保安資訊--本周(台灣時間2023/02/24)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 85 萬 5,100 台受保護端點上總共阻止了 1 億 440 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/02/20)**

- 在**16萬3,200**台端點上，阻止了**4,100**萬次嘗試掃描**Web**服務器的漏洞。
- 在**29萬9,200**台端點上，阻止了**2,320**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬8,800**台**Windows**伺服主機上，阻止了**1,670**萬次攻擊。
- 在**8萬8,300**台端點上，阻止了**300**萬次嘗試掃描伺服器漏洞。
- 在**2萬1,500**台端點上，阻止了**130**萬次嘗試掃描在**CMS**漏洞。
- 在**7萬3,100**台端點上，阻止了**220**萬次嘗試利用的應用程式漏洞。
- 在**28萬5,200**台端點上，阻止了**580**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬1,100**台端點上，阻止了**210**萬次加密貨幣挖礦攻擊。
- 在**14萬9,200**台端點上，阻止了**1,290**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,900**台端點上，阻止了**15萬7,700**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。

2023/02/23

HardBit 勒索軟體推出2.0新版本

HardBit 是一種勒索軟體變種，於 2022 年 10 月前後首次被發現。後續在 11 月推出新的版本 2.0，並且仍在廣泛傳播。勒索軟體具有停用指定程序和服務以及刪除受感染端點上的捲影副本的功能。該惡意軟體會加密用戶的檔案後新增 .hardbit2 的附檔名。贖金支付說明檔會以 .txt 和 .hta 檔案格式，置防於根目錄和所有被加密檔存放的資料夾。

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：

- AGR.Terminate!g2
- Sonar.SuspLaunch!g18
- Sonar.SuspLaunch!g193
- Sonar.SuspLaunch!g257
- Sonar.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Hardbit
- Scr.Malcode!gdn32
- Trojan Horse
- 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.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.Crysis Activity 3
- Attack: Ransom.Gen Activity 29

2023/02/23

全新駭客集團～Clasiopa

觀察到一個前所未聞的駭客組織以亞洲的一家材料研究組織為鎖定目標。該組織被賽門鐵克命名為 Clasiopa，其特點是具有獨特的工具集，其中包括一個自定義惡意軟體 (Backdoor.Atharvan)。Clasiopa 使用的感染媒介是未知的，儘管有一些證據表明攻擊者透過提供透過在網際網路上的提供公眾服務的伺服主機進行暴力攻擊來獲得存取權限。

在我們的部落格文章中有更詳細內容：全新駭客集團：Clasiopa～鎖定亞洲的材料研究組織

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDrop!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Atharvan
- Hacktool
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2023/02/22

全新駭客組織～Hydrochasma瞄準的亞洲的組織

賽門鐵克觀察到針對亞洲航運和醫療機構的明顯情報收集活動。這項活動專門使用公開可用的就地取材工具，應該是以前未曾曝光的 Hydrochasma 駭客攻擊組織。

在我們的部落格文章中有更多資訊可供參考：以前未曾曝光的 Hydrochasma 駭客攻擊組織以亞洲的醫療和航運組織為目標

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(SONAR)的防護：

- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- SecurityRisk.LaZagne
- Trojan Horse
- Trojan.Dropper
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2023/02/22

越南和韓國產業正面臨利用Formbook竊密程式所發動的攻擊行動

Formbook 的脅嚴重危害全球是有目共睹。賽門鐵克最近檢測到一個發動 Formbook 的攻擊者，其目標是越南和韓國的產業，以及在當地設有辦事處的外國公司。儘管這些國家是主要目標，但也試圖感染英國、新加坡、澳洲、南非和美國等其他國家的組織。攻擊者通常使用帶有惡意壓縮檔附件（.GZ 是用於韓國，.ZIP 是用於越南）的電子郵件作為感染受害者的主要媒介。攻擊者利用貨運和付款等常見社交工程伎倆，誘使受害者開啟附件進而執行 Formbook 竊密程式。

郵件主旨：

- 지불을 확인하십시오
- Thông tin giao hàng

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：

- scr.malcode!gdn30
- scr.malcode!gdn34

2023/02/21

Stealc～破壞力更強的竊密程式

Vidar、Raccoon、Mars 和 Redline 等知名竊密程式催生一種破壞力更強的 Stealc 的全新惡意軟體。據報導，在地下論壇中，Stealc 因其優異的竊密功能（例如：執行自訂的檔案擷取）而迅速竄紅起來。它讓攻擊者竊取符合其“擷取規則”的檔案，並將竊取的檔案上傳到攻擊者的專用 C&C 伺服器，然後清除感染軌跡。

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
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2023/02/21

DarkCloud(*暗雲)竊密程式

DarkCloud 是一種在網路上散佈很廣的竊密程式。該惡意軟體主要透過偽裝成訂單發票的垃圾郵件傳播。這些電子郵件夾帶的惡意程式 .zip 壓縮檔附件，具有呼叫或下載惡意酬載的功能。Darkcloud 竊密程式具有許多功能，包含鍵盤側錄、螢幕截取或加密貨幣換算。它收集 MS office、pdf 和文字檔案以及儲存在網路瀏覽器中的各種機密訊息，包括信用卡詳細訊息、憑證、cookie 和許多其他訊息。該惡意軟體將透過 Telegram、SMTP 和 FTP 等不同管道收集資料。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

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：

- MSIL.Packed.31
- Packed.Generic.681
- Packed.Generic.683
- Packed.NSISPacker!g14
- Scr.Malcode!gdn14
- Scr.Malcode!gdn30
- Scr.Malcode!gdn32
- Scr.Malcode!gdn34
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

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

2023/02/21

針對西班牙組織的攻擊行動，GuLoader又上榜了

惡意軟體載入程式 (Loader) 是網路犯罪分子在受害電腦上傳遞和執行惡意軟體的慣用伎倆，因為本身不帶惡意酬載，所以很容易躲避安全軟體的檢測。某些駭客組織和個體戶專門在攻擊鏈中提供載入程式的服務。威脅領域有許多載入程式，GuLoader 則是在世界各地的攻擊行動中經常被發現到的一種。

賽門鐵克最近發現一個針對西班牙組織的攻擊行動，該行動使用看似來自西班牙建築公司帳單的惡意電子郵件。如果受害者落入社交工程圈套並下載附件檔 (PAGO SIXTO.rar) 中的惡意執行檔，最終將會執行 GuLoader 載入程式。

多年來，這種複雜的惡意軟體載入程式已被用於傳送各種類型的惡意軟體。Guloader 提供的部分惡意軟體系列包括 Formbook、Lokibot、Agent Tesla 和 SystemBC。

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.Guloader

基於機器學習的防禦技術：

- Heur.AdvML.C

2023/02/20

防護亮點：Chaos勒索軟體持續肆虐全球造成錯亂

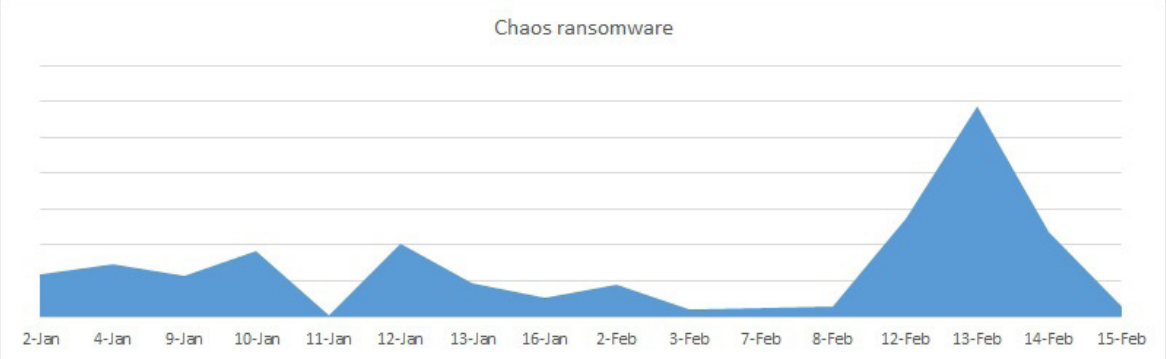
～防護亮點～

在過去一年左右的時間裡，我們已經發布十幾個直接或間接與 Chaos 勒索軟體相關的公告，顯示它在威脅領域的普遍性。Chaos 勒索軟體於 2019 年首次出現，對全球企業和個人發起多次攻擊。現在有如此多的變種，惡意軟體以各種不同的方式傳播，但通常仍透過網路釣魚電子郵件或惡意網站傳播，目的是利用老舊軟體中的漏洞來獲得對受害者系統的存取權限。安裝後，Chaos 會加密受害者的檔案並顯示勒索資訊，要求支付贖金以換取解密密鑰。

Chaos 勒索軟體在威脅領域存在如此多變種的原因之一是該惡意軟體的原始碼於 2020 年在網路上被公開洩露。這使得網路犯罪分子更容易建立新的勒索軟體變種，根據自己的攻擊需求對其進行客製化。全球多個駭客組織和個體戶目前都在使用 Chaos 勒索軟體，針對不同規模和行業的消費者和組織，感染單獨一台或大量的電腦。

Chaos 變種激增的另一個原因是，勒索軟體的攻擊行動通常是一項有利可圖的業務。勒索軟體攻擊可以產生可觀的利潤，特別是如果受害者是一個願意支付大筆贖金以恢復其資料的大型

組織。之前 Chaos 攻擊的成功可能鼓勵其他威脅攻擊者建立他們自己的勒索軟體版本。也因此更該應採用用信譽良好的安全解決方案來保護您的網路，該解決方案必須具有多層級的保護機制，並能優化其配置以確保您的安全狀況堅如磐石。



由於有新變種出現的緣故，2月12~14日這三天有一波很明顯的攻擊增加。

只要有安裝 Symantec Data Center Security 就能套用預設的安全強化政策來提供針對未知威脅的**零時差**攻擊，當然預設強化安全政策就能偵測到以前從未見過的 Royal 勒索軟體變種和行為，如下所示：

基於行為偵測技術(SONAR)的防護：

- SONAR.*

基於機器學習的防禦技術：

- Heur.AdvML.*

* 這表示存在多個類似名稱的檢測，例如：SONAR.Heur.Dropper、SONAR.Psdownloader!g1；Heur.AdvML.B、Heur.AdvML.C 等

有興趣深入了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。

有興趣深入了解賽門鐵克行為安全技術如何提供針對零時差攻擊的保護，請點擊此處。

2023/02/20

巴西的政府機構和產業遭受星際檔案系統(IPFS-InterPlanetary File System)類型的網路釣魚攻擊

電子郵件憑證很重要，如果遭到破壞，它們會為網路犯罪分子提供一個強大的切入點來進行進一步的惡意活動。多年來，某些駭客組織和個體戶專門收集電子郵件憑證，然後在黑市上出售。每天都會目睹無數與電子郵件憑證相關的網路釣魚活動。最近，賽門鐵克觀察到一場針對巴西政府機構和產業的攻擊行動，包括在巴西設有辦事處的外國企業。這些電子郵件相當簡單，主旨列呈現“O seu e-mail [你的電子郵件]”，並包含指向代管在 IPFS（星際檔案系統）上的網 路釣魚登錄頁面的連結。

基於 IPFS 的網路釣魚攻擊是一種使用分散式檔案系統 (IPFS) 來上架和散佈網路釣魚登錄頁面的網路釣魚攻擊。在這種類型的攻擊中，攻擊者建立一個釣魚登陸頁面並將其儲存在 IPFS 網路上，使任何人都可以透過唯一的 IPFS 位址存取。攻擊者利用 IPFS 進行網路釣魚攻擊並非少見，因為它提供一定程度的匿名性、持續性、彈性和速度。

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。

2023/02/20

全新後門程式～WhiskerSpy

WhiskerSpy 是一種新發現的後門程式，歸屬於 Earth Kitsune 這個駭客組織。該駭客集團最近發起的一項攻擊行動是利用水坑攻擊來傳播惡意軟體。包含攻擊者注入到受入侵網站的惡意腳本會讓不知情的用戶下載偽裝成影片播放程式安裝檔的 WhiskerSpy 載入程式。惡意軟體的功能包括下載任意檔、載入可執行檔以及將 shellcode 注入程序等。

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
- 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：

- 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。

2023/02/20

利用ProxyShell漏洞來散佈惡意加密貨幣挖礦程式的全新攻擊行動

在真實網路上發現一個全新的傳播 ProxyShellMiner 惡意軟體的攻擊行動。攻擊者濫用 2021 年的 Microsoft Exchange ProxyShell 漏洞（CVE-2021-34473 和 CVE-2021-34523）進行初始存取和有效籌載傳遞。注入的加密貨幣挖礦程式酬載屬於 XMRig coinminer 系列。為了實現持續性，惡意軟體將在受感染的電腦上建立一個工作排程，該排程被設定為在每次登入時執行。

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
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Coinminer
- Trojan.Gen.2
- 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.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：

- Web Attack: Microsoft Exchange Server CVE-2021-34473
- Web Attack: Microsoft Exchange Server Elevation of Privilege CVE-2021-34523

基於安全強化政策(適用於使用DCS)：

Symantec Data Center Security 預設的 Microsoft Exchange 伺服器強化政策可防止 ProxyShell 漏洞被利用。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2023/02/19

網路上下載挖礦程式請小心：Bruh 勒索軟體鎖定比特幣(BTC)挖礦程式的使用者

賽門鐵克最近注意到一個勒索軟體攻擊者，其目標是在網路上搜尋下載比特幣 (BTC) 挖礦程式的使用者。一旦受害者被偽裝成比特幣挖礦程式的惡意執行檔成功詐騙，他們的檔案將會被加密。出現在受感染電腦上的勒索贖金支付說明以“ATTENTION BRUH”開頭，要求支付 150 美元等值的彼特幣 (BTC)、以太幣 (ETH) 或 萊特幣 (LTC) 支付 150 美元。該勒索軟體是 Chaos 勒索軟體的變種。

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

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/02/17

與WIP26駭客組織相關的惡意活動

根據最新一份報導，一個被稱為 WIP26 的全新駭客組織針對中東的電信業者進行一系列攻擊。該駭客組織一直依賴公有雲基礎設施（例如：MS Mail 365、Microsoft Azure、Google Firebase 或 Dropbox），可能試圖規避偵測並不讓安全軟體發現下。WIP26 使用兩個不同的後門，分別稱為 CMD365 和 CMDEmber，它們偽裝成合法的應用程式，例如：pdf 閱讀器或軟體更新程式。已發現的攻擊行動的目的可能是偵察、間諜活動和資料洩露。

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
- WS.Malware.2

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。