保安資訊--本周(台灣時間2024/03/22)
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 55 萬 2,400 台受保護端點上總共阻止了 6,100 萬次攻擊。這些攻擊中有 84.9% 在感染階段前就被有效阻止：**(2024/03/18)**

- 在**11萬5,400**台端點上，阻止了**2,090**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**13萬9,300**台端點上，阻止了**1,200**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬8,200**台**Windows**伺服主機上，阻止了**9,500**萬次攻擊。
- 在**6萬9,500**台端點上，阻止了**230**萬次嘗試掃描伺服器漏洞。
- 在**1萬7,000**台端點上，阻止了**98萬5,400**次嘗試掃描在**CMS**漏洞。
- 在**5萬3,400**台端點上，阻止了**150**萬次嘗試利用的應用程式漏洞。
- 在**20萬4,900**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**1萬400**台端點上，阻止了**150**萬次加密貨幣挖礦攻擊。
- 在**10萬9,400**台端點上，阻止了**790**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**538**台端點上，阻止了**4萬7,700**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 萬個受保護端點上阻止了總計 600 萬次攻擊。**(2024/03/19)**

- 使用網頁信譽情資，在 **134.5K** 個端點上阻止 **530** 萬次攻擊。
- 攔截 **32.4K** 個端點上 **580.1K** 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 **12.3K** 個端點上攔截 **135.6K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **485** 個端點上攔截 **30.7K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

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。

2024/03/22

勿因小失大，請購買正版軟體～「破解版」電郵群發軟體：Atomic Mail Sender暗藏Chaos勒索軟體

Atomic Mail Sender 是一款用於群發電子郵件的工具軟體。企業、行銷人員和個人通常會使用此類軟體，他們需要透過電子郵件向大量受眾發送行銷郵件、電子報、公告和促銷資訊。

最近，一個勒索軟體攻擊者一直以潛在的 Atomic Mail Sender 使用者為目標，將 chaos 勒索軟體偽裝成「破解版」，透過偷渡式下載傳播。一旦成功入侵，檔案就會被加密，並在現有資料夾中投放贖金支付說明檔 (read_it.txt)，索要價值 1500 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：

自適應防護技術(包含於SESC)：

- 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

2024/03/22

偽冒法國郵政旗下國際快遞公司Geopost的DPD快遞與郵政服務--威脅者發動網路釣魚來竊取憑證

賽門鐵克發現新一輪冒充 DPD 公司 (法國郵政旗下國際快遞公司 Geopost 的快遞與郵政服務公司) 來竊取憑證的網路釣魚攻擊。Geopost 是一家全球包裹遞送服務公司，總部位於法國 Issy-les-Moulineaux。在此行動中，以德語版的網路釣魚電子郵件偽裝成重新安排送貨時間或檢查包裹詳情的通知。電子郵件內容簡短，鼓勵收件人點擊釣魚網址。一旦點擊，受害者就會看到用於收集憑證的釣魚網頁。

- 電子郵件主旨： Ihre Paketzustellungsnachricht Nr#[random_numbers]?
- 翻譯後的電子郵件主旨：您的包裹投遞狀態No#[隨機號碼]？

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。

2024/03/22

Linux平台出現AcidPour資料破壞軟體(Wiper)

AcidPour 是全新採用 C 語言撰寫的 Linux 惡意軟體，被認為是 AcidRain 資料破壞軟體 (Wiper) 的進化版。AcidPour 是針對 x86 架構編譯，它擴充之前資料破壞的功能。當前的功能集使該惡意軟體可以針對在 Linux x86 發行版本上運行的各種網路和物聯網設備、專用 RAID 陣列或 ICS 設備。

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
- WS.Malware.1

2024/03/22

全新的 StrelaStealer 惡意竊密程式傳播行動

據報導，在真實網路情境上出現了一起新的 StrelaStealer 惡意竊密程式傳播行動。該惡意軟體是 2022 年首次發現的。StrelaStealer 的目標是從各種電子郵件用戶端滲出電子郵件登錄憑證。該惡意軟體透過.zip 壓縮檔中發送惡意 JScript 檔的惡意垃圾郵件進行傳播。有效籌載以 .DLL 二進位檔案的形式發送。最新的 StrealStealer 變種在感染鏈和使用的混淆方法中導入了更新，所有這些更新都是為了逃避檢測。

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：

自適應防護技術(包含於SESC)：

- ACM.Crtutl-CPE!g1
- ACM.Findstr-Dl!g1
- ACM.Ps-Rd32!g1
- ACM.Ps-Wscr!g1
- ACM.Wscr-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspPE!gen7

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen
- Scr.Malcode!gen130
- Trojan Horse
- Trojan.Gen.MBT
- 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。

2024/03/22

GlorySprout惡意竊密程式

駭客論壇上出現一款名為 GlorySprout 的全新惡意竊密程式，該程式由 C++ 撰寫，帶有 Golang 後端面板。雖然該惡意竊密程式標榜是反虛擬機器和鍵盤側錄功能，但它還採用 API hashing、字串混淆和排程工作來達成常駐。它支援日誌的備份並可在特定國家或特定的 IP 可以不備份。一旦入侵系統後，它有能力針對敏感性資料，例如：瀏覽器歷史記錄、加密貨幣錢包、遊戲帳戶和訊息應用程式進行資料收集，並將收集到的資料外洩到其 C&C 伺服器。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1
- ACM.Vss-DlShcp!g1

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.B
- Heur.AdvML.B!100

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: Bad Reputation Application Activity
- Audit: Untrusted Telegram API Connection
- System Infected: Trojan.Backdoor Activity 564

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。

2024/03/21

針對歐洲國家的Remcos遠端存取木馬(RAT)垃圾郵件網路攻擊行動

據報導，有多個散播 Remcos 遠端存取木馬 (RAT) 的垃圾郵件網路攻擊行動以歐洲國家為目標。發動這些攻擊行動的威脅分子利用 AceCryptor 嵌入惡意軟體進行傳播，目的是從瀏覽器和電子郵件用戶端竊取使用者憑證。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspCreate!g12
- SONAR.SuspBeh!gen633

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Remcos
- 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

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)。

2024/03/21
Elfin(*精靈)使用FalseFont後門

FalseFont 是疑似由與伊朗有關聯的 Elfin 駭客集團所開發全新後門程式。該駭客集團至少從 2013 年就開始活躍，目標是航太和國防工業，它有很多名字，包括 Curious Serpens、Peach Sandstorm、APT33、Holmium Magnalium和Refined Kitten。FalseFont 後門偽裝成求職招募廣告，並使用偽造的可執行檔進行安裝。它可用於在受感染的機器上執行程序和命令、操縱檔案系統、截取螢幕並從瀏覽器中竊取憑證。它還能以多種方式即時接收攻擊者的命令。

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.2
- Backdoor.Trojan
- 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。
- 賽門鐵克網路隔離技術可主動阻止這種攻擊。

2024/03/21
Waterbug(又名Turla)駭客組織發動對歐洲非政府組織的TinyTurla後門惡意程式網路攻擊行動

Waterbug 駭客組織 (又名 Turla) 針對一個歐洲非政府組織持續性網路攻擊行動的詳情已被公佈。該組織在受害者的環境中建立灘頭堡，並利用安裝 TinyTurla 後門程式進行資料竊取。觀察到戰術包括但不限於橫向移動、安全軟體規避、透過部署自訂 Chisel beacon 開啟反向代理通道等。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- 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

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。

2024/03/21

Sysrv殭屍網路新變種涉入傳播惡意挖礦軟體XMRig的網路攻擊行動中

在最近一次傳播 XMRig 加密劫持惡意軟體的網路攻擊行動中，觀察到 Sysrv 殭屍網路的一個新變種。該攻擊開採濫用 Apache Struts(CVE-2017-9805) 和 Atlassian Confluence(CVE-2023-22527 和 CVE-2021-26084) 中幾個廣為人知的應用程式漏洞。據報導，攻擊者還入侵一個學術機構的合法網站，並利用該網站上架惡意有效籌載。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.NPE
- WS.Malware.1
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.B

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: Apache Struts CVE-2017-9805 2
- Web Attack: Atlassian Confluence RCE CVE-2023-22527
- Web Attack: Confluence RCE CVE-2021-26084

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。

2024/03/21

Springtail 進階持續威脅(APT)駭客組織濫用知名韓國公共實體的有效憑證

據觀察，Springtail(又稱 Kimsuky) 進階持續威脅 (APT) 駭客組織，傳播偽裝成知名韓國公共實體應用程式的惡意軟體植入器。一旦被入侵，惡意軟體植入器就會安裝 Endoor 後門惡意軟體。這種威脅使攻擊者能夠收集受害者的敏感資訊或安裝其他惡意軟體。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1
- ACM.Ps-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g266
- SONAR.SuspLaunch!g13

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
- 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。

2024/03/21

安卓平台上惡意軟體：Tambir

據悉，Tambir 是一款針對土耳其安卓平台使用者的後門惡意軟體。該惡意軟體具有許多惡意竊密程式的功能，包括竊取簡訊、按鍵、撥打電話、執行其他應用程式等。與其他行動惡意軟體變種類似，Tambir 濫用安卓系統無障礙服務來展開行動。惡意軟體執行後會從 Telegram 或 ICQ 等公共管道獲取攻擊者的 C&C 位址。

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
- AppRisk:Generisk

2024/03/20

Stonefly進階持續威脅(APT)駭客組織在魚叉式網路釣魚行動中使用MeshAgent惡意程式

據報導，Stonefly(又名 Andariel) 進階持續威脅 (APT) 駭客組織在真實網路情境上，發起一場全新的魚叉式網路釣魚行動。MeshAgent 與惡意軟體有效籌載一起部署為該行動的一部分，利用的是已安裝軟體中已知漏洞。與其他遠端系統管理工具一樣，MeshAgent 惡意程式 也提供各種遠端控制功能。不過，駭客通常會利用它來達到惡意目的。

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：

- Hacktool.Mimikatz
- Scr.Malcode!gdn32
- 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。

2024/03/20

採用Python撰寫的EvilAnt(*邪惡螞蟻)勒索軟體

Evil Ant 勒索軟體是一款採用 Python 撰寫，並經 PyInstaller 編譯的惡意軟體。除了執行檔案加密和顯示贖金支付說明等基本的勒索軟體活動外，Evil Ant 還具有反分析 (虛擬環境感知) 和反檢測 (停用 Windows Defender) 功能。值得注意是，這款勒索軟體的檔案相當大，大約有 27MB。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.C

2024/03/20

Jasmin勒索軟體透過開採濫用JetBrains公司所開發的構建管理和持續整合伺服器TeamCity的漏洞進行傳播

CVE-2024-27198 和 CVE-2024-27199 是最近被揭露的兩個影響 JetBrains 公司所開發之構建管理和持續整合伺服器 TeamCity 的漏洞。自這兩個漏洞的概念驗證 (PoC) 程式出現以來，已發現多個威脅者在其攻擊行動中開採濫用這兩個漏洞。其中一個觀察到的攻擊行動就是利用 JetBrains 漏洞部署被稱為 Jasmin 的勒索軟體。該惡意軟體具有加密使用者檔案的功能，並冠上 .lsoc 副檔名，並以檔名為『un-lock your files.html』留下勒索贖金支付說明檔。據報導，最近觀察到的其他利用 JetBrains 漏洞的網路攻擊行動會讓受害者感染不同的有效籌載，例如：XMRig Coinminer、Cobalt Strike beacon 或 SparkRAT 後門。

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：

自適應防護技術(包含於SESC)：

- ACM.Crtutl-CNPE!g1
- ACM.Schtsk-TBat!g1
- ACM.Untrst-FlPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g250

檔案型(基於回應式樣本的病毒定義檔)防護：

- PUA.Gen.2
- Ransom.Zombie
- Scr.Malcode!gdn14
- 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!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：

- Web Attack: JetBrains TeamCity Authentication Bypass CVE-2024-27198
- Web Attack: JetBrains TeamCity Authentication Bypass CVE-2024-27199

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 對 TeamCity 應用程式的安全強化可透過多種不同方式減少攻擊面和降低暴險：

- 鎖定 TeamCity 網路暴露，使漏洞無法在公共網路上被利用。
- 防止存取關鍵檔案，進而防止敏感系統資訊外洩。

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。

2024/03/20
WhiteSnake(*白蛇)惡意竊密程式的全新變種

在真實網路情境上發現 WhiteSnake 惡意竊密程式的全新變種。這種惡意軟體據有增強的反虛擬機器 (AntiVM) 功能，可以檢測沙箱和虛擬環境。它能夠劫持受害者的麥克風和網路攝影機，有效地將個人設備轉化為監控工具。此外，它還能從遭入侵的機器中擷取各類敏感資訊，包括系統資訊、cookie、登錄憑證、瀏覽歷史和加密貨幣錢包。一旦收集到這些資訊，遭擷取的資料就會上傳到威脅者操控的命令與控制 (C&C) 伺服器。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1
- SONAR.MalTraffic!gen1

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

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: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity 568
- Web Attack: Webpulse Bad Reputation Domain Request

2024/03/20
在最近一次網路攻擊行動中傳播StealC惡意軟體

StealC 是一種惡意竊密程式，主要用於竊取機密資訊，包括瀏覽器儲存的資料、cookie、加密貨幣錢包或各種訊息應用程式中的資料。在最近一次網路攻擊行動中，StealC 二進位檔案被偽裝成各種知名應用程式或破解軟體的安裝程式。偽裝的安裝程式透過 GitHub、Mega 或 Dropbox 等可公開存取的檔案庫傳播。

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!gen2

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.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。

2024/03/20

Springtail(*春尾)(又名Kimsuky)進階持續威脅(APT)駭客組織發起新的DEEP#GOSU網路攻擊行動

一個名為『DEEP#GOSU』的全新惡意網路攻擊行動被認為是由 Springtail (又名 Kimsuky 或 Thallium) 進階持續威脅 (APT) 駭客組織所為。該攻擊鏈利用 .LNK 檔、嵌入 PowerShell 指令碼和 VBScript stager 等，導致下載上架在 Dropbox 文件庫中的有效籌載。攻擊行動中最終有效籌載是一個具有後門功能的惡意竊密程式，可用於剪貼簿監控、鍵盤側錄和資料滲出。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Http!g2

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen241
- Scr.Mallnk!gen2
- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.NPE
- 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。

2024/03/19

由SocGholish惡意程式下載器(又名 FakeUpdates)觸發的Raspberry Robin感染鏈

我們研究團隊觀察到最近由 SocGholish 惡意程式下載器涉入的網路攻擊行動，這種惡意軟體通常暗藏在假的軟體更新背後。無疑有他的受害者可能是收到一封電子郵件，導致他們瀏覽遭入侵的網站，也可能是使用者正在積極尋找軟體更新，卻不幸發現自己進入其中一個假網站。這些網站被注入惡意 JavaScript，一旦執行就會下載另一個副檔名為 .WSF 的檔案。這個 .WSF 檔包含一個 JavaScript(這個檔案被高度混淆，並伴隨著一系列反沙箱和反分析功能)，它最終會導致 Raspberry Robin 被植入，這是一個可透過 USB 隨身碟傳播的蠕蟲並具有惡意軟體載入器的功能，可以再下載其他的惡意程式。

SocGholish 會執行以下條件檢查，以驗證是否應繼續執行後續感染程序：

- 如果樣本在桌面資料夾中執行，請退出
- 如果 Windows 版本低於 17063 版本號 (Windows 10 版本 17063)，請退出
- 如果機器的處理器與產品清單相符，請退出
- 如果機器的 MAC 位址與 MAC 首碼清單相符，請退出
- 如果執行進程與指定進程清單相符，退出
- 如果腳本執行時沒有參數，則使用隨機參數重新開啟另一個實例，然後退出

如果惡意軟體資格檢查全部通過，它將刪除自身並設置路徑排除，以繞過 Windows Defender，然後嘗試啟動 curl.exe，從專用遠端伺服器下載有效籌載。

最終有效籌載的檔案名是一個單詞，副檔名是 .dll。使用『msiexec.exe -z』即可啟動該程式。

儘管有這些刻意干擾會影響安全分析和檢測，我們的啟發式引擎還是在無需更新的情況下攔截了 SocGholish。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen53

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：

- 34049_Audit: Scripting Host Processes Making Network Connections

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。

2024/03/19
防護亮點：賽門鐵克進階機器學習技術(AML)

賽門鐵克進階機器學習技術 (AML) 是如何防範零時差威脅

機器學習 (通常簡稱為 ML) 是一種無特徵碼的技術，可在執行前階段阻止全新的惡意軟體。在賽門鐵克機器學習被應用在許多層面，以保護我們的客戶免受網路威脅。這些層級的設計目的是在我們的解決方案 (包括端點、閘道和我們的後端分析平臺) 看到可疑檔案、作業系統事件、登錄檔的機碼、網頁或網路活動的每個環節主動和被動地『把關』。賽門鐵克有能力利用一套全面的威脅掃描引擎，在新內容出現時立即對其進行動態分析，並將威脅情資同步到賽門鐵克全球威脅情資網路 (GIN：Global Intelligence Network)。賽門鐵克使用來自數百萬個端點的安全遙測資料、安全協力廠商提供的威脅相關資料以及海量的乾淨檔案集來訓練和評估各種 ML 模型。這些模型部署在眾多解決方案，用於檢測威脅，既包括作為我們代理一部分的用戶端點，也包括我們的後端分析系統。

零時差防護相當重要

除上述分析平臺外，我們還利用 Cynic 雲端沙箱分析引擎 (以『Cynic』恰如其分的命名) 執行多個 ML 模型和叢集演算法，根據檔案的威脅類型、潛在風險、動態和靜態中繼資料 (metadata) 以及行為對檔案進行分門別類。賽門鐵克利用自動系統和人工惡意軟體分析師儘快分析客戶提交的檔案，並將分析結果輸入到 ML 訓練模型中，以提高分類效率。我們的多模型進階機器學習技術可在 32 位和 64 位版本的各種檔案類型上執行，以提供可付諸行動的分析。在發現防護漏洞時，後臺 ML 模型會對其進行分析，並透過信譽查詢立即阻止漏洞。賽門鐵克進階機器學習 (AML) 主要目標是防範全新的未知惡意軟體，即資安術語所說的零時差攻擊。這正是 ML 的優勢所在。

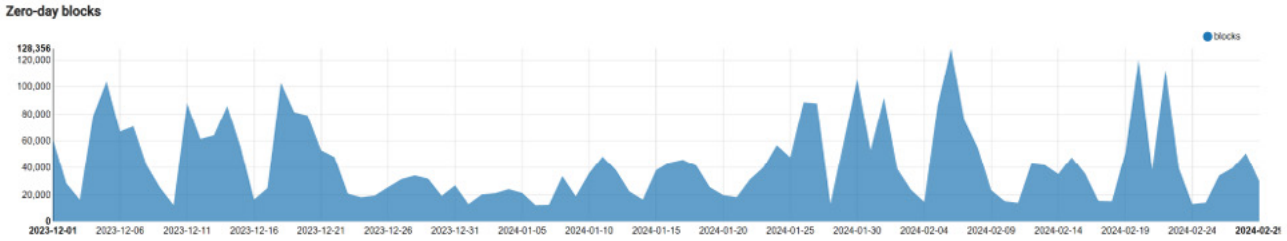
僅在上一季度，賽門鐵克的進階機器學習 (AML) 在賽門鐵克端點和閘道解決方案上攔阻將近 2,300 萬次威脅。其中約 390 萬次阻止的是零時差攻擊，也就是我們的任何安全產品或防護技術從未見過的攻擊。這就是所謂『主動』防護，而不是『被動』防護，後者是指針對攻擊增加新的防護措施或更新現有防護措施。主動防護是應對網路威脅的靈丹妙藥，也是各地網路犯罪分子的剋星。

在上一季度，賽門鐵克僅進階機器學習部分提就供了以下保護：

- 在閘道產品上，賽門鐵克進階機器學習攔截了 1,350 萬個威脅
- 在端點上封鎖了 930 萬個威脅
- 透過 ML 攔截了 390 萬個零時差威脅，其中包括
- 9K 個勒索軟體 (Cerber、Cryptodefence、Gandcrab、Ryuk、Wannacry、Zombie 等)
- 512K 個木馬程式 (Emotet、Cridex、Whispergate 等)
- 160K 以『Win32.』開頭的威脅 (Qakbot、Fujacks、Expiro 等)
- 230K 個後門 (Cobalt、Limitail、Berbew 等)
- 在端點上攔截了 110 萬個瀏覽器類型的威脅 -32% 來自 Chromium，24% 來自 MSEdge，15% 來自 Firefox
- 在端點產品上攔截了 73.1 萬個透過命令列下載和執行惡意檔案的威脅
- 攔截了 585K 次試圖從 USB 隨身碟等外部來源進入系統的威脅

- 阻止了 20 萬次使用伺服器訊息區塊 (Server Message Block，SMB) 網路傳輸協定進行網路檔案共用的攻擊
- 攔截了 105K 個使用點對點 (P2P) 網路程式 (例如：Anydesk (RDP)、Utorrent 和 Bittorrent) 下載的威脅
- 攔截了 5.9K 個使用腳本主機 (Powershell/csript/wcript) 下載的威脅

本季度在端點和閘道上的零時差防護圖表



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。
欲深入瞭解更多有關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的雲沙盒分析引擎 (Cynic)，請點擊此處。

2024/03/19

由Earth Krahang進階持續威脅(APT)駭客組織所發動的惡意活動

在真實網路情境上觀察到由 Earth Krahang 進階持續威脅 (APT) 駭客組織所發動的惡意活動。據瞭解，威脅者鎖定目標是世界各地的政府單位。該威脅組織攻擊採用的策略、技術和程序 (TTPs) 包括使用開源掃描工具、發起魚叉式網路釣魚行動、暴力攻擊、漏洞利用、使用各種提權的工具或促進遠端桌面連接到遭入侵的電腦。據觀察，Earth Krahang 最近使用的惡意軟體包括 RESHELL 和 XDealer 後門。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.ProcHijack!g45
- SONAR.ProcHijack!g47
- SONAR.SuspInject!gen3
- SONAR.SuspLaunch!g13
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt!gm1
- Downloader
- Trojan Horse
- Trojan.Coinminer
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Nancrat
- 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.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：

- 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。

2024/03/19

威脅者假冒人資部門(HR)人員散佈假的薪資通知

有趣的是，威脅者現在似乎變成假冒人資部門的工作人員，傳播新一波的網路釣魚電子郵件。在最近一次網路釣魚行動中，有人向收件人發送包含釣魚網頁並偽裝成未薪資通知單的電子郵件。郵件主旨包含收件人的姓名，以及『missing payroll』的關鍵字。這樣做是為了增加良好的人際互動，引誘用戶打開郵件。電子郵件本文內容簡短，『寄件者』欄位顯示收件人的公司郵件主機網域名稱＋『人力資源』的文字。郵件內文提到人資入口網站上有一個待執行的行動項目，並包含一個用於竊取憑證的網路釣魚網頁。

電子郵件標頭：

- 主旨：[收件人名字].[收件人姓氏] Missing Payroll
- 寄件者："[收件人的公司郵件主機網域名稱] HR " <假冒的郵件帳號>

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。

2024/03/17

Revenge遠端存取木馬(RAT)透過惡意的PowerPoint 附加元件(.ppam)在拉丁美洲、葡萄牙和西班牙傳播

.ppam 檔是一種 PowerPoint 附加元件。PPAM 檔可包含載入到 PowerPoint 中的代碼、腳本和資源，以提供附加功能，包括自訂命令、工具或與外部服務的整合。攻擊者可利用這些功能在受害者的系統上執行惡意程式碼。此類惡意 PPAM 檔可以使用各種程式設計語言建立，包括 Visual Basic for Applications (VBA) 或 HTML、CSS 和 JavaScript 等現代網路技術。由於 PPAM 檔在組織中的廣泛使用及其執行代碼的能力，它們已成為傳播惡意軟體的誘人媒介。

在過去的幾個月中，一個攻擊者一直在拉丁美洲、葡萄牙和西班牙透過電子郵件利用惡意 PPAM 檔。檔名範例包括『Reserva Detalhes.ppam』、『reservas.ppam』、『powerPoint.ppam』、『Reserva Cancelar.ppam』、『Reserva detalhada.ppam』等。

這些 PPAM 檔包含一個惡意巨集，它會執行一個 PowerShell 下載程式，反過來又會發送一個名為 Revenge 遠端存取木馬 (RAT)。這種威脅能讓攻擊者遠端控制受害者的系統，允許進行查看桌面、存取檔案、竊取敏感資訊和監控使用者活動等操作。

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：

- ISB.Heuristic!gen10
- ISB.Heuristic!gen125
- Scr.Malcode!gen103
- Scr.Malcode!gen125
- CL.Downloader!gen9

基於機器學習的防禦技術：

- Heur.AdvML.B

2024/03/17

Cerberus惡意程式假冒Chrome瀏覽器的更新，出現在手機／行動裝置威脅環境中

假冒更新程式是灰色軟體和惡意軟體攻擊者常用的社交工程伎倆，也是交付有效籌載的一種手段。雖然電腦是受影響最大的平臺，但安卓等手機／行動裝置也會受到影響。在最近一個案例中，有人觀察到一個駭客團體或個人用假的 Chrome 更新 (Chrome_Update_[隨機版本號].apk 和／或 Chrome.apk) 引誘手機／行動裝置用戶，而這些更新實際上是一種名為 Cerberus 的遠端存取木馬--一種具有遠端存取功能的複雜安卓銀行惡意軟體，於 2019 年左右首次出現在威脅環境中。

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

2024/03/15

假冒東京電力公司釣魚電子郵件中使用以.top結尾的通用頂級網域

在最近的網路釣魚活動中，以 .top 結尾的通用頂級網域 (gTLD:Generic Top Level Domain。頂級域名是域名的最後一個部份，即是域名最後一點之後的字母。) 被各種威脅者大量濫用。.top 是為品牌和行銷目的而推出。賽門鐵克觀察到冒充東京電力公司 (TEPCO) 的網路釣魚浪潮，其 .top 網域名稱用於竊取用戶憑證。這些網路釣魚通常偽裝成東京電力公司要求支付未繳電費的通知資訊，其主旨包含如下的常見關鍵字：

- 期限が迫っています -> 翻譯：期限將至
- 即時対応が必要 -> 翻譯：需要立即採取行動

由於主旨中的關鍵字顯示了急迫性，使用者會被引誘打開此類電子郵件並點擊釣魚網頁。這些網頁會將受害者導向詐騙憑證的 .top 釣魚網頁。與 .top 相關的網域名稱大多不正規，註冊時間至少為 1 或 2 年。

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。

2024/03/15

惡意軟體即服務(MaaS)網路攻擊行動針對印度的安卓手機用戶

一個向印度安卓用戶散布惡意 APK 手機應用軟體安裝包的全新網路攻擊行動，在真實網路情境上被發現。據了解，這種惡意軟體以惡意軟體即服務 (MaaS) 的形式出售，目標是從受害者的裝置上竊取銀行資訊、簡訊和其他機密資訊。攻擊者偽裝成各種客戶支援、線上預訂、計費或快遞服務等類型的應用程式，傳播惡意 .apk手機應用軟體安裝包。

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
- 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。

2024/03/15

希臘國家銀行(NBG)的存戶遭受到新一波網路釣魚攻擊

希臘國家銀行(NBG)是全球最大的銀行和金融服務機構之一，總部位於希臘雅典。最近，賽門鐵克發現有釣魚網站冒充希臘國家銀行的服務，誘使使用者打開假冒的驗證電子郵件。郵件內容提到，有一筆不尋常的資金轉帳，因此通報。使用者需要驗證異常交易，以避免帳戶受到進一步限制。這些釣魚電子郵件試圖引誘使用者打開並點擊準備竊取憑證的釣魚網址。

電子郵件主旨：I-BANK NBGEmail From: NBG I-BANK <假冒的郵件帳號>

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。

2024/03/15
隱藏的威脅～PixPirate手機金融木馬

PixPirate 是一款具有遠端存取木馬 (RAT) 功能的手機金融惡意軟體，其目標是從遭入侵的手機／行動裝置上竊取憑證和銀行詳細資訊。該惡意軟體可以存取和操縱設裝置上安裝的手機應用程式、編輯或刪除簡訊、存取連絡人清單、安裝其他的手機應用程式並允許鍵擊記錄等功能。PixPirate 的最新變種有兩個元件--下載器和有效籌載的安裝檔 (.APK)。該惡意軟體採用新的技術向受害者隱藏惡意 APK 的啟動圖示。據了解，PixPirate 是透過惡意簡訊或 WhatsApp 訊息傳播的。

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
- AppRisk:Generisk

2024/03/15
BunnyLoader惡意程式載入器3.0最新版

BunnyLoader 惡意程式載入器於 2023 年 9 月首次被發現，它是一個具有竊取和剪貼功能的惡意載入程式。最近，研究人員發現該惡意軟體的最新版本，其中包含功能增強、漏洞修復和額外的安全軟體規避和保護功能。

以下是 BunnyLoader 以前和最近的功能列表：

- 無檔案載入
- 憑證盜竊
- 鍵盤側錄
- 剪貼簿內容竊取
- 下載其他惡意軟體
- 遠端命令執行
- 加密錢包盜竊
- 應用程式憑證盜竊

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.MalTraffic!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn32
- SMG.Heur!gen
- Trojan.Gen.MBT
- Trojan.Gen.2
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

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

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。