ประจำวันพุธที่ 8 มิถุนายน 2565

Microsoft เข้ายึด 41 โดเมนที่ใช้โดยกลุ่ม APT Bohrium ซึ่งเกี่ยวข้องกับอิหร่าน

Digital Crimes Unit (DCU) ของ Microsoft ประกาศว่าได้ดำเนินการทางกฎหมายเพื่อขัดขวางการดำเนินการฟิชชิ่งที่เชื่อมโยงไปยังกลุ่ม APT Bohrium ที่มีส่วนเกี่ยวข้องกับอิหร่าน โดยได้ยึดโดเมนที่ผู้คุกคามใช้ในการโจมตี spear-phishing โดยมุ่งเป้าไปที่องค์กรในภาคเทคโนโลยี การขนส่ง รัฐบาล และการศึกษาที่ตั้งอยู่ในสหรัฐอเมริกา ตะวันออกกลาง และอินเดีย โดย Microsoft ยึดเว็บไซต์ 41 แห่ง รวมถึง ".com" ".info" ".live" ".me" ".net" ".org" และ ".xyz" ที่ใช้ในการโจมตี

โดยทางกลุ่ม APT ดังกล่าว ได้สร้างโปรไฟล์โซเชียลมีเดียปลอม ซึ่งมักแอบอ้างเป็นผู้จัดหางาน จากนั้นจึงใช้เพื่อหลอกล่อเป้าหมายทำการส่งข้อมูลส่วนบุคคลให้กับทางกลุ่ม และเมื่อได้รับข้อมูลนี้จากเหยื่อแล้ว Bohrium ส่งอีเมลฟิชชิ่งไปยังเหยื่อที่มีลิงก์ ซึ่งเมื่อคลิกแล้วจะเริ่มต้นกระบวนการติดไวรัสสำหรับคอมพิวเตอร์ของเป้าหมาย

เมื่อต้นเดือน Microsoft ประกาศว่าได้บล็อกการโจมตีหลายครั้งโดยมุ่งเป้าไปที่องค์กรในอิสราเอล ซึ่งดำเนินการโดยกลุ่มแฮกเกอร์ในเลบานอน ซึ่งรู้จักในชื่อ POLONIUM โดย POLONIUM นี้ได้พุ่งเป้าหรือเข้าโจมตีองค์กรของอิสราเอลมากกว่า 20 แห่ง และองค์กรระหว่างรัฐบาลหนึ่งแห่งที่ดำเนินงานในเลบานอน ในช่วงสามเดือนที่ผ่านมา ตั้งแต่เดือนกุมภาพันธ์ การโจมตีได้กำหนดเป้าหมายองค์กรในอุตสาหกรรมการผลิตที่สำคัญ ไอที และอุตสาหกรรมการป้องกันประเทศของอิสราเอล

ที่มาของข่าว : https://securityaffairs.co/wordpress/132002/apt/microsoft-seized-bohrium-apt-domains.html