วันที่ 12 กันยายน 2568

กลุ่มแฮ็กเกอร์ APT41 ที่เชื่อมโยงกับจีนโจมตีเจ้าหน้าที่การค้าสหรัฐฯ ท่ามกลางการเจรจาในปี 2025

คณะกรรมาธิการคัดเลือกสภาผู้แทนราษฎรจีน ได้ออกประกาศเตือนอย่างเป็นทางการถึงการโจมตีทางไซเบอร์ที่กำลังเกิดขึ้น โดยมีการมุ่งเป้าอย่างเฉพาะเจาะจงและเชื่อมโยงกับสาธารณรัฐประชาชนจีน (PRC) ในช่วงการเจรจาการค้าระหว่างสหรัฐฯ–จีนที่เต็มไปด้วยความตึงเครียด

“การโจมตีเหล่านี้มีเป้าหมายเพื่อเจาะระบบขององค์กรและบุคคลที่เกี่ยวข้องกับนโยบายการค้าระหว่างสหรัฐฯ–จีนและการทูต รวมถึงหน่วยงานรัฐบาลสหรัฐฯ, องค์กรธุรกิจสหรัฐฯ, สำนักงานกฎหมายในกรุงวอชิงตัน ดี.ซี., สถาบันวิจัย และอย่างน้อยหนึ่งรัฐบาลต่างชาติ” แถลงการณ์ของคณะกรรมาธิการระบุ

คณะกรรมาธิการกล่าวเพิ่มเติมว่า กลุ่มผู้ต้องสงสัยที่เชื่อมโยงกับจีนได้ปลอมตัวเป็นสมาชิกสภาคองเกรสจากพรรครีพับลิกัน จอห์น โรเบิร์ต มูลีนาร์ (John Robert Moolenaar) เพื่อส่งอีเมลฟิชชิ่งไปยังผู้ที่ไว้ใจได้ โดยมีเป้าหมายเพื่อหลอกให้พวกเขาเปิดไฟล์และลิงก์ ซึ่งจะเปิดทางให้ผู้โจมตีเข้าถึงระบบและข้อมูลที่อ่อนไหวโดยที่เหยื่อไม่รู้ตัว

กลไกการโจมตีและการเชื่อมโยงกับ APT41

เป้าหมายสูงสุดของการโจมตีคือการขโมยข้อมูลสำคัญ ด้วยการอาศัยช่องโหว่ของซอฟต์แวร์และบริการคลาวด์เพื่อปกปิดร่องรอยการกระทำ วิธีการลักษณะนี้มักถูกใช้โดยกลุ่มแฮกเกอร์ที่หนุนหลังโดยรัฐเพื่อหลีกเลี่ยงการถูกตรวจจับ

“นี่เป็นอีกหนึ่งตัวอย่างของปฏิบัติการไซเบอร์เชิงรุกของจีนที่ออกแบบมาเพื่อขโมยกลยุทธ์ของสหรัฐฯ และนำมาใช้ต่อสู้กับสภาคองเกรส, รัฐบาล และประชาชนอเมริกัน” มูลีนาร์ ซึ่งดำรงตำแหน่งประธานคณะกรรมาธิการคัดเลือกด้านพรรคคอมมิวนิสต์จีน (CCP) กล่าว “เราจะไม่ยอมให้ถูกข่มขู่ และจะเดินหน้าทำงานเพื่อปกป้องอเมริกาต่อไป”

แถลงการณ์นี้มีขึ้นไม่กี่วันหลังจากรายงานของวอลสตรีทเจอร์นัลเมื่อวันที่ 7 กันยายน 2025 ซึ่งเปิดเผยว่า กลุ่มการค้า, สำนักงานกฎหมาย และหน่วยงานรัฐบาลสหรัฐฯ หลายแห่งได้รับอีเมลจากมูลีนาร์ โดยขอความคิดเห็นเกี่ยวกับมาตรการคว่ำบาตรจีน เนื้อหาในอีเมลเขียนไว้ว่า “ความคิดเห็นของคุณมีความสำคัญ” พร้อมแนบไฟล์ร่างกฎหมาย ซึ่งเมื่อเปิดใช้งานแล้วจะปล่อยมัลแวร์เพื่อเก็บข้อมูลที่สำคัญและสร้างช่องทางการเข้าถึงระบบขององค์กรเป้าหมายในระยะยาว

การโจมตีนี้เชื่อว่าเป็นฝีมือของ APT41 กลุ่มแฮกเกอร์ที่มีชื่อเสียงในด้านการโจมตีภาคส่วนต่างๆ และภูมิภาคต่างๆ เพื่อจารกรรมข้อมูลทางไซเบอร์

ข้อโต้แย้งจากจีนและมุมมองของผู้เชี่ยวชาญ

“จีนยืนหยัดคัดค้านและปราบปรามการโจมตีและอาชญากรรมทางไซเบอร์ทุกรูปแบบ” สถานทูตจีนในกรุงวอชิงตัน กล่าวกับรอยเตอร์ในแถลงการณ์ “เรายังคัดค้านการกล่าวหาใส่ร้ายผู้อื่นโดยปราศจากหลักฐานที่ชัดเจน”

“ด้วยการปลอมเป็น ส.ส. มูลินาร์ (R-MI) ซึ่งเป็นผู้วิจารณ์ปักกิ่งอย่างตรงไปตรงมา ทำให้ผู้โจมตีสร้างความเร่งด่วนและความน่าเชื่อถือที่กระตุ้นให้มีการตอบสนองอย่างรวดเร็ว” เยจิน จาง รองประธานฝ่ายกิจการรัฐบาลของ Abnormal AI กล่าวกับ The Hacker News

“การสื่อสารทางการเมืองไม่ได้จำกัดอยู่แค่การใช้อุปกรณ์หรือบัญชีอย่างเป็นทางการ คู่ต่อสู้ที่มีความเชี่ยวชาญเข้าใจความจริงข้อนี้ และใช้ประโยชน์อย่างเต็มที่ ด้วยการปลอมตัวเป็นเจ้าหน้าที่ที่น่าเชื่อถือผ่านช่องทางส่วนตัวหรือช่องทางที่ไม่เป็นทางการ ทำให้สามารถเลี่ยงระบบรักษาความปลอดภัยแบบเดิมๆ ได้ และยังเสริมความน่าเชื่อถือมากขึ้นอีกด้วย”

การโจมตีที่เชื่อมโยงกัน

คณะกรรมาธิการยังระบุว่า การโจมตีในครั้งนี้มีความเชื่อมโยงกับการโจมตีฟิชชิ่งเมื่อเดือนมกราคม 2025 ที่มุ่งเป้าบุคลากรของคณะกรรมาธิการเอง โดยในครั้งนั้นมีการส่งอีเมลปลอมที่อ้างว่าเป็นตัวแทนประจำทวีปอเมริกาเหนือของ ZPMC บริษัทผู้ผลิตเครนของรัฐจีน การโจมตีใช้การแจ้งเตือนปลอมจากระบบแชร์ไฟล์ เพื่อหลอกให้ผู้รับคลิกลิงก์ที่ออกแบบมาเพื่อขโมยรหัสล็อกอินของ Microsoft 365 อีกทั้งยังมีการใช้เครื่องมือสำหรับนักพัฒนาในการสร้างเส้นทางซ่อนเร้น เพื่อแอบส่งข้อมูลกลับไปยังเซิร์ฟเวอร์ที่ผู้โจมตีควบคุม

นอกจากนี้ คณะกรรมาธิการยังได้เผยแพร่รายงานการสอบสวนเมื่อเดือนกันยายน 2024 ที่กล่าวหา ZPMC ว่า การครองตลาดเครนตู้คอนเทนเนอร์ (STS) ของบริษัท อาจถูกใช้เป็น “ม้าไม้เมืองทรอย” ที่ช่วยให้พรรคคอมมิวนิสต์จีนและรัฐบาลจีนสามารถแทรกแซงและควบคุมอุปกรณ์และเทคโนโลยีทางทะเลของสหรัฐฯ ได้เมื่อใดก็ตามที่พวกเขาต้องการ

“จากรูปแบบการโจมตี, เวลา, และวิธีการที่ใช้ และเมื่อเปรียบเทียบกับการประเมินจากภายนอก คณะกรรมาธิการเชื่อว่ากิจกรรมเหล่านี้เป็นการจารกรรมไซเบอร์ที่ได้รับการสนับสนุนจากรัฐจีน มีเป้าหมายเพื่อแทรกแซงกระบวนการกำหนดนโยบายและกลยุทธ์การเจรจาของสหรัฐฯ เพื่อสร้างความได้เปรียบด้านการค้าและการต่างประเทศ” แถลงการณ์สรุป

ข้อมูลอ้างอิง

Sep 10, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/09/china-linked-apt41-hackers-target-us.html