保安資訊--本周(台灣時間2023/12/15)
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 7,700 台受保護端點上總共阻止了 6,230 萬次攻擊。這些攻擊中有 78.9% 在感染階段前就被有效阻止：**(2023/12/11)**

- 在**10萬4,800**台端點上，阻止了**1,910**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**15萬9,500**台端點上，阻止了**1,450**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬2,000**台**Windows**伺服主機上，阻止了**1,170**萬次攻擊。
- 在**6萬1,200**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,700**台端點上，阻止了**70萬9,800**次嘗試掃描在**CMS**漏洞。
- 在**4萬3,700**台端點上，阻止了**120**萬次嘗試利用的應用程式漏洞。
- 在**22萬6,800**台端點上，阻止了**420**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,700**台端點上，阻止了**390**萬次加密貨幣挖礦攻擊。
- 在**11萬9,800**台端點上，阻止了**930**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**744**台端點上，阻止了**23萬500**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。

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 1.421 萬個受保護端點上阻止了總計 630 萬次攻擊。**(2023/12/11)**

- 使用網頁信譽情資，在 **1.261** 萬個端點上阻止 **550** 萬次攻擊。
- 攔截 **30.4K** 個端點上 **596.3K** 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 **12.4K** 個端點上攔截 **158.5K** 次瀏覽器通知詐騙攻擊。
- 在 **567** 個端點上攔截 **44.4K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。
- 在 **1.2K** 個端點上阻止 **1.9K** 次技術支援詐騙攻擊。
- 在 **210** 個端點上阻止 **584** 次加密劫持嘗試。

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。

2023/12/14

機器學習平臺MLflow的CVE-2023-3765漏洞正被大肆開採濫用

CVE-2023-3765 是一個影響 MLflow 平臺的嚴重等級 (CVSS 評分 10.0) 路徑遍歷漏洞。成功開採濫用該漏洞可在系統上列出、下載、寫入和刪除檔案。我們注意到有報告顯示，該漏洞在真實網路情境正被大肆開採濫用。賽門鐵克的網路防護技術：入侵預防系統 (IPS) 會阻止這些漏洞利用嘗試，以防止對系統造成進一步感染／入侵。

SEP 的 IPS 入侵預防技術在這兩三年來有持續強化及整合新的防護技術，特別是無檔案型態攻擊以及瀏覽器相依的威脅防護。

IPS 的相關技術細節請參考簡報檔：讓網路威脅未攻先破--賽門鐵克的IPS入侵預防技術。

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：

- Attack: MLflow Path Traversal Vulnerability CVE-2023-3765

2023/12/14

GraphicalProton後門涉入TeamCity的CVE-2023-42793漏洞開採濫用攻擊

俄羅斯駭客組織 APT29(又稱 CozyDuke 或 NOBELIUM) 最近所涉及一連串的惡意活動中，TeamCity 的 CVE-2023-42793 嚴重等級漏洞被開採濫用於初始攻擊。該駭客組織透過劫持 Zabbix 和 Webroot 防毒軟體的 DLL 以及名為 vcperf 的開源應用程式，來植入 GraphicalProton 後門程式。GraphicalProton 的破壞力著重在內部偵察和資料竊取外洩。該後門程式可以收集系統和網路資訊，以及受感染端點上運行程序的相關資料等。為了避免被發現，該惡意軟體利用 OneDrive 和 Dropbox 等雲端服務作為 C&C 通訊管道。

以下為保安補充--網路上的知識：

TeamCity 是一套由 JetBrains 開發的持續整合與持續交付 (CI/CD) 系統，能協助開發人員依據專案特性，從開發、編譯、整合、測試到發佈軟體等流程，建立一套專屬的 DevOps。TeamCity 整合多家套件，例如：版本控管、測試框架、通知、視覺化圖表、問題追蹤、雲端支援……等，協助開發人員順行進行各種整合工作，功能相當強大。

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.Ps-RgPst!g1
- ACM.Ps-Rd32!g1
- ACM.Untrst-RgPst!g1
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.9
- 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!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: TeamCity Authentication Bypass CVE-2023-42793

基於安全強化政策(適用於使用DCS)：

賽門鐵克的 DCS(Data Center Security) 重要主機防護系統：其預設就啟用 sym_win_hardened_sbp 安全強化政策，就能保護底層Windows 作業系統免受此漏洞遭開採利用，包括防止執行任意 cmd shell (例如：某些公開漏洞利用示例所示)。政策集的網路規則可設定只讓特定版本的 TeamCity 應用程式信任限定的的用戶端。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。

2023/12/14

中國駭客組織Mustang Panda，開發新的惡意軟體企圖攻擊台灣政府及外交人員

中國駭客組織 Mustang Panda(*野馬熊貓) 的頑強侵略政策，總是造成世界各地政府和非政府組織的困擾與災難。該駭客組織最近被發現涉及一個新的 PlugX 惡意軟體的攻擊行動，目標是臺灣政府和外交人員。利用 PDF 檔案為誘餌來啟動初始攻擊，後繼是一個合法的可執行檔被用來部署一個用 Nim 程式設計語言編寫的惡意 DLL，最終包含 PlugX 的 DAT 檔隨後會被解密並載入到記憶體中。

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：

- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.2

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：

- 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。

2023/12/13
Editbot(*編輯機器人)惡意竊密程式

Editbot 是最近發現一種採用 Python 撰寫的惡意竊密程式，它以社交媒體使用者為目標，透過多階段傳播。感染鏈包括散播包含惡意 .bat 批次檔和 PowerShell 腳本的 .rar 壓縮檔，這些檔案和腳本反過來又會導致最終有效籌載的交付和執行。Editbots 的功能包括竊取機密資料，例如：系統資訊、憑證、網路資料、與各種社交媒體平臺相關的瀏覽器 cookie，以及將用戶檔案和文件檔直接外洩到攻擊者操控的 Telegram 頻道。

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.MBT
- WS.Malware.1

2023/12/13
MrAnon惡意竊密程式

MrAnon 是一種全新惡意竊密程式，最近在一次網路釣魚攻擊行動中被發現，該惡意軟體偽裝成酒店預訂查詢系統，來散播惡意的 PDF 檔案。最終有效籌載透過 .NET 可執行檔和惡意 PowerShell 腳本傳輸。MrAnon 目標是從遭入侵的電腦中竊取各種使用者資料，包括：使用者憑據／帳密、瀏覽器中存儲的資料、加密貨幣擴充和桌面錢包中的資料、VPN 應用程式資料、各種通訊應用程式中的資訊、機器上存儲的檔案等。被擷取的資料會被壓縮並上傳到攻擊者有權限存取的雲端硬碟上。

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(SONAR)的防護：

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

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：

- Backdoor.Trojan
- Infostealer.Limitail
- Trojan Horse
- Trojan.Pidief
- Web.Reputation.1
- 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：

- System Infected: Trojan.Backdoor Activity 641
- 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。

2023/12/13

BuLock勒索軟體

BuLock 是最近在真實網路情境所監控到 MedusaLocker 勒索軟體的後繼新變種。該惡意軟體會加密使用者檔案，並冠上 .bulock(*number) 的副檔名。勒索 (贖金支付) 說明以名為『HOW_TO_BACK_FILES.html』的 html 格式檔案來呈現，並要求受害者透過指示的電子郵寄地址來聯繫攻擊者。BuLock 還可以刪除受感染電腦上的磁卷陰影複製 (volume shadow copies)。該勒索軟體背後的威脅者還威脅受害者，如果不乖乖就範付贖金，就會將已竊得的資料公開。。

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
- 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

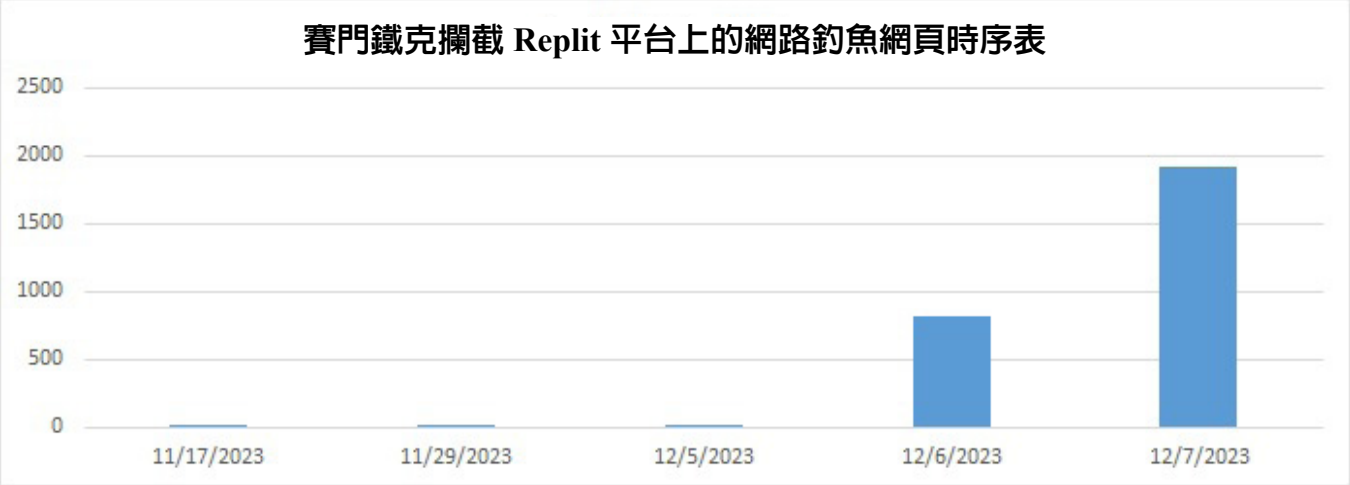
2023/12/12

防護亮點：濫用Replit線上平臺的釣魚攻擊行動在南韓興風作浪

Replit 是一款具有多人協作和開發者社群功能的線上平臺，能為各種程式設計語言提供整合式開發環境 (IDE)。它還提供一項名為『Repl.it』線上開發環境並提供內建資料庫，允許用戶直接從 Replit 帳戶建立靜態網站。用戶可以設計 HTML、CSS 和 JavaScript 等型態的網頁來建立自己的網站，然後只需點擊幾下即可進行部署。

賽門鐵克持續偵測到有人濫用 Replit 並在該平臺上上架其網路釣魚網頁。這與人們濫用 Cloudflare R2 物件儲存服務代管和星際檔案系統 (IPFS) 的方式相似，儘管不那麼普遍，但仍然很危險。

在過去幾周裡，我們破獲一個在南韓發動多起上架在 Replit 平台上的網路釣魚行動的始作俑者，他的目標是南韓本地和國際公司，初期似乎只是小規模測試，然後在 12 月 6 日開始擴大攻擊量能。



如果使用者成功中惡意電子郵件的圈套，並碰巧點擊提供的網頁 (例如：hxxps[:]//view-file--kisiy37297[.]repl[.]co/#[收件人電子郵寄地址])，他們最終會進入一個上架在 Replit 平台上的網路釣魚頁面，該頁面實際上是一個假冒的 MailPlug(韓國流行的網路電子郵件服務) 登錄頁面。

觀察到的電子郵件主旨：

- [KOTRA인천지원단] 사업제안
- [주식회사 켄드리드마트]로부터 [주문서]가 도착했습니다.
- (주)썬패치테크노에서 주문서를 보냈습니다.

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 多重防護技術能在第一時間就偵測到該惡意程式及有效對應**零時差**攻擊的防護機制及其威脅名稱：

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。

欲深入瞭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。
欲深入瞭解有關賽門鐵克基於雲的網絡安全服務 (WebPulse) 的更多訊息，請點擊此處。

2023/12/12

Blacksmith(*鐵匠)網路攻擊行動

北韓駭客組織 Lazarus 是最近『鐵匠網路攻擊行動』(Operation Blacksmith) 的幕後黑手，他們濫用兩年前就已揭露的 Log4Shell 重大漏洞 (CVE-2021-44228)，攻擊 VMware 桌面虛擬化平臺入侵受害組織。在這次網路攻擊行動中，使用 Dlang 程式語言撰寫的三個新惡意軟體家族系列--木馬程式：NineRAT、DLRAT 和惡意程式下載工具：BottomLoader 可以被用來部署有效籌載，而 NineRAT 和 DLRAT 則會執行從攻擊者的 C&C 伺服器接受各種命令。

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：

基於行為偵測技術(SONAR)的防護：

- ACM.Ps-Http!g2
- ACM.Ps-Sc!g1
- ACM.Untrst-RLsass!g1
- ACM.Untrst-RunSys!g1
- SONAR.MalTraffic!gen1
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- PUA.Gen.2
- 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.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：

- Audit: Log4j2 RCE CVE-2021-44228
- Attack: Log4j2 RCE CVE-2021-44228 2
- Attack: Log4j2 RCE CVE-2021-44228 3
- Attack: Log4j2 RCE CVE-2021-44228 4
- Attack: Log4j2 RCE CVE-2021-44228 5
- Attack: Log4j2 RCE CVE-2021-44228 7

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。

2023/12/08
在真實網路情境發現有全新的Phobos勒索軟體後繼版本的蹤跡

Phobos 是一個在威脅領域赫赫有名的勒索軟體家族，至少從 2019 年起就開始活躍。這種惡意軟體的後繼新變種每月都曾在真實網路情境不斷出現。就在上周，我們觀察到其三個新變種，分別被稱為 Elpy、Elbie 和 GrafGrafel。它們會加密使用者檔案，並在加密檔中附加一串資料，其中包括一個唯一的 ID 號、威脅行動者的聯繫電子郵寄地址以及冠上 .Elpy、.Elbie 或 .GrafGrafel 副檔名。勒索 (贖金支付) 說明通常以文字檔的形式留下，其中包含如何解密檔案的說明。Phobos 勒索軟體具有刪除卷影副本、停用 Windows 防火牆以及終止特定系統程序的功能。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspDataRun

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Phobos
- Ransom.Phobos!g2
- Ransom.Phobos!gm1
- WS.SecurityRisk.4

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: Ransom.Crysis Activity 3

2023/12/08
Csharp-streamer遠端存取木馬(RAT)

2021 年，Revil 駭客組織在其所發動的勒索軟體攻擊行動中導入 Csharp-streamer 遠端存取木馬 (RAT)。今年觀察到的該惡意軟體新案例展示資料竊取、鍵盤記錄、憑證竊取、網路搜尋和有效籌載部署等功能。該惡意軟體可以使用網際網路控制訊息通訊協定 (ICMP：Internet Control Message Protocol) 與攻擊者的命令和控制 (C&C) 伺服器建立連接。

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
- Trojan.Gen.MBT

- 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.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。

2023/12/08

變本加厲的駭客組織RansomHouse

RansomHouse 是一個至少從 2021 年起就活躍在勒索軟體領域的駭客組織。據瞭解，該組織利用 WhiteRabbit 或 MarioLocker 等 Babuk 勒索軟體後繼變種針對 Linux 實例和 VMware ESXi 虛擬機器發動加密勒索攻擊行動。這種威脅行動者通常濫用網路釣魚行動或已知的漏洞利用發動初始感染攻擊。根據最新報告，RansomHouse 在 2023 年依然活躍。威脅行動者還採用雙重勒索策略，將已竊得使用者資料脅迫受害者就範，否則將其發佈到公共洩密網站上。

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(SONAR)的防護：

- SONAR.ProcHijack!g45
- SONAR.SuspLaunch!g12
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Ransom.Babuk
- Ransom.Gen
- Trojan Horse
- Trojan.Gen.2
- 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

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。