保安資訊--本周(台灣時間2022/12/09)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：**(2022/12/05)**

- 在**16萬5,600**台端點上，阻止了**4,480**萬次嘗試掃描**Web**服務器的漏洞。
- 在**32萬7,300**台端點上，阻止了**2,530**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬4,400**台**Windows**伺服主機上，阻止了**1,770**萬次攻擊。
- 在**11萬2,200**端點上，阻止了**370**萬次嘗試掃描伺服器漏洞。
- 在**3萬800**台端點上，阻止了**160**萬次嘗試掃描在**CMS**漏洞。
- 在**6萬2,700**台端點上，阻止了**210**萬次嘗試利用的應用程式漏洞。
- 在**32萬7,800**台端點上，阻止了**790**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**4萬7,000**台端點上，阻止了**390**萬次加密貨幣挖礦攻擊。
- 在**5萬3,500**台端點上，阻止了**540**萬次向惡意軟體**C&C**連線的嘗試。
- 在**4,400**台端點上，阻止了**13萬4,900**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。

2022/12/08

網路釣魚常假冒商機～冒充韓國半官方組織的新一波網路釣魚郵件攻擊行動

觀察到一種新的網路釣魚行動，該攻擊行動使用偽裝成 GobizKOREA 登錄頁面的網頁。GobizKOREA 由韓國中小企業和新創局 (KOSME) 提供服務。網路釣魚電子郵件針對貿易行業的用戶。該電子郵件偽裝成買家向已註冊的賣家探詢新商機。透過點擊電子郵件中的超鏈接，用戶將被重新導引到一個偽裝成 GobizKOREA 登錄頁面的網頁。一旦用戶輸入帳號密碼並登錄，他們的帳號密碼就會洩露上傳到攻擊者 C&C 伺服器，這些帳號密碼隨後可能會被出售和濫用。

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。

2022/12/08

修補漏洞是物聯網的罩門～Zerobot殭屍網路透過未修補的漏洞攻擊各種物聯網裝置

Zerobot 是一種基於 Go 的殭屍網路最近透過利用各種物聯網 (IoT) 裝置中的 20 多個漏洞而傳播。Zerobot 支持多種不同的架構，包括 i386、amd64、arm、arm64、mips、mips64、mips64le、mipsle、ppc64、ppc64le、riscv64 和 s390x。該惡意軟體能夠透過 WebSocket 協議與 C&C 伺服主機通信。一旦建立 C&C 連接，Zerobot 將等待來自 C&C 伺服主機的命令。該惡意軟體具有針對各種通訊協定的攻擊能力，例如：TCP、UDP、TLS、HTTP、ICMP。

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.NPE
- WS.Malware.1
- WS.Malware.2

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: D-Link DNS-320 RCE CVE-2020-25506

- Attack: FLIR AX8 Thermal Camera Command Injection CVE-2022-37061
- Attack: Hikvision Command Injection CVE-2021-36260
- Attack: Telesquare SDT OS Command Injection CVE-2021-46422
- Attack: Zyxel Firewall Unauthenticated Command Injection CVE-2022-30525
- Web Attack: f5 Big-IP iControl Rest RCE CVE-2022-1388
- Web Attack: Huawei Router RCE CVE-2017-17215
- Web Attack: phpMyAdmin RFI CVE-2018-12613
- Web Attack: Realtek SDK RCE CVE-2014-8361
- Web Attack: Spring Framework CVE-2022-22965
- Web Attack: Spring Framework CVE-2022-22965 2
- Web Attack: Tenda Router RCE CVE-2020-10987

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。

2022/12/08

一箭雙鵰～Cova載入程式被用於傳播Nosu竊密程式和SystemBC代理機器

最近發現的惡意軟體散佈行動中使用 Cova 載入程式。威脅發動者使用載入程式傳播兩個不同的有效籌載，一個是名為 Nosu 的全新竊密程式，另一個是眾所周知的代理機器人 SystemBC。Nosu 惡意軟體具有從受感染端點竊取憑證、加密錢包、cookie 或資料檔案的功能。已證實在世界各地有多起攻擊行動，其中大部分感染發生在北美和南美。

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!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.SystemBC
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

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。

2022/12/07

專門鎖定Mikrotik路由器漏洞的WindiGo(又名 RanaumBot)殭屍惡意軟體

WindiGo (又名 RanaumBot) 是惡名昭彰的 Glupteba 殭屍網路相關的模組之一。該惡意軟體最近被濫用於利用 Winbox (MikroTik RouterOS 使用的專有協議) 的攻擊行動中。WindiGo 掃描網路以搜索打開 Winbox 埠號 8291 的 MikroTik 設備，然後嘗試利用已知的 MikroTik 漏洞 (CVE-2018-14847) 竊取憑證並進一步傳播。

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(Snoar)的防護：

- SONAR.Glupteba!gen2
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- W32.Fixflo.B!inf
- 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：

- Attack: Mikrotik Admin Password Leak CVE-2018-14847
- System Infected: Trojan.Backdoor Activity 634

基於安全強化政策(適用於使用DCS)：

- Symantec DCS 可以阻止可疑程序執行：預防策略可防止 Windigo 殭屍網路在系統上被植入或執行。
- Symantec DCS 強化能夠阻止與網際網路的出埠連接並限制進出伺服器所需的流量。

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。

2022/12/07

Remcos遠端存取木馬(RAT)和Agent Tesla透過基於KoiVM的載入程式傳播

遠端存取木馬 (RAT) 和 Agent Tesla 惡意軟體已在最近利用 KoiVM 虛擬化二進位檔案形式 .NET 載入程式的攻擊行動中傳播。據報導，初始下載程式透過惡意垃圾郵件傳播。一旦被下載並執行後，它會下載一個基於 KoiVM 的植入程式，該植入程式會導致 Remcos 或 Agent Tesla 的第 3 階段最終有效酬載。此惡意軟體散佈行動一直在利用 Pastebin 網站作為惡意程式的 C&C 伺服器。Agent Tesla 和 Remcos 都是威脅領域中穩居霸主地位的惡意軟體家族，並在過去幾年中的各種攻擊中無役不與。

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.SuspDataRun

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.2
- 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。

2022/12/07

偽造的加密貨幣交易網站傳播全新AppleJeus惡意軟體變種

Lazarus 進階持續威脅組織 (APT) 的一項新活動顯示，威脅攻擊者使用全新 AppleJeus 惡意軟體鎖定加密貨幣用戶。攻擊者利用一個以加密貨幣為主題的欺詐性網站，該網站模仿一個名為 BloxHolder 的合法交易平台。透過該網站，攻擊者正在散佈與 AppleJeus 惡意軟體捆綁在一起的加密貨幣交易手機應用程式 (APP) 的 Windows MSI 安裝程式。至少自 2018 年以來，AppleJeus 一直被 Lazarus 濫用於各種竊取加密貨幣的攻擊行動中。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen347
- ISB.Downloader!gen411
- ISB.Downloader!gen420
- Scr.Malcode!gen1
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- W97M.Downloader
- WS.Malware.1
- WS.SecurityRisk.4

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。

2022/12/06

雪上加霜～Cryptonite勒索軟體兼具資料刪除程式(Wiper)的功能

Cryptonite 是另一種基於 Python 的勒索軟體變種。這是第二個名稱完全相同的惡意軟體變種--另一個 Cryptonite 勒索軟體是基於較舊的 Chaos 勒索軟體。Cryptonite 加密檔案後會新增 .cryptn8 的附檔名。該惡意軟體可以刪除陰影複製 (shadow copies)，它包含多個用於逃避檢測的功能，例如：繞過 AMSI 機制或停用事件日誌記錄。據報導，該惡意軟體的一些最新樣本可能根本就不是加密檔案，而是完全無法復原的資料刪除程式。

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：

- Ransom.Cryptonite
- Trojan.Gen.2
- 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。

2022/12/06

Redigo--由Go語言(Golang)撰寫的後門程式，鎖定Redis資料庫伺服器

Redigo 是一種基於 Golang 的惡意軟體，透過利用 CVE-2022-0543 Redis 漏洞來攻擊 Redis 服務器。該惡意軟體能夠透過埠號 6379 模仿 Redis 伺服器的通訊，從而允許攻擊者隱藏受感染服務器與惡意 C2 服務器之間的流量。Redigo 將受感染的伺服器添加到殭屍網路中，隨後執行分佈式拒絕服務 (DDoS) 攻擊，並在伺服主機上執行加密貨幣挖礦。

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.Trojan
- Trojan Horse
- WS.Malware.2

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: Redis CVE-2022-0543

基於安全強化政策(適用於使用DCS)：

- Symantec Data Center Security 使用針對 Redis 伺服器的自定義沙箱進行強化，可抵禦 Redigo 類型的惡意軟體。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2022/12/06

躬逢其盛，駭客更喜歡世界盃足球賽(FIFA)～Remcos遠端存取木馬(RAT)利用世界盃足球賽(FIFA)如火如荼地激戰正酣！

由於 FIFA 世界杯正在如火如荼地激戰正酣，獲勝的球隊將在 16 強賽中展開較勁，駭客組織和個人繼續在這一場世界盛事中左右逢源。例如：賽門鐵克最近觀察到一個用土耳其語編寫的惡意垃圾郵件攻擊行動 (電子郵件主題：FIFA DÜNYA KUPASI KATAR 2022 SATIN ALIM SİPARİŞİ)，其中一名威脅者聲稱是卡達的 FIFA 官員。惡意電子郵件被發送到世界各地的組織，使用 FIFA 和普通的“採購訂單”社交工程策術。如果成功引誘受害者下載附加的 .IMG 檔案並執行其中的惡意可執行檔，它將安裝惡名昭彰的 Remcos 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：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspDataRun

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：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/05

Freya 比特幣剪貼簿竊密程式

另一個加密貨幣錢包剪貼簿竊密程式正在被多個駭客組織和個人大辣辣地使用。被稱為 "Freya" 的比特幣剪貼簿竊密程式，在今年初引發一連串的關注，當時它的開發者在各種駭客論壇、網站和社交媒體上引起了共鳴，這種威脅的主要針對消費者。攻擊者除了把受害者的加密貨幣錢包位址與惡意軟體威脅者擁有的位址進行對調與交換，其他什麼都沒做。

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
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/12/05

正在全世界流竄的Vohuk勒索軟體

最近有人觀察到另一種名為 Vohuk 的勒索軟體在全世界流竄。這種威脅具有普通勒索軟體功能，並且檔案被加密後附加 .Vohuk 副檔名。根據贖金說明，這些威脅者似乎採用可怕的雙重勒索策略來進一步迫使受害者支付贖金。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.PsDownloader!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Generic.1

2022/12/05

Qvoid Stealer竊密程式活動有所增加

寄生在公共站台上的惡意軟體原始程式碼被多個威脅發動利用也就不足為奇。賽門鐵克觀察到過去幾個月相關活動有所增加，Qvoid 竊密程式的活動當然也難逃過賽門鐵克的雷達。這種威脅類似於許多其他竊密程式，它們在 Discord 的能力方面受到吸引，使用 Discord 的 webhook 向運營商報告。它能夠收集 Discord 權杖和密碼、洩露的系統資訊、屏幕截圖、竊取 Web 瀏覽器資訊 (密碼和 cookie)、加密錢包的剪貼簿竊密程式。最近的攻擊行動是藉由瀏覽網頁時的偷渡式下載攻擊行動，在該行攻擊動中威脅者將 Qvoid Stealer 偽裝成破解程式和假冒軟體。

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：

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：

- SMG.Heur!gen

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 632
- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 656

基於機器學習的防禦技術：

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

2022/12/04

Lust(*慾望)竊密程式

Lust (*慾望) 竊密程式是最近剛出現在威脅領域的新面孔。這種威脅並不局限於某個群體，而是作為惡意軟體即服務來銷售。此時，威脅主要透過瀏覽網頁時的順道下載攻擊來進行散佈。在觀察到的攻擊行動中，大多數攻擊者都將他們的 Lust Stealer 二進位檔案偽裝成熱門遊戲、Discord 和抖音 (TikTok)。

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：

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/04

“School yard bully*校園霸凌”惡意APP，鎖定Facebook帳密

“School yard bully*校園霸凌”是一種 Android 惡意軟體，其主要目標是竊取 Facebook 憑證。這種威脅至少從 2017 年開始就很活躍，多年來已經觀察到多次攻攻擊行動。威脅發動者的攻擊手法並沒有真正改變太多，通常將他們的惡意軟體會偽裝成 Android 平台上的教育性 APP。這些已勁上架在 Google Play 和其他第三方應用商店和網站上看到。安裝成功後，惡意 APP 會提示受害者登錄他們的 Facebook 帳戶，並在此過程中竊取他們的帳密。

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

2022/12/04

RAXNET比特幣竊盜程式

當竊取加密貨幣錢包以及劫持加密貨幣交易時變得垂手可得，為什麼還要大費周章去挖礦呢？這就是許多網路犯罪分子所選擇的捷徑，地下黑市和公共資源中都不難搜尋到此類加密貨幣剪貼簿竊密器 (Clipper)。RAXNET 比特幣竊盜程式是最近觀察到的其中之一。這些威脅通常是透過瀏覽網頁時的順道下載攻擊而非其他常見的感染媒介 (例如：惡意電子郵件) 傳遞。

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

2022/12/02

與紐約證券交易所無關的～NYX勒索軟體

NYX 是一種用 C/C++ 程式語言撰寫的勒索軟體，部分源於被洩露的 Conti 勒索軟體原始程式碼。NYX 被認為是透過在網際網路上利用暴險的遠端桌面協議 (RDP) 漏洞進行散佈。此惡意軟體變種背後的攻擊者採用雙重勒索技術，在加密之前先竊取用戶的機密資料。NYX 勒索軟體會將 .nyx 副檔名附加到被加密檔案。

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：

- Ransom.Conti!gm1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2022/12/02

BlackBasta 2.0勒索軟體

BlackBasta 勒索軟體的全新 2.0 變種已在真實網路世界被發現。新版本包含對先前版本的多項改進，包括最新的加密演算法、透過 ADVObfuscator 進行的字串混淆以及為每個受害者客製化的被加密檔案的副檔名。最新 BlackBasta 變種的贖金說明以 instructions_read_me.txt 檔名的文字格式檔案的形式存放在受害者的電腦上。

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：

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.RansomGen!gen4
- SONAR.Ransomware!g19
- SONAR.Ransomware!g30
- SONAR.SuspLaunch!g18
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Basta
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/02

善於搭各種事件的順風車～Formbook利用政治有關事件來瞄準土耳其組織

Formbook 依舊非常流行，並每天都還在危害全球使用者。隨著賽門鐵克繼續觀察到其攻擊行動不管是針對組織還是個人，主要感染媒介仍偏愛惡意電子郵件。最近正在發動 Formbook 攻擊行動主要針對土耳其組織，但在美國、法國、泰國、塞爾維亞等其他國家／地區也發現這種情況。該惡意垃圾郵件攻擊行動背後的發動者聲稱自己是一家生產客製化產品的土耳其公司，善於搭各種事件的順風車，包括與政治有關的的事件。他們還利用與付款相關的社交工程，像是發送郵件主旨 (土耳其文) 為：Ödeme 的惡意電郵。

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：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/01

Misha(*米莎)竊密程式

最近有報導稱另一個名為 Misha (也稱為 Granda Misha) 竊密程式是一種能夠收集機敏資訊 (憑證、自動填充、歷史記錄等) 的威脅，這些資訊已暫時保存在 Chrome、Firefox 等主流及熱門網頁瀏覽器中像是 QQ、Vivaldi、Brave、Opera、Yandex、Chromium 和 Torch Web。它還能夠從 Outlook 竊取 IMAP、POP3、SMTP 和 HTTP 電子郵件協議的服務器、埠號、用戶和密碼詳細資訊。添加到列表中，它可以從以下通訊服務、FTP 程序和加密錢包收集資訊：

- Telegram
- Pidgin
- Swift
- Psi
- Gajim
- NppFTP
- WinSCP
- Psi++
- CoreFTP
- FileZilla
- Trillian

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!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Horse
- Infostealer

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/01

網路上買蝦子也要提高警覺～DarkStealer竊密程式假冒海鮮供應商？

DarkStealer並不是一個全新的竊密程式，雖然它不像惡名昭彰同源惡意程式家族那樣熱門，但我們確實持續有繼續到來自多個駭客組織和個人的偷渡式下載和惡意垃圾郵件活動。在最近的一次攻擊行動中，威脅者們聲稱自己是一家專門提供蝦類的哥倫比亞海鮮供應商。這種與出貨明細發票相關的惡意垃圾郵件攻擊行動已在全球範圍內被觀察到。DarkStealer 具有標準竊密程式和遠端存取木馬的功能，並使用 Telegram 發送日誌。

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：

- Scr.Malcode!gdn30

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/01

BlackMagic(*黑魔術)勒索軟體

一個名為 Black Magic 的伊朗駭客組織最近針對企業公司發動勒索軟體攻擊，並聲稱目標鎖定在以色列。成功加密後，受害電腦上會留下簡短的勒索說明，上面寫著“Black Magic 已經瞄準了你”以及加害者的 Telegram、YouTube、Twitter 和 Facebook 的聯繫方式。

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
- Trojan.Gen.MBT