保安資訊--今日最新(台灣時間2025/04/02)
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 37 萬 1,600 台受保護端點上總共阻止了 4,930 萬次攻擊。這些攻擊中有 84.8% 在感染階段前就被有效阻止：**(2025/04/01)**

- 在**8**萬**200**台端點上，阻止了**2,110**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7**萬**8,000**台端點上，阻止了**620**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2**萬**4,300**台**Windows**伺服主機上，阻止了**700**萬次攻擊。
- 在**5**萬台端點上，阻止了**210**萬次嘗試掃描伺服器漏洞。
- 在**1**萬**2,800**台端點上，阻止了**84**萬**7,700**次嘗試掃描在**CMS**漏洞。
- 在**4**萬**7,600**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**10**萬**5,900**台端點上，阻止了**240**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,900**台端點上，阻止了**76**萬**9,700**次加密貨幣挖礦攻擊。
- 在**11**萬**400**台端點上，阻止了**680**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**531**台端點上，阻止了**7**萬**4,300**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 17 萬 3,900 個受保護端點上阻止了總計 720 萬次攻擊。**(2025/04/02)**

- 使用網頁信譽情資，在 **167.2K** 個端點上阻止 **680** 萬次攻擊。
- 攔截 **19.2K** 個端點上 **284.1K** 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 **5.5K** 個端點上攔截 **106.9K** 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 **156** 個端點上攔截 **1.6K** 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。

點擊此處獲取--關於賽門鐵克原廠防護週報

2025/04/01

Masslogger木馬程式透過以銀行為幌子的釣魚郵件傳播，主要針對羅馬尼亞，並擴展至歐洲各地

賽門鐵克發現一個主要針對羅馬尼亞組織的 Masslogger 木馬程式散播行動，攻擊者假冒一家羅馬尼亞銀行。除了鎖定羅馬尼亞之外，這個攻擊行動也波及到歐洲其他幾個國家。

網路釣魚電子郵件的主旨行為「RUGĂM CONFIRMARE DE PRIMIRE」，翻譯為「請確認收到」。它聲稱包含一份日期為 2025 年 3 月 31 日的對帳單，並敦促收件者確認收件，以增加緊迫感與合法性。

附件是一個檔名為「SWIFTACTURA.UUE」的檔案。雖然現在很少使用，但 .UUE 檔案格式曾是電子郵件傳輸中編碼二進位檔案常用格式。攻擊者現在偶爾會使用這種格式來逃避偵測。

.UUE 編碼檔案內有一個惡意的 PE 檔案，執行時會部署 Masslogger，這是一個竊取憑證的惡意軟體，目的是從受感染的系統中擷取敏感資訊。惡意軟體被設定為透過 Telegram 來滲出資料，這是現代憑證竊取程式常用的手法，因為 Telegram 易於使用且有加密通道。

目標行業：汽車與運輸、科技與資料、製造與工業、金融與投資、媒體與出版、教育與訓練、零售與貿易、建築與屋宇服務、醫療保健與製藥、電信、設計與工程。

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。

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.Suspexec!gen8
- Packed.Generic.666
- Scr.Malcode!gdn34

2025/04/01

防護亮點：賽門鐵克領先業界的ScriptNN神經網路模型機器學習技術，有效拆解日新月異的網路釣魚伎倆

網路釣魚是一種非常常見的社交工程攻擊手法，它試圖透過發送欺詐性通訊 (通常透過電子郵件或簡訊) 來竊取使用者資料，這些通訊來源看起來出於合法。網路釣魚主要在惡意軟體攻擊的第一階段使用，其最終目標是偵察或入侵。惡意軟體作者製作的網頁看起來與不知情的使用者日常會提交個人或敏感資訊 (通常稱為「PII」或「個人識別資訊」)的網站相似甚至相同，例如：電子郵寄地址、帳號名稱、密碼、信用卡號碼等。一旦這些資訊遭竊取，就很容易滲透到該用戶的機器或企業網路中，並根據攻擊的性質和意圖引入額外的惡意軟體、竊取資料或造成更嚴重的損害。傳播網路釣魚頁面最常用手段是透過電子郵件，賽門鐵克的使命是持續創新以保護我們的企業電子郵件客戶免受惡意行為者攻擊，我們採用一種稱為 ScriptNN 的進階機器學習 (SML) 技術來掃描電子郵件並攔截阻擋此類型的網路釣魚頁面。

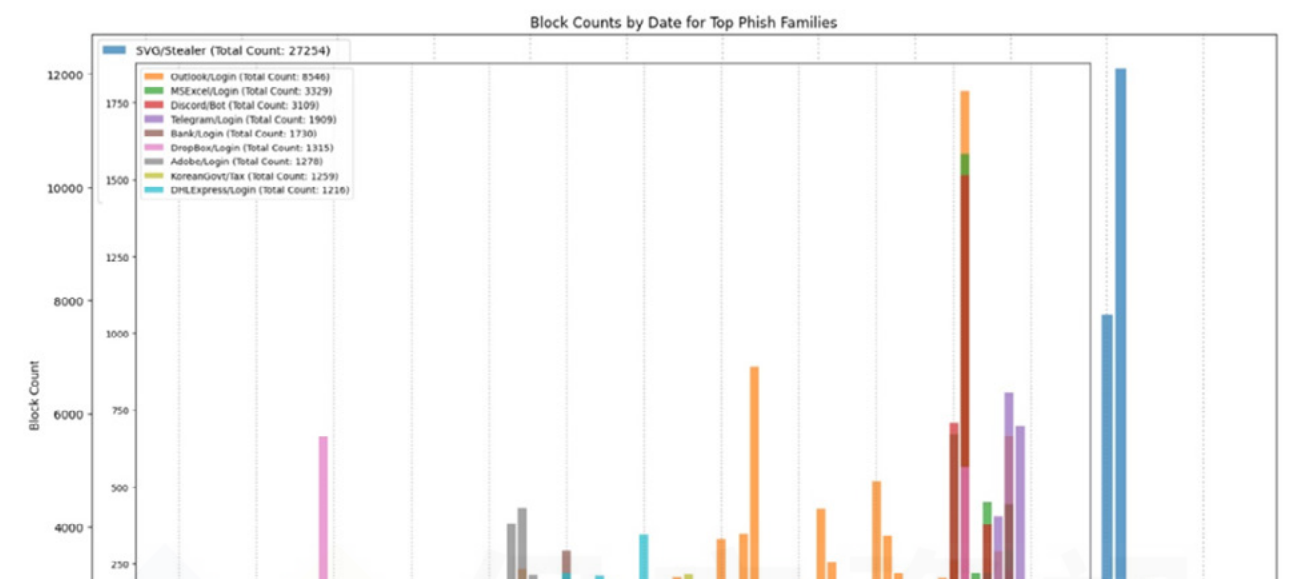
什麼是 ScriptNN

ScriptNN，即「HTML 和 JavaScript 神經網路模型 (Neural Network-based)」的縮寫，可掃描電子郵件附件中的 HTML 和 JavaScript 內容，並使用基於深度神經網路的機器學習 (Deep Neural Network-based Machine Learning (ML)) 模型，該模型經過訓練以通過分析數百萬個頁面 (包括乾淨頁面和已被識別為網路釣魚嘗試的頁面) 來區分網路釣魚企圖和合法網頁，使其能夠偵測與攔截零日攻擊，同時避免對有效電子郵件的錯誤阻止 (誤攔)。ScriptNN 模型採用最先進的工程架構，在磁碟和記憶體上的佔用空間極小，並採用極快的掃描和檢測模型 (每次掃描只需微秒)，確保我們的電子郵件伺服器和電子郵件終端使用者，不會因為這項技術的導入而感受到任何明顯的時間落差。此類模型的挑戰性任務在於如何將誤報幾乎降至可忽略的程度--這意味著不應阻止任何乾淨的附件，以免接收者未能收到電子郵件。我過去幾個月來，我們的 ScriptNN 模型的誤判次數都是零。

ScriptNN 的優點

下面的圖表顯示由 Symantec 保護的電子郵件伺服器上，ScriptNN 在過去 3 個月內對釣魚頁面的偵測與攔截實績。圖表分為兩個部分，分別是 3 月 16 日之前和之後，以顯示常規趨勢和激增趨勢。在 3月 17 日和 3 月 18 日，出現顯著的激增。

在封鎖網路釣魚網頁的同時，我們也會追蹤網路釣魚家族和釣魚手法的趨勢。如今，除了舊的假登錄頁面 (如：Microsoft／Adobe／Dropbox 登錄) 外，還使用各種新的網路釣魚技術。二進位格式的 SVG 圖檔，能夠輕鬆在瀏覽器中呈現，越來越多被用來繞過基於文本的掃描器。我們最近經歷一次巨大的激增，保護我們客戶環境內的數千個企業端點 (請參閱下文)。Discord 機器人也被大量使用來欺騙使用者，讓他們誤以為有來自授權或已知角色的直接訊息 (DM)，要求他們點選連結或在與某些優惠、贈品、服務續訂或付款驗證等相關的連結上提供憑據，有時甚至會讓用戶經歷一個假驗證碼。類似的技倆也套用在 Telegram 的即時訊息。在某些情況下，被盜取的憑證直接張貼到 Telegram 上。我們定期看到針對特定客戶在特定地區發送有針對性的網路釣魚，有時使用假政府授權頁面。快遞送貨的網路釣魚驗證頁面也在上升。一些網路釣魚是自動化的，通過機器人在特定的星期幾發送 (垂直虛線表示的星期一)。所有這些網路釣魚攻擊呈波浪式出現，如下所示。



在電子郵件伺服器上安裝賽門鐵克 ScriptNN 防護的最大好處，在於以深度學習為基礎的進階機械學習技術可辨識零日攻擊，而無需不斷自我重新訓練。相較之下，我們注意到上述的網路釣魚波在零日時，大多數其他廠商都無法偵測到。

欲深入瞭解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。
欲深入了解賽門鐵克的端點多層次防護解決方案中「進階機器學習」防護技術，請點擊此處。

2025/04/01

TsarBot Android惡意軟體

TsarBot 是安卓平台上新出現的銀行金融木馬，報告指出其鎖定超過 750 種不同的銀行、金融和加密貨幣相關應用程式 (APP)。該惡意軟體經由偽裝成合法金融入口網站進行傳播。與其他行動銀行金融木馬類似，TsarBot 要求受害者在目標設備上啟用無障礙服務，然後利用覆蓋攻擊竊取銀行詳細資訊和憑據等。收集到的資訊經由 WebSockets 被傳輸到攻擊者控制的 C&C 伺服器。其他惡意功能包括螢幕錄製、鍵盤記錄和鎖定抓取技術，使攻擊者能夠收集現有的鎖定的憑據並操控感染的設備。

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

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。

2025/03/31

SnakeKeylogger惡意竊密軟體涉入一起多階段的資訊竊取行動

SnakeKeylogger 是一款惡意竊密軟體，會收集憑證和其他敏感資料。目標是常見的應用程式，例如：Google Chrome、Mozilla Firefox 等網頁瀏覽器，以及 Microsoft Outlook 和 Thunderbird 等電子郵件用戶端程式。它也會從 FileZilla 擷取儲存的 FTP 認證。此多階段攻擊由一封包含 IMG 檔案附件的惡意垃圾郵件開始，當開啟此附件時會建立一個虛擬磁碟機。在虛擬磁碟中，可執行檔案會偽裝成 PDF 文件，以增加收件者開啟的可能性。

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。

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.Malcode!gen43
- Scr.Malcode!gen139
- Trojan.Gen.MBT
- WS.Malware.1
- WS.SecurityRisk.4

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

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。

2025/03/31

安卓平台出現的全新手機惡意軟體：Crocodilus

Crocodilus 是最近在威脅生態圈出現安卓平台上的全新行動銀行特洛伊木馬。該惡意軟體具有廣泛的遠端控制和資訊竊取功能，可讓攻擊者進行應用程式覆蓋攻擊、遠端存取遭攻擊的裝置、竊取儲存在行動裝置上的憑證／資料、鍵盤記錄和執行從 C&C 伺服器接收的指令等。與許多其他手機惡意軟體一樣，Crocodilus 須先取得目標裝置上的存取服務，才能進行惡意作業。

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

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。

2025/03/31

威脅生態圈出現全新的惡意軟體載入器：CoffeeLoader

CoffeeLoader 是一款全新的精密惡意軟體載入器，用來執行次要有效酬載，同時逃避偵測。此惡意軟體載入器利用在系統 GPU 上執行程式碼的打包程式。CoffeeLoader 可透過 Windows 工作排程建立持久性／常駐能力，並可透過預先寫死在程式碼的工作排程來維持持久性。對於 C&C 通訊，它使用 HTTPS 與預先寫死在程式碼的伺服器進行通訊。如果這些伺服器無法連線，它會使用動態網域產生演算法 (DGA，Domain Generation Algorithm)，並使用憑證綁定 (certificate pinning) 的方式以確保安全性。

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

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
- WS.Reputation.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.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。

2025/03/30

MassLogger惡意竊密程式涉入多起網路釣魚行動，以採購業務相關誘餌來引誘全球企業上鉤

MassLogger 是一款種專門擷取受害者憑證、擊鍵和剪貼簿資料的惡意竊密程式，在威脅生態圈已有明顯的影響力，全球各地已發現不同規模和受害者類型的攻擊行動。

在最近一次攻擊行動中，有人觀察到一名攻擊者假冒一家在中東經營航空燃料和潤滑油、海事、運輸、科技、包裝、旅遊、水處理和房地產的公司的採購人員，以假亂真來降低受害者的警覺。

惡意電子郵件會施壓收件者確認、簽署虛構的 XLS 文件並蓋章，以增加急迫感。如果使用者開啟惡意附件，Excel 檔案 (PO 23-179、PO 23-181.xls) 將開採濫用 CVE-2017-0199 漏洞，此漏洞是 Microsoft Office 的陳年老漏洞，當開啟精心製作的檔案，就會執行遠端惡意指令碼。接續就會觸發下載和執行 HTA(HTML 應用程式) 檔案，進而呼叫和執行 MassLogger。

目標行業：航太、農業、汽車、建築、人力仲介與就業服務、能源、工程、娛樂、金融服務、醫療保健、工業氣體過濾、IT 服務、實驗室服務、物流、製造、遠洋與離岸、專業服務、公共部門、科技、公用事業。

目標國家：美國、比利時、挪威、阿聯酋、荷蘭、希臘、芬蘭、瑞士、瑞典、沙烏地阿拉伯、馬來西亞、印度、澳洲、南非、法國、新加坡、台灣、印尼、土耳其、肯亞、日本、香港、阿曼、摩洛哥和以色列。

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。

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!gen12
- ISB.Downloader!gen80
- Scr.Malcode!gen59