สรุปข่าวสาร IT Security ประจำสัปดาห์

วันที่ 1-7 พฤศจิกายน พ.ศ.2565

1 มีช่องโหว่ร้ายแรงมากบน Juniper Junos OS ที่กระทบอุปกรณ์เครือข่ายระดับองค์กร

มีการเปิดเผยช่องโหว่ระดับร้ายแรงมากหลายรายการบนอุปกรณ์ของ Juniper Networks ที่อาจทำให้เข้าไปรันโค้ดอันตรายได้ ที่ร้ายแรงที่สุดได้แก่ช่องโหว่แบบ Deserialization ของไฟล์ Archive uu PHP แบบยืนยันตนล่วงหน้าจากระยะไกล เป็นช่องโหว่ภายใต้รหัส CVE-2022-22241 คะแนนความร้ายแรงอยู่ที่ 8.1 ตามสเกลของ CVSS พบในส่วนของ J-Web บน Junos OS เป็นช่องโหว่แบบ XPATH Injection ที่เปิดให้ผู้โจมตีจากระยะไกลที่ยืนยันตนได้ สามารถจารกรรมและควบคุมเซสชั่นแอดมินบน Junos OS ได้ เป็นต้น

ข้อมูลจาก :

< https://www.enterpriseitpro.net/high-severity-flaws-in-juniper-junos-os-affect-enterprise-networking-devices/ > 4/11/2022

2 Emotet Botnet กลับมาเริ่มโจมตีอีกครั้ง

nEmotet เป็นมัลแวร์ที่พยายามกระจายตัวผ่านทาง Phishing Campaign ด้วยการส่งไฟล์ Excel หรือ Word ให้ผู้ใช้งานเปิดอ่าน โดยจะทำการเข้าสู่เครื่องเป้าหมายผ่านทางการเปิดใช้งาน Macro หลังจากนั้นจะฝังตัวอยู่ในเครื่องเพื่อค้นหาไฟล์และอีเมลเพื่อใช้ในการส่งสแปมเมลต่อไป หรือแม้กระทั่งติดตั้งแรนซัมแวร์ลงในเครื่องของเหยื่อ ล่าสุดผู้เชี่ยวชาญทางด้านความปลอดภัยตรวจพบการเคลื่อนไหวของ Emotet อีกครั้ง หลังจากที่หยุดการโจมตีไปกว่า 5 เดือน มีการเริ่มส่งสแปมเมล กระจายออกไปทั่วโลก พร้อมแนบไฟล์ Excel และตั้งชื่อไฟล์ในหลายรูปแบบ เช่น Invoice, Scan และ Electronic Form เพื่อหลอกล่อให้เหยื่อเปิดไฟล์ ผู้ใช้งานจึงควรเพิ่มความระมัดระวังในการเปิดอ่านอีเมลหรือดาวน์โหลดไฟล์จากแหล่งต่างๆ

ข้อมูลจาก : <https://www.techtalkthai.com/emotet-botnet-reattack-after-5-months-break/ > 3/11/2022

3 Dropbox แจ้งเหตุข้อมูลรั่วไหลจากการที่พนักงานถูก Phishing

Dropbox ได้เปิดเผยเหตุการณ์ที่องค์กรตกเป็นเหยื่อของ Phishing จนทำให้ Repository ถูกคนร้ายเข้ามาขโมยข้อมูลได้ จากการสืบสวนพบว่าโค้ดที่ถูกเข้าถึงมี Credential อยู่บ้างและ API Keys ที่ใช้โดยนักพัฒนาของเรา รวมถึงไลบรารีจาก Third-party ที่นำมาปรับปรุงใช้ภายใน ไปจนถึงโค้ด Prototype เครื่องมือบางส่วน ไฟล์คอนฟิคของทีมด้านความมั่นคงปลอดภัย อย่างไรก็ตามไม่มีโค้ดหลักของแอปหรือ Infrastructure เนื่องจากมีการจำกัดการเข้าถึงเหล่านั้นอย่างเข้มข้น มีข้อมูลบางส่วนที่กระทบถึงบุคคลหลายพันชื่อ โดยเป็นชื่อและอีเมลของพนักงาน รวมถึงลูกค้า Dropbox ทั้งปัจจุบัน และในอดีต เซลล์ และVendor เป็นอีกหนึ่งเหตุการณ์ที่ Phishing ทำงานได้สำเร็จแม้กับบริษัทเทคโนโลยีรายใหญ่ก็ตกเป็นเหยื่อได้

ข้อมูลจาก : < https://www.techtalkthai.com/dropbox-breached-by-phishing-attack-102022/ > 2/11/2022