保安資訊--本周(台灣時間2023/07/28)
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 68 萬 4,600 台受保護端點上總共阻止了 8,080 萬次攻擊。這些攻擊中有 93.1% 在感染階段前就被有效阻止：**(2023/07/24)**

- 在**13萬5,500**台端點上，阻止了**3,080**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**23萬**台端點上，阻止了**1,740**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬1,500**台**Windows**伺服主機上，阻止了**1,440**萬次攻擊。
- 在**9萬1,000**台端點上，阻止了**230**萬次嘗試掃描伺服器漏洞。
- 在**1萬5,200**台端點上，阻止了**82萬600**次嘗試掃描在**CMS**漏洞。
- 在**7萬600**台端點上，阻止了**140**萬次嘗試利用的應用程式漏洞。
- 在**23萬3,200**台端點上，阻止了**530**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬3,000**台端點上，阻止了**210**萬次加密貨幣挖礦攻擊。
- 在**14萬800**台端點上，阻止了**950**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,200**台端點上，阻止了**8萬6,600**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。

2023/07/28

賽門鐵克觀察到GuLoader惡意軟體的活動激增

上周，賽門鐵克發現 GuLoader 系列惡意軟體的活動激增。GuLoader 是一種基於 shellcode 的高級下載器，其目的是傳播各種惡意軟體，包括勒索軟體、竊密程式、銀行金融木馬、遠端存取木馬 (RAT) 和代理伺服器等。GuLoader 主要透過利用各種主題的垃圾郵件進行傳播。最終的有效載荷也可能不同，因為已知 GuLoader 會發送不同的惡意軟體，包括 Formbook、Agent Tesla、NanoCore 等。

在 GuLoader 攻擊鏈中所採用的 TTPs 依 MITRE 所分類的包括以下內容：

- Credentials from Password Stores: Windows Credential Manager [T1555.004]
- Credentials from Password Stores: Credentials from Web Browsers [T1555.003]
- Unsecured Credentials: Credentials In Files [T1552.001]
- Ingress Tool Transfer [T1105]
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547.001]
- Exfiltration Over C2 Channel [T1041]
- Browser Bookmark Discovery [T1217]
- Forge Web Credentials: Web Cookies [T1606.001]
- Hide Artifacts: NTFS File Attributes [T1564.004]
- Command and Scripting Interpreter [T1059]
- Command and Scripting Interpreter: PowerShell [T1059.001]
- Process Injection: Process Hollowing [T1055.012]
- Boot or Logon Autostart Execution: Winlogon Helper DLL [T1547.004]
- Boot or Logon Autostart Execution: Active Setup [T1547.014]
- Application Layer Protocol [T1071]

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：

- ACM.Wscr-Ps!g1
- ACM.Wscr-RgPst!g1
- SONAR.Powershell!g74
- SONAR.SuspBeh!gen82
- SONAR.SuspStart!gen2
- SONAR.SuspStart!gen6
- SONAR.TCP!gen1

端點偵測與回應(EDR)：

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序(Tactics、Techniques、Procedures，TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多訊息，請參閱此 GitHub 儲存庫：https://github.com/Symantec/threathunters/tree/main/Trojan/GuLoader

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.NSISPacker!g14
- 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.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 758

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。

2023/07/28

新一波IcedID惡意軟體，透過惡意垃圾郵件傳播

IcedID 又名 Bokbot，是 2017 年前後首次發現的惡意軟體。從歷史上來看，IcedID 最初的主要功能僅只是銀行金融木馬，但隨著時間的推移，它的重點轉移到成為各種有效載荷（包括勒索軟體）後續感染的載入程式。就在本周，我們在真實網路情境偵測到傳播 IcedID 的新型惡意垃圾郵件。感染鏈中的郵件包含偽裝成出貨明細／發票通知的 .PDF 附件，檔案名為『INV-Details-JUL23.pdf』或『Scan_Doc_07-26.pdf』。這些 PDF 檔案包含一個鏈接，將受害者重定向到下載一個壓縮的、有密碼保護的壓縮套件包。解壓縮並運行其中的可執行檔後，IcedID 有效載荷就會被發送給受害者。

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.IcedID!g4

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.IcedID!gen3
- Scr.Malcode!gdn28
- Scr.Malpdf!gen2
- Trojan.Gen.MBT
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

- 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。

2023/07/27

RisePro竊密程式沒有式微的跡象

RisePro 竊密程式在 2022 年底，首次被發現，目前仍有活動的跡象，主要透過私人載入器以惡意合法軟體的破解程式的形式傳播。2023 年 7 月，觀察到更多的命令和控制伺服器 (C&C) 的跡象。這並不是一個複雜的惡意軟體，就其功能而言，是一個相當普通的竊密程式，其目的是利用瀏覽器外掛程式等功能從網路瀏覽器、信用卡和加密貨幣錢包中擷取檔案和竊取敏感性資料。雖然消費者和小型企業似乎是其主要的目標，但中大型企業組織仍然面臨著來自可能採用其他感染媒介的駭客組織和個體戶的風險。

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.A!300
- Heur.AdvML.B!200
- Heur.AdvML.B!100

2023/07/27

冒充澳洲郵政的網路釣魚活動呈上升趨勢

針對澳大利亞消費者和企業用戶的網路釣魚攻擊並不新鮮，事實上經常發生。今年 7 月，賽門鐵克偵測到許多新註冊的近似澳洲郵政的網域名稱，被用於網域誤植詐騙攻擊。這些近似網域名稱被發現涉入了惡意簡訊攻擊行動。以下是一些被發現的傳播惡意簡訊的例子。

- 投遞不成功。請在 hxxps://post[.]service-center[.]cc 更新您的包裹資訊，以便成功投遞。我們珍視您的合作。
- 投遞失敗後，請在 hxxps://post[.]case-center[.]cc 更新您的包裹資訊 [.] 感謝您的迅速行動和理解。
- 由於投遞失敗，請在 hxxps://post[.]admess[.]cc 更新您的包裹資訊。請確保您的詳細資訊準確無誤，以便成功投遞。
- 我們很遺憾地通知您投遞嘗試不成功。要繼續投遞，請在 hxxpps://post[.]case-center[.]cc 更新您的包裹資訊。
- 由於投遞失敗，我們懇請您在 hxxps://post[.]pack-handle[.]cc 更新您的包裹資訊，以便成功派送。

在利用電子郵件和簡訊所發動的網路釣魚攻擊行動中，郵政服務經常被用作社交工程的誘餌，因為它們是人們熟悉和信任的機構。與郵政服務有關的資訊會給人一種緊迫感或擔憂感，使收件人更有可能在未核實資訊合法性的情況下迅速採取行動。透過冒充郵政服務，攻擊者可以以包裹跟蹤或投遞問題為幌子要求提供個人資訊，這往往會導致身份盜竊和金錢損失。

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：

Symantec Endpoint Protection Mobile (賽門鐵克端點安全手機/行動版) 能夠分析簡訊中內嵌的鏈接。它根據賽門鐵克全球情資網路 (GIN) 中的威脅情報偵測簡訊中內嵌的網址 (URL)，並在鏈接有疑慮時向使用者發出警告，從而保護使用者免受簡訊類型的網路釣魚的攻擊。GIN 中的 WebPulse 網頁安全情資生態系統，已於第一時間完整收納此次行動中被濫用的近似澳洲郵政的網域名稱。

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。

2023/07/27

Nitrogen(*氮氣)，透過惡意廣告嘗試駭入系統的入侵初期(Initial Access)所採用的惡意軟體

Nitrogen 被歸類為攻擊鏈中嘗試駭入系統的入侵初期（Initial Access) 所採用的惡意軟體的家族。它透過惡意廣告感染，濫用搜尋引擎上的付費廣告(搜尋引擎下毒)，偽裝成熱門軟體的合法來源。受害者會從偽裝成合法網站的 ISO 檔中下載一個安裝程式，該程式會安裝受害者正在尋找的合法軟體，以避免一開始就露餡，同時還會安裝一個 Python 運行環境和一個惡意 Python 套裝軟體。利用安裝的 Python 模組，下一步將確保受害者的電腦能夠連接到 C&C 伺服器，讓歹徒

知道新的電腦已被感染，並安裝 Meterpreter 和／或Cobalt Strike 等滲透測試工具。到了這個階段，歹徒就可以自己操弄這些電腦或將入侵的權限出售給其他駭客組織。

保安網路知識註解：Metasploit 是開放社群與 Rapid7 之間的開源專案，提供許多滲透測試的工具，和漏洞資訊與漏洞酬載(payload)。

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：

- Meterpreter
- Trojan Horse
- Trojan.Emotet
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B
- 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。

2023/07/26

Casbaneiro(*卡斯巴內羅)銀行金融木馬持續推陳出新

Casbaneiro，又名 Metamorfo 或 Ponteiro，是 2018 年出現的一種惡名昭彰的銀行金融木馬。因專門攻擊銀行金融行業，尤其是拉丁美洲的銀行而聲名大噪。由於該惡意軟體主要作為銀行金融木馬運行，其目的是竊取受害者的敏感金融資訊和憑證 (帳密)，使網路犯罪分子能夠進行欺詐交易並在未經授權的情況下存取銀行帳戶。

在最近觀察到的行動中，惡意攻擊利用帶有 html 檔連結的釣魚電子郵件，如果點擊該鏈接，就會下載惡意 RAR 壓縮檔，進而啟動多階段感染程序。Casbaneiro 銀行惡意軟體家族背後的歹徒出於經濟動機使用了使用者帳戶控制 (User Account Control，UAC) 繞過技術，這說明他們在發動惡意攻擊行動方面不斷進化並日益刁鑽。

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

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.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。

2023/07/26

Realst竊密程式假冒區塊鏈遊戲傳播

被稱為 Realst 的惡意軟體是採用 rust 程式語言所撰寫的，它的出現為網路威脅領域投下了震撼彈，尤其是對 Windows 和 macOS 系統使用者而言。Realst 背後的攻擊者採用假冒的區塊鏈遊戲，例如：《Brawl Earth》、《Dawnland》、《Destruction》、《Evolion》、《WildWorld》等作為幌子，誘使毫無戒心的用戶下載並安裝該惡意軟體。這些遊戲可能會承諾令人興奮的獎勵或其他激勵措施，以吸引用戶參與其中。在 Realst 惡意軟體中觀察到的一致行為模式表明，該惡意軟體有意專注於竊取與瀏覽器、加密貨幣錢包和蘋果鑰匙圈 (keychain) 資料庫相關的有價值資訊。鑒於它最近對 macOS 14 Sonoma 的關注，似乎正在積極發展，以最新的作業系統版本為目標。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Heuristic!gen21
- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- Trojan Horse
- Trojan.Gen.MBT
- Web.Reputation.1

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。

2023/07/26

Decoy Dog(*誘餌狗)惡意軟體工具包在真實網路情境仍存在威脅

Decoy Dog 是今年初所發現的惡意軟體工具包，被歹徒用於逃避安全軟體的偵測。該惡意軟體利用網域名稱系統 (DNS) 與指揮與控制 (C&C) 伺服器進行通訊。Decoy Dog 源於 Pupy RAT，Pupy RAT 是一種源於開放原始碼的遠端存取木馬，允許攻擊者遠端控制、執行命令和竊取憑證等。Decoy Dog 惡意軟體的最新變種也針對常見的通信協定、新的 DGA (動態網域產生演算法) 等進行各種改進。

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.Mirai
- 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。

2023/07/25

保護亮點：SEP Mobile(賽門鐵克端點安全手機／行動版)利用WebPulse網頁安全情資生態系統攔截簡訊釣魚攻擊

簡訊釣魚也稱為簡訊網路釣魚，歹徒利用簡訊來欺騙智慧型手機用戶，誘騙他們洩露敏感資訊、點擊惡意鏈接或下載有害附件。

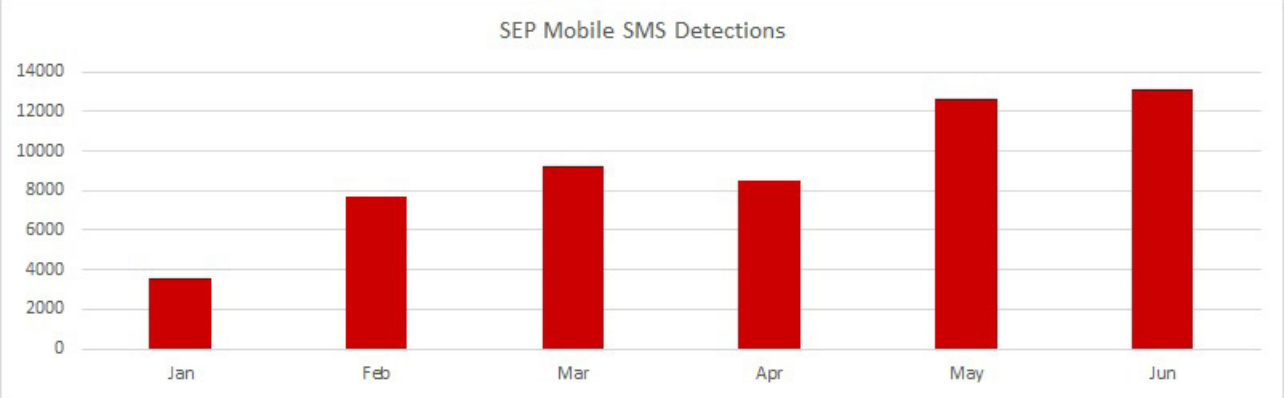
過去幾年，詐騙活動一直在穩步增加，這主要是由於消費者和企業用戶廣泛採用智慧型手機和其他行動裝置。其他種種因素也在其增長中發揮了至關重要的作用：

- **智慧型手機的連網天性**：許多應用程式和服務要求用戶提供手機號碼以進行認證或身份驗證。網頁服務和智慧型手機之間的這種互連性為攻擊者提供了一種獲取用戶電話號碼和精心製作個性化簡訊的額外手段。
- **發動電子郵件網路釣魚越來越困難**：電子郵件服務提供商和安全解決方案在檢測和阻止電子郵件網路釣魚方面變得更加出色。因此，一些攻擊者將注意力轉向簡訊，將其視為一種相對尚未開發的網路釣魚攻擊途徑。
- **缺乏安全認知意識**：許多人對簡訊不像對待電子郵件那樣謹慎，使他們更容易遭受詐騙。
- **短網址**：攻擊者經常利用簡訊發送短網址的惡意鏈接，使收件人更難在手機上辨識其真實的最終網址。
- **跟踪和歸因方面的困難**：與可以追踪標頭和發件人資訊的電子郵件類型的網路釣魚不同，簡訊類型的攻擊很難追溯到其源頭，為攻擊者提供了一定程度的匿名性。

雖然簡訊類型的網路釣魚最初針對的是消費者，但由於獲取企業資訊與情報的潛在回報，企業用戶越來越成為歹徒覬覦的主要目標。企業用戶通常可以存取敏感且有價值的企業資料，

包括知識產權、財務資訊、客戶資料庫和專有技術。

過去幾個月，簡訊攻擊呈上升趨勢。Symantec Endpoint Protection Mobile 已攔截發送給全球企業行動用戶（包括 Android 和 iOS）的 50,000 多則惡意簡訊。



Symantec Endpoint Protection Mobile (賽門鐵克端點安全手機/行動版)能夠分析簡訊中內嵌的鏈接。它根據賽門鐵克全球情資網路（GIN）中的威脅情報偵測簡訊中內嵌的網址(URL)，並在鏈接有疑慮時向使用者發出警告，從而保護使用者免受簡訊類型的網路釣魚的攻擊。

賽門鐵克的端點安全企業版 (SESE)／端點安全完整版(SESC)內含防護 IOS／Android 的最先進防護技術，請點擊此處瀏覽更完整的資訊。

要了解有關賽門鐵克利用WebPulse 網頁安全情資生態系統的更多資訊，請點擊此處。

要了解有關賽門鐵克全球情資網路 (GIN) 的更多資訊，請單擊此處#1，請單擊此處#2。

2023/07/25

LaplasClipper剪貼簿竊密程式推出基於.NET的新變種

LaplasClipper 惡意程式被歸類為剪貼簿竊密程式，最初於 2022 年被發現。顧名思義，Laplas 就是一種剪貼簿竊密程式的惡意軟體，可監視遭駭入電腦上的剪貼簿以擷取加密貨幣錢包的位址。一旦發現，惡意軟體就會將受害者的加密貨幣錢包位址與攻擊者擁有的位址交換。雖然之前觀察到的 LaplasClipper 是用 GO 或 C++ 撰寫，但最近在真實網路情境觀察到的樣本已有採用基於 .NET 編譯並使用 Babel 混淆程式進行混淆。

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.Heur.Dropper
- SONAR.Heuristic.170

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- 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: Laplas Clipper Malware Activity

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。

2023/07/24

Reptile～Linux平台上的Rootkit惡意軟體

Reptile 是一種針對 Linux 系統的源於開放原始碼的 Rootkit 惡意軟體，在真實網路情境經常出現新的變種。該惡意軟體主要用於隱藏惡意目錄／檔案、程序以及與歹徒所操控 C&C 伺服器的通訊。Reptile 還包含一個例行從目標主機對攻擊者主機發起連線的 Reverse shell (源於 TinyShell)，其可允許攻擊者遠端控制受感染的系統。

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

2023/07/21

Kanti--採用Nim程式語言所撰寫的全新勒索軟體

Kanti 是在真實網路情境所發現的另一種標準型勒索軟體。該惡意軟體是採用 NIM 程式語言所撰寫的。它會加密用戶檔案並隨後附加 .kanti 副檔名。該勒索軟體具有避開特定檔案及資料夾以加速加密重要檔案的速度。加密完成後，機器上會出現勒索贖金支付說明，建議受害者透過電子郵件與歹徒聯繫。

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!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

基於機器學習的防禦技術：

- Heur.AdvML.C