

CHUYÊN GIA MẠNG MỸ NGHI NGỜ MODEM TRÊN CẦU DO TRUNG QUỐC SẢN XUẤT

12/03/2024



Thiết bị liên lạc được tìm thấy trên cần cầu do Trung Quốc sản xuất ở Mỹ đã làm dấy lên lo ngại mới về hoạt động gián điệp.

Thiết bị do ZPMC thuộc sở hữu nhà nước, một trong những nhà chế tạo cần cầu lớn nhất thế giới, sản xuất, đã bị giám sát chặt chẽ tại các cảng của Hoa Kỳ.

Một cuộc điều tra của Quốc hội đã tìm thấy, tại một cảng, 12 modem di động trên thiết bị cần cầu và một modem khác trong phòng máy chủ của cảng; Chính quyền cảng khẳng định họ không nói rõ rằng cần cầu có những khả năng này và nói rằng họ không biết tại sao thiết bị liên lạc lại được lắp đặt.

Trong khi các cảng đang bị điều tra chưa được xác định, cần cầu của ZPMC được biết là hoạt động tại các cảng ở Los Angeles, New York/New Jersey, Oakland, Houston, Miami và nhiều cảng khác.

Hiệp hội Chính quyền Cảng Hoa Kỳ (AAPA) trước đây đã bác bỏ những tuyên bố như vậy là 'sự báo động của giới truyền thông', cho biết vào giữa năm ngoái rằng "các cần cầu hiện đại rất nhanh và tinh vi, nhưng thậm chí chúng còn không thể theo dõi nguồn gốc, điểm đến hoặc bản chất của hàng hóa". vận chuyển hàng hóa".

Nhưng mối lo ngại là, chính phủ Trung Quốc không chỉ có thể sử dụng cần cầu để thu thập dữ liệu chiến lược về hoạt động vận chuyển hàng hóa của Mỹ, mà còn trong trường hợp xảy ra xung đột lớn - chẳng hạn như nỗ lực sáp nhập Đài Loan của Trung Quốc - một 'công tắc tiêu diệt' của Trung Quốc. có thể phong tỏa nước Mỹ một cách hiệu quả.

Chuẩn đô đốc John Vann, người đứng đầu bộ chỉ huy mạng của Cảnh sát biển Hoa Kỳ, phát biểu trong các phiên điều trần vào tuần trước: "Tôi có thể nói là chúng tôi đã tìm thấy các lỗ hổng, lỗ hổng... theo thiết kế, những cần cầu này có thể được điều khiển, bảo trì và lập trình từ các địa điểm xa". Tuy nhiên, ông nói thêm rằng "phần mềm độc hại hoặc phần mềm kiểu ngựa Trojan" vẫn chưa được tìm thấy.

Đặc biệt trong thời đại Internet vạn vật (IoT), không có gì lạ khi các thiết bị hạng nặng được trang bị hệ thống thông tin liên lạc, vừa để thu thập dữ liệu để người vận hành sử dụng vừa để trao đổi dữ liệu với nhà sản xuất nhằm mục đích giám sát tình trạng và bảo trì.

Khả năng giám sát và điều khiển cần cầu và các thiết bị cảng khác bằng kết nối từ xa — và không cần con người vận hành — cho đến nay vẫn được các cảng coi là niềm tự hào, trong khi các nhà sản xuất thiết bị cảng khác như Konecranes, Kalmar và Liebherr đều cung cấp các khả năng tương tự.

Cần cầu cảng ZPMC hoạt động hoàn toàn bằng điều khiển từ xa có thể được tìm thấy tại một số bến container lớn nhất thế giới, bao gồm Jebel Ali, Singapore, Rotterdam và không có gì đáng ngạc nhiên là Thượng Hải.

Tuy nhiên, Mark Green, chủ tịch Ủy ban An ninh Nội địa Hạ viện, cáo buộc Trung Quốc “đào sâu” một cách có hệ thống vào cơ sở hạ tầng của Mỹ.

Nhưng Mao Ning, người phát ngôn của Bộ Ngoại giao Trung Quốc, cho biết: “Cáo buộc rằng cần cầu do Trung Quốc sản xuất gây ra rủi ro an ninh là hoàn toàn vô căn cứ. Chúng tôi kiên quyết phản đối việc Mỹ... lạm dụng quyền lực nhà nước để truy đuổi các sản phẩm và công ty Trung Quốc. Việc vũ khí hóa các vấn đề kinh tế và thương mại sẽ làm trầm trọng thêm rủi ro an ninh trong chuỗi cung ứng và công nghiệp toàn cầu và chắc chắn sẽ gây phản tác dụng.”

Nguồn: <https://theloadstar.com/us-cyber-experts-probe-suspect-modems-on-china-made-cranes/>