วันที่ 4 กันยายน 2568

แฮ็กเกอร์อิหร่านเจาะอีเมลสถานทูตกว่า 100 บัญชี ใช้การฟิชชิงโจมตีนักการทูตทั่วโลก

นักวิจัยด้านความปลอดภัยได้ออกมาเปิดเผยว่า กลุ่มผู้โจมตีขั้นสูงที่เชื่อมโยงกับอิหร่าน กำลังดำเนินการแคมเปญ สเปียร์ฟิชชิง แบบ “ประสานงานกัน” และ “หลายระลอก” โดยมุ่งเป้าไปที่สถานทูตและกงสุลในยุโรปและภูมิภาคอื่นๆ ทั่วโลก

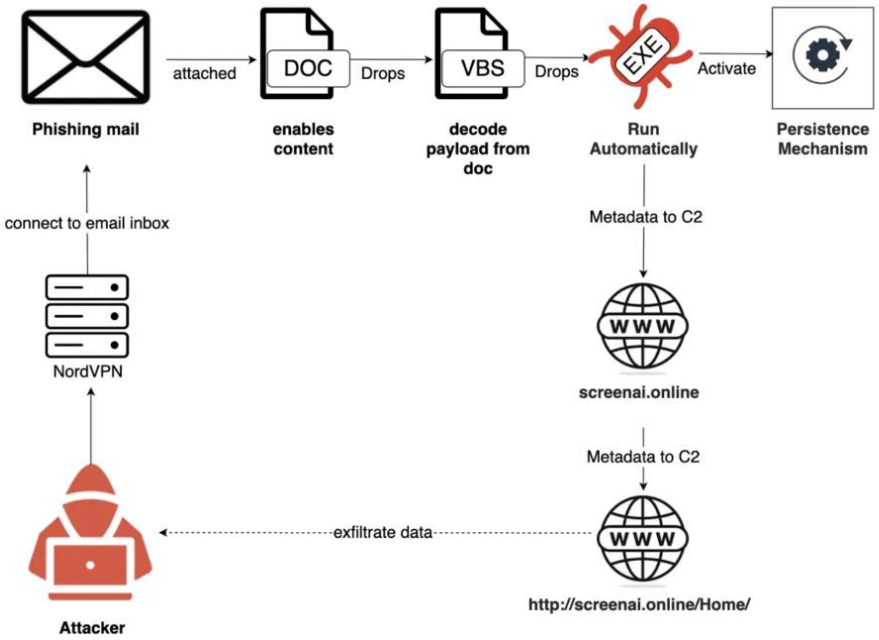
บริษัทความปลอดภัยไซเบอร์ Dream จากอิสราเอลระบุว่ากิจกรรมนี้มีความเชื่อมโยงกับผู้ปฏิบัติการที่ฝักใฝ่อิหร่าน ซึ่งเกี่ยวข้องกับการโจมตีไซเบอร์เชิงรุกในวงกว้างของกลุ่มที่รู้จักกันในชื่อ Homeland Justice

“มีการส่งอีเมลไปยังหน่วยงานรัฐบาลหลายแห่งทั่วโลก โดยปลอมแปลงให้เหมือนเป็นการสื่อสารทางการทูตจริง” บริษัทกล่าว “หลักฐานชี้ว่ามีความพยายามสอดแนมในระดับภูมิภาคที่มุ่งเป้าไปยังหน่วยงานการทูตและรัฐบาล ในช่วงที่สถานการณ์ทางภูมิรัฐศาสตร์ตึงเครียด”

กลไกการโจมตีที่ซับซ้อน

รูปแบบการโจมตีใช้เทคนิค สเปียร์ฟิชชิง โดยส่งอีเมลที่อ้างอิงถึงความขัดแย้งทางการเมืองระหว่างอิหร่านและอิสราเอล พร้อมไฟล์ Microsoft Word ที่เมื่อเปิดแล้วจะแจ้งให้ผู้รับ “Enable Content” เพื่อรันมาโคร VBA ที่ซ่อนอยู่ ซึ่งจะใช้ในการติดตั้งมัลแวร์

ตามข้อมูลของ Dream อีเมลเหล่านี้ถูกส่งไปยังสถานทูต กงสุล และองค์กรระหว่างประเทศในตะวันออกกลาง, แอฟริกา, ยุโรป, เอเชีย และอเมริกา แสดงให้เห็นว่าการโจมตีครั้งนี้มีขอบเขตกว้าง โดยสถานทูตในยุโรปและองค์กรในแอฟริกาเป็นกลุ่มที่ถูกโจมตีหนักที่สุด



ข้อความฟิชชิงถูกส่งมาจากบัญชีอีเมลที่ถูกแฮ็กจำนวน 104 บัญชี ซึ่งเป็นของเจ้าหน้าที่และหน่วยงานที่มีลักษณะคล้ายรัฐบาล เพื่อเพิ่มความน่าเชื่อถือ โดยบางส่วนถูกส่งจากกล่องจดหมายของกระทรวงการต่างประเทศโอมานในปารีส (@fm.gov.om)

“เนื้อหาล่อเหยื่อในอีเมลอ้างถึงการติดต่อที่เร่งด่วนจากกระทรวงการต่างประเทศ แสดงอำนาจ และอาศัยพฤติกรรมปกติของผู้ใช้ที่มักเปิดใช้งานมาโครเพื่อเข้าถึงเอกสาร สิ่งเหล่านี้เป็นลักษณะของปฏิบัติการสอดแนมที่ถูกวางแผนมาอย่างดีและตั้งใจปกปิดตัวตนผู้โจมตี” Dream กล่าว

เป้าหมายสุดท้ายของการโจมตีคือการใช้มาโคร VBA ติดตั้งไฟล์ที่สามารถคงอยู่ในระบบ, ติดต่อกับเซิร์ฟเวอร์ควบคุม (C2) และดึงข้อมูลของระบบออกมา

การเชื่อมโยงกับกลุ่มแฮกเกอร์

บริษัทความปลอดภัยไซเบอร์ ClearSky ซึ่งได้เปิดเผยรายละเอียดบางส่วนเมื่อปลายเดือนที่แล้ว กล่าวว่าอีเมลฟิชชิงถูกส่งไปยังหลายกระทรวงการต่างประเทศ

“เทคนิคการพรางตัวแบบเดียวกันนี้เคยถูกกลุ่มผู้โจมตีไซเบอร์จากอิหร่านใช้ในปี 2023 เมื่อพวกเขาโจมตี Mojahedin-e-Khalq ในแอลเบเนีย” บริษัทกล่าวบน X “เราประเมินด้วยความมั่นใจในระดับปานกลางว่ากิจกรรมครั้งนี้เชื่อมโยงกับกลุ่มผู้โจมตีไซเบอร์อิหร่านกลุ่มเดียวกัน”

ข้อมูลอ้างอิง

Sep 3, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/09/iranian-hackers-exploit-100-embassy.html