惡意軟體擅於擷取瀏覽器 cookie，並從受害者的社交媒體帳戶利用社交媒體對話中竊取敏感資訊，目的是獲得控制權並為自己的經濟利益做廣告。

在最近一次攻擊行動，人們發現 Ducktail 惡意軟體偽裝成日本知名服裝品牌，以市場行銷專業人員為目標。該惡意竊密程式幕後的主使者鎖定的重點在與服裝公司相關的數位行銷專案、工作描述、各種職位的計畫以及政策和薪資資訊。攻擊者使用 Telegram 作為他們的 C&C 管道，利用 Telegram Bot 轉出竊取的資料。

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：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen1
- Trojan.Ducktail!gen1
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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。

2024/01/30

KrustyLoader後門程式開採濫用VPN連線軟體漏洞

CVE-2024-21887 和 CVE-2023-46805 是 Ivanti(一款遠端存取 VPN 連線軟體) 最近披露的兩個零時差漏洞。這兩個漏洞被證實是存在未經驗證的遠端程式碼執行和身份驗證繞過的缺陷。報告顯示，老練的駭客集團很快就開採利用這些漏洞以部署一個採用 Rust 撰寫的惡意軟體，發現該漏洞的研究人員似乎將其命名為『KrustyLoader』。該惡意軟體目的終究是下載與 Cobalt Strike 性質類似的駭客工具 Sliver。

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.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: Ivanti ICS CVE-2023-46805
- Web Attack: Ivanti ICS CVE-2024-21887

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。

2024/01/30

Werewolves勒索軟體

Werewolves 是至少從 2023 年初就開始活躍的勒索軟體家族，他們採取檔案加密破壞和恐嚇出售被盜資料的雙重勒索伎倆。根據其受害者名單，他們主要以俄羅斯的公司為目標，但也向歐洲和美國的公司擴展。

賽門鐵克發現兩個由 Werewolves 勒索軟體變種發佈的勒索 (贖金支付) 說明。從內容上看，兩者都是用俄語書寫，措辭相同，但格式不同。在最近分析的一個樣本中，勒索軟體會在每個資料夾中存放 LETTER.TXT 檔案。加密檔的副檔名為 .crypt。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Generic.1

基於機器學習的防禦技術：

- Heur.AdvML.B!200

2024/01/30

防護亮點：如何避免空投(Airdrop)騙局？賽門鐵克發現以加密貨幣熱門流行語為幌子的惡意網域名稱

利之所在、趨之若鶩～隨著加密貨幣孳生的網路犯罪的日益增加，在我們對威脅環境的持續監控過程中，賽門鐵克發現一大批可疑的網域名稱 (800 多個)，它們的名稱中使用『airdrop(*空投)』。Airdrop一詞通常與更廣泛的加密貨幣領域相關聯，加密貨幣空投是指將數位資產從加密貨幣專案轉帳分發至多個錢包位址。這種分發可以出於各種原因，例如：推廣新專案、獎勵

現有加密貨幣持有者或鼓勵用戶採用。Airdrop 通常被用作一種行銷策略，以提高知名度並吸引更多用戶。

不幸的是，那些心懷不軌的人也注意到這些熱門流行語，並在他們的網域名稱或計畫中使用 Airdrop(包括些許的變化) 一詞，以利用該詞在加密貨幣社群的流行和熟悉程度。在過去 6 個月中，已有 2700 多個黑心網域名稱使用這個熱門流行語。

加密貨幣和 Airdrop 的關聯造成合法的假像，吸引對接收免費代幣或貨幣感興趣的人。事實上，網域名稱資料庫目前紀錄有 5,800 多個網域名稱包含『airdrop-』、『-airdrop』或『aiirdrop』字樣。賽門鐵克已對這些網域名稱進行審查和適當分類，並對惡意或可疑的網域名稱進行特別警示。

在最近觀察到可疑網域名稱中，大部分都是透過 Cloudflare 或 DDoS-Guard Ltd (俄羅斯) 的IP所代管的，還有一些分佈在熱門的社交媒體平臺上。一些案例包括仿造已知區塊鏈平臺 (例如：Manta Network) 和加密交易服務所 (例如：Binance 和 Coinbase) 的網域名稱。雖然有些網域名稱是活躍的，但許多網域名稱目前還不是，但以後可能會與網路釣魚、詐騙或惡意軟體偷渡式下載有關。

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：

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。

賽門鐵克端點防護(SEP)的瀏覽器延伸功能：

- 根據我們 2023 年 1 月發佈的瀏覽器延伸公告，如果瀏覽器延伸偵測到某個網址是惡意的，SEP 就會將用戶轉導向到賽門鐵克的預設封鎖頁面，通知已攔截 (注意，該瀏覽器延伸功能現在也適用於 Microsoft Edge 瀏覽器)。

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。
欲瞭解有關賽門鐵克端點防護 (SEP) 瀏覽器擴展的更多訊息，請點擊此處。

2024/01/29
Atlantida惡意竊密程式

有報導指出，另一種名為 Atlantida 的惡意竊密程式已在網路上四處流竄，透過遭入侵網站上的惡意 HTA 檔案進行傳播。這種威脅與許多其他同類的威脅類似，同樣以登錄憑證、加密貨幣錢包和瀏覽歷史記錄……等大量資料為目標，毫無新意可言。

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.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

基於機器學習的防禦技術：

- Heur.AdvML.B!100

2024/01/29
GitLab帳戶接管漏洞CVE-2023-7028

CVE-2023-7028 是一個帳戶接管漏洞，被評為嚴重漏洞 (CVSS 風險評分為 10)。該漏洞影響 GitLab Community Edition (CE) 和 Enterprise Edition (EE) 應用程式的身份驗證機制。如果成功開採濫用該漏洞，攻擊者可以在不與使用者互動的情況下接管 Gitlab 帳戶。GitLab 已在產品版本 16.7.2、16.5.6 和 16.6.4 中發佈修復程式。該修復程式也已回溯至產品版本 16.1.6、16.2.9 和 16.3.7。

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: GitLab Account-Take-Over Vulnerability CVE-2023-7028

2024/01/29
DHC勒索軟體

據觀察，DHC 勒索軟體有多個流通的版本。在成功入侵電腦並加密檔案後，檔名為 READ_IT.txt 的勒索贖金支付說明檔會存放到受害者的電腦上，提示支付 42 美元比特幣以購買解密軟體。勒索贖金支付說明包括電子郵件地址和 Discord 伺服器參考資料等詳細聯繫資訊。值得注意的是，該惡意軟體可以停止各種系統進程和服務，並刪除卷影副本備份。

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.SuspDrop!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.HiddenTear!g1
- Ransom.Sorry
- WS.Malware.1

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

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。

2024/01/28

虛構的線上遊戲別入戲太深～小心NOOSE勒索軟體

在另一起 Chaos 勒索軟體案例中，攻擊者自稱是國安局 (National Office of Security Enforcerment／NOOSE)，這是一個在《俠盜獵車手》線上遊戲中，但不存在真實世界中的虛擬政府機構。若成功入侵並加密後，勒索軟體會留下勒索 (贖金支付) 說明文字檔 (OPEN_ME.txt)，指示受害者向提供的加密錢包支付價值 1,540 美元的門羅幣 (XMR)。目前，該攻擊者沒有採用雙重勒索策略，似乎是透過偷渡式下載的社交工程來手法來攻擊單一台電腦。

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-RLsass!g1
- ACM.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry

2024/01/28

透過惡意廣告傳播的遠端存取木馬(RAT)

據報導，駭客利用 Google 搜索結果，透過惡意廣告向試圖規避中國對 Telegram 或 LINE 的嚴格限制的使用者安裝惡意軟體。VPN 可以讓使用者能夠瀏覽受限平臺並搜索上述被禁應用程式，但他們可能會被誘騙下載一個宣告成被禁的應用程式的惡意軟體安裝檔，而實際上該安裝程式是一個遠端系統管理木馬 (RAT) 的安裝檔，能夠讓攻擊者完全控制受害者的裝置。

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

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

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。

2024/01/26

全新竊密惡意程式：Rage(*狂怒煉獄) Stealer

Rage Stealer 是一種全新竊密惡意程式，它能秘密潛入受害者系統，將各種形式的個人儲存資料 (登錄憑證、自動填入的歷史記錄、信用卡／加密貨幣錢包……等)，從遭入侵的電腦上蒐集並透過 Telegram API，與攻擊者所操控的 C&C 伺服器協作來滲出。

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：

- 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

2024/01/26

觀察到Ivanti Secure Connect VPN的零時差漏洞被大肆開採濫用

最近揭露 Ivanti Connect Secure 和 Ivanti Policy Secure 的兩個零時差漏洞 CVE-2023-46805 和 CVE-2024-21887 已被大肆開採濫用。拆解其涉入的攻擊鏈發現，該漏洞利用攻擊得以讓攻擊者在未經驗證的情況下遠端執行程式碼。已觀察到的攻擊顯示，透過可存取網際網路和內部的遭入侵電腦與裝置部署 webshell。

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 ICS CVE-2023-46805
- Web Attack: Ivanti ICS CVE-2024-21887

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。

2024/01/26

AllaKore遠端存取木馬(RAT)涉入最近鎖定墨西哥銀行的網路攻擊行動

AllaKore 遠端存取木馬 (RAT) 已經被證實涉入在真實網路情境上，鎖定墨西哥銀行和加密貨幣交易機構的網路攻擊行動。該行動的最新軌跡顯示，攻擊者利用惡意 .msi 檔案和基於 .NET 的惡意程式載入器，來部署被加過料的 AllaKore RAT 惡意有效酬載。AllaKore 是一種基於 Delphi 的開源惡意軟體，至少在 2013 年就已為人所知。該惡意軟體具有多種功能，包括鍵盤側錄、螢幕截圖、反向殼層執行、剪貼簿劫持或下載和執行惡意二進位檔案。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer.Bancos
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Reputation.1
- 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

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: Bad Reputation Application Network Activity
- System Infected: Bad Reputation Process Request 4
- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 638

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PD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)。