


# 防護Linux供應鏈攻擊第一選擇

## 賽門鐵克重要主機防護系統：DCS~Data Center Security

2024 年 8 月 20 日發布



Linux 是資料中心作業系統的首選，因為它具有多項關鍵優勢，包括可擴充性及可靠性、安全性、自訂性、效能及成本效益。但這些系統並無法隨時跟上建議的安全修補程式，且這些修補程式的發佈頻率越來越高。這些系統也經常執行舊的應用程式，廠商的安全修補程式可能無法使用，或者為了維持業務連續性，系統可能根本不會排定修補程式更新的時間，而修補程式停機無法滿足持續營運計畫 (BCP：Business Continuity Planning)。因此，資料中心環境受到網路攻擊和供應鏈攻擊的風險可能非常高。攻破單一資料中心可存取多個相互連線的系統和應用程式，使攻擊的潛在風險難以估計。

供應鏈攻擊是惡意軟體設計者和進階持續性威脅 (APT) 駭客組織為了在其目標主機或系統中取得一席之地而採用的顯著「初始存取」策略。此方法涉及攻擊目標信任第三方服務或軟體，並將惡意程式碼注入合法的軟體更新或發行版本。

## Linux.Gomir後門程式

賽門鐵克的威脅獵手團隊 (Threat Hunter Team) 發現一個由北韓 Springtail 間諜組織 (又名 Kimsuky) 所開發的全新 Linux後門，該後門與最近一次針對南韓組織攻擊行動中使用的惡意軟體有關。該後門 (Linux.Gomir) 應該是 GoBear 後門的 Linux 版本，GoBear 後門被用於最近 Springtail 的攻擊行動中，攻擊者透過特洛伊木馬化的軟體安裝套件傳送惡意軟體。Gomir 在結構上幾乎與 GoBear 完全相同，兩者之間存在大量共用的程式碼。

Kimsuky 也稱為 Velvet Chollima，是北韓的進階持續威脅 (APT) 駭客組織，主要從事網路間諜行為。自 2012 年左右出現以來，Kimsuky 已針對韓國、日本、美國和多個歐洲國家的單位進行攻擊。該組織擅長開採濫用常用軟體中的漏洞，利用零時差漏洞和已知的安全漏洞來滲透系統。這起事件突顯保護軟體供應鏈安全的重要性，因為即使是可信賴的軟體，如果在其散佈或傳遞更新過程中的任何階段受到攻擊，也可能成為複雜網路攻擊的媒介。

## 賽門鐵克重要主機防護系統：DCS～Data Center Security有效解決方案

賽門鐵克重要主機防護系統：DCS～Data Center Security 提供全面深度的防護方法，以確保 Linux 伺服器的安全與防護。我們的解決方案能有效提供零時差防護，以對抗日益猖獗的供應鏈攻擊和其他針對 Linux 資料中心環境的網路威脅。

## 專為UNIX資料中心提供DCS內建強化政策

其出廠就內建的 Unix 保護政策，底層邏輯是最小權限／最少資源原則，可鎖定 Linux 資料中心。DCS 的亮點在於它能夠拆解 Gomir 攻擊鏈的每一步驟並在每個步驟都提供完善的保護。

## 初始存取

Gomir 惡意軟體支援從遠端伺服器接收指令的執行功能，據說是透過偽裝成韓國運輸組織應用程式的假驅動程式進行傳播。DCS 網路控制可將用戶端應用程式的邊界定義為可信賴的網路和裝置，進而限制初始存取。此外，您也可以僅允許在特定連接埠上進行網路連接。

## 惡意軟體執行

在 DCS 強化 Linux 伺服器中軟體執行控制可禁止惡意軟體從 temp 或其他可寫入位置執行。

## 持續性／常駐功能

持續性機制取決於 syscall 202 或 getegid32() 呼叫的輸出。如果程序的群組 ID 在 root 下執行，範例會將自己安裝在 crontab 或 systemd 服務中。

- **CronTab**

  範例將嘗試將其安裝到現有的 crontab 中。樣本首先會透過本機 shell 使用「crontab -l」指令取得現有的 cron 紀錄。命令輸出將被複製到新的 cron 緩衝區。此緩衝區包含新的 cron 記錄「@reboot <可執行檔路徑>」。
  新的 cron 排程為其持續機制，在系統重啟時會啟動/重啟該程序。cron 標籤項目會儲存在檔名為「cron.txt」的暫存檔中，此檔案會作為「crontab」指令的第一個參數導入。一旦 crontab 更新新項目，'cron.txt' 就會被刪除。
  在 DCS 強化的 Linux 伺服器中，軟體安裝限制和作業系統限制會阻止建立新的 crontab。

- **Systemd 服務**

  範例會取得其目前執行的可執行路徑，並在 '/var/log/syslogd' 中建立副本。在 '/etc/systemd/system/' 目錄中建立一個新的 systemd' 服務。該檔名為「syslogd.service」。這是用來混淆系統管理員，讓他們忽略這個服務，它會指向一個假的 '/var/log/syslogd'，也就是目前正在執行的樣本。這個新的服務檔案會讓 Gomir 在重新啟動系統時執行，並確保在『network』項目之後載入。這表示後門將有能力存取已初始化的網路介面。經 DCS 強化過的 Linux 伺服器中，軟體安裝限制和作業系統限制會阻止建立新的服務或服務設定檔。

## 指令與控制

本範例將透過 HTTP 使用硬體編碼的 IP 和 URL。本範例使用 HTTP 發送請求來執行指令，並將結果傳送至 C2 基礎架構。C2 可在樣本中 '.rodata 部分的 0x0834F79F' 位址找到。命令以整數值組成，表示要執行的命令類型。這部份很容易被威脅者變更，而有效負載格式的結構是四個位元組的加密金鑰和長度可變的指令。DCS 網路控制可以拒絕所有傳入或傳出的網路連線。此外，您也可以僅允許特定連接埠的網路連線。

## 解析Linux.Gomir採用TTPs在MITRE ATT&CK框架上的分類

Symantec DCS 提供下列 TTPs(策略、技術與程序) 的預設防護：

- TA0001 初始存取
- TA0002 執行
- TA0003 持續性
- TA0004 權限提升
- TA0005 防護規避
- TA0007 搜尋
- TA0009 收集
- TA0010 滲漏
- TA0011 指揮與控制
- TA0040 影響
- T1005 本機系統資料
- T1036 偽裝
- T1053 排程任務／工作
- T1053.003 Cron
- T1059 命令和腳本編譯器
- T1070 指示符移除
- T1070.004 檔案刪除
- T1071 應用層通訊協定
- T1071.001 網路通訊協定
- T1189 偷渡式入侵
- T1204 使用者執行
- T1204.002 惡意檔案
- T1217 瀏覽器資訊搜尋
- T1529 系統關機/重新開機
- T1543 建立或修改系統程序
- T1543.002 Systemd 服務
- T1546 事件觸發執行
- T1546.016 安裝套件

## 保護資料中心的環境是重中之重

企業必須優先採取安全措施，包括及時修補程式、強大的存取控制和持續監控，以降低供應鏈攻擊的風險，並保護敏感資料不被探刺利用。賽門鐵克重要主機防護系統：DCS～Data Center Security 其出廠就內建許多預設政策可套用，可確保提供強大的防護，避免資料中心伺服器和工作負載遭受不斷增加的入侵點探刺利用攻擊。

關於賽門鐵克的重要主機防護系統：DCS～Data Center Security 的完整資訊可點擊網頁說明或最新簡報檔。網頁或簡報如有說明不夠清楚的地方，歡迎與保安資訊的業務或技術顧問提供建議。

### 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好用資源。
保安資訊連絡電話：**0800-381-500**。