Handsomeware

รายวิชา CP 422 031 Introduction to Cybersecurity
เสนอ อาจารย์ประจำวิชา ศ.ดร.จักรชัย โสอินทร์ และ ผศ. ดร.สาธิต กระเวนกิจ

หลักการ และ เหตุผล

ในปัจจุบัน การเข้าถึงเทคโนโลยีมีความสะดวกสบายยิ่งขึ้น ซึ่งส่งผลให้จำนวนอาชญากรทางไซเบอร์เพิ่มสูงขึ้นตามไปด้วย ดังนั้น การศึกษาและทำความเข้าใจในกลไกและวิธีการทำงานของภัยคุกคามทางไซเบอร์จึงเป็นสิ่งสำคัญ เพื่อเตรียมความพร้อมในการรับมืออย่างมีประสิทธิภาพและสามารถป้องกันได้อย่างรอบคอบ

วัตถุประสงค์

- เพื่อเข้าใจกลไกการทำงานของ Ransomware
- เพื่อทดสอบความเป็นไปได้ที่ hacker สามารถกระทำกับเหยื่อได้เมื่อเหยื่อติดตั้งมัลแวร์
- เพื่อเสริมสร้างความรู้และความตระหนักรู้
- เพื่อลดความเสียหายจากการโจมตีจริง

เครื่องมือที่ใช้

Python
VS code
ChatGPT
VMware
Kali linux

วิธีการใช้งาน

1.ที่ C2 server (kali linux) รันสคริปไฟล์ c2_server.py จะเป็นการเปิด service http ไว้ติดต่อและส่งข้อมูลกับเครื่องเหยื่อ
2.เมื่อมีเครื่องเหยื่อติดต่อเข้ามา เปิด terminal ใหม่ขึ้นมาและใช้คำสั่ง curl ไปที่ c2 service (http) เพื่อสั่งการเครื่องเหยื่อ

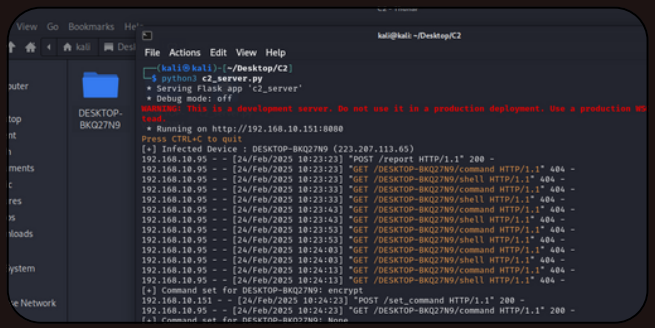
ขอบเขต

ในการพัฒนามัลแวร์ตัวนี้ ถูกจัดทำขึ้นและทดสอบภายในเครือข่ายเดียวกัน ไม่ได้มีการจดโดเมนเซิฟเวอร์ ดังนั้นจะไม่สามารถควบคุมเครื่องเหยื่อที่มาจากนอกเครือข่ายได้

Reference

Beast (Trojan Horse)

ตัวอย่าง (C2 server)



สรุป

สิ่งที่ทำได้ :

1. สามารถหลบจากการตรวจจับของ Windows 8.1 และเวอร์ชันที่เก่ากว่า

3. C2 สามารถสั่งการเครื่องเหยื่อให้รัน powershell ตามที่ต้องการได้

4. C2 ส่ง command ไปที่เครื่องเหยื่อให้ทำงานตามที่สั่งได้ เช่น สั่งให้ encrypt ไฟล์ / decrypt ไฟล์

สิ่งที่ทำไม่ได้ :

1. บางคำสั่ง powershell ที่ C2 ส่งไป อาจจะติดสิทธิ์ของ user

กลุ่มที่ 1 Section 3

นาย ทัพพ์โยธิน วิษณุโยธิน	663380106-7
นาย อนาวิล อุทัยสาง	663380136-8
นาย กฤษกร สีหะคลัง	663380448-9
นาย ณันสพัทธ์ เติมทรัพย์	663380456-0
นาย ภูมินทร์ ฤทธิแผลง	663380121-1
นาย ธราดล สุขสำราญ	663380459-4