保安資訊--本周(台灣時間2023/04/07)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 78 萬 500 台受保護端點上總共阻止了 9,540 萬次攻擊。這些攻擊中有 92% 在感染階段前就被有效阻止：**(2023/04/03)**

- 在**15萬600**台端點上，阻止了**4,000**萬次嘗試掃描**Web**服務器的漏洞。
- 在**27萬4,900**台端點上，阻止了**2,040**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬3,900**台**Windows**伺服主機上，阻止了**1,540**萬次攻擊。
- 在**8萬1,500**台端點上，阻止了**260**萬次嘗試掃描伺服器漏洞。
- 在**1萬9,800**台端點上，阻止了**99萬800**次嘗試掃描在**CMS**漏洞。
- 在**6萬1,500**台端點上，阻止了**190**萬次嘗試利用的應用程式漏洞。
- 在**26萬5,500**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**3萬2,000**台端點上，阻止了**250**萬次加密貨幣挖礦攻擊。
- 在**15萬2,000**台端點上，阻止了**1,150**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,700**台端點上，阻止了**14萬6,500**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。

2023/04/07

Clop勒索軟體的活動增加

2023 年 2-3 月，由 Clop 勒索軟體引起的惡意活動有所增加。Clop 勒索軟體家族最初於 2019 年被發現，此後經常被發現透過各種感染媒介 (包括魚叉式網路釣魚、漏洞利用攻擊伺服器和 RDP 暴力攻擊) 以組織和機構為目標。最近攻擊利用 Fortra 提供知名的檔案傳輸管理系統 GoAnywhere 之代管檔案傳輸 (MFT：Managed File Transfer) 的 (CVE-2023-0669) 遠端程式碼執行漏洞來傳播惡意軟體。這是 Clop (TA505) 背後威脅者利用檔案傳輸軟體中漏洞的另一起事件。早在 2021 年，他們就開採利用 Accellion 檔案傳輸裝置 (File Transfer Appliance：FTA) 中的一個漏洞。

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!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Packed.Generic.620
- Ransom.Ploc
- 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
- 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: GoAnywhere MFT RCE CVE-2023-0669

2023/04/06

BlackByteNT勒索軟體--採用C++語言重新撰寫的新變種

在網路上發現一種採用 C++ 語言重新撰寫被命名為 BlackByteNT 的 BlackByte 勒索軟體之新變種。該惡意軟體會對用戶檔案進行加密，被其加密後檔案會新增 .blackbytent 的副檔名。加密完成後，名為“BB_Readme_ [random_string] .txt”的勒索贖金說明文字檔將被存放在受害者電腦上。勒索贖金說明建議受害者透過駭客所操控 TOR 加密網站來聯繫攻擊者，以獲得進一步指示。

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.Ransomware!g38
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Blackbyte
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.C

2023/04/06

Color1337--Linux平台上的加密貨幣挖礦行動

Color1337 是最近發現一種針對 Linux 裝置的加密貨幣挖礦網路威脅行動。已傳播的惡意軟體執行 Monero 加密貨幣挖礦惡意軟體，並試圖散布到網路已遭感染的網路中其他電腦。威脅攻擊者一直透過 Discord 伺服器取得從遭駭電腦蒐集到的資訊。

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：

- Hacktool
- Miner.XMRig
- 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。

2023/04/06

只勒索100美元～PayMe100USD勒索軟體

PayMe100USD 是上個月發現另一種一般普通的勒索軟體。該惡意軟體是採用 Python 撰寫，展現出標準的勒索軟體行為並執行典型功能。它避免對某些檔案格式進行加密，被其加密後檔案會新增 .PayMe100USD 的副檔名。如果不在 48 小時內支付 100 美元等值比特幣，攻擊者威脅要公開發布洩露受害者的資料。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2023/04/05

專門設計為鎖定使用葡萄牙文的人士的全新加密貨幣錢包剪貼簿竊密器(Clipper)

加密貨幣盜竊的伎倆不勝其數，其中一種方法是隨時檢測比特幣錢包地址，複製到剪貼簿時，馬上置換為攻擊者的加密貨幣錢包地址。這是為了誘騙用戶將比特幣發送到錯誤的錢包地址。這種方法非常有效，因為比特幣交易是不可逆。

已經觀察到採用上述伎倆的惡意軟體行動針對多個行業的受害者，包括 IT、房地產和製造業。發動此攻擊行動的威脅者購買搜尋引擎最佳化 (SEO) 廣告將搜尋葡萄牙語系網頁版的 WhatsApp 的受害者重導向到冒充合法 Web 應用程式的惡意網站。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan Horse
- Trojan.Malscript

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已於第一時間收錄於不安全分類列表中。

2023/04/05

Money Message--針對Windows和Linux系統的全新勒索軟體

在網路上發現一種名為 Money Message 的全新勒索軟體。雖然最初僅被報導發生在Windows 平台，但賽門鐵克的威脅獵手團隊還發現該勒索軟體家族的 Linux ESXi 版本。Money Message 採用 ChaCha20／ECDH 演算法對檔案進行加密。加密完成後，檔名為 money_message.log 的勒索熟金支付說明檔會被存放到受感染的電腦上。該針對 Linux 系統的惡意軟體變種似乎仍在開發中，

但它也具有加密檔案的功能。這個勒索軟體背後的攻擊者正營運一個公開的勒索網站，他們還聲稱在加密之前已從受害者那裡竊取資料。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!gen4
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.MoneyMess
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

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

2023/04/04

Typhon Reborn竊密程式釋出V2新版本

Typhon Reborn 是一種惡意竊密程式，首次被發現是在 2022 年年中左右。該惡意軟體的新版本正在俄羅斯網路犯罪論壇上以相對便宜的價格出售，並提供買斷式或按月訂閱的銷售模式。該惡意軟體背後的威脅者聲稱增強規避安全軟體偵測與分析和虛擬環境感知的功能，這可能會增加其在未來攻擊中被採用的普及率。

該竊密程式包含以下功能：

- 竊取系統檔案／資訊
- 竊取加密貨幣錢包資料
- 從 Chromium 和 Edge 瀏覽器外掛中竊取資料
- 螢幕截圖
- 從標準應用程式中竊取密碼、令牌和其他機敏資訊

收集後，資料將轉發到攻擊者使用 Telegram API 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：

基於行為偵測技術(SONAR)的防護：

- SONAR.maltraffic!gen1
- SONAR.Zbot!gen8

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn32
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan Horse
- WS.Malware.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: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 568

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。

2023/04/04

APT-C-36駭客集團積極利用LimeRAT惡意軟體

LimeRAT 是 APT-C-36 (又名 Blind Eagle) 駭客集團所掌控的惡意軟體。該惡意軟體已經為人所知多年，且在過去幾個月中一直被該駭客集團所採用，並在各種惡意攻擊行動中被觀察到。LimeRAT 是一種相當多功能的遠端存取木馬 (RAT)，它允許對遭駭的端點進行遠端控制，但也表現出各種竊密程式和鍵盤側錄功能。借助這種惡意軟體，攻擊者可以遠端執行任何指令、下載檔案或發動加密貨幣挖礦惡意行動等。

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：

- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.LimeRat
- WS.Malware.1

基於機器學習的防禦技術：

- 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。

2023/04/04

Mantis進階持續威脅(APT)駭客集團的最新活動

Mantis 網路間諜組織 (又名 Arid Viper、Desert Falcon、APT-C-23) 是一個被公認為在巴勒斯坦境外活動的威脅組織，在持續發動攻擊部署更新的工具集，並竭盡全力在目標網路上持續蟄伏。雖然該組織以針對中東的組織而聞名，但賽門鐵克 (目前是博通的軟體部門的企業安全部門) 發現最近一次活動主要針對巴勒斯坦領土內的組織，惡意活動從 2022 年 9 月開始，至少持續到 2023 年 2 月。這個目標對於 Mantis 並非史無前例，因賽門鐵克先前於 2017 年曾發現針對位於巴勒斯坦境內的個人的攻擊。

在我們部落格文章中有更多資訊可供參考：Mantis：針對巴勒斯坦目標的新工具

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.SuspPE!gen19
- SONAR.TCP!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Trojan Horse
- Trojan.Aridgopher
- Trojan.Exmatter
- Trojan.Micropsia
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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: Trojan.Backdoor Activity 634
- 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。

2023/04/04

Blitzed(*閃電)網頁資料抓取(爬蟲)工具

威脅情境中顯然不乏網頁資料抓取 (爬蟲) 工具 (Grabber)，有些在地下論壇上出售，但許多也在知名的軟體開發和版本控制的代管服務站台上共享。Blitzed 算是 Grabber 中的翹楚，初期是由其作者分享出來，然後社群製作副本並在各種平台（包括論壇、網站和社交媒體）上進一步傳播。最近，賽門鐵克發現透過瀏覽網頁時的偷渡式下載攻擊有所增加，這些攻擊採用詐騙伎倆（例如：偽裝成假冒常用軟體或遊戲破解）來散播 Blitzed Grabber。

實際上，此惡意軟體沒有提供任何與眾不同的獨特之處。它透過 Discord webhooks 自動發送訊息報告／洩露被盜資料，它具有典型的資料盜竊功能，包括從 Chromium 瀏覽器竊取 PC 資料、登錄憑證、cookie 和一鍵自動填入資料。它還會截取螢幕截圖並竊取“ROBLOSECURITY”cookie。此 cookie 是一個小的文字檔，在用戶登錄後由 Roblox 網站建立並儲存在用戶的網頁瀏覽器上。它包含一個唯一標識符，使 Roblox 能夠追踪用戶的連線並提供個性化服務。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g13
- SONAR.SuspLaunch!g266

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

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/04/03

Venom Drainer駭客組織所提供的"詐騙即服務"呈上升趨勢

如今，加密貨幣和非同質化代幣 (NFT) 經常面臨資產被惡意軟體和網路釣魚攻擊者竊取的風險，世界各地每天都有攻擊行動發生。最近一個被稱為“Venom Drainer”攻擊者所發動特定的攻擊行動者被曝光，他們提供詐騙即服務。這種網路犯罪形式由個體戶或駭客集團向他人提供詐欺服務或工具，通常收取議定的服務費用或一定比例的分潤。

在過去的幾個月裡，涉案人員已經建立 500 多個釣魚網域，目標是各種已知的加密和 NFT 交易服務，例如：Blur、Metamask、Arbitrum 等。據報導，他們可能盜取價值數百萬美元的加密貨幣交易。

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: 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。

2023/04/03

AlienFox工具包被大肆濫用於竊取憑證

Alienfox 是一種模組化的惡意軟體工具包，在最近的攻擊中被利用，目標是在熱門的雲端服務商（例如：AWS、MS Office365、Twillio、Zimbra 等）搜刮憑證。AlienFox 使用資料收集腳本在設定錯誤的伺服器中搜尋通常用於儲存機密的敏感配置檔，例如：API 密鑰、帳戶憑證和身份驗證權杖。AlienFox 由威脅攻擊者透過私人 Telegram 頻道出售，其中一些模組也可以在 Github 儲存庫中輕鬆獲得。

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
- Trojan Horse
- 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。

2023/04/03

防護亮點：應對惡意XMRig挖礦應用程式，賽門鐵克游刃有餘

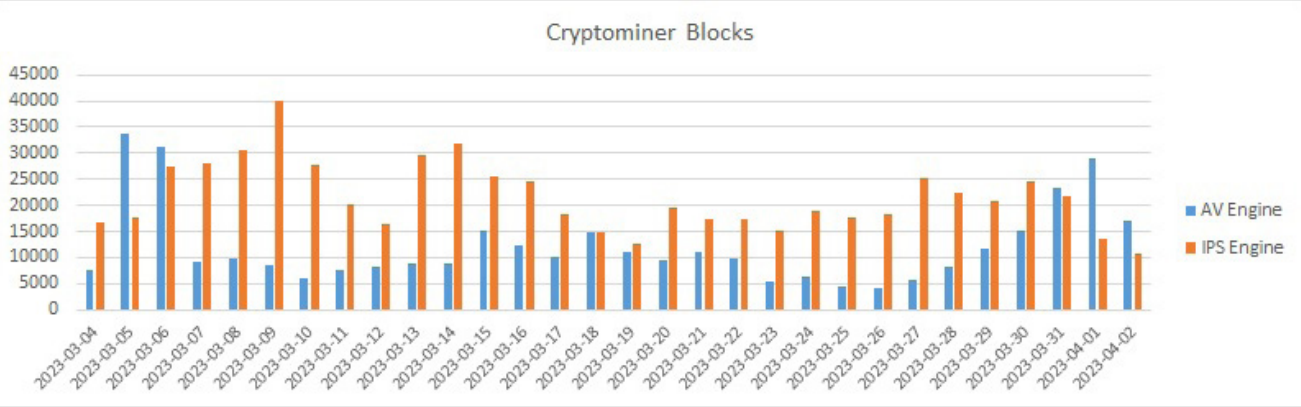
～防護亮點～

XMRig 是一種占用 CPU 的熱門的開放原始碼密貨幣挖礦應用程式，常用於開採門羅幣(XMR)。雖然 XMRig 是一種合法工具，但它經常被惡意軟體作者用來在遭駭入的系統未經用戶同意的情況下使用（即竊取）其運算能力來開採門羅幣。這種做法稱為加密劫持。從這點上，當我們提到 XMRig 時，我們指的是加密劫持之案例。

XMRig 雖然很流行，但它只是眾多不受歡迎的加密挖礦程式中之一種，其中一些會先被我們的防毒--AV (檔案分析) 引擎技術阻止，而另一些則被我們的 IPS (網路流量分析) 技術捕獲，具體取決於特定的感染方式。這裡用“先”是因為大多數都會被這兩種防護技術攔截，但一旦

威脅被移除，它通常不會觸發後續防護技術，所以績效會列入先攔截。也就是說，威脅的某些元件可能會被一種防護類型攔截，而同一威脅的其他元件可能會被不同的技術攔截。這其實凸顯“多層式安全”的重要性。

下圖顯示過去一個月所攔截的 AV／IPS 分類。



此處包含的 XMRig 只是賽門鐵克阻止眾多不需要的加密挖礦程式之一。

XMRig 可能會使用造駭入電腦的中央處理單元 (CPU) 和／或圖形處理單元 (GPU) 70% 到 80% 的效能。當 XMRig 執行時，用戶可能會注意到他們的電腦執行速度比平時慢，遊戲或應用程式運作不順暢或停頓。根據當時電腦的狀況，它也可能會變得很熱，進而可能對硬體元件造成損壞。長時間使用也會比平時消耗更多的電量，所以可能會增加電費。

XMRig 成為惡意軟體作者的熱門選擇有以下幾個原因：

- XMRig 相對易於使用和設定，即使是新手網路犯罪份子也可以使用它。
- XMRig 是開放原始碼，這意味著它的程式碼可供任何人免費修改和散播。惡意軟體作者可以輕鬆修改程式碼以試圖逃避檢測並增加利潤。
- 門羅幣 (Monero) 是一種廣受歡迎的加密貨幣，因為它被設計成使用 CPU 的效能進行挖礦，進而更容易使用遭駭入系統的殭屍網路進行大規模挖礦。
- XMRig 效率高，可以在不消耗過多系統資源的情況下，以相對較高的速率挖掘門羅幣，使其成為加密貨幣劫持的理想選擇。

XMRig 挖礦程式透過多種方式傳播，包括網路釣魚和其他類型的電子垃圾郵件、惡意廣告、惡意植入程式、漏洞利用、破解軟體、潛在有害應用程式 (PUA)、網頁瀏覽時的順道下載等。

賽門鐵克對 XMRig 進行長期檢測，並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 **零時差**防護技術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：

- CL.XMRig!gen1
- Miner.XMRig
- Miner.XMRig!gen*
- OSX.Miner.XMRig!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Suspdrop!g61

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)。

基於機器學習的防禦技術：

- Heur.AdvML.*

* 這表示存在多個類似名稱的檢測，例如：Heur.AdvML.B, Heur.AdvML.C 等

要了解有關賽門鐵克端點安全安全完整版更多資訊，請點擊此處。
要了解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
要了解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
要了解 Symantec Endpoint Protection 如何使用進階機器學習，請點擊此處。

2023/04/03

GoatRAT安卓銀行木馬

GoatRAT 是另一個利用自動轉帳系統 (ATS) 框架的安卓銀行木馬惡意程式，它允許攻擊者自動執行多項詐騙操作，而無需攻擊者的手動或遠端互動。一旦用戶開啟目標銀行的APP，惡意軟體將顯示一個覆蓋層，該層將收集銀行憑證，並將它們發送到攻擊者控制的 C&C 伺服器，並啟動從受害者帳戶向攻擊者轉移資金。GoatRAT 已經出現在針對利用 PIX 即時支付平台的巴西銀行用戶的攻擊行動中。

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。

- 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。

2023/03/31

Creal竊密程式鎖定加密貨幣用戶

威脅攻擊者在最近惡意網路釣魚行動中，一直以加密貨幣用戶為目標，並利用一種名為“Creal”的全新惡意竊密程式。

Creal 是符合 Python 的惡意軟體，具有以下功能：

- 從 chromium 瀏覽器竊取登錄憑證、cookie 和一鍵自動填入資料
- 從聊天和遊戲應用程式中竊取資料
- 針對 Chrome 類型的瀏覽器外掛
- 竊取與加密錢包應用程式相關的錢包和機密檔案

總之，該惡意軟體目的是使用 Discord webhook 獲取訊息並將其洩露到其預先配置好的 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：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- W32.Beapy

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。

2023/03/31

針對Linux伺服器的Mélofée植入載體(Implant)家族

Mélofée 是一個新發現針對 Linux 伺服器的植入載體 (Implant) 家族。已知 Mélofée 變種之一已利用開放原始碼 Repile 專案作為修改版本來傳播 rookit。由於此惡意軟體似乎正在持續開發中，所以最近植入樣本展示新的後門功能。根據最近一份報告，Mélofée 攻擊者使用的基礎架構與其他威脅組織共享一些共同連結，並使用 Winnti、PlugX、Cobalt Strike 或 HelloBot 等各種惡意工具。

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!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- Backdoor.Cobalt!gen1
- Backdoor.Cobalt!gen7
- Backdoor.Cobalt!gm
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- 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。