保安資訊--本周(台灣時間2024/03/01)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 58 萬 3,700 台受保護端點上總共阻止了 5,610 萬次攻擊。這些攻擊中有 83.1% 在感染階段前就被有效阻止：**(2024/02/26)**

- 在**11萬2,800**台端點上，阻止了**1,800萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**14萬8,500**台端點上，阻止了**1,280萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬8,600**台**Windows**伺服主機上，阻止了**9,400萬**次攻擊。
- 在**6萬5,000**台端點上，阻止了**190萬**次嘗試掃描伺服器漏洞。
- 在**1萬2,900**台端點上，阻止了**75萬9,700**次嘗試掃描在**CMS**漏洞。
- 在**5萬8,900**台端點上，阻止了**120萬**次嘗試利用的應用程式漏洞。
- 在**21萬6,600**台端點上，阻止了**470萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬7,000**台端點上，阻止了**160萬**次加密貨幣挖礦攻擊。
- 在**13萬700**台端點上，阻止了**800萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**583**台端點上，阻止了**7萬5,700**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 15.41 萬個受保護端點上阻止了總計 620 萬次攻擊。**(2024/02/26)**

- 使用網頁信譽情資，在 **138K** 個端點上阻止 **540** 萬次攻擊。
- 攔截 **34K** 個端點上 **654.7K** 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 **12.7K** 個端點上攔截 **114.8K** 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 **482** 個端點上攔截 **34.6K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

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。

2024/02/29

Bifrost惡意遠端存取木馬在Linux平台出現新變種

在真實網路情境發現 Bifrost(又稱 Bifrose) 惡意軟體在 Linux 平台上的新變種。Bifrost 是一種惡意遠端存取木馬 (RAT)，已知會透過惡意網站或惡意垃圾郵件傳播。該惡意軟體具有收集受感染主機資訊的功能。最新的 Bifrost 變種採用 C&C 網域搶註冊／(輸入誤植網域名稱) 技倆，以逃避檢測。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- 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。

2024/02/29

Mac OS請留意～Atomic惡意竊密程式(AMOS)出現基於Python腳本的新變種

Atomic 惡意竊密程式 (AMOS) 是一種針對 macOS 平臺的惡意軟體。據觀察，該惡意軟體出現一種新的變種，它利用 Python 腳本來逃避檢測和收集資料。截取的資料包括儲存在基於 Chromium 瀏覽器中的資訊，例如：密碼或 cookie、系統資訊、憑證或與已安裝的加密錢包和加密貨幣擴展相關的資料……等。所有收集到的資訊都會壓縮成一個 .zip 壓縮檔，並轉發到攻擊者所操控的 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：

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。

2024/02/29

Louse(*蝨子)(又名 Patchwork)進階持續威脅(APT)駭客組織

Louse 進階持續威脅 (APT) 駭客組織 (又名 Patchwork 或 Quilted Tiger) 是一個早在 2015 年就被發現的駭客組織，據瞭解，該組織主要針對世界各地的高知名度組織、金融和政府單位以及媒體、能源和製藥行業。該駭客組織一直濫用各種惡意軟體和自訂工具發動攻擊。BadNews 後門和 VajraSpy RAT 只是出於該駭客組織的惡意軟體的兩個例子。Louse APT 一直在使用魚叉式網路釣魚和水坑式漏洞攻擊，並利用已知漏洞入侵所針對的目標。

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：

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：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.NPE
- Trojan.Mdropper
- W97M.Downloader
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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：

- 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。

2024/02/28

中東產業疑似成為伊朗Tortoiseshell駭客組織攻擊的目標

伊朗支援的網路間諜組織 Tortoiseshell(又名 Imperial Kitten、Smoke Sandstorm、UNC1549) 正利用兩個全新的後門程式瞄準中東的國防產業企業。這些威脅份子與伊斯蘭革命衛隊 (IGRC) 有關聯，他們散播政治消息和假的技術類職缺來詐騙以色列、阿拉伯聯合大公國和大中東地區其他國家的公司員工並入侵其系統。據報導，該行動執行魚叉式網路釣魚和水坑式攻擊，以獲取憑證並注入名為 MINIBIKE 或其最新變種 MINIBUS 的後門惡意軟體。該行動至少可追溯到 2022 年 6 月，目前仍處於活躍狀態，它使用 Microsoft Azure 雲端基礎設施來執行命令和控制以及託管功能。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-RgPst!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Trojan.Coinminer
- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2024/02/28

Dark Crystal(*黑暗水晶)遠端存取木馬(RAT)惡意軟體

Dark Crystal RAT (DCRat) 是一種惡意竊密程式。這種惡意軟體具有許多功能可以隨需擴充，因為它的模組化架構允許針對特定目標類型的攻擊進行客製化。這種模組化結構還能讓程式碼不斷變異，以繞過檢測。一旦受害者的機器受到感染，DCRat 就會收集螢幕截圖、網路攝影機／麥克風資料、.NET 資料和串流／telegram 資料……等資訊進行資料滲出。

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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspLoad!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!100
- Heur.AdvML.B!200
- 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。

2024/02/28

針對Linux和Windows發動的挖礦劫持行動

駭客組織 8220，過去曾使用過加密貨幣挖礦攻擊。在其最新版本中，Linux 的部份變動不大，而 Windows 版本則強化許多功能。

該惡意挖礦程式的 Windows 部署利用 PowerShell 實現無檔案執行。新技術包括 DLL 側載、繞過用戶帳戶控制 (UAC) 以及更改 AMSIscanBuffer 和 ETWEventWrite 函數攻擊。該駭客組織也導入各種技術來規避檢測，繞過防毒 (AV)、端點檢測和 EDR 系統。

Linux 的新版本沒有重大變化，它是一個下載惡意軟體的 shell 腳本。該腳本會尋找易受攻擊的應用程式，並使用較新版本的 masscan 和 spirit 進行偵查。這個新版本也更難被發現。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.NPE
- Trojan Horse
- WS.Malware.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。

2024/02/28

Appleworm進階持續威脅(APT)駭客組織透過惡意PyPI套裝軟體散播Comebacker惡意軟體

在 Python 官方軟體套件庫 PyPI(Python Package Index) 中發現幾個惡意的 Python 套件軟體。這些被發現的惡意套件軟體 (pycryptoenv、pycryptoconf、quasarlib 和 swapmempool) 會助長 Appleworm APT 駭客組織 (又名 Lazarus) 的 Comebacker 惡意軟體的傳播。該惡意軟體具有下載和執行其他額外任意有效酬載的破壞力。

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

2024/02/28

在真實網路情境上觀察到PrivateLoader惡意軟體的最新版本

PrivateLoader 是一種下載程式類型的惡意軟體，以按安裝付費 (PPI) 的營運模式，攻擊者可以購買這項服務向目標個人發送惡意有效酬載。服務費是根據成功感染的數量來支付。PrivateLoader 在之前被揭露的行動中提供多種有效酬載，包括 Vidar、Raccoon Stealer、Redline、Smokeloader……等。最近的行動也散播 RisePro 這種惡意竊密程式。PrivateLoader 最新版本採用新的加密演算法、使用商業 VMProtect 封裝程式和更新通訊協等面向進行了創新。

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-Rgasm!g1
- ACM.Rgasm-Lnch!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.ProcHijack!g45
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn32
- 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.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 Process Request 4
- 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。

2024/02/28

垃圾郵件散播行動，以報稅為幌子向墨西哥使用者散播TimbreStealer惡意軟體

全新的惡意竊密程式經證實，透過以財務工程為幌子的垃圾郵件散播行動到處肆虐。該垃圾郵件散播行動只針對墨西哥用戶，透過與報稅為幌子的主旨誘使受害者下載有效酬載。最終的有效酬載被確認為 TimbreStealer，這是一個精密複雜的竊惡意竊密程式，利用多個嵌入式模組來執行工作。

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：

自適應防護技術(包含於SESC)：

- SONAR.TCP!gen6

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：

- Packed.Generic.739
- Trojan Horse
- Trojan.Gen.MBT
- 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: 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。

2024/02/27

小心.LNK的惡意捷徑檔～Funnelweb駭客組織針對臺灣發起新一輪魚叉式網路釣魚電子郵件攻擊行動

據報導，Funnelweb 駭客組織 (又稱 Earth Lusca) 針對臺灣用戶發起新的魚叉式網路釣魚電子郵件行動。攻擊開始時，網路釣魚電子郵件包含一個帶有 .LNK 的惡意捷徑檔的 7z 壓縮檔附件，打開後會執行 JavaScript 程式碼，最終傳送 Cobalt Strike 有效酬載。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g372

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt!gm1
- Backdoor.Cobalt
- Trojan Horse
- Trojan.Mallnk
- Trojan.Malscript
- 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

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：

- 32486_Audit: Bad Reputation Application Activity
- 33837_System Infected: Bad Reputation Application Network Activity
- 33986_System Infected: Trojan.Backdoor Activity 721
- 29565_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)：

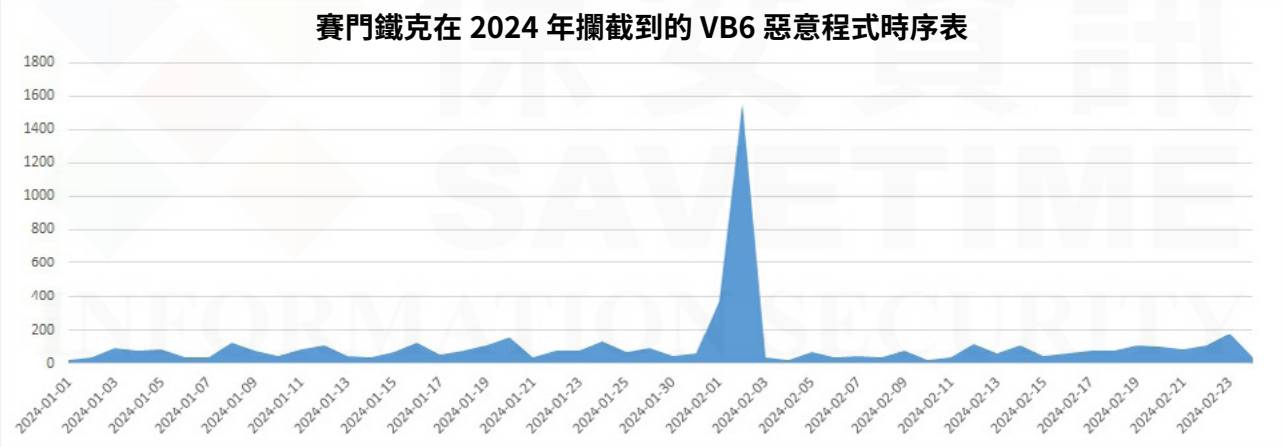
被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2024/02/27
防護亮點：基於VB6的惡意軟體威脅在2024年依然活躍

根據維基百科，經典的 Visual Basic(通常稱為『VB』) 於 1991 年首次發佈，是基於 BASIC 程式設計語言 (早在 1963 年就發佈了！) 和微軟 Windows 整合式開發環境 (IDE) 的第三代程式設計語言。其最終版本是 1998 年發佈的第 6 版 (VB6)。2008 年 4 月 8 日，微軟停止對 VB6 IDE 的支援，取而代之是微軟為新的 .NET Framework 設計之 VB.NET，突破傳統模式的許多限制。

儘管已經過 25 年，但由於微軟確保 VB6 應用程式在受支援 Windows 作業系統上的相容性，因此 VB6 可執行檔仍然可以在最新的 Windows 版本上運行。得益於這種相容性，我們仍然可以在工廠、醫院和企業中，還看得到許多採用 VB6 設計的系統還在運作。但另一方面，攻擊者仍然可以利用 VB6 建立新病毒，這可能是希望安全研究人員更難分析和檢測這些使用老式工具製作的可執行檔。

Vilsel 蠕蟲就是這樣一種一段時間就會出風頭的 VB6 惡意軟體。自 2015 年底安全研究人員首次發現以來，Vilsel 已被修改過好多次，2024 年我們仍能在全球範圍內看到它的存在，它是整個 VB 惡意軟體生態系的要角。



Vilsel 是在過時的 Visual Basic 編譯器編譯選項中利用 PCode(Pseudo-code) 或偽代碼／虛擬代碼建立。PCode 不是本地 (Native) 的 CPU 程式碼，而是 VB6 特定的中間程式碼，由微軟的相容程式逐步執行。因此，許多常用的現代分析工具都無法分析這些檔案，需要使用 VB 反編譯器或類似工具才能分析它們。Vilsel 某些變種會進一步將 VB6 可執行檔封裝在原生代碼混淆程式中，導致一些不太強大的反 VB6 保護功能失靈。

我們分析的一個 Vilsel 的特定版本是這樣運作：

- 建立一個自身副本，在程式碼末尾新增部份額外位元組
- 將自身複製到現有資料夾，對系統中的所有資料夾重複此動作
- 使用以下檔案名稱：backup.exe、System Restore.exe、update.exe、data.exe

有趣的是，選擇 System Restore.exe、update.exe 和 data.exe 的概率分別為 1/30，因此選擇 backup.exe 的概率為 27/30，即 90%，這意味著該檔最終很可能使用這個名稱，將自己隱藏在名稱相似的合法系統檔中。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- W32.Vilsel!gen1
- W32.Vilsel!gen2

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。

2024/02/27

IDAT惡意程式載入器的新變種被用於傳播Remcos惡意軟體

IDAT Loader (惡意程式載入器) 的最新變種被發現涉入最近一場針對位於芬蘭烏克蘭附屬組織的攻擊行動。IDAT 是一種多用途惡意程式載入器，已知可用於傳播各種惡意有效酬載。以前曾出現過該載入器傳播 Danabot、SystemBC 或 Redline Stealer 等惡意軟體的情況。最新的攻擊行動由 UAC-0184 威脅組織所發起。該威脅分子一直在使用隱寫技術來混淆所發送的惡意有效酬載--已知為 Remcos 這種商品化的 RAT(遠端存取木馬)。

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
- ACM.Wscr-CNPE!g1
- ACM.Wscr-FlPst!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen111
- ISB.Downloader!gen63
- Scr.Malcode!gen
- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Mdropper
- Web.Reputation.1
- 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
- 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。

2024/02/27

利用遠端桌面連線軟體ConnectWise ScreenConnect的網路釣魚行動

ConnectWise ScreenConnect 是一款合法的遠端支援工具。最近，有人發現攻擊者利用該軟體的功能，在未經授權的情況下存取目標系統。據報導，目標是醫療保健行業和加密貨幣用戶。

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：

- WS.Reputation.1

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／IP位址已於第一時間收錄於不安全分類列表中。

2024/02/26

SYSDF勒索軟體

SYSDF 是最近發現源於 Dharma／Crysis 勒索軟體的全新變種。該惡意軟體會加密使用者檔案並冠上 .SYSDF 副檔名。此外，它還會新增一個屬於個別受害者的獨立 ID 和惡意軟體開發者的電子郵寄地址。SYSDF 會以文字檔的形式將勒索贖金說明發送到受害者的機器上。該惡意軟體具有刪除受感染主機上的磁碟備份功能。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Vss-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomCrys!g2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Crysis
- Ransom.Crysis!gm
- SMG.Heur!gen
- 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

2024/02/26

WingOfGod遠端存取木馬(RAT)惡意軟體

WingOfGod 遠端存取木馬 (RAT) 惡意軟體，最近因涉入名為 aNotepad 的免費線上記事本平臺的攻擊行動而聲名大噪。該惡意軟體既針對 Windows 系統，也針對 Linux 平臺。該 RAT 具有執行任意指令、下載／上傳檔案和收集遭入侵主機資訊……等功能。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Msbuild!g1

ACM.Ps-Rd32!g1

ACM.Ps-Wscr!g1

ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- Scr.Malcode!gdn14
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1
- 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

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
- 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。

2024/02/26
Xehook惡意竊密程式

最近幾周，人們發現更多與 Xehook 相關的偷渡式下載和測試活動。這種惡意軟體是一種惡意竊密程式，在地下論壇和 Telegram 上都有廣告，訂閱費最低從每月 31 美元到 600 美元的無限制存取不等。

就功能而言，Xehook 與市面上大多數惡意竊密程式類似，沒有什麼特別之處。它能夠從基於 Chromium 和 Gecko 的瀏覽器以及各種瀏覽器加密貨幣和 2FA 擴展中竊取敏感性資料。

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：

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

2024/02/26
Power(*強力)惡意竊密程式

Power Stealer (又名 NTstealer) 是一種典型的惡意竊密程式，在過去幾個月裡，它在各種平臺上大肆宣傳，並涉入多起網路攻擊。它並非只由個體戶者使用，而是由多個駭客團體和個體戶，這些駭客團體和個體戶攻擊者主要還是針對個人用戶，但也包括一些企業發動瀏覽網頁時的偷渡式下載攻擊。

以功能而言，它可以竊取以下資料(以及其他資料)，這些資料將被壓縮並上傳到設定中指定的 Gofile 帳戶。

- 竊取系統資訊 (主機名稱、使用者資訊、IP 位址……等)
- 來自 Discord 的權杖和備份代碼
- 各種瀏覽器的自動填入、書籤、cookie、信用卡、歷史記錄和密碼
- 來自以下應用程式的敏感檔和資訊：Steam、Roblox、Telegram、ICQ 和 Instagram

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