保安資訊--今日最新(台灣時間2023/06/02)
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 77 萬 3,400 台受保護端點上總共阻止了 9,430 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/05/29)**

- 在**16**萬**3,900**台端點上，阻止了**4,180**萬次嘗試掃描**Web**服務器的漏洞。
- 在**26**萬**8,400**台端點上，阻止了**1,940**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5**萬**4,200**台**Windows**伺服主機上，阻止了**1,390**萬次攻擊。
- 在**9**萬**2,900**台端點上，阻止了**250**萬次嘗試掃描伺服器漏洞。
- 在**1**萬**5,800**台端點上，阻止了**95**萬**2,200**次嘗試掃描在**CMS**漏洞。
- 在**7**萬**600**台端點上，阻止了**200**萬次嘗試利用的應用程式漏洞。
- 在**27**萬**1,100**台端點上，阻止了**600**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1**萬**2,700**台端點上，阻止了**210**萬次加密貨幣挖礦攻擊。
- 在**15**萬**8,300**台端點上，阻止了**1,030**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,300**台端點上，阻止了**14**萬**8,900**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。

點擊此處獲取--關於賽門鐵克原廠防護週報

2023/05/31
會講中文的勒索軟體駭客要求被害者利用TRC20區塊鏈錢包支付贖金

一名會講中文的勒索軟體駭客被發現到處犯案。如果勒索軟體在受害者的電腦上成功執行，它會在檔案被加密時留下多條勒索支付說明（檔名：请阅读解锁.txt）。目前，留下的勒索支付說明也是中文的，要求受害者向 TRC20 錢包支付 8,000 美元。根據他們的勒索支付說明，這個勒索軟體駭客似乎沒有採用雙重勒索策略。

TRC20 為基於波場 (TRON) 的區塊鏈錢包，在中國廣受歡迎。自 2017 年推出以來，TRON 在中國吸引大量追隨者，並因其備受矚目的合作夥伴關係和營銷努力而備受關注。與以太坊區塊鏈上的 ERC20 代幣類似，TRC20 智能合約代幣 (Token) 是互相取代，可以代表任何可交易的數位資產，例如：加密貨幣、應用型代幣 (Utility Token)，甚至是房地產或商品等代幣化資產。TRC20 標準定義一套規則和功能，可以在 TRON 區塊鏈平台上建立、傳輸和管理代幣。

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.SuspDrop!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：
- Ransom.HiddenTear!g1

基於機器學習的防禦技術：
- Heur.AdvML.B

2023/05/31
RomCom惡意後門程式由Void Rabisu進階持續威脅(APT)駭客組織大肆散播

最近，RomCom 惡意後門程式被稱為 Void Rabisu（又名 Tropical Scorpius）的駭客組織所發起攻擊行動中被大量散播。去年 8 月，同一個駭客組織也鎖定古巴發動勒索軟體的散播行動。RomCom 遠端存取木馬 (RAT) 的精密攻擊鏈涵蓋網路釣魚郵件、社交工程和上架在雲端或第三方網站上，偽造成熱門合法軟體的 .msi 安裝程式檔之惡意檔案，例如：ChatGPT、WinDirStat、AstraChat、GIMP、Veeam Backup 等知名應用程式。攻擊者還濫用 Google Ads 平台來推廣他們的虛假網站。RomCom 具有在受感染裝置上運行攻擊者命令、竊取資料、下載和執行其他惡意有效籌載等功能。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：
- Trojan Horse
- Trojan.Gen.MBT
- WS.Reputation.1
- WS.Malware.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。

2023/05/31
PixBankBot手機銀行金融木馬

PixBankBot 是另一種針對巴西銀行用戶的手機銀行金融木馬，具有濫用巴西央行支付系統Pix平台的能力。該惡意軟體利用自動轉帳系統（Automatic Transfer System，ATS） 框架，允許攻擊者執行自動欺詐操作執行，而無需操作員端的手動或遠端互動。一旦駭入遭入侵的裝置，PixBankBot 將提示受害者啟用輔助功能服務，一旦登入該服務，就可以實現 ATS 功能以及額外的鍵盤記錄功能。

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：

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.Malapp
- Android.Reputation.2

2023/05/30
DogeRAT安卓手機惡意軟體

DogeRAT 是一種安卓 (Android) 平台上的手機惡意軟體，因造成不少包含銀行和娛樂等不同規模的企業組織的損害而闖出名號。該惡意軟體偽裝成合法和知名品牌（例如：YouTube、Netflix、ChatGPT...等）APP 進行傳播。一旦被執行，DogeRAT 就會嘗試竊取敏感的用戶資訊，包括剪貼簿資料、聯絡人、郵件、憑證和銀行資料。借由此遠端木馬，攻擊者還可能操控遭駭入的裝置並執行其他惡意動作。

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

2023/05/30
Invicta竊密程式透過社群媒體管道大肆氾濫

全新的 Invicta 竊密程式其開發者透過 Telegram 和 YouTube 等各種社交媒體平台大肆氾濫。Invicta 能夠收集系統資訊，竊取瀏覽器資料、cookie、銀行詳細資料、加密貨幣錢包和來自 Discord、Steam 或 KeyPass 等應用程式的其他資料。Invicta 竊密程式已被發現利用偽裝來自 GoDaddy（知名網路代管公司）的退款發票惡意垃圾郵件來散播。這些電子郵件也包含會誘導後續感染的惡意 .html 網頁檔案。

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：

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：
- MSH.Downloader
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Malscript
- WS.Malware.1

基於機器學習的防禦技術：
- Heur.AdvML.B

2023/05/29
BLX惡意竊取程式

GitHub 上每天都會有新的竊密程式出現，其中許多是以前 Discord 竊密程式的分支。雖然這些並不太複雜，而且許多並沒有很流行，但賽門鐵克會密切監視它們，因為它們最終會在一定程度上被世界各地的某些團體和個人使用。BLX 是最近常見的竊密程式之一，根據我們的觀察，攻擊者和研究人員正在對其進行測試。這種威脅包括 Discord 登錄、加密錢包、網路瀏覽器歷史記錄和密碼，以及許多其他常見的竊密功能。

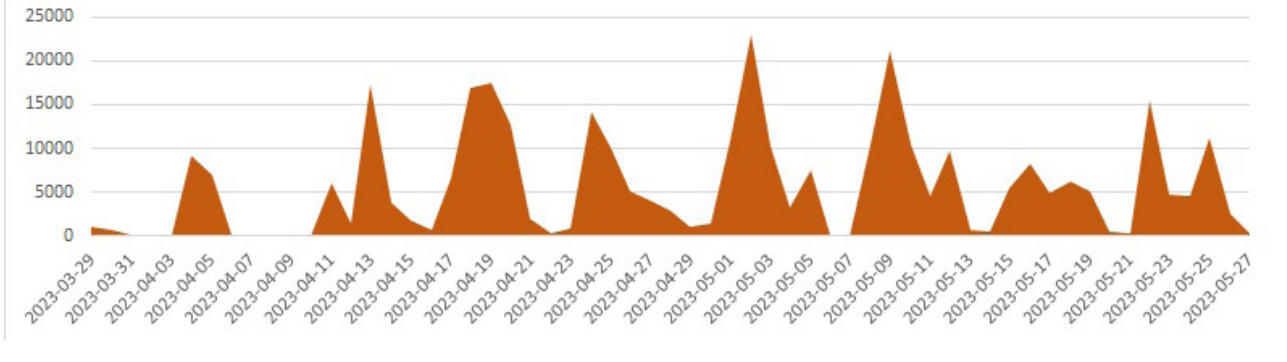
賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：
- Trojan.Gen.2
- Trojan.Gen.MBT

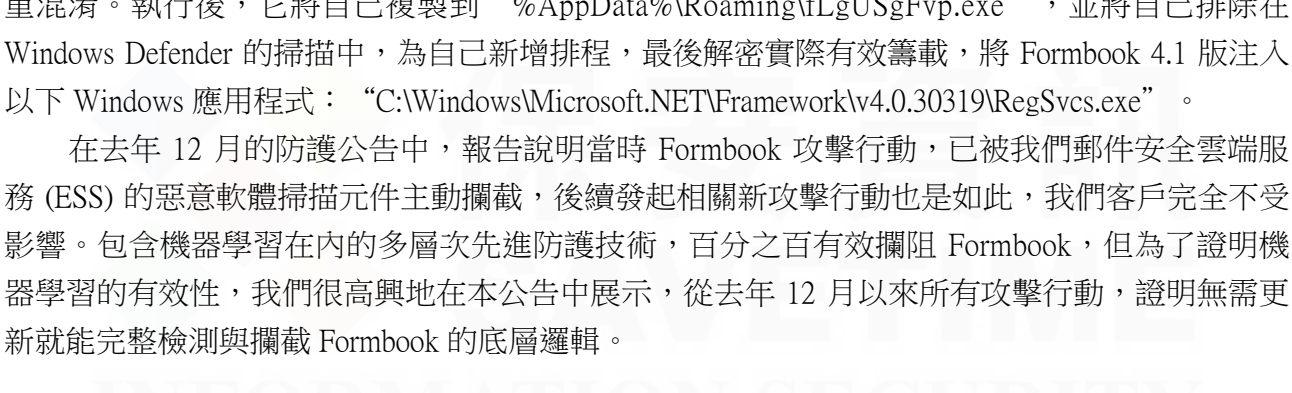
2023/05/29
防護亮點：Formbook 被機器學習了

～防護亮點～

更精準地來談，我們自動化機器學習能力能隨時與時俱進有效遏止 Formbook。我們在 2022 年 12 月 8 日的公告中詳細討論 Formbook，而現在正是重新來討論並更新資訊的好時機。簡要回顧一下，自 2016 年左右以來，Formbook 一直被用來從遭駭入的電腦中竊取資訊，利用電子郵件作為主要感染媒介，並使用各種主旨，包括常見的假訂單、出貨明細、對帳單與發票和 SWIFT 外匯轉帳。主要目的是從網頁瀏覽器竊取憑證、收集螢幕截圖和按鍵側錄。以惡意軟體即服務 (MaaS) 的形式出售，針對全球多個國家、地區的各行各業發動目標式和亂槍打鳥式的攻擊行動。很頻繁，至少可以這麼說。真的很頻繁。



這是一封典型 Formbook 電子郵件的範例，這封保加利亞語的郵件包含一個附件，其檔名以狡猾的“pdf.zip”為結尾。寄件人的電子郵件位址與寄件人簽名中的公司名稱和網站完全不同，這顯然就是一個警訊。



在此具體的範例中，zip 壓縮檔包含一個可執行檔，該檔案已使用 .NET 加殼程序進行嚴重混淆。執行後，它將自己複製到“%AppData%\Roaming\fLgUSgFvp.exe”，並將自己排除在 Windows Defender 的掃描中，為自己新增排程，最後解密實際有效籌載，將 Formbook 4.1 版注入以下 Windows 應用程式：“C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe”。

在去年 12 月的防護公告中，報告說明當時 Formbook 攻擊行動，已被我們郵件安全雲端服務 (ESS) 的惡意軟體掃描元件主動攔截，後續發起相關新攻擊行動也是如此，我們客戶完全不受影響。包含機器學習在內的多層次先進防護技術，百分之百有效攔阻 Formbook，但為了證明機器學習的有效性，我們很高興地在本公告中展示，從去年 12 月以來所有攻擊行動，證明無需更新就能完整檢測與攔截 Formbook 的底層邏輯。

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 **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：
- MSIL.Packed31
- Scr.Malcode!gdn32
- Scr.Malcode!gdn34

基於機器學習的防禦技術：
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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)。

欲深入瞭解賽門鐵克端點防護(SEP)的進階機器學習防護技術，請點擊此處。
欲深入瞭解更多有關於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。

2023/05/29
Volt Typhoon駭客組織的活動

至少從 2021 年開始，Volt Typhoon 駭客組織就活躍在威脅領域。已知這個攻擊者以通訊業、資訊技術業、製造業、政府、教育界和全球其他幾個領域的各種企業和組織為目標。Volt Typhoon 將攻擊重點放在網路間諜活動和資訊竊取上。攻擊者通常透過有連線網際網路的易受攻擊裝置獲得初始存取權限。之後，他們會嘗試竊取 AD 憑證並使用它們對目標網路中的其他裝置進行身份驗證。Volt Typhoon 透過各種品牌的小型辦公室／家庭辦公室 (SOHO) 路由器代理其惡意流量，以便與正常流量活動混合。該組織還相當依賴就地取材 (LOTL) 工具以保持低調，以暗度陳倉。

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.TCP!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：
- Hacktool
- Hacktool.Jsprat
- Hacktool.Mimikatz
- PUA.Gen.2
- Remacc.Remadmin
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.NPE
- WS.Malware.2
- WS.SecurityRisk.3

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：
- Audit: Zoho ManageEngine ADSelfService Plus CVE-2021-40539
- Web Attack: Zoho ManageEngine ADSelfService Plus RCE CVE-2021-40539

2023/05/29
Bandit竊密惡意軟體

在真實網路上發現一種名為 Bandit 全新惡意竊密程式。該惡意軟體主要針對各種網頁瀏覽器和加密貨幣錢包等。Bandit 竊密惡意軟體是用 Go 語言撰寫，透過惡意網站或網路釣魚進行傳播。該竊密程式能夠在執行前對虛擬或沙箱環境進行各種檢查。該惡意軟體會從遭駭入的電腦上收集系統資訊、儲存在瀏覽器中的機密資料、cookie、銀行詳細資訊、加密貨幣相關資料等。

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：

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.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：
- System Infected: Trojan.Backdoor Activity 564

2023/05/29
全新的Mirai變種IZ1H9針對最新的物聯網漏洞

據報導，一個被命名為 IZ1H9 全新的 Mirai 變種，已經針對幾個最新的物聯網漏洞--CVE-2023-27076、CVE-2023-26801 和 CVE-2023-26802 等進行開採利用。一旦遭駭入，易受攻擊的裝置就會成為 Mirai 殭屍網路的一部分，並允許攻擊者進行完全遠端控制。該惡意軟體將嘗試終止在受感染主機上，已被執行的其他殭屍網路或不同 Mirai 變種的各種程序。然後，遭駭入的裝置可被操控用於發動 DDoS 等攻擊。

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：
- Downloader.Trojan
- Linux.Mirai
- Linux.Mirai!g1
- Linux.Mirai!g2
- Trojan.Gen.NPE
- WS.SecurityRisk.4

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。

2023/05/26
在Magalenha惡意網路攻擊行動部署PeepingTitle後門

Magalenha 行動是以葡萄牙多家知名銀行和金融機構客戶為目標的惡意網路攻擊行動。攻擊者正在散布一個基於 Delphi被稱為PeepingTitle 的後門程式，它屬於 Maxtrilha 銀行金融惡意軟體家族。Magalenha 惡意網路攻擊行動的攻擊鏈涵蓋透過各種媒介散布惡意軟體，包括網路釣魚、社交工程和上架在受感染網站上的惡意安裝程式。部署的後門具有允許攻擊者遠端控制遭駭入的電腦、憑證竊取、資料竊取滲漏和部署多種額外有效籌載的功能。

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：
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：
- ISB.Downloader!gen60
- ISB.Downloader!gen68
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.4

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

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。

2023/05/26
以禮品卡的形式支付贖金～Obsidian(*黑曜石)ORB勒索軟體

Obsidian ORB 是一種源於 Chaos 勒索軟體原始程式碼再修改的新型勒索軟體變種。該勒索軟體根據預先定義的檔案副檔名清單來加密檔案，並且僅加密檔案大小小於 2MB 的檔案。較大的檔案會被以隨機的資料覆蓋，使得較大的檔案損壞且無法恢復。被Obsidian ORB 加密後的檔案會被新增隨機的四個字元的附檔名，並以 .txt 文字檔的形式置放贖金支付說明，並更改受感染電腦的桌面背景。Obsidian ORB 幕後的攻擊者要求以禮品卡的形式支付贖金，而不是常見的使用加密貨幣支付贖金。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：
- Ransom.Sorry
- 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

2022/12/08
防護亮點：惡馬惡人騎，胭脂馬遇到關老爺～Formbook難逃賽門鐵克郵件安全服務(ESS)的手掌心

～防護亮點～

難以置信電子郵件問世數十年後，還能成為主要的溝通工具，尤其在企業中。我們可以看到電子郵件的流行，每天有數千億封電子郵件發送到世界各地，因此它也成為垃圾郵件發送者的頭號目標。根據您的來源，估計目前發送的所有電子郵件中大約有一半到四分之三以上是垃圾郵件。這些垃圾郵件中的絕大多數是“malspam”，也就是包含或傳遞惡意軟體的垃圾郵件。

2016年出現的 Formbook 原本是一隻鍵盤側錄木馬，但是後來被發現功能強大，被用於發動大規模垃圾郵件感染全球企業。這也是最惡名昭彰的竊密程式之一，它搞得我們天昏地暗。大家對於Formbook 耳熟能詳的事蹟如下：

- Formbook 使用**電子郵件**作為其主要感染媒介，但也可能使用驅動下載、漏洞利用工具包和軟體漏洞
- 使用一系列令人眼花繚亂的電子郵件主旨，但似乎更喜歡相當普通的“支付”類型的社交工程戰術，包括虛假訂單電子郵件、運輸和 SWIFT外匯轉帳
- 至少從 2016 年開始，一直是最常見的竊密惡意程式和表單劫持惡意程式
- 主要目的從瀏覽器收集憑證並收集螢幕截圖和點擊或鍵盤側錄
- 有能力下載和執行額外的惡意檔案
- 負責暗網上的大量憑證轉存
- 以惡意軟體即服務 (MaaS) 的形式出售，並被世界各地的多個駭客組織和個人所採用
- 針對許多不同的行業和業務部門以及全球多個地區和國家部署有針對性和無針對性的攻擊行動

惡馬惡人騎，胭脂馬遇到關老爺～Formbook 難逃賽門鐵克郵件安全服務(ESS)的手掌心
對過去幾週我們的全球情資網路遙測大數據的分析顯示：
- 超過一萬封與 Formbook 相關的惡意郵件
- 針對多個地區和行業的多個攻擊者和攻擊行動
- 使用數百個電子郵件主旨的數十個攻擊行動

所有這些威脅都被賽門鐵克郵件安全服務(ESS) 的惡意軟體掃描元件**主動攔截阻止**。

賽門鐵克郵件安全服務 (ESS) 客戶請放心，我們卓越並深受信任的郵件安全技術將替你為贏得勝利做好準備。『好』還不夠好。卓越才會給你帶來成果。卓越才會為你帶來競爭優勢。卓越才能勝出。

要了解有關賽門鐵克雲端郵件安全服務的更多資訊，**請點擊此處下載我們型錄及簡報檔**。