保安資訊--本周(台灣時間2022/12/02)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 100 萬台受保護端點上總共阻止了1.272億次攻擊。這些攻擊中有 92% 在感染階段前就被有效阻止：**(2022/11/28)**

- 在**16萬6,700**台端點上，阻止了**5,030**萬次嘗試掃描**Web**服務器的漏洞。
- 在**32萬1,600**台端點上，阻止了**2,570**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬3,800**台**Windows**伺服主機上，阻止了**1,840**萬次攻擊。
- 在**10萬9,300**端點上，阻止了**380**萬次嘗試掃描伺服器漏洞。
- 在**3萬2,600**台端點上，阻止了**180**萬次嘗試掃描在**CMS**漏洞。
- 在**6萬3,300**台端點上，阻止了**220**萬次嘗試利用的應用程式漏洞。
- 在**40萬6,700**台端點上，阻止了**1070**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2萬2,400**台端點上，阻止了**450**萬次加密貨幣挖礦攻擊。
- 在**4萬9,300**台端點上，阻止了**540**萬次向惡意軟體**C&C**連線的嘗試。
- 在**4,200**台端點上，阻止了**15萬900**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。

2022/12/01

功能強大的DuckLogs--竊密程式和鍵盤側錄器

DuckLogs 是一種具有竊密功能的惡意軟體，以 MaaS（惡意軟體即服務）的形式出售。它可以從受感染的機器收集並過濾各種資訊，包括憑證、cookie、加密錢包、瀏覽器資料等。它還標榜有其他附加功能如監視按鍵、執行任意檔案、鎖住使用者設備或對受感染機器進行電源管理。DuckLogs 以管理員權限執行，能夠繞過 UAC（使用者帳號控制）。

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.Malcode!gdn32
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2022/12/01

Redline Stealer竊密程式偽裝成 VPN 應用程式安裝檔傳播

Redline Stealer 竊密惡意軟體最近偽裝成名為 ExpressVPN 的 VPN 應用程式進行散佈。出於傳播惡意軟體的目的，攻擊者建立多個模仿合法 ExpressVPN 網頁的釣魚網站，並提供假的安裝程式供下載。根據從 C&C 伺服器收到的指令，Redline Stealer 將嘗試從受感染的端點收集各種資訊，包括銀行帳戶詳細資訊、登錄憑證、加密錢包、cookie 和瀏覽器資料等。

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.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。

2022/11/30

在印度觀察到更多 Android 的銀行惡意軟體

在過去的幾週裡，我們觀察到更多針對印度手機行動用戶的 Android 銀行惡意軟體冒充 SBI、Axis 和 HDFC 等知名銀行的 Android 應用程序 (APP)。銀行惡意軟體類似於 Drinik 的早期版本，貌似目標銀行的釣魚頁面並竊取簡訊 (SMS) 內容以攔截雙因素身份驗證 (2FA)。這些攻擊行動幕後的參與者正在將受害者引誘到上架管惡意應用程序的假網站。

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

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。

2022/11/30

改名換姓～WannaRen勒索軟體以Life之名，捲土重來

WannaRen 是 2020 年發現一個較舊的勒索軟體變種。據報導，WannaRen 現在已更名為 Life 勒索軟體的品牌名稱捲土重來，並且針對印度用戶。該惡意軟體以 MSI 二進位封裝檔的形式傳播，它濫用合法的系統元件進行 DLL 側載。該惡意軟體會將 .life 副檔名附加到被加密的檔案。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.ASync!gm
- Scr.Malcode!gdn14
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/29

加密貨幣助長加密勒索～NULLTHEGAME 勒索軟體要求支付門羅幣

在威脅生態系中觀察到一個勒索軟體攻擊者稱其惡意軟體為“NULLTHEGAME”，它還只是執行通常的加密攻擊，並沒有採用雙重勒索戰術。成功入侵後，被加密檔案將被附加一個 .NULL 的副檔名，並在機器上留下一個贖金說明檔，索價 30 個門羅幣，在撰寫本文時價值 4,209.63 美元。

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(Snoar)的防護：

- SONAR.SuspDrop!gen1

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

2022/11/29

防護亮點：健全的底層邏輯，可以應對千變萬化的世局：賽門鐵克無須更新也能防護最新的Emotet零時差攻擊

安全研究人員早在 2014 年就首次發現 Emotet 銀行木馬，現已證明它是威脅領域中最受歡迎且最強悍的木馬之一。最初是一支單純的銀行惡意軟體，試圖從受害者那裡竊取敏感的銀行相關訊息，後來的版本逐漸引入了新的模組化功能和感染媒介，包括垃圾郵件、惡意軟體交付服務（包括其他銀行木馬和勒索軟體）和隱身修改。美國國土安全部甚至表示，Emotet 是他們見過的成本最高、破壞性最強的惡意軟體之一。

Emotet 已經經歷幾個活動顯著下降的平靜時期，大概是在當局緊追不捨或者可能是由於內鬥或結構重組的時候。然而，在 11 月初，Emotet 背後的參與者發起一場新的惡意電子郵件攻擊行動，其中包括新的 URL 格式和個人化的登錄頁面，似乎是從休眠的活火山復發一樣。在此特定實例中，電子郵件包含負責下載 Emotet 的 Excel 附件，該 Excel 檔案利用社交工程，需要用戶輸入才能成功執行惡意內容，有效地讓毫無戒心的用戶感染。

雖然有許多不同的方法可以防禦像 Emotet 這樣的惡意軟體（正如我們在11 月 2 日的 Emotet 公告中所指出的那樣），但最好的方法當然是主動阻止它，無需更新簽章、定義檔、規則等，不過需要更新相對應的安全產品才能生效。雖然肯定沒有網路安全供應商敢於在每次威脅來襲時都聲稱主動防禦，但在這種情況下，啟發式保護是幾個月前使用過去變種的多種特徵、進階的叢集技術和經過我們惡意軟體分析團隊的大量努力，賽門鐵克產品無需任何更新即可阻止這些以前未發現的新 Emotet 變種。

賽門鐵克已提供零時差保護，具體偵測如下：

檔案型(基於回應式樣本的病毒定義檔)防護：

- XLM.Downloader!gen1
- XLM.Downloader!gen2
- XLM.Downloader!gen4
- CL.Suspexec!gen128

2022/11/29

蠢蠢欲動~Bulwark 勒索軟體活動有增加的跡象

在過去幾個星期，Bulwark 勒索軟體活動呈上升趨勢。該勒索軟體背後的攻擊者採用雙重勒索策略，並在遭加密的電腦上留下較長的勒索贖金說明。在贖金說明文，他們脅迫受害者必須在 72 小時內支付贖金，並警告他們不得聯繫媒體。如果受害者不付款，他們將洩露部分遭竊資料以損害受害者的聲譽，然後繼續在暗網上出售所有資料。此外，攻擊者還威脅要對其網站和基礎設施執行 DDoS 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：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspBeh!gen54
- SONAR.SuspDrop!gen7
- SONAR.SuspLaunch!g189
- SONAR.UacBypass!gen30

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Locky!g35
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/29

印度政府開發的身分驗證應用程式：Kavach，成為SpyNote間諜軟體覬覦的目標

SpyNote 是一種 Android 手機行動平台上的間諜軟體，已經存在好幾年，並且仍然被全球各種駭客組織和個人所採用。最近，有報導稱在印度有威脅攻擊者將他們的 SpyNote 偽裝成 Kavach 的更新。Kavach 是一種印度政府開發的身分驗證應用程式，可保護對印度政府的各種公眾解決方案的存取。

SpyNote 惡意軟體具有以下的窺竊功能：

- 檔案、簡訊、通話、聯絡人、位置、帳戶和相機管理器
- 下載並安裝其他 apk 行動 APP 套件檔
- 鍵盤側錄
- 麥克風錄音和螢幕錄製

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

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。

2022/11/29

macOS也遭殃：Aobo鍵盤側錄程式

Aobo 是一款適用於 macOS 的鍵盤側錄程式，它可以執行按鍵記錄、密碼截取、網站和訊息聊天監控等。雖然商業化的買賣鍵盤側錄程式已行之多年，但已知有威脅行為者利用它進行惡意目的的範例。在此類攻擊中，Aobo 可能由惡意軟體植入程序、惡意腳本啟動或偽裝成合法應用程序進行散佈。

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.Spyware.AoboKeyLog
- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- WS.SecurityRisk.1

2022/11/29

更難偵測得到的～以Rust程式語言重新撰寫的RansomExx加密勒索變種

RansomExx 勒索軟體的新變種已在真實網路環境造成多起危害，並使用基於表達式 (expression-based) 語言的 Rust 程式語言重新撰寫。RansomExx 是較舊 Defray 勒索軟體家族的後繼版本。至少自 2020 年以來，該勒索軟體一直在積極針對全球多家公司。轉向 Rust 的原因主要是由於各個供應商對使用這種程式語言編寫的惡意軟體其 防毒軟體 (AV) 規避率更高。新 RansomExx2 變種針對 Linux 環境進行資料加密，被加密後的檔案其副檔名是隨機不固定。

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.RansomEXX
- WS.Malware.1

2022/11/28

Titan(*泰坦)竊密程式

竊密程式每隔一段時間就會大翻新，並且大多數通常是透過瀏覽網頁的順道下載攻擊方式來散佈，也常會假冒成熱門的軟體讓人受騙。itan (*泰坦) 竊密程式就是其中之一，最近有人發現它。這種惡意軟體相當通用，下面是它的一些收集功能。遭竊的資訊會被打包成一個 zip 壓縮檔並存到記憶體中，且將該 (base64) 編碼檔案發送到其命令和控制伺服器(C&C)。

- 來自基於 Chromium 和基於 Gecko 的瀏覽器的密碼、本機狀態、歷史和自動填入的訊息
- 55 個與加密相關的瀏覽器擴充功能的訊息和文件
- 截圖
- 來自各個 APP 位置的加密貨幣錢包（Coinomi、Zcash、Armory、bytecoin、Atomic、Ethereum、Guarda 和 Exodus）
- 帳號、MAC 位址、CPU 和 GPU 訊息
- 已安裝的軟體
- 來自 C:/Program Files (x86)/Steam/ 和 C:/Program Files (x86)/Steam/config/ 的訊息
- 來自 FileZilla 的 Recentservers.xml
- Total Commander 的 Wcx_ftp.ini
- 來自 Telegram Desktop 的 Key_datas 和地圖

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(Snoar)的防護：

- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan.Gen.2
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/28

Patriot(*愛國者)竊密程式

Patriot Stealer 是另一種普通的竊密程式，據報導已被商業化上架買賣。這種威脅能夠竊取各種密碼、cookie、書籤、歷史記錄、自動填充資料、電報會話和加密錢包。遭感染後，它會使用 Discord webhook 向營運商回報。最近的活動顯示攻擊者正在使用順道下載作為感染媒介。在一個例子中，他們將 Patriot 竊密程式二進位檔案偽裝成一個假的 Eve 線上安裝程序--一種熱門的多人線上角色扮演遊戲。

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：

- Infostealer

2022/11/28

Bahamut手機行動間諜軟體透過假的VPN應用程式(APP)散播

Bahamut 手機行動間諜軟體最近以假的 VPN 應用程式 (APP) 至少從 2022 年 1 月就開始的攻擊行動中進行散佈。該惡意軟體冒用知名合法 SecureVPN 應用程式 (APP) 的名稱，並以兩個木馬化手機應用程式版本的形式出現--SoftVPN 和 OpenVPN。Bahamuts 的功能包括從受感染設備中竊取資訊--通話記錄、聯絡人和簡訊 (SMS) 內容等。該惡意軟體還可以監控許多熱門的手機通訊應用程式 (例如：WhatsApp 和 Telegram) 的聊天記錄。

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

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。

2022/11/27

無法根除的Joker(*小丑)手機行動惡意軟體，令人不堪其擾

這種手機行動威脅繼續困擾著 Android 用戶並在 Google Play 商店上架，偽裝成用戶最有可能下載的常用APP--最近觀察到通訊應用程式、設計和鍵盤字體等APP。這種手機行動惡意軟體試圖透過攔截簡訊 (SMS) 來模擬點擊並為受害者訂閱高資費服務。

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
- AppRisk:Generisk

2022/11/27

沒有鬆手的跡象～Play勒索軟體依舊肆虐歐洲和亞洲

在過去的幾個星期裡，有越來越多的歐洲和亞洲的組織，成為這個相對較新的勒索軟體駭客集團之攻擊目標。Play 勒索軟體幕後的攻擊者，採用許多其他駭客家族所用令人痛惡的雙重勒索戰術，來脅迫受害者支付贖金。被加密的檔案通常會被重新命名以 .Play 為副檔名。

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(Snoar)的防護：

- SONAR.Ransomware!g1
- SONAR.Ransomware!g3
- SONAR.Ransomware!g7
- SONAR.Ransomware!g20

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.PlayCrypt
- Trojan.Gen.2

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2022/11/27

Hydra偽裝成Google Play商店

賽門鐵克持續觀察到全球範圍內的 Hydra 安卓(Android) 手機行動惡意軟體活動。許多駭客組織和個人利用這種惡意 APP，通常試圖透過非官方的第三方市場、假網站和其他社交平台感染受害者，冒充合法APP。在最近的報導中，一位威脅發動者實際上將其 Hydra 偽裝成 Google Play 商店，寄生在 Discord平台 (熱門的網路即時通話平臺) 上。

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

2022/11/27

以新冠疫情為釣餌的網路釣魚網站，上鉤者將招惹Punisher(*處罰者)勒索軟體纏身

根據最近的報導，Punisher 勒索軟體背後的攻擊者利用一個假的智利新冠疫情為釣餌的網路釣魚網站，來引誘受害者下載並執行他們的勒索軟體，該勒索軟體偽裝成新冠疫情追踪軟體。被成功引誘的受害者的檔案將遭加密，並要求 1,000 美元的比特幣贖金。

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

基於機器學習的防禦技術：

- 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已於第一時間收錄於不安全分類列表中。

2022/11/24

Aurora(*極光)竊密程式

Aurora 是另一個以惡意軟體即服務 (Malware-as-a-Service) 的形式銷售的竊密程式。據報導，它於今年初首次被發現，最近在地下網站常見它的廣告。雖然它的曝光度還沒有達到其他更惡名昭彰的竊密程式的水準，但它已經開始被各種駭客組織和個人所採用，這些駭客組織和個人正在進行透過典型瀏覽網頁時的偷渡式下載攻擊活動。Aurora 具有一般竊密程式的常見功能--與其他竊密程式的功能相比並沒有特別顯眼。

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(Snoar)的防護：

- SONAR.Dropper
- SONAR.PsDownloader!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Suspicious: Content
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan Horse
- WS.Reputation.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：

- System Infected: Trojan.Backdoor Activity 634

基於機器學習的防禦技術：

- Heur.AdvML.B