保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

行動網路正成為攻擊途徑 -- 我們的資料揭示了什麼

2025 年 12 月 2 日發布

點擊此處可獲取--**最完整的賽門鐵克解決方案資訊**

行動裝置已成為主要工作終端--保持連線、隨身攜帶，且持續在組織無法掌控的網路環境中運作。然而員工每日仰賴的網路，卻日益成為阻礙其工作的隱患。

在我們近期對數千起企業管理 iOS 與 Android 裝置網路事件的分析中，一個模式格外顯著：行動終端正遭受網路層面的主動探測、攔截與操控。攻擊者並非透過裝置上的惡意軟體，而是採用與攻擊企業伺服器及筆記型電腦相同的「中間人攻擊」技術手段。

當前形塑行動網路威脅模型的三大類活動：

- 網路在傳輸過程中改寫網頁內容
- 遭入侵的路由器掃描手機以尋找暴露服務
- 利用中間人攻擊截取 TLS 連線

這些行為對企業資料外洩、驗證完整性及存取路徑濫用具有直接影響--即使行動作業系統本身未遭入侵亦然。

內容操控--網路悄然改寫員工所見內容

在我們於受管裝置上觀察到的所有網路行為中，內容操控尤為突出，因其代表著對終端設備接收內容的直接干預。所有案例中，傳輸至裝置的網頁皆在途中遭修改，且由網路本身注入了 JavaScript 程式碼。

某些注入是診斷性質的，有些與政策相關，還有一些則屬不必要的侵入性操作--但其核心能力本質相同：該網路具備在使用者看見內容前，技術上篡改企業內容的能力。

飛機上與旅館網路--具備完整重寫權限的診斷腳本

在多個交通運輸及旅館 Wi-Fi 網路中，我們觀察到 HTML 回應透過中間人攻擊的代理伺服器被重寫。注入的 JavaScript 包含效能計時程式碼與遠端腳本載入功能，所有內容皆在未加密流量通過網路邊緣代理伺服器時被加入。

儘管意圖看似無害，其能力卻絕非如此。

能夠注入計時腳本的網路，同樣能注入：

- 憑證竊取程式
- 單一登入憑證攔截器
- 修改過的表單操作指令
- 遭篡改的行動網頁應用程式邏輯

從企業角度來看，任何基於網路的工作流程--無論是 VPN 登入、身分提供者重定向、SaaS 儀表板，還是內部工具--皆有可能被竄改，且不需要真的對伺服器或裝置入侵。

圖 1. Row44 代理注入的程式碼

```
<script type="text/javascript">
  var r44_btime=new Date();
  var r44_curl="http://getconnected.[redacted].com",
      r44_smu_time=1762447208.250;
  var r44_is_cached=false;
</script>
<script src="http://getconnected.[redacted].com/ltime/ltime.js"></script>
```

ISP 層級注入--鍵盤輸入與 DOM 監控

在多個 ISP 環境中，我們觀察到被注入的 JavaScript 用於強制執行家長控制設定。技術層面上，該腳本的功能遠超其必要範圍：它將 MutationObserver 附加至完整 DOM 樹，監控鍵盤輸入、文字編輯、表單互動、介面變更，並透過反覆重新注入自身以維持持久性。擷取的資料會傳回 ISP 的後端系統。

此等級的可見性將暴露：

- 員工在人力資源入口網站內的鍵盤輸入
- 輸入至企業網路應用程式的文字內容
- 雲端管理操作期間的會話行為
- 對內部儀表板或票務系統的查詢操作

此舉雖意在過濾消費者資訊，卻導致企業瀏覽活動的完整行為軌跡暴露無遺，透過未受控的第三方網路洩漏敏感資訊。

圖 2. 注入的 MutationObserver 程式碼

```
var observer = new MutationObserver(function(mutations) {
  mutations.forEach(function(mutation) {
    sendAuditData(mutation);
  });
});
observer.observe(document.documentElement, {
  childList: true,
  subtree: true,
  characterData: true,
  attributes: true
});
```

內容篡改為何對企業安全至關重要

對組織而言，風險不在於腳本本身，而在於其背後的存取模式。

一旦網路能重寫網頁：

- 單一登入與多因素驗證流程可能遭竄改
- SaaS 交易內容可能被篡改
- 伺服器無需遭入侵,內部網站也可能被修改
- 敏感輸入資料--憑證、客戶資料、企業文件--可能遭攔截
- 依賴 TLS 或伺服器信任的安全控管機制將被削弱

行動裝置高度依賴瀏覽器驅動的驗證機制。

即使裝置未受感染且企業應用程式未遭入侵，網路重寫仍構成直接的資料外洩管道。

端口掃描--本地網路遭入侵的證據

我們遙測資料中出現另一種傳統上屬於物聯網或伺服器調查的模式：針對行動裝置的入埠端口掃描。這些並非理論性掃描--而是主動嘗試在員工裝置上發現可利用服務的攻擊行為。

家用路由器作為攻擊發起者

許多掃描直接源自遭入侵的家用路由器。這些探測鎖定高價值端口：

- 資料庫服務（3306、1433）
- 遠端桌面（5800、5900）
- 傳統VPN介面（1720、1723）
- 開發者HTTP伺服器（8008、8888）

對企業而言，風險顯而易見：

- 開發人員運行本地測試伺服器可能洩露內部原型
- 工程師為測試運行資料庫恐導致資料外洩
- 過時的遠端存取工具可能意外暴露於共享網路
- 遭入侵的路由器將企業管理設備視為橫向移動目標

即使行動作業系統阻斷了連線，掃描結果本身已顯示該員工正透過遭入侵的基礎設施進行工作。

圖 3. 來自家用路由器的埠位掃描

```
Source: 192.168.1.1 (gateway_router)
SSID: [redacted]

Ports Scanned:
 3306/tcp (MySQL)
 1433/tcp (MSSQL)
 5900/tcp (VNC)
 1723/tcp (PPTP)
 8888/tcp (HTTP-alt)

Router: [redacted]
Behavior: Multi-port sequential SYN probes
```

行動熱點上的連線裝置--橫向移動企圖

在某個案例中，同一台行動 5G 路由器上的另一台裝置對員工手機發動了超過 60 次連續探測行為--此舉與惡意軟體執行網路映射及橫向移動偵察的模式相符。

這顯示使用行動熱點的員工可能在不知情的情況下，與受感染的連線裝置共享網路，使本地子網路轉變為活躍的威脅環境。

圖 4. 來自對等裝置的埠掃描

```
Source: 192.168.29.111 (peer_device)
SSID: [redacted]
Target: [redacted] 5G

Total Probes: 60 (12 per port)
Ports:
 8888/tcp
 5900/tcp
 5800/tcp
 3306/tcp
 1720/tcp

Pattern: Repeated 5-port SYN sequence every ~2s
Note: Typical lateral-movement scan from an infected peer.
```

通訊埠端口掃描對企業的影響

即使未成功發動攻擊，端口掃描事件仍揭示以下事實：

- 員工正在已遭入侵的網路內部運作。
- 企業設備正被視為潛在的企業入侵入口。
- 開發工具與測試環境加劇了資訊外洩風險。

此威脅模式特別適用於遠端辦公、出差中，或使用混合個人與企業網路配置的員工。

TLS 攔截--採用中間人攻擊技術的強制登入頁面

多數 TLS 攔截事件源自公共及交通運輸 Wi-Fi 網路實施的強制登入流程。此類網路會暫時以自身受信任的憑證鏈取代伺服器憑證，藉此強制顯示登入頁面。

圖 5. 憑證鏈被替換

```
Certificate Chain:
  [1] [redacted] Commercial Root CA 1
      FP: df:71:7e:aa:4a:d9:4e:c9:55:84:99:60:2d:48:de:5f:bc:f0:3a:25

  [2] [redacted] Server CA 01
      FP: 3c:97:cb:b4:49:1f:c8:d6:3d:12:b4:89:0c:28:54:81:64:19:8e:db

  [3] [redacted].com
      Org: [redacted] Co.
      FP: d0:3d:36:0d:be:a6:dd:76:d0:27:d4:3c:a8:8c:d2:75:93:45:93:c7

Network Path:
  BSSID: 24:1f:bd:bb:ca:b0
  Gateway: 10.194.100.3
  Encryption: 0 (open)
```

這是預期中的行為--但僅限於可信賴的環境中。

技術上而言，此機制與惡意中間人攻擊採用的原理相同：

- 憑證替換
- 路徑上 TLS 解密
- 使用不同根憑證重新加密

在正常受控網路中，此為正常註冊流程。

在未受信任的網路中，相同模式則顯示主動攔截行為。

對企業風險團隊而言，這意味著：

- 身分供應商的重定向可能遭攔截
- 受 TLS 保護的企業網路應用程式可能遭操控
- 基於 Cookie 的會話可能遭暴露
- 員工可能無法視覺化偵測異常狀況

即使是合法的 TLS 攔截，也會帶來可量化的風險，包括資料外洩、身分遭竊取以及會話遭操控。

強化行動裝置安全防護：SEP Mobile 解決方案

隨著行動終端面臨日益複雜的網路威脅，企業需要超越裝置狀態與應用程式安全管理的全面防護。賽門鐵克終端防護行動版 (SEP Mobile) 為企業提供關鍵可視性與防禦能力，有效抵禦現實世界中的網路操控、TLS 攔截及遭入侵的本地基礎設施--這些正是當今多數攻擊的發源地。

採用 SEP Mobile 可賦予安全團隊偵測惡意網路、防止資料外洩，並在任何工作場所保護員工裝置的能力。轉換過程簡便、成效立竿見影，其長期安全價值更是毋庸置疑。

了解 SEP Mobile 如何保護您的行動工作團隊免受當今網路層威脅的侵害。

點擊此處深入瞭解賽門鐵克行動端點防護解決方案。

原廠網址：https://www.broadcom.com/support/security-center/protection-bulletin/protection-highlight-mobile-networks-are-becoming-attack-paths-what-our-data-reveals

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，以及基於比原廠更熟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求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。