สรุปข่าวสาร
IT Security ประจำสัปดาห์
วันที่ 22 - 28 พฤศจิกายน พ.ศ. 2565

QBot ใช้ช่องโหว่ zero-day บน Windows
เพื่อ bypass Mark of the Web (MoTW) ฟีเจอร์ และติดตั้งมัลแวร์ลงบนเครื่องเหยื่อได้

พบการโจมตีแบบ phishing รูปแบบใหม่ โดยการใช้ช่องโหว่ Zero-day บน Windows เพื่อแพร่กระจายมัลแวร์ Qbot โดยทำให้ Windows ไม่แสดงคำเตือนด้านความปลอดภัย (Mark of the Web) เมื่อผู้ใช้งานพยายามเปิดไฟล์ ซึ่งโดยปกติ Windows จะแสดงคำเตือนลักษณะดังกล่าวเมื่อมีการเปิดไฟล์ที่ต้องสงสัยที่ถูกดาวน์โหลดมาจากอินเทอร์เน็ต หรือ จากไฟล์แนบในอีเมล ซึ่งจะถูกเรียกว่า Mark of the Web (MoTW) Microsoft รับทราบเกี่ยวกับช่องโหว่ Zero-day ดังกล่าว และขณะนี้มีแคมเปญของมัลแวร์ตัวอื่น ๆ กำลังใช้ประโยชน์จากช่องโหว่นี้ด้วยเช่นเดียวกัน โดยคาดว่าช่องโหว่ดังกล่าวน่าจะได้รับการแก้ไขในการอัปเดต Patch รอบเดือนธันวาคม 2022

ข้อมูลจาก : < https://www.i-secure.co.th/2022/11/qbot-ใช้ช่องโหว่-zero-day-บน-windows-เพื่อ-bypass-mark-o/ > 25/11/2022

แก๊งค์แรนซั่มแวร์ Daixin จารกรรมข้อมูลลูกค้าและพนักงาน AirAsia ไปมากถึง 5 ล้านรายการ

กลุ่มอาชญากรไซเบอร์ชื่อ Daixin Team ได้ปล่อยตัวอย่างข้อมูลที่เป็นของบริษัทแอร์เอเชียสายการบินโลว์คอสสัญชาติมาเลเซียที่เรารู้จักกันดี บนพอทัลเว็บมืดของตัวเอง หลังจากที่บริษัทตกเป็นเหยื่อแรนซั่มแวร์เมื่อประมาณ วันที่ 11 - 12 พฤศจิกายน กลุ่มนี้อ้างว่าได้ข้อมูลส่วนตัวของผู้โดยสารและพนักงานบริษัทมากกว่า 5 ล้านคน ซึ่งตัวอย่างข้อมูลหลุดที่อัพโหลดขึ้นมานั้นเป็นรายละเอียดของผู้โดยสารพร้อมรหัสบุ๊กกิ้ง รวมทั้งข้อมูลส่วนตัวที่เกี่ยวข้องกับเจ้าหน้าที่แอร์เอเชียด้วย ทั้งนี้โฆษกของแก๊งค์ไดซินได้ให้ข่าวกับ DataBreaches.net ว่าสามารถเจาะระบบได้ง่ายๆ เพราะระบบแอร์เอเชียไม่ได้รัดกุม และ “เป็นเครือข่ายองค์กรที่ยุ่งเหยิง ไม่เป็นระบบ” สำหรับกลุ่ม Daixin Team นี้กำลังเป็นที่เฝ้าระวังของหน่วยงานด้านข่าวกรองและความมั่นคงทางไซเบอร์ของสหรัฐฯ จากการออกประกาศเตือนการโจมตีโดยเฉพาะในกลุ่มบริการทางการแพทย์

ข้อมูลจาก : <https://www.enterpriseitpro.net/daixin-ransomware-gang-steals-5-million-airasia-passengers// > 23/11/2022

หน่วยงานรัฐบาลกลางสหรัฐฯ ถูกแฮ็กจากแฮ็กเกอร์ชาวอิหร่านด้วยช่องโหว่ Log4Shell

FBI และ CISA เปิดเผยข้อมูลของกลุ่มแฮ็กเกอร์ที่คาดว่าได้รับการสนับสนุนจากรัฐบาลอิหร่าน ในเหตุการณ์การโจมตีองค์กร Federal Civilian Executive Branch (FCEB) เพื่อติดตั้งมัลแวร์ XMRig cryptomining ซึ่งในครั้งนี้ผู้โจมตีเข้าสู่เครือข่ายผ่านเซิร์ฟเวอร์ VMware Horizon ที่ไม่ได้แพตช์ ผ่านช่องโหว่ Log4Shell (CVE-2021-44228) Log4Shell สามารถถูกใช้ในการโจมตีจากระยะไกลเพื่อเข้าถึงเซิร์ฟเวอร์ที่มีช่องโหว่ จากนั้นมันจะทำการ lateral Movement เพื่อเข้าถึงระบบอื่น ๆ ในองค์กรเพื่อขโมยข้อมูลที่สำคัญ

แนวทางการป้องกัน

- อัปเดตระบบ VMware Horizon และ Unified access gateway (UAG) ที่ได้รับผลกระทบเป็นเวอร์ชันล่าสุด
- ลดจำนวนระบบที่เป็น Internet-facing ให้เหลือน้อยที่สุด
- ดำเนินการทดสอบและตรวจสอบ Security Program ขององค์กรให้สามารถตรวจจับภัยคุกคามได้
- ดำเนินการทดสอบความปลอดภัยที่มีอยู่ขององค์กรโดยใช้เทคนิค ATT&CK

ข้อมูลจาก : < https://www.i-secure.co.th/2022/11/แฮ็กเกอร์รัสเซียใช้แรน/ > 16/11/2022