วันที่ 12 กรกฎาคม 2567

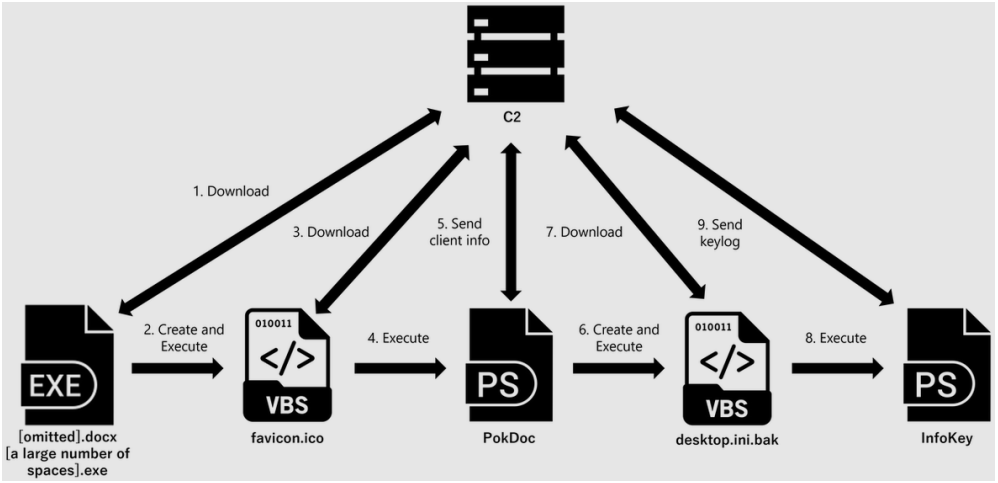
ญี่ปุ่นเตือนการโจมตีที่เชื่อมโยงกับกลุ่มแฮ็กเกอร์ Kimsuky ของเกาหลีเหนือ

Executive Summary

ทางศูนย์ CSOC พบรายงานการแจ้งเตือนจาก Japan's Computer Emergency Response Team Coordination Center (JPCERT/CC) ที่ได้เตือนว่าองค์กรของญี่ปุ่นกำลังถูกเป็นเป้าหมายในการโจมตีโดยกลุ่ม Kimsuky ของเกาหลีเหนือในฐานะกลุ่มภัยคุกคามขั้นสูง (APT) ที่ได้ดำเนินการกำหนดกลุ่มเป้าหมายในการโจมตีทั่วโลก เพื่อรวบรวมข้อมูลที่เกี่ยวกับรัฐบาลเกาหลีเหนือ เป็นที่รู้กันว่ากลุ่มผู้โจมตีนี้ได้ใช้วิธีการโจมตีในรูปแบบ social engineering และ phishing เพื่อเข้าถึงเครือข่าย และนำไปใช้งานเพื่อกำหนดการทำงานของมัลแวร์ที่จะใช้ในการขโมยข้อมูลและเพื่อการดำรงอยู่ในเครือข่าย

Starts with phishing

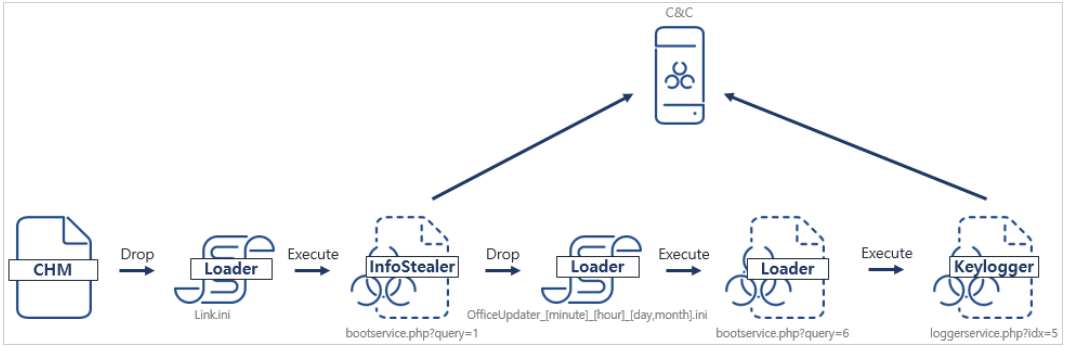
ผู้โจมตีเริ่มการโจมตีโดยการส่งอีเมลฟิชชิงปลอมไปยังองค์กรทางการทูตเป้าหมายในประเทศญี่ปุ่นโดยใช้ไฟล์ ZIP ที่มีไฟล์ปฏิบัติการที่เป็นอันตรายและนำไปสู่การติดเชื้อมัลแวร์ โดยเมื่อเหยื่อดาวน์โหลดไฟล์ที่มี Payload และมีการเรียกใช้ไฟล์ VBS เพล์โหลดในไฟล์จะดำเนินการเรียกใช้งานสคริปต์ที่ได้กำหนดไว้รวมถึงการได้กำหนดค่าที่ C:\Users\Public\Pictures\desktop.ini.bak เพื่อเรียกใช้งานแบบอัตโนมัติผ่าน Wscript โดยไฟล์ VBS จะดาวน์โหลด script PowerShell เพื่อรวบรวมข้อมูลกระบวนการทำงานต่างๆ ข้อมูลบัญชีผู้ใช้งานและเครือข่าย เพื่อส่งไปยัง URL ที่ถูกกำหนดโดยกลุ่มผู้โจมตี



Kimsuky attacks in Japan Source: JPCERT/CC

Latest Kimsuky attacks

ในช่วงเดือนพฤษภาคม 2567 ASEC ได้ค้นพบการซื้อขายมัลแวร์ CHM จากกลุ่ม Kimsuky ในเกาหลี ที่เคยแพร่กระจายในรูปแบบต่างๆ เช่น LNK, DOC และ OneNote จากการโจมตีเป็นการดำเนินการไฟล์ Compiled HTML Help (CHM) ที่แสดงหน้าจอขอความช่วยเหลือในขณะที่เรียกใช้สคริปต์ที่เป็นอันตรายในการทำงานพื้นหลังพร้อมกัน



Latest Kimsuky attack flow Source: ASEC

สคริปต์นี้ได้สร้างและดำเนินการไฟล์ในโปรไฟล์ของผู้ใช้ หลังจากนั้นจะเชื่อมต่อไปยัง URL ภายนอกเพื่อดำเนินการเข้ารหัส Base64 โดยสคริปต์นี้มีหน้าที่ในการขโมยข้อมูลผู้ใช้และสร้างสคริปต์ที่เป็นอันตรายเพื่อเป็นการดำเนินการคีย์ล็อก

ศูนย์ CSOC แนะนำให้ลูกค้าตรวจสอบรายละเอียดด้านความปลอดภัยเกี่ยวกับการเฝ้าระวังการโจมตีแบบ Phishing ที่อาจก่อให้เกิดความเสี่ยงที่**ยอมรับไม่ได้ต่อองค์กร** ควรต้องมีการดำเนินการตรวจสอบเพื่อลดความเสี่ยงที่อาจเกิดขึ้น ทั้งนี้ในช่วงเวลาที่รายงานฉบับนี้ออกยังพบ Proof-of-concept สำหรับการโจมตีด้วยช่องโหว่นี้และยังพบรายงานเกี่ยวกับการโจมตีช่องโหว่เหล่านี้ในอินเทอร์เน็ต

รายละเอียดของช่องโหว่โดยสรุป

- ผลิตภัณฑ์ที่ได้รับผลกระทบ: -
- หน่วยงานที่ออกคำแนะนำด้านความปลอดภัย: Japan's Computer Emergency Response Team Coordination Center (JPCERT/CC)
- ผลกระทบ (Impact): C2, Malware, Phishing, Social engineering
- CVE Name: -
- การแก้ไขปัญหา:
    - ดำเนินการตรวจสอบเครือข่ายเพื่อหาพฤติกรรมที่ผิดปกติหรือมีลักษณะของการติดต่อกับเซิร์ฟเวอร์
    - ติดตั้งระบบกรองอีเมลเพื่อลดความเสี่ยงจากอีเมลฟิชชิ่ง และควรตรวจสอบลิงก์หรือไฟล์แนบในอีเมลก่อนเปิดใช้งาน
    - กำหนดสิทธิ์การใช้งานของผู้ใช้เพื่อจำกัดการแพร่กระจายของมัลแวร์

ทั้งนี้การแก้ไข Configuration เพื่อลดความเสี่ยงจากช่องโหว่ดังกล่าว ลูกค้าควรปฏิบัติตาม Change Management Policy หรือ Risk Management Policy หรือ Business Impact Assessment ของหน่วยงานอย่างเคร่งครัด

ข้อมูลอ้างอิง

- https://www.bleepingcomputer.com/news/security/japan-warns-of-attacks-linked-to-north-korean-kimsuky-hackers/