



## 保安資訊--今日最新(台灣時間2022/03/02) 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/伺服器)。

過去的7天內，SEIP的網路層保護引擎(IPS)在130萬個受保護端點上總共阻止了2.0463億次攻擊。這些攻擊中有95%在感染階段前就被有效阻止：**(2022/02/27)**

- 在23萬7,800台端點上，阻止了1,068億次嘗試掃描Web服務器的漏洞。
- 在51萬6,200台端點上，阻止了4,580萬次嘗試利用的Windows作業系統漏洞的攻擊。
- 在8萬6,500台Windows伺服器上，阻止了2,660萬次攻擊。
- 在18萬5,000端點上，阻止了1,030萬次嘗試掃描伺服器漏洞。
- 在10萬800台端點上，阻止了510萬次嘗試掃描在CMS漏洞。

- 在15萬3,400台端點上，阻止了410萬次嘗試利用的應用程式漏洞。
- 在44萬7,800台端點上，阻止了1,330萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在4,800台端點上，阻止了490萬次加密貨幣挖礦攻擊。
- 在13萬2,700台端點上，阻止了560萬次向惡意軟體C&C連線的嘗試。
- 在7,500台端點上，阻止了28萬940次加密勒索嘗試。

強烈建議用戶在桌機/筆電/伺服器上啟用IPS(不要只把SEIP/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。

[點擊此處獲取--關於賽門鐵克原廠防護週報](#)

2022/03/01

### OutSteel 和 SaintBot 惡意軟體被用於針對烏克蘭能源部門的攻擊中

被稱為UAC-0056(又名TA471或SaintBear)的威脅集團，與2月初針對烏克蘭能源組織的攻擊活動有關。根據最近發佈的一份報告，攻擊者一直在利用Word附加檔案的魚叉式網路釣魚資訊。這些附加檔案包含惡意的Javascript檔，下載SaintBot下載程式和OutSteel竊密程式等有效籌載。這個惡意軟體具有雙重角色既可滲透機密資料，也能下載額外有效籌載到受感染的電腦。該威脅集團一直在使用Discord內容遞送網路(Content Delivery Network, CDN)架構來託管惡意軟體的有效籌載。

賽門鐵克已經於第一時間提供多種有效保護(SEIP/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：

- Bloodhound.RTF.20
- CL.Downloader!gen10
- Downloader
- Infostealer
- ISB.Downloader!gen69
- ISB.Downloader!gen80
- Trojan.Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Mdropper
- Scr.Malcode!gdn30
- W97M.Downloader

#### 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：

- Audit: PowerShell Process Accessing discordapp[.].com
- Malicious Site: Malicious Domain Request 59
- 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。

2022/03/01

### Jester 竊密程式--威脅版圖中的另一個竊密程式

一個被稱為Jester竊密程式的新變種已在真實環境中被觀察到。Jester主要針對用戶的登錄憑證、瀏覽器cookies、加密貨幣錢包資料和銀行資訊。雖然這種惡意軟體的最初版本早在2021年7月就已經在各種地下論壇上提供銷售，但最近報告顯示，Jester仍在不斷發展，經反覆修正最近也具備額外的反沙箱和反虛擬機器功能。

賽門鐵克已經於第一時間提供多種有效保護(SEIP/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.C

2022/02/28

### 利用烏克蘭和俄羅斯衝突有關的社交工程攻擊越來越多！

賽門鐵克已經開始觀察利用烏克蘭和俄羅斯衝突的社交工程攻擊。最近的例子，一個參與者一直試圖透過惡意電子郵件和通訊軟體，來引誘受害者，呼籲利用加密貨幣捐款幫助烏克蘭，使用的電子郵件主題是：與烏克蘭站在一起--你可以透過這種方式捐款。與烏克蘭站在一起--這裡是你可以捐款的方式。這位肆無忌憚的參與者，還在郵件中加入一條類似2月27日從烏克蘭官方推特帳戶發出的推文。如果成功引誘，受害者最後將進入Formbook，這是一個已經存在多年著名的竊密爬蟲。它仍然是威脅領域的頂尖竊密程式，被許多集團和個人所使用。

賽門鐵克已經於第一時間提供多種有效保護(SEIP/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離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.MalPbs!gen1

2022/02/28

### Daxin (\*大新)，精密且隱秘的後門程式

賽門鐵克發現一種高度精密的惡意軟體，該惡意軟體被與中國有關聯的威脅行為者使用。這種隱形後門被稱為Daxin(\*大新)，已被用於針對特定政府和其他關鍵基礎設施目標的間諜活動。有關此惡意軟體和活動的更多資訊，請參閱此處：

Daxin(\*大新)：一支專為攻擊安全強化的網路環境而設計隱秘的後門程式

賽門鐵克已經於第一時間提供多種有效保護(SEIP/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.Daxin
- Backdoor.Trojan
- Backdoor.Zala
- Trojan.Horse
- Trojan.Emulov
- Trojan.Gen.2
- Trojan.Gen.MBT

#### 基於機器學習的防禦技術：

- Heur.AdvML.C

#### 基於安全強化政策(適用於使用DCS)：

DCS自建的強化安全政策能預防惡意驅動程式被植入Windows作業系統。

2022/02/25

### MuddyWater (\*混沌的水)威脅集團所使用的惡意軟體和工具

根據美國和英國當局發佈的聯合公告，被稱為Small Sieve(\*小篩子)的惡意軟體已被Seedworm(又名MuddyWater)駭客集團用於針對全球關鍵基礎設施的攻擊。Small Sieve(\*小篩子)是一個用Python撰寫的後門程式，威脅者主要是使其在被攻擊的目標上持續存在。該組織利用的其他惡意軟體變種包括：PowGooP載入器、Canopy(又名StarWhale)、Mori後門、PowerStats和一個新發現用於加密命令和控制(C&C)通信管道的PowerShell後門...等。

賽門鐵克已經於第一時間提供多種有效保護(SEIP/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
- Trojan.Horse
- Trojan.Gen.MBT
- Trojan.Mdropper
- VBS.Downloader.Trojan
- WS.Malware.2

#### 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：

- 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。

2022/02/24

### 困擾MacOS用戶--惡意廣告軟體載入程式：AdLoad

多年來，眾所周知，在MacOS威脅環境中觀察到的廣告軟體變得不僅更先進，還更有耐心。一個惡名昭彰的廣告軟體載入程式--AdLoad，隨著其流行程度的增加，繼續在新聞和社交媒體中看到。賽門鐵克每天跟蹤Adload(及其變種)活動，繼續透過過度下載散播，同時偽裝成假冒的熱門應用程式Apps。

賽門鐵克已經於第一時間提供多種有效保護(SEIP/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.AdLoad
- OSX.AdLoad!g1

#### 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: OSX.Hydrumac Activity
- System Infected: OSX.Trojan.Gen Activity 1

2022/02/24

### 古巴勒索軟體幕後的威脅者，利用各種漏洞作為其攻擊的手段

據報導，古巴勒索軟體幕後的威脅者--UNC2596越來越常利用各種漏洞作為其攻擊的初始感染媒介。在去年一些與古巴勒索軟體有關行動中，UNC2596一直在利用MS Exchange ProxyLogon漏洞。據瞭解，該威脅集團還使用各種偵察工具和不同的惡意軟體變種，其中包括：Cobalt Strike、Wedgetcut偵查工具、Bughatch下載程式或Termite植入程式。

賽門鐵克已經於第一時間提供多種有效保護(SEIP/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.Cobalt
- Backdoor.Cobalt!gen11
- Backdoor.Cobalt!gen12
- CL.Downloader!gen12
- Downloader
- ISB.Downloader!gen80
- Ransom.Cuba
- Trojan.Horse
- Trojan.Gen.2
- Trojan.Gen.MBT

#### 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：

- 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。