保安資訊--本周(台灣時間2023/03/31)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 78 萬 4,900 台受保護端點上總共阻止了 9,350 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/03/27)**

- 在**15萬1,000**台端點上，阻止了**3,750**萬次嘗試掃描**Web**服務器的漏洞。
- 在**27萬8,500**台端點上，阻止了**2,300**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**1,580**萬次攻擊。
- 在**8萬6,700**台端點上，阻止了**270**萬次嘗試掃描伺服器漏洞。
- 在**2萬100**台端點上，阻止了**110**萬次嘗試掃描在**CMS**漏洞。
- 在**6萬4,300**台端點上，阻止了**200**萬次嘗試利用的應用程式漏洞。
- 在**26萬2,000**台端點上，阻止了**490**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2萬3,500**台端點上，阻止了**260**萬次加密貨幣挖礦攻擊。
- 在**14萬7,200**台端點上，阻止了**1,130**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,700**台端點上，阻止了**11萬8,300**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。

2023/03/30

3CX網路電話系統遭受供應鏈攻擊

據信與北韓關係匪淺的駭客組織已將 3CX 網路電話系統公司的：3CX DesktopApp 植入惡意木馬程式，這是一種被廣泛使用的影音通話桌面應用程式。讓人再次想起之前針對 SolarWinds 的供應鏈攻擊，該軟體幾個最新 Windows 和 Mac 版本的安裝程式被駭客入侵並修改植入惡意程式以利後續布署攻擊鏈所需的惡意酬載及竊密程式。該惡意軟體收集的資訊想必是是讓攻擊者可以篩選潛在得進一步攻擊對象。

在我們的部落格文章中有更多資訊可供參考：3CX 網路電話系統遭受供應鏈攻擊，全球已有數千個用戶遭殃

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：

- Infostealer
- SecurityRisk.Samsis
- Trojan Horse
- Trojan.Dropper
- Trojan.Malfilter
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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：

- Malicious Site: Malicious Domains Request
- Malicious Site: Malicious Domain Request 59
- 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。

2023/03/30

全新竊密程式～OpcJacke偽裝成VPN安裝程式，鎖定加密貨幣用戶

據報導，一種偽裝成 VPN 安裝程式的全新竊密程式正在透過惡意廣告傳播。這種稱為 OpcJacker 的最新威脅具有典型的竊密程式功能，但其採用加密貨幣錢包地址剪貼簿置換的劫持伎倆特別顯眼。此外，它也具有執行 NetSupport RAT 和 hVNC 等模組的功能。該惡意攻擊行動主要針對消費者。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Gen.NPE

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。

2023/03/29

Moobot和Shellbot攻擊漏洞未補的高風險伺服器

Moobot 是一種知名的惡意軟體，可以劫持 Linux 的聯網設備成為被遠端控制的殭屍電腦。ShellBot（又名 PerlBot）是另一種用 Perl 開發的殭屍網路，已知以物聯網 (IoT) 設備和 Linux 伺服器為鎖定對象。

據報導在過去的幾個月裡，這兩種 Linux 惡意軟體再次捲土重來，因為觀察到威脅攻擊者利用兩個已知的遠端程式碼執行 (RCE) 漏洞（CVE-2021-35394（Realtek Jungle SDK 遠端程式碼執行漏洞）和 CVE-2022-46169（Cacti 命令注入漏洞）），以便繼續傳播 Moobot 和 Shellbot。如果攻擊嘗試成功，遭感染的機器將透過其操控的 C&C 伺服器所控制，進而可以部署更縝密的攻擊。

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：

- IRC.Backdoor.Trojan
- Linux.Mirai
- Linux.Mirai!g2
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2

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: Realtek Jungle SDK RCE CVE-2021-35394
- Attack: Cacti Unauthenticated Command Injection Vulnerability CVE-2022-46169

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。

2023/03/29

IcedID脫胎換骨，老牌銀行木馬不再鎖定銀行

IcedID 是一種老牌銀行惡意木馬程式，於 2017 年首次被發現。最近被觀察到除原始版本外還有兩個新變種。雖然以往 IcedID 主要功能是銀行木馬，但新變種卻刪除銀行功能，轉而成為後續感染鏈中（包括勒索軟體）具有呼叫或下載惡意酬載功能的載入器。多個變種已被不同的駭客組織中所濫用，包含 Emotet 背後的原始營運商。

最初 IcedID 變種包含一個初始呼叫或下載惡意酬載的功能，建立與 C&C 伺服器的連線，下載後續的惡意 DLL。第一個新變種的 Lite IcedID 已被觀察到可以傳染 Emotet。第二種變種 Forked IcedID 被少數威脅攻擊者使用，並提供一個機器人來感染電腦。這些新變種很可能會繼續被用於強化其他惡意軟體攻擊。

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：

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.2
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B

2023/03/29

Koi和CrashedTech惡意程式家族也濫用NullMixer病毒植入程式來發動攻擊

NullMixer 是一種病毒植入程式，常見於各種惡意軟體家族的有效籌載散播行動中。攻擊鏈通常涵蓋購買搜尋引擎最佳化 (SEO) 廣告、惡意廣告攻擊和社交工程，以及被植入後門常用的工具軟體和應用程式或破解版本來傳播。最近發現 NullMixer 攻擊行動一直在傳播來自 Koi 和 CrashedTech 家族的惡意酬載。一旦遭受入侵並感染該病毒植入程式，將會呼朋引伴般地招引更多惡意程式，例如：Redline 竊密程式、PseudoManuscrypt 或 Fabookie 竊密程式。

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：

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.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: Trojan.Backdoor Activity 634
- 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。

2023/03/28

被植入木馬程式的洋蔥瀏覽器被濫用於加密貨幣錢包地址剪貼簿置換偷竊行動

加密貨幣錢包劫持程式的危害日益嚴重，並且變本加厲。此類型的惡意程式大多是透過瀏覽網頁時常見的偷渡式下載傳播，攻擊者將惡意程式偽裝成常用軟體和更新程式的安裝檔案、電玩破解程式、加密貨幣挖礦程式等。最近發現，被植入木馬程式的洋蔥瀏覽器被濫用於加密貨幣錢包地址剪貼簿置換偷竊行動日益增多。洋蔥瀏覽器 (Tor Browser) 是一款免費的基於開放原始碼得網路瀏覽器，讓用戶匿名瀏覽網際網路。

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.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/03/28

散播Formbook竊密程式和Remcos遠端存取木馬，DBatLoader同流合污

DBatLoader 惡意程式最近被濫用於散播 Formbook 竊密程式和 Remcos 遠端存取木馬 (RAT) 惡意軟體。DBatLoader（又名 ModiLoader）是一種基於 Delphi 具有呼叫或下載惡意酬載功能的載入器，過去曾用於傳送各種惡意籌載，例如：Remcos、Netwire 或 Warzone RAT。已知 DBatLoader 在初始攻擊階段利用圖像隱碼術 (steganography)，並從各種公有雲儲存庫下載惡意軟體有效籌載。在最近觀察到的行動，Formbook 和 Remcos 有效籌載透過有授權 SSL 證書的 WordPress 網站傳播。攻擊者還利用各種格式的檔案（例如：.pdf、.html、.zip 或 .one）來傳遞有效籌載。

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(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：

- Downloader
- ISB.MalOneNote!gen1
- Scr.MalPbs!gen1
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- 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
- 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。

2023/03/28

MAC用戶請小心～出現MacStealer竊密程式

MacStealer 是一個新發現針對 macOS 平台的竊密程式。MacStealer 具有洩露各種機密資料的功能，包括登錄憑證、cookie、信用卡資料、文件檔等。該惡意軟體還能夠將部分竊取的訊息直接轉發到攻擊者控制的 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- 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。

2023/03/27

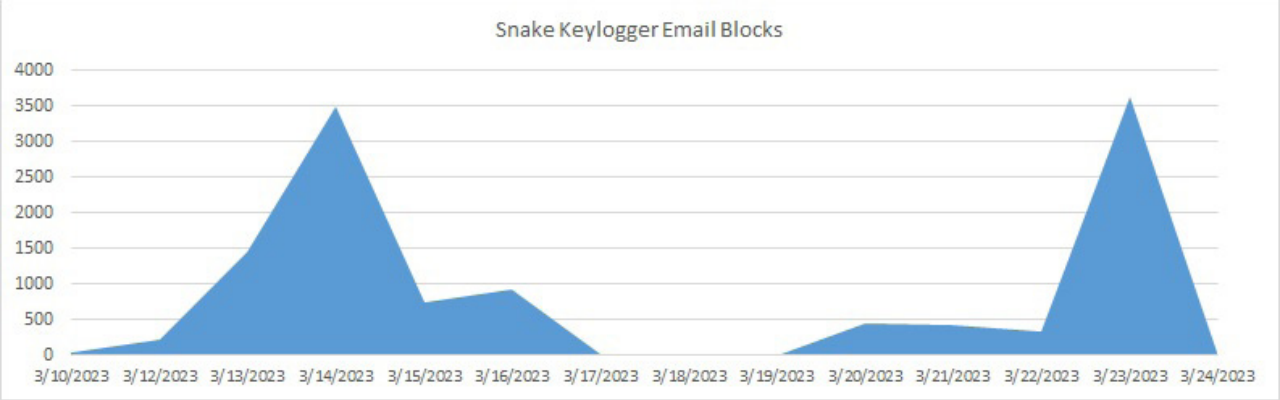
防護亮點：面對Snake鍵盤側錄程式，賽門鐵克用戶～高枕無憂

～防護亮點～

Snake 鍵盤側錄程式是一種基於 .NET 開發的惡意軟體，已經存在多年，但仍然非常流行。它主要在暗中記錄電腦上的按鍵、螢幕截圖和剪貼簿資料一起傳輸到遠端伺服器，它被世界各地的多個駭客組織和個體戶用於發動各種規模的目標式和隨機式垃圾郵件攻擊行動。

其主要的傳播方法與其他兩個非常熱門的竊密程式：Formbook 和 Agent Tesla 相似，多採用夾帶特定附件的電子郵件，例如：Microsoft Office 或 PDF 類型的檔案。電子郵件顯示常見的社交工程主旨，包括報價單、採購訂單、發票、付款、SWIFT、運輸等關鍵字。附件通常是一個壓縮檔案，在解壓和執行時，可能會採用多種規避伎倆來試圖避免檢測，包括嵌入文件、呼叫或下載遠端漏洞利用工具和加密 shellcode，最終部署該竊密程式的效籌載。

如下圖所示，Snake 鍵盤側錄程式在威脅領域中持續活躍，並且賽門鐵克擁有為數最多的防護科技。我們的首要任務是透過阻止威脅來保護我們的客戶，最好的保護策略是各種不同防護技術都能攔截到各種不同的惡意軟體，而不是特定的技術對應特定的威脅，只能攔截一種特定的攻擊（雖然我們每個防護技術也能做到 --> Trojan.SnakeKeylogger)。



圖表只是賽門鐵克全天候監控的一個時間區間，很清楚顯示攻擊行動明顯增加。

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：

- Scr.Malcode!gdn*
- Scr.Malcode!gen*
- Packed.NsisPacker!g*
- Msil.Packed.*
- Bloodhound.RTF.*
- WS.Malware.*
- WS.SecurityRisk.*
- Trojan.Gen.*
- Trojan Horse
- Trojan.SnakeKeylogger

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：Scr.Malcode!gen25、Scr.Malcode!gen34等

欲深入瞭解更多有關於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。

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。

2023/03/27

Cinoshi惡意軟體即服務(MaaS)

Cinoshi 是一種全新的惡意軟體，以惡意軟體即服務 (MaaS) 的營運模式進行推廣。該惡意軟體由多個模組組成，包括竊密程式、資料裁剪、殭屍網路和惡意挖礦程式。Cinoshi 基於 .Net 並結合多種防篡改和持久性技術。它針對網頁瀏覽器相關資料，包括 cookie、憑證和銀行資訊等。竊密程式模組還允許它從加密錢包中獲取資料、屏幕截圖或竊取各種正在運行的應用程式（例如：Discord 或 Telegram）的連線密鑰。

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
- Trojan.Gen.MBT
- 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。

2023/03/24

安卓用戶請小心～Nexus網路銀行惡意軟體

Nexus 是一種針對 Android 平台開發的新型金融惡意軟體，以惡意軟體即服務 (MaaS) 訂閱模式來銷售。原始碼的相似性和執行命令的一些重疊顯示，Nexus 可能是眾所周知的 SOVA 金融惡意軟體之進化版本。Nexus 能夠發動帳戶接管 (ATO) 攻擊，攻擊者藉助竊取的憑證、 攔截簡訊或多因子認證 (2FA) 碼來接管網路銀行或加密貨幣帳戶的所有權。

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。

2023/03/24

新變種BlackGuard，新增更多功能

BlackGuard 竊密程式於 2022 年首次被發現。該惡意軟體在地下論壇砸錢買廣告，並以惡意軟體即服務 (MaaS) 的形式出售。竊密程式能夠各類網路瀏覽器、電子郵件用戶端、即時通訊軟體和 VPN 應用程式等竊取帳密及資訊。在真實網路環境中發現的 BlackGuard 新變種新增更多功能，讓它可以劫持加密貨幣錢包並透過抽取式磁碟機或共用磁碟傳播。

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：

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
- 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。

2023/03/24

兩個惡意軟體家族：ChinaZ和ShellBot鎖定Linux SSH伺服器發動DDOS攻擊

ChinaZ分散式阻斷服務 (DDoS) 殭屍網路和 ShellBot (又名 PerlBot) 是最近在針對 Linux SSH 伺服器的攻擊中觀察到的兩個惡意軟體家族。Shellbot 是基於 Perl 的分散式阻斷服務 (DDoS) 殭屍網路，已知會採用常見密碼作暴力破解來攻擊配置不當又連上網的設備。Shellbot 使用 IRC 通訊協定進行 C&C 通訊。ChinaZ 是另一種 DDoS 殭屍網路，存在於威脅領域約 10 年之久，以攻擊 Linux 和 Windows 平台而聞名。ChinaZ 支援多種不同類型的 DDoS 攻擊，包括 SYN、UDP、ICMP 和 DNS Flood 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：

- Backdoor.IRC.Bot
- IRC.Backdoor.Trojan
- DDoS.Trojan
- Perl.Pircbot
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- 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。