保安資訊--本周(台灣時間2022/11/18)
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 95 萬 5,600 台受保護端點上總共阻止了1.27億次攻擊。這些攻擊中有 90% 在感染階段前就被有效阻止：**(2022/11/08)**

- 在**17萬5,600**台端點上，阻止了**5,540**萬次嘗試掃描**Web**服務器的漏洞。
- 在**32萬7,000**台端點上，阻止了**2,630**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬5,700**台**Windows**伺服主機上，阻止了**1,880**萬次攻擊。
- 在**10萬9,800**端點上，阻止了**410**萬次嘗試掃描伺服器漏洞。
- 在**3萬4,200**台端點上，阻止了**170**萬次嘗試掃描在**CMS**漏洞。
- 在**6萬6,300**台端點上，阻止了**220**萬次嘗試利用的應用程式漏洞。
- 在**33萬2,000**台端點上，阻止了**830**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,800**台端點上，阻止了**700**萬次加密貨幣挖礦攻擊。
- 在**5萬2,900**台端點上，阻止了**530**萬次向惡意軟體**C&C**連線的嘗試。
- 在**3,900**台端點上，阻止了**15萬2,300**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。

2022/11/17

好無辜！維基(Wiki)遭冒用與濫用--Crysis勒索軟體的新變種

Wiki 是另一個已經被證實的 Crysis 勒索軟體變種。據報導，該惡意軟體通常透過遠端桌面通訊協定 (RDP) 連線進行傳播，或偽裝成無害的軟體安裝程式。被 Wiki 加密後的檔案會新增帶有依不同受害者的 "唯一代碼" + "郵件帳號" + "Wiki" 不同副檔名。該惡意軟體還會停用特定的系統程序和服務，並刪除磁碟區陰影複製副。

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(Snoar)的防護：

- SONAR.RansomCrys!g2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Crysis
- Ransom.Crysis!gm
- SMG.Heur!gen
- WS.Malware.1

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

2022/11/17

免費的常常最貴～竊密程式偽裝成文法檢查擴充程式的安裝程式

AcridRain 並不是一個全新的竊密程式，它至少從 2018 年就存在。多年來，它的熱門程度從未登上竊密程式的排行榜，但它仍然隨處可見。最近，發現一個全新的 AcridRain 命令和控制 (C&C) 伺服器，與透過瀏覽網頁時的順道下載 (drive-by-download) 攻擊方式來傳播的攻擊行動有關聯。攻擊者將他們的 AcridRain 二進製檔案偽裝成 Grammarly 安裝程式，這是一種熱門的英文文法檢查的雲端服務工具。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/16

麒麟未必受歡迎～Qilin(*麒麟)勒索軟體

Qilin (*麒麟) 勒索軟體（也稱為 Agenda）採用雙重勒索戰術，最近在加密勒索圈小有名氣。在過去的幾個星期，其活動絡繹不絕，針對全球各地的各種組織，特別是拉丁美洲。贖金說明包含有關已被加密／竊取的檔案類型以及連接到攻擊者洋蔥網域的憑證訊息。

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.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/11/16

寶刀未老～DTrack惡意軟體持續受到Lazarus進階持續威脅(APT)組織青睞

DTrack 是一種相對較老舊的後門惡意軟體，但仍然被惡名昭彰的 Lazarus 進階持續威脅 (APT) 組織積極傳播。該惡意軟體可以從受害者那裡收集資訊、鍵盤側錄、螢幕擷取以及在受感染端點上下載和執行多種有效籌載。據報導，最近利用 DTrack 惡意軟體所發動的攻擊行動一直以歐洲和拉丁美洲的用戶為目標。

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(Snoar)的防護：

- SONAR.TCP!gen1
- SONAR.Trafic2.RGC!g16

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
- WS.Malware.2

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: Bad Reputation Process Request 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。

2022/11/16

網路攻擊甚於武器攻擊～Somnia勒索軟體攻擊烏克蘭組織危害不亞於飛彈攻擊

最近，烏克蘭組織成為俄羅斯國家支助的組織進行的勒索軟體攻擊的目標。這些攻擊者使用名為 Somnia 的勒索軟體，他們透過存取代理傳播該軟體，而存取代理又透過 Vidar 竊密程式和 Cobalt Strike 等其他工具感染受害者。竊密程式偽裝成存放在虛假網站上的虛假 Advanced IP Scanner（一種眾所周知的網路掃描工具）。這個勒索軟體組織真正的目的是要破壞組織而不是勒索贖金。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.TCP!gen1
- SONAR.Ransomware!g34

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Crysis
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

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：

- 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。

2022/11/15

會變更「桌布」的勒索軟體～Inlock

Inlock 是另一種常見的勒索軟體變種。被該惡意軟體加密後的檔案會被附加“.inlock”的副檔名。除了以 .txt 文字檔格式提供贖金支付說明外，Inlock 還會更改被加密電腦上的「桌布」並刪除磁碟區陰影複製副本。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn32
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/11/15

BillBug～國家級駭客組織：鎖定憑證簽發機構為目標

賽門鐵克最近發布一篇關於 Billbug 的部落客，Billbug 是一個受國家支持的駭客組織，在一場針對多個政府機構的攻擊活動中入侵一個亞洲國家的數位憑證簽發機構。這個威脅者至少從 2009 年開始就存在，並在亞洲發動多起攻擊行動。他們使用像 Hannotog 和 Sagerunex 這樣的後門程式，但也使用多種兩用工具來發動就地取材攻擊。

在我們的部落格文章中有更多資訊可供參考：Billbug：國家資助的攻擊者以多個亞洲國家／地區的數位憑證簽發機構、政府機構為目標

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(Snoar)的防護：

- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Hannotog
- Backdoor.Sagerunex
- Backdoor.Sagerunex!gm
- Backdoor.Trojan
- Hacktool
- Hacktool.Gen
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Trensil

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
- Web Attack: Webpulse Bad Reputation Domain Request

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2022/11/14

熱愛韓國～Koxic 勒索軟體

Koxic 是一種勒索軟體變種，最近有報導稱它已經在韓國使用者之間互相傳播。該惡意軟體會加密使用者檔案，被該惡意軟體加密後的檔案會被附加“.koxic”的副檔名。Koxic 的功能還包括會刪除磁碟區陰影複製副本以及在進行加密程序之前停用特定的系統程序和服務。

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(Snoar)的防護：

- SONAR.RansomNemty!g2
- SONAR.SuspLaunch!g18
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/14

Google Play商店未必安全～Xenomorph網路銀行木馬，透過Google Play商店重出江湖

根據最近一份報告，Xenomorph 這款手機網路銀行木馬已透過上架在 Google Play 商店中的吃喝玩樂（Lifestyle）應用程式(APP)散播。有效惡意籌載可從 GitHub 程式碼托管平台下載，一旦下載完成就會自動安裝。Xenomorph 具有竊取網路銀行憑證或攔截受害者簡訊的功能。攔截的簡訊內容可以幫助攻擊者竊取一次性密碼或任何類似的多因素身份驗證請求。

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
- AppRisk:Generisk

2022/11/13

鎖定亞洲少數民族和宗教團體的Android手機行動間諜應用程式(APP)～BadBazaar

根據最近的報導，亞洲的少數民族和宗教團體已成為一種全新的 BadBazaar 間諜軟體的目標。這種惡意軟體偽裝成為特定分眾定制的常見 Android 手機行動應用程式(APP)，例如：字典和宗教相關、影片播放器等。這種普通的間諜軟體透過第三方應用程式商店和網站進行分發。

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

2022/11/13

鎖定消費者和中小型企業～Key Group勒索軟體集團

在過去的幾星期裡，消費者和中小型企業一直是另一個名為 Key Group（也稱為 keygroup777）的勒索軟體駭客集團的鎖定目標。這些駭客使用普通的勒索軟體，在成功執行後，被該惡意軟體加密後的檔案會被附加“.keygroup777”或“.keygroup”的副檔名。勒索／贖金說明會要求受害者透過電報或電子郵件聯繫攻擊者，卻沒有列出贖金金額。

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(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.Heur.Dropper
- SONAR.SuspBeh!gen1
- SONAR.SuspDataRun
- SONAR.SuspDrop!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.HiddenTear!g1
- Ransom.Sorry
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/13

不用道士咒語也能控制的～殭屍電腦--SaintBot，可能即將發動新的攻擊行動

殭屍電腦--SaintBot 首次曝光的時間是在 2021 年初，此後一直有發現其零星的活動。攻擊者利用這種威脅來發動惡意垃圾郵件攻擊行動，進一步下載整起攻擊鏈所需的其他惡意軟體。最近，發現一個與該殭屍電腦有關聯的全新 C&C (命令和控制伺服器)，這意味著可能即將發動新的攻擊行動。

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.MBT

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。

2022/11/11

針對郵件帳號憑證(帳密)～全新StrelaStealer竊密惡意軟體

已在真實網路環境發現到使用西班牙語的 StrelaStealer 竊密惡意軟體。攻擊鏈涉及透過電子郵件附件的 ISO 檔。ISO 檔包含 LNK 和 HTML 檔案，這些檔案在執行時會載入惡意軟體。然後，該惡意軟體會搜索 Outlook 和 Thunderbird 等常用電子郵件用戶端的帳號憑證(帳密)，並將該資訊洩露上傳到 C&C 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：

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：

- Downloader
- Trojan Horse
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/11

全新殭屍電腦～KmsdBot可以發動DDoS攻擊以及執行加密貨幣挖礦攻擊

KmsdBot 是一種使用 Golang 程式語言撰寫的全新殭屍電腦變種，支持包括 Winx86、x86_64、Arm64 和 mips64 在內的多種架構。惡意軟體透過安全外殼協定 (SSH) 連接進行攻擊，並以具有預設或弱登錄憑證的系統為目標。KmsdBot 的功能非常先進，可以發動 DDoS 攻擊以及執行加密貨幣挖礦攻擊。

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：

基於行為偵測技術(Snoar)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.NPE
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/11/11

由Iridium進階持續威脅(APT)組織所主導的Prestige勒索軟體攻擊行動

Prestige 是一種勒索軟體的新變種，上個月針對烏克蘭和波蘭的運輸和物流部門的組織進行一系列攻擊。根據最新報告，使用 Prestige 勒索軟體的攻擊現已歸因於 Iridium APT 組織（也稱為 Sandworm）。被 Prestige 勒索軟體加密後的檔案，會被新增" .enc"的副檔名。該惡意軟體還能夠刪除受感染端點上的備份和磁碟區陰影複製副本。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.Ransomware!g1
- SONAR.RansomGen!gen3
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen
- 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

2022/11/11

基於Javascript的殭屍(電腦)網路：Cloud9

Cloud9 是一個基於 Javascript 的殭屍(電腦)網路，通常以惡意的瀏覽器的外掛形式出現。底層的 Javascript 也可以被威脅者單獨執行，因此透過用戶重新導向到有包含這些惡意 .js 腳本的網站。Cloud9 的功能包括竊取 cookie、鍵盤側錄、加密貨幣挖礦、廣告注入和傳遞額外的任意有效籌載。

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(Snoar)的防護：

- SONAR.SuspBeh!gen667

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Malscript
- WS.Malware.1

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。

2022/11/11

採用更棘手的雙重勒索戰術～Mallox 勒索軟體

Mallox 勒索軟體駭客組織，主要還是採用更棘手的雙重勒索戰術，也就是如果受害者不支付贖金，遭竊的資訊可能會被出售或洩露。最近，發現多起 Mallox 活動，該勒索軟體在加密後會給加密檔案新增 ".mallox" 的副檔名。

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(Snoar)的防護：

- SONAR.Cryptlocker!g42
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g230
- SONAR.SuspLaunch!gen4

檔案型(基於回應式樣本的病毒定義檔)防護：

- MSIL.Downloader!gen8
- Trojan.Gen.MBT
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/10

年初至年終～XorDdos分散式阻斷服務(DDOS)持續發威...

今年初據報所謂的 XorDdos 活動有所增加，截至今天，這種分散式阻斷服務(DDOS) Linux 木馬程序仍然活躍，主要鎖定目標是端點、物聯網 (IoT) 設備和雲端基礎設施。憑藉精密複雜的規避功能，XorDos 還能透過 SSH 暴力攻擊進行散播。

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.Xorddos

基於安全強化政策(適用於使用DCS)：

DCS 安全強化政策可以預防惡意軟體的安裝以及XorDdos 分散式阻斷服務(DDOS)的惡意活動，有效提供零時差攻擊保護。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。