保安資訊--本周(台灣時間2024/01/19)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 3,800 台受保護端點上總共阻止了 5,810 萬次攻擊。這些攻擊中有 82% 在感染階段前就被有效阻止：**(2024/01/15)**

- 在**10萬5,400**台端點上，阻止了**1,780**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**15萬9,100**台端點上，阻止了**1,350**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬1,000**台**Windows**伺服主機上，阻止了**1,040**萬次攻擊。
- 在**5萬9,700**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬3,900**台端點上，阻止了**80萬5,900**次嘗試掃描在**CMS**漏洞。
- 在**5萬4,400**台端點上，阻止了**130**萬次嘗試利用的應用程式漏洞。
- 在**21萬8,700**台端點上，阻止了**480**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,600**台端點上，阻止了**170**萬次加密貨幣挖礦攻擊。
- 在**11萬4,500**台端點上，阻止了**880**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**763**台端點上，阻止了**30萬2,700**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。

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 15.26 萬個受保護端點上阻止了總計 650 萬次攻擊。**(2024/01/15)**

- 使用網頁信譽情資，在 **137.6K** 個端點上阻止 **570** 萬次攻擊。
- 攔截 **30.7K** 個端點上 **622K** 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 **11.8K** 個端點上攔截 **161.9K** 次瀏覽器通知詐騙攻擊。
- 在 **543** 個端點上攔截 **51.3K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。
- 在 **931** 個端點上阻止 **1.5K** 次技術支援詐騙攻擊。
- 在 **205** 個端點上阻止 **634** 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。

2024/01/18

Bigpanzi：駭入並操弄智慧電視與聯網機上盒的駭客組織

最近有報導稱，近十年來，一個相對不起眼的駭客組織『Bigpanzi』一直在全世界感染安卓平台的聯網電視和 eCos 作業系統的機上盒。Bigpanzi 主要利用兩種惡意軟體工具：『pandoraspear』和『pcdn』，採用假冒正牌的 APP 和韌體版本更新……等多種欺騙手法對聯網電視或聯網機上盒進行滲透。

Pandoraspear 是一個複雜的後門程式，它能控制 DNS 配置，建立命令與控制 (C&C) 通訊，並執行接收到的命令。它採用先進的規避技術，包括修改動態連結、OLLVM 編譯、UPX shell 和反偵錯機制。

同時，可利用 Pcdn 在遭入侵裝置上構建點對點 (P2P) 內容分發網路(CDN)，操弄其成為擁有分散式拒絕服務 (DDoS) 攻擊能力的殭屍裝置。

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 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。

2024/01/18

以Cash App手機上應用程式為誘餌的社交工程伎倆誘騙用戶感染Chaos勒索軟體

一個 Chaos 勒索軟體的後繼新變種在網路上大肆氾濫，透過 Cash App 社交工程為誘餌誘騙用戶進而感染手機。CashApp 是一個行動金融服務平臺，在美國和英國均有服務據點。

此活動背後的犯罪分子將惡意二進位檔案偽裝成一個與 CashApp 有關聯，但已遭駭客加料的惡意檔案。如果用戶執行該檔案，就會發現自己的檔案被加密、桌布被更換，隨附的勒索贖金支付說明，會要求用戶向指定的加密錢包地址支付價值 100 美元的比特幣。

保安網路知識：Cash App 是一個集合現金返還、投資、朋友間轉帳、行動支付、銀行帳戶功能於大成的 App。

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

2024/01/18

監控網路設備狀態流量開源工具Cacti(仙人掌)，存有CVE-2023-51448的SQL注入漏洞

CVE-2023-51448 是存在 Cacti(仙人掌) 的 SNMP 通知接收器產生盲目 SQL 注入 (SQLi) 的漏洞，Cacti 是一個網路監控和故障管理框架。成功開採濫用該漏洞，未經驗證的攻擊者可傳送精心打造的 HTTP GET 請求到端點 '/cacti/managers.php'，並帶有加料的 SQLi 籌載。這可能導致 Cacti 資料庫內容外洩或允許遠端指令執行。

保安網路知識：CACTI是一個結合 SNMP、RRDtool、MySQL 的前端管理軟體，提供相當豐富的網路或系統管理平台重要的分析工具，只要監控設備有支援 SNMP ……等通訊協定，就可以快速加入 CACTI 管理。

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: Cacti SQL Injection Vulnerability CVE-2023-51448

2024/01/18

Kuiper勒索軟體

Kuiper 是一個相對較新的勒索軟體家族，於 2023 年 9 月左右首次被觀察到，當時以勒索軟體即服務 (RAAS) 的形式進行銷售。Kuiper 勒索軟體家族支持不同的作業系統平臺，包括 Windows、Linux 和 macOS。該惡意軟體會加密使用者檔並冠上 .kuiper 副檔名。某些副檔名和資料夾會列為加密排外清單。其他功能會依不同版本而不同，可能包括更改桌布、加密後會自動刪除惡意軟體自身的二進位檔案、終止選定的系統進程或刪除卷影副本……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：

基於行為偵測技術(SONAR)的防護：

- ACM.Ps-Enc!g1
- ACM.Ps-Net!g1
- ACM.Untrst-RunSys!g1
- AGR.Terminate!g2
- SONAR.Cryptlocker!g42
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g190
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Heuristic!gen58
- OSX.Trojan.Gen
- Ransom.Kuiper
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- Heur.AdvML.C

基於端點偵測與回應(EDR)：

- 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/Ransomwares/Kuiper
- 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、Procedures，TTPs)。針對 Kuiper 勒索軟體攻擊的 TTPs 特別增強規則包括：

- Process Injection: Process Hollowing [T1055.012]
- Command and Scripting Interpreter: Windows Command Shell [T1059.003]
- Service Stop [T1489]
- Impair Defenses [T1562]
- System Services: Service Execution [T1569.002]
- Indicator Removal: Clear Windows Event Logs [T1070.001]
- Process Discovery [T1057]
- Data Encrypted for Impact [T1486]
- Command and Scripting Interpreter: PowerShell [T1059.001]
- Command and Scripting Interpreter [T1059]
- Obfuscated Files or Information [T1027]
- File and Directory Discovery [T1083]
- Command and Scripting Interpreter: Unix Shell [T1059.004]
- Ingress Tool Transfer [T1105]

● 賽門鐵克的端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

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。

2024/01/18

CVE-2021-3129--正被大肆開採濫用的Laravel網路應用程式框架中的遠端程式碼執行(RCE)漏洞

CVE-2021-3129 是 Laravel 網路應用程式框架中的一個嚴重等級的 (CVSS 風險評分：9.8) 遠端程式碼執行 (RCE) 漏洞。如果成功開採濫用此漏洞，未經認證的遠端攻擊者可以操控受害者系統，操控 Laravel 使用的所有資料庫和服務，並對整個基礎設施造成嚴重影響。賽門鐵克的網路防護技術入侵預防系統 (IPS) 已根據威脅狀況監測結果進行掃描，掃描結果表明近期利用該漏洞的情況有所上升。賽門鐵克的網路防護技術入侵防禦系統 (IPS) 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: Laravel RCE CVE-2021-3129

2024/01/17

Inferno Drainer(*地獄排水器)詐騙即服務(Scam-as-a-Service)

加密貨幣和非同質化代幣 (Non-Fungible Token，NFT) 每天都在遭受惡意軟體和網路釣魚攻擊者竊取資產的風險。其中一個值得注意的攻擊行動涉及使用『Inferno Drainer』詐騙即服務，這是一種網路犯罪服務，提供個體戶或駭客團體欺詐性服務或工具，收取費用或分潤。Inferno Drainer 利用惡意腳本模仿流行的 Web3 協議，使其能夠連接加密貨幣錢包並獲得使用者同意授權交易。

在過去一年中，Inferno Drainer 幕後主使者建立數千個釣魚網站用途的域名，覬覦的目標是各種知名的加密貨幣和 NFT 交易服務。報導顯示，他們可能已經竊取價值數百萬美元的加密貨幣。儘管 Inferno Drainer 的域名已被其運營商正式關閉，但其下線仍逍遙法外，並積極尋求其他詐騙即服務業者的參與。

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

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。

2024/01/17

新興的勒索軟體即服務(RaaS)：Pings勒索軟體

2024 年，勒索軟體依舊是網路安全領域不斷演變的重大威脅。新興的勒索軟體即服務(RaaS)改變網路犯罪的營運模式，允許同盟下線付費購買勒索軟體的攻擊服務，在不具備任何專業技術知識的情況下發起攻擊，通常透過社交工程和網路釣魚伎倆進行傳播。

最近一份報導凸顯一種以此模式而嶄露頭角的『Pings』之全新勒索軟體。這種惡意軟體會加密檔案，並冠上『.pings』的副檔名，然後在每個包含被加密檔案的目錄中留下一個檔名為『FILE RECOVERY.txt』的勒索 (贖金支付) 說明文字檔。攻擊者要求受害者支付比特幣，並指示受害者透過電子郵件與他們聯繫，提供受害者編號 ID，以進行贖金談判和解密程式。

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：

- 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

2024/01/17

瀏覽網頁的順道下載攻擊，助長Xeno-RAT遠端存取木馬的生生不息

Xeno-RAT 是一種遠端存取木馬，在過去幾個月中一直在網路環境中肆虐。由於該惡意軟體是開源的，公眾可以在公共軟體發展和版本控制代管服務、駭客論壇和社交媒體上獲取，因此許多駭客團體和個體戶都在使用該惡意軟體發動瀏覽網頁時的順道下載攻擊。

以受害者的分佈而言，消費者還是目前主要目標，因為 Xeno-RAT 二進位檔案被偽裝成熱門的線上遊戲安裝程式和駭客。不過，企業客戶也不能完全倖免，因為賽門鐵克也發現偽裝成驅動程式和設備相關軟體的伎倆。

這種威脅包括 HVNC(隱藏虛擬網路連線)、操控受害者的視訊像頭、即時麥克風監控、鍵盤側錄、螢幕控制……等常見的功能。

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：

- ACM.Untrst-Schtsk!g1
- SONAR.Dropper
- SONAR.SuspBeh!gen609

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

2024/01/17

SmokeLoader惡意程式持續鎖定烏克蘭機構組織為目標

SmokeLoader 是一種眾所周知的惡意軟體，它可以連線到攻擊者所操控的 C&C 伺服器，以便根據接收到的命令下載擴充模組或惡意軟體有效籌載。這種惡意軟體主要透過網路釣魚行動傳播。在最近觀察到的攻擊行動中，它繼續以烏克蘭的政府和公共機構以及醫療、建築和製造業的公司為目標。

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!g45

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.9

- 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

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。

2024/01/17

正在肆虐義大利的路攻擊行動：冒充義大利金融公司的手機APP上藏有Irata手機木馬

在義大利又發現一起 IRATA 手機木馬涉入的網路攻擊行動，這次行動的目標是義大利一家提供金融服務的金融機構 (CheBanca) 的手機／平板用戶。惡意 APP 的安裝檔『CheBancaToken.apk』很可能是透過惡意簡訊傳播，這是近年來手機被駭最典型的作案手法。用戶會收到一個惡意的網址鏈接 (hxxps[:]//www[.]app-nuova[.]com/CheBancaToken.apk)，假冒 CheBanca 的 APP 就透過這個網址下載並安裝。

Irata(又名伊朗遠端存取木馬) 是一款具有間諜軟體功能的安卓金融惡意軟體，至少從 2022 年起就開始活躍，並在全球範圍內不斷被發現。

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：

- 廣告資料庫：Generisk
- 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 已知道此次攻擊行動中使用假冒或誤植的域名。

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。

2024/01/17

AndroxGh0st惡意軟體

賽門鐵克安全機制應變中心 (Symantec Security Response) 瞭解到，最近美國網路安全暨基礎設施安全局 (CISA) 和聯邦調查局 (FBI) 就 AndroxGh0st 惡意軟體的一些活動聯合發出的警戒報告。AndroxGh0st 是一個採用 python 撰寫的殭屍網路，用於讀取各種廣泛使用的應用程式 (例如：AWS、SendGrid、Microsoft Office 365 或 Twilio) 的 .ENV 環境變數檔。該惡意軟體會對基於 Laravel 網路應用程式框架的網站進行掃描 (Laravel 是基於 MVC 架構模式來打造的框架，並且設計出許多讓開發者更有效率的工具)。它還支援其他功能，例如：部署惡意 webshell 或掃描和濫用從內部蒐集到的憑證。據報導，AndroxGh0st 幕後的威脅分子在其攻擊鏈中利用幾個陳年老舊的遠端程式碼執行 (RCE) 漏洞，包括 CVE-2017-9841、CVE-2021-41773 和 CVE-2018-15133。

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
- PHP.Backdoor.Trojan
- 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: Apache HTTP Server RCE CVE-2021-41773
- Web Attack: Apache HTTP Server CVE-2021-41773 2
- Web Attack: PHPUnit RCE CVE-2017-9841

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。

2024/01/17

屬於APT28駭客集團的OceanMap後門

OceanMap 是一個基於 C# 的後門惡意程式，與 APT28 駭客集團 (Fancy Bear* 奇幻熊) 有所關聯，主要的功能是在執行遠端命令。它透過在遭感染電腦的 AUTORUN 資料夾植入 .URL 檔案，以利可常駐在受感染電腦上。透過 IMAP 協議與攻擊者進行聯繫。在最近的 APT28 所發動的網路攻擊行動中發現，OceanMap 經常與 Masepie 惡意軟體、SteelHook PowerShell 腳本以及其他用於網路偵察和入侵的駭客工具交叉變換組合使用。

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：

基於行為偵測技術(SONAR)的防護：

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- Web.Reputation.1
- 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。

2024/01/17

SilverRAT遠端存取木馬惡意軟體

SilverRAT 是一個在真實網路情境發現的遠端存取木馬惡意軟體，最近它的破解版透過駭客論壇和 Telegram 頻道傳播。SilverRAT 是採用 C# 撰寫，針對 Windows 平臺，具有鍵盤側錄、竊取瀏覽器瀏覽歷史紀錄資料、cookie、檔案和憑證……等功能。此外，該惡意軟體還能讓攻擊者在受感染系統上啟動隱藏的遠端連線。

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-CPE!g2
- ACM.Mshta-Masq!g1
- ACM.Ps-RLsass!g1
- SONAR.SuspStart!gen14
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Suspexec!gen135
- Backdoor.Silverrat
- Backdoor.Silverrat!g1
- SMG.Heur!gen
- 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.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2024/01/16

提高警覺～安卓平台上的駭人遠端存取木馬：Rat4Droid

2023 年，Rat4Droid 遠端存取木馬，在駭客網站、Facebook、Youtube 和 Telegram 頻道……等各種平臺上引起大騷動，從涉入的多起網路攻擊行動中被觀察到，多個駭客組織和個體戶將其偽裝成不同的 APP(例如：色情、文件、免費電話號碼、Players Unknown's Battlegrounds (PUBG) 冒險遊戲兌換代碼、音樂、影像編輯軟體)，並鎖定不同的受眾目標。

作者已將其操作介面改為當地的語系，以鎖定阿拉伯語、法語、英語、西班牙語和德語的用戶。它具有一般資料擷取和執行命令的功能，包括：

- 資料滲漏：連絡人、照片、檔案、簡訊內容、通話記錄、位置資訊。
- 執行命令：刪除檔案、播放聲音、更換桌面圖案、振動、發送語音和文字通知、打開閃光燈、打開 APP、螢幕鎖定、重置成出廠狀態、自動撥號、發送簡訊、錄音。

從流行程度來看，雖然它不像 Spynote 和 Irata 等其他安卓遠端存取木馬那樣活躍，但賽門鐵克仍在多個國家觀察到測試階段和真實的惡意活動 (阿拉伯語系國家的數量略高)。

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.2

2024/01/16

防護亮點：端點防護--SEP多重防護技術中的入侵預防系統元件(IPS)去年(2023年)為您做了什麼？

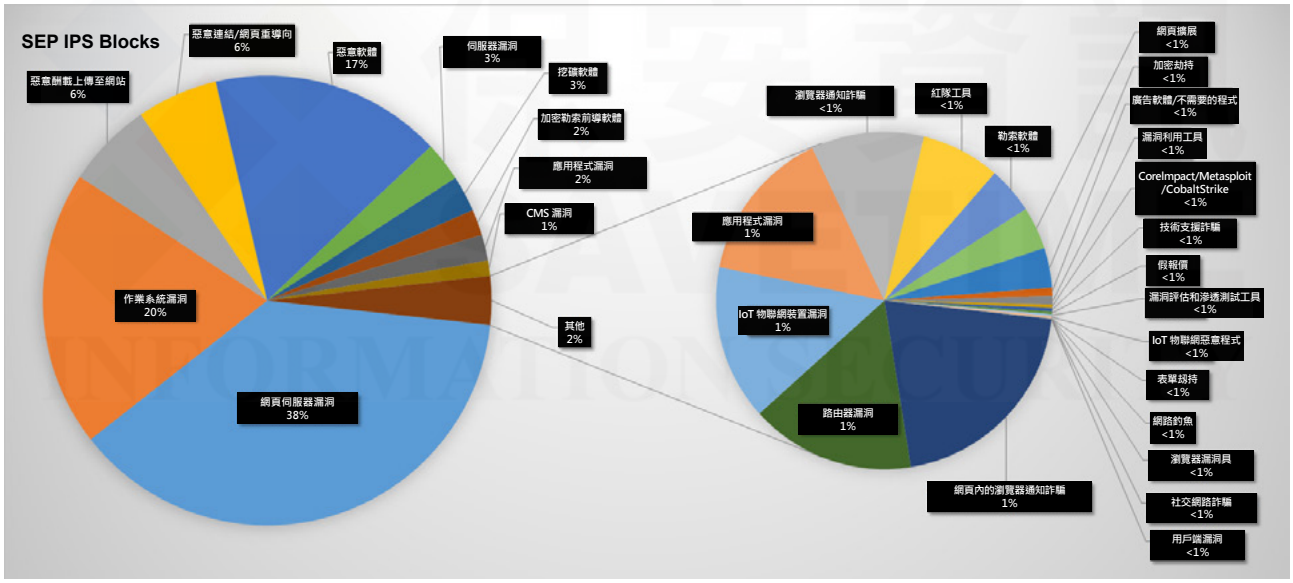
賽門鐵克 IPS 是同類最佳的深度資料封包檢測引擎，可保護包括財富 500 強企業和消費者在內的數億個端點 (桌上型電腦和伺服器)。

我們曾多次發布介紹在防禦態勢中使用 IPS 的好處--從攔截技術支援詐騙，到制止無休止的 Log4j 攻擊，再到網路釣魚、SMB 攻擊、CMS 漏洞、高效的 IPS 瀏覽器擴展……等，不一而足。引用上一篇文章中的評論：『*如果您的安全設置不包括入侵防禦，那麼您的組織就有可能在威脅防護方面遭受重大損失*』。

讓我們回顧一下過去的一年，看看 IPS 如何協助保護我們的客戶。

在 2023 年期間，SEP 多重防護技術中，單單入侵預防系統元件 (IPS) 的網路防護引擎，在賽門鐵克保護的端點上攔截超過 47 億次威脅。其中 93% 的攻擊在感染前階段就被攔截。

- 利用網路伺服器漏洞的嘗試：38%
- 企圖利用 Windows 作業系統漏洞：20%
- 惡意軟體 C&C 連線嘗試：17%
- 試圖執行 Web 有效載荷上傳：6%
- 試圖將用戶重導向到攻擊者控制的網站：6%
- 試圖利用伺服器漏洞：3%
- 試圖挖礦 (開採數位貨幣)：3%
- 試圖利用應用程式漏洞：2%
- 勒索軟體前期攻擊：2%
- 試圖利用 CMS 漏洞：11%
- 其他：2%



建議客戶在桌機／筆電和伺服器上啟用 IPS，以獲得最佳保護。點擊此處瞭解啟用 IPS 的說明。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。

2024/01/16

小心點擊YouTube鏈接～躲在YouTube鏈接網址後面的Lumma惡意竊密程式

Lumma 惡意竊密程式是由 C 語言所撰寫，已知至少從 2022 年起就開始在威脅環境中伺機而動，它一直在透過 YouTube 教學影片進行傳播。這些教學影片以提供破解軟體為誘餌，隱藏在短網址的鏈接後面，導致毫無戒心的用戶下載而遭害。

一旦入侵成功，Lumma 就會試圖竊取儲存在系統瀏覽器中的資料以及任何存在的加密貨幣錢包。這種惡意軟體繼續在地下論壇上出售，其功能並與時俱進，最新版本增加在受感染端點上載入額外任意有效酬載的新功能。

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：

- MSIL.Packed.12
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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: Infostealer LummaC2 Activity
- System Infected: Infostealer LummaC2 Activity 02

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。

2024/01/16

macOS平台上的竊密惡意軟體：KeySteal

KeySteal 是一款針對 macOS 平臺的惡意竊密程式。該惡意軟體的主要目的是從 MacOS 的密碼管理系統 Keychain 中竊取資訊。KeySteal 惡意軟體的最新變種以 Mach-O 多重架構二進位檔案的形式傳播，其名稱包括『UnixProject』、『CodeSignature』或最近的『ChatGPT』。KeySteal 能與預先已寫在程式中的 C&C 位址進行通訊，並有能力在受感染系統上植入具有常駐能力的元件。

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
- OSX.Trojan.Gen.2
- 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。

2024/01/16

Pure(*純)惡意軟體家族

Pure 是一個至少從 2021 年起就活躍在威脅領域的惡意軟體家族，其開發者名為 PureCoder。PureCrypter 多功能勒索加密軟體和 PureLogs 惡意竊密程式是屬於該家族比較知名的惡意軟體。PureCrypter 為攻擊者提供加密和混淆功能，在攻擊鏈中強化躲避偵測的能力。另方面，PureLogs 是一種惡意竊密程式，側重於資料滲出，包括電腦資訊、瀏覽器資料、加密貨幣錢包……等。Pure 家族的最新成員是 PureMiner--它是一種挖礦惡意軟體，用於在遭感染的端點上部署 XMRig 挖礦軟體。

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!g5
- AGR.Terminate!g7
- SONAR.SuspBeh!gen667
- SONAR.SuspLoad!g59

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.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!200
- 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。

2024/01/16

散播StealC惡意竊密程式的垃圾郵件活動

去年，有報導指出，Vidar、Raccoon…… 等多種惡意竊密程式有盛行的態勢，連帶著 StealC 惡意竊密程式也有流行的趨勢。據觀察，最近一次惡意垃圾郵件散播行動中，透過惡意 PDF 文件檔內嵌的 StealC 惡意軟體，該檔案的連結最終會下載並執行一個 JS 檔，隨後導致在遭入侵的電腦植入 StealC 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：

- ISB.Downloader!gen48
- ISB.Downloader!gen89
- Scr.Malcode!gen
- 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。

2024/01/15

Azorult間諜程式涉入多層級攻擊鏈的網路攻擊行動

根據最近的報告，有攻擊者持續在利用多層級攻擊鏈以發動 Azorult 間諜程式的網路攻擊行動，意圖躲避檢測。攻擊初始階段，惡意電子郵件會載入一個偽冒的 PDF 附件，實際上是一個 .LNK 捷徑檔。如果用戶被誘騙執行惡意 .LNK 捷徑檔，就會啟動 PowerShell 腳本和惡意程式載入器的其餘攻擊鏈。

Azorult 間諜程式已經存在好長一段時間，它會竊取瀏覽歷史紀錄、cookie、登錄憑證和加密貨幣資訊……等資料。它還能讓攻擊者在被入侵的系統中上傳更多惡意軟體。

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：

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)。

基於行為偵測技術(SONAR)的防護：

- ACM.Crtutl-CNPE!g1
- ACM.Ps-TBat!g1
- ACM.Ps-Schtsk!g1
- ACM.Schtsk-TBat!g1
- ACM.Ps-Http!g2
- ACM.Ps-Wscr!g1
- ACM.Wscr-CNPE!g1
- ACM.Wscr-Ps!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.NPE

- CL.Suspexec!gen171
- ISB.Heuristic!gen23
- ISB.Heuristic!gen102
- ISB.Downloader!gen178

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: Webpulse Bad Reputation Domain Request

2024/01/15

Mirai殭屍網路惡意程式的後繼版本：Rimasuta

Mirai 是一個眾所周知的殭屍網路惡意程式，多年來一直困擾著 Linux 系統的設備和機器。人們經常觀察到新舊變種涉入的網路攻擊行動。例如：有報告指出，與 2021 年首次觀察到一個舊版本涉入的新活動。該變種名為 Rimasuta，它利用漏洞傳播並將設備劫持成為殭屍電腦。此外，該威脅背後的攻擊者已開始使用 ChaCha20 加密演算法進行強大的通訊。

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：

- Trojan.Gen.NPE

2024/01/15

PatchWork APT駭客組織散播的專屬勒索軟體

近期網路上有 PatchWork APT 駭客組織散播源於 Chaos 最新變種的勒索軟體正在肆虐。在對使用者資料進行加密後，會冠上隨機的副檔名。勒索贖金支付說明以檔名『look_this.txt』的文字檔提供，駭客要求受害者與他們聯繫，以獲取如何解密檔案的指示。該惡意軟體具有刪除受感染機器上卷陰影副本的功能。

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：

- ACM.Untrst-RLsass!g1
- SONAR.SuspDrop!gen1
- SONAR.SuspLaunch!g22
- SONAR.SuspLaunch!g266

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

2024/01/15

針對網頁伺服器和雲端服務主機的FBot惡意軟體攻擊

FBot 是一種用 Python 撰寫的惡意軟體，最近被濫用於鎖定網頁伺服器和雲端服務主機的惡意攻擊行動。該惡意軟體含多種功能，專門用於 AWS 帳戶劫持攻擊、憑據收集、針對其他各種軟體即服務 (SaaS) 的雲端服務攻擊或針對一些主流熱門的內容管理系統 (CMS) 的入侵。FBot 還包括各種工具軟體的功能，例如：IP 位址生成器、埠掃描器、反向 IP 掃描器、IP 和電子郵件驗證器……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 Horse

2024/01/15

針對Apache Hadoop和Apache Flink應用程式的全新網路攻擊行動

在真實網路情境觀察到針對 Apache Hadoop 和 Apache Flink 應用程式的全新網路攻擊行動。攻擊者一直在開採濫用這兩個應用程式中，現有安全錯誤配置進行遠端存取和程式碼執行。攻擊者利用 BGP 打包軟體有效籌載的二進位檔案進行混淆，並利用兩個不同的 rootkit 隱藏惡意軟體和執行的命令。在此攻擊行動中，受感染的機器上會植入一個 Monero 挖礦程式作為最終有效籌載。

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：

- PUA.Gen.2
- 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。

2024/01/12

Medusa(*美杜莎)勒索軟體

Medusa 勒索軟體以勒索軟體即服務 (RaaS) 的方式營運，攻擊者初始入侵階段的破口是利用已知漏洞開採和帳戶洩露接管。感染後，Medusa 會加密用戶檔案，並冠上 .medusa 副檔名，並將 .dll 和 .exe ……等特定檔案類型排除在加密之外。檔名為『read_me_medusa!!!.txt』勒索 (贖金支付) 說明文字檔指示受害者聯繫攻擊者以獲取解密說明。該惡意軟體具有停止特定進程、刪除卷影副本和在完成加密程序後自我刪除的功能。

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：

- ACM.Ps-Net!g1
- ACM.Untrst-RunSys!g1
- SONAR.Ransomware!g7
- SONAR.Ransomware!g12
- SONAR.RansomGen!gen3

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen
- Ransom.Medusa
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!
- Heur.AdvML.A!500
- Heur.AdvML.C

2024/01/12

Spotify線上數位音樂串流媒體服務平台，成為釣魚電子郵件覬覦的目標

Spotify 是一項線上數位音樂串流媒體服務平台，使用者可即時播放其數位歌曲庫和 Podcast 播客。最近，賽門鐵克發現新一波利用虛假付款通知欺騙 Spotify 服務的釣魚電子郵件。電子郵件內容指出『支付失敗』問題，並誘使用戶透過點擊意圖竊取憑證的釣魚網址來查看和更新支付狀況。

- 電子郵件主旨： 我們無法處理您的付款。

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。

2024/01/12

針對法國農業信貸銀行手機用戶的惡意簡訊

賽門鐵克在網路釣魚攻擊中發現各種類型的社交工程伎倆，其目的都是操縱人性以洩露敏感資訊。常見的手法包括發送虛假發票、謊稱技術支援、提供虛假工作機會以及使用誘騙密碼重置電子郵件。詐騙者採用的伎倆五花八門，例如：虛假軟體更新、國稅局或稅務威脅、中獎詐騙和醫療保健相關資訊。

每種策略都由子伎倆所組成。本防護公告專門針對其中一種與謊稱意圖密碼重置有關的伎倆。賽門鐵克最近檢測到針對法國農業信貸銀行行動裝置用戶的網路釣魚行動，該行動利用虛構網路攻擊導致的 SécuriPass 重置／重啟要求。攻擊者利用這些用戶依賴農業信貸銀行提供的數位服務 SécuriPass 來提高網上銀行交易安全性這一事實，相應地調整社交工程和網路釣魚技術。

據法國農業信貸銀行稱，用戶必須注意，SécuriPass 只能在銀行應用程式（Ma Banque）中啟動；任何其他啟動方式都可能被視為欺詐企圖。

發現的惡意簡訊：

- 法國農業信貸銀行：遭受網路攻擊後必須更新您的 SécuriPass，請點擊以下連結啟動：hxxps[:]//servicecaactiverapide[.〕

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 已知道此次攻擊行動中使用假冒或誤植的域名。

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。

2024/01/11

假冒HDFC銀行用戶獎勵計畫的手機APP導致金融盜竊

HDFC Bank Limited 是一家印度銀行和金融服務公司，總部位於孟買。截至 2023 年 8 月，在收購母公司 HDFC 後，它是印度資產規模最大的私人銀行，也是全球市值第五大銀行。由於其規模，它被印度儲備銀行歸類為國內系統重要性銀行。雖然 HDFC 銀行主要在印度運營，但在其他國家也有業務。該銀行的用戶與全球其他金融機構的使用者一樣，一直是網路釣魚和惡意

軟體攻擊的目標。

最近，賽門鐵克發現有不法分子利用假冒 HDFC 用戶獎勵計畫手機 APP8 安裝程式 (offer.apk 和 hdfc-reward.apk) 針對 HDFC 手機用戶發動網路攻擊行動。如果使用者被成功誘騙，該 APP 就會開始收集存儲在行動裝置上的連絡人、簡訊和其他敏感資訊。惡意軟體主要目的是收集受害者的財務資訊，包括信用卡資訊，要求受害者提供這些資訊以進入獎勵計畫。攻擊者向使用者保證不會存儲他們的信用卡認證編號 (CVV)(信用卡和簽帳金融卡背面印有的三或四位數安全碼)，這當然不能相信。

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。

- AppRisk:Generisk