Group 20

Key Logger and Screen Capture

วิทยาลัยการคอมพิวเตอร์ สาขาเทคโนโลยีสารสนเทศ ภาคพิเศษ

อาจารย์ประจำวิชา: ศ.ดร.จักรชัย โสอันทร์ | ผศ.ดร.สาธิต กระเวนกิจ

หลักการและเหตุผล

Keylogger เป็นมัลแวร์คลาสสิคที่ใช้ขโมยข้อมูล โดยปัจจุบันมักเป็นส่วนหนึ่งของ Banking Trojan และ Infostealer ล่าสุด Cyber Security News รายงานการค้นพบ Nova Keylogger ซึ่งพัฒนาด้วย VB.NET มีระบบป้องกันการตรวจจับและหลบเลี่ยงระบบความปลอดภัย เช่น การใช้เครื่องมือเสริมเพื่อปกปิดการทำงาน และซ่อนตัวใน Process ของระบบ

วัตถุประสงค์

- เป็นการลองฝึกพัฒนาไวรัสที่สามารถเก็บข้อมูลจากผู้อื่นได้
- เป็นการทดสอบว่าเมื่อใช้งานแล้ว จะสามารถทำงานได้ตามเป้าหมายที่ถูกสร้างขึ้น
- เพื่อปรับปรุงความเข้าใจเกี่ยวกับ Key Logger และ Screen Capture

งานที่เกี่ยวข้อง

Keylogger คือ มัลแวร์ประเภทหนึ่งที่ทำหน้าที่ บันทึกหรือเก็บข้อมูลการพิมพ์ (keystrokes) ที่ผู้ใช้พิมพ์ลงไปบนแป้นพิมพ์ เช่น รหัสผ่าน ข้อความ ข้อมูลบัตรเครดิต หรือข้อมูลสำคัญอื่น ๆ ที่ผู้ใช้พิมพ์ลงบนคอมพิวเตอร์หรืออุปกรณ์มือถือ โดยที่ผู้ใช้ไม่รู้ตัว

วิธีการทำงานของ Keylogger

การบันทึกการกดปุ่ม (Keystroke Logging):
Keylogger บันทึกทุกการกดแป้นพิมพ์ รวมถึงตัวอักษร, ตัวเลข, และปุ่มพิเศษ ครอบคลุมข้อมูลที่พิมพ์ในอีเมล, โซเชียลมีเดีย, เว็บไซต์, และการทำธุรกรรมออนไลน์

การส่งข้อมูลที่ขโมยมา (Data Exfiltration):
ข้อมูลที่บันทึกจะถูกส่งไปยังแฮ็กเกอร์ผ่านอินเทอร์เน็ต โดยอาจส่งแบบอัตโนมัติหรือเมื่อเครื่องออนไลน์

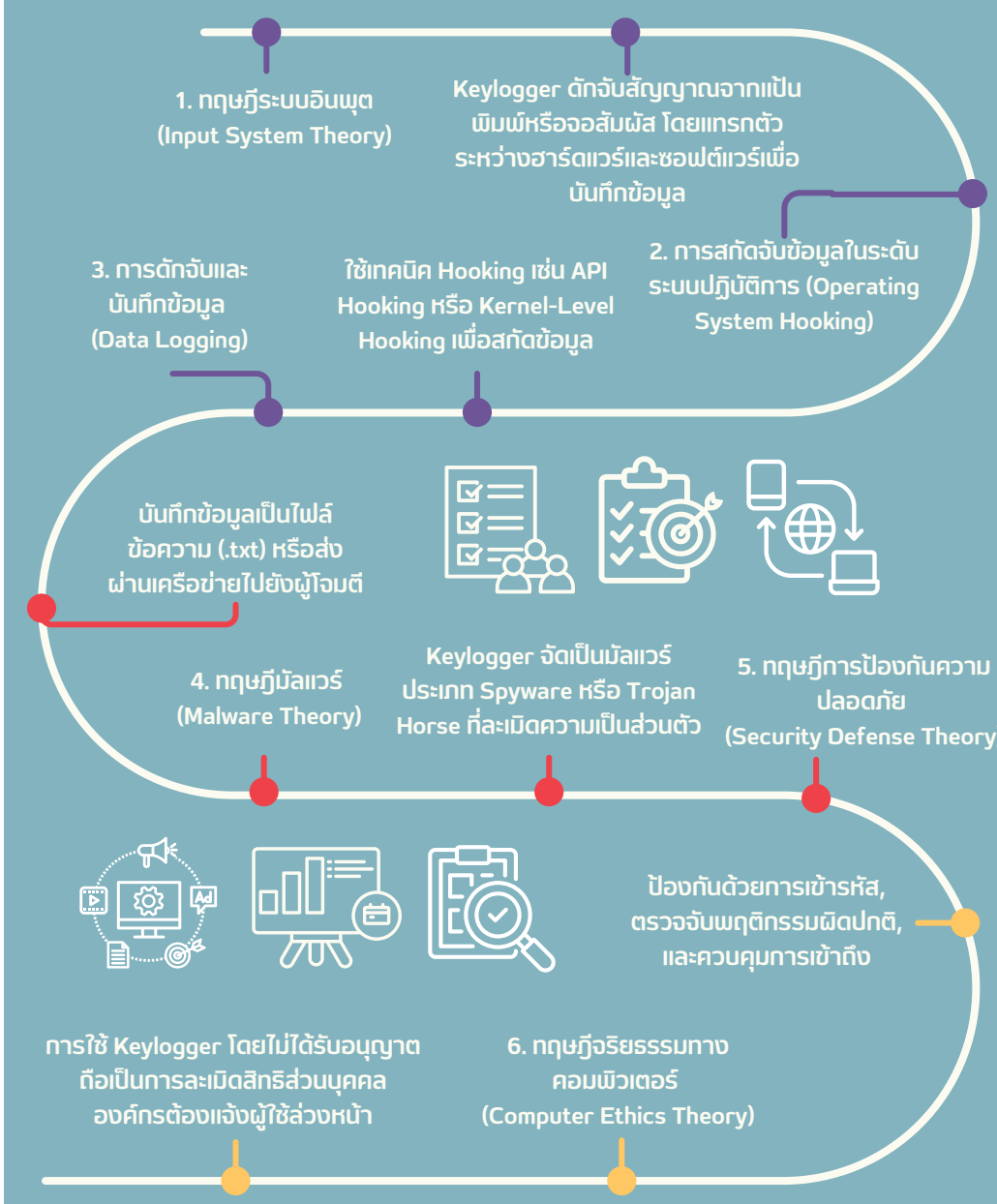
การซ่อนตัว (Stealth):
Keylogger ทำงานในพื้นหลัง ซ่อนตัวจากผู้ใช้และโปรแกรมแอนตี้ไวรัส บางตัวซ่อนในระบบปฏิบัติการหรือโฟลเดอร์ที่มองไม่เห็น

การแพร่กระจาย (Propagation):
Keylogger แพร่กระจายผ่านเว็บไซต์ไม่น่าเชื่อถือ, อีเมลฟิชชิ่ง, แอปไม่ปลอดภัย, หรือไฟล์แนบที่มีมัลแวร์

สิ่งที่ Keylogger สามารถทำได้

- ถ่ายภาพหน้าจอ
- สั่งเปิด Webcam แล้วบันทึกภาพ
- แอบดักฟังผ่านไมโครโฟน
- บันทึก URL ของเว็บไซต์ที่คุณเยี่ยมชม
- ดักจับข้อมูลทุกอย่างที่เก็บบนคลิปบอร์ด (Clipboard)
- บันทึกปุ่มบนหน้าจอที่คุณคลิก
- แอบดูข้อมูลที่ถูกส่งผ่านอินเทอร์เน็ต

ทฤษฎีที่เกี่ยวข้อง

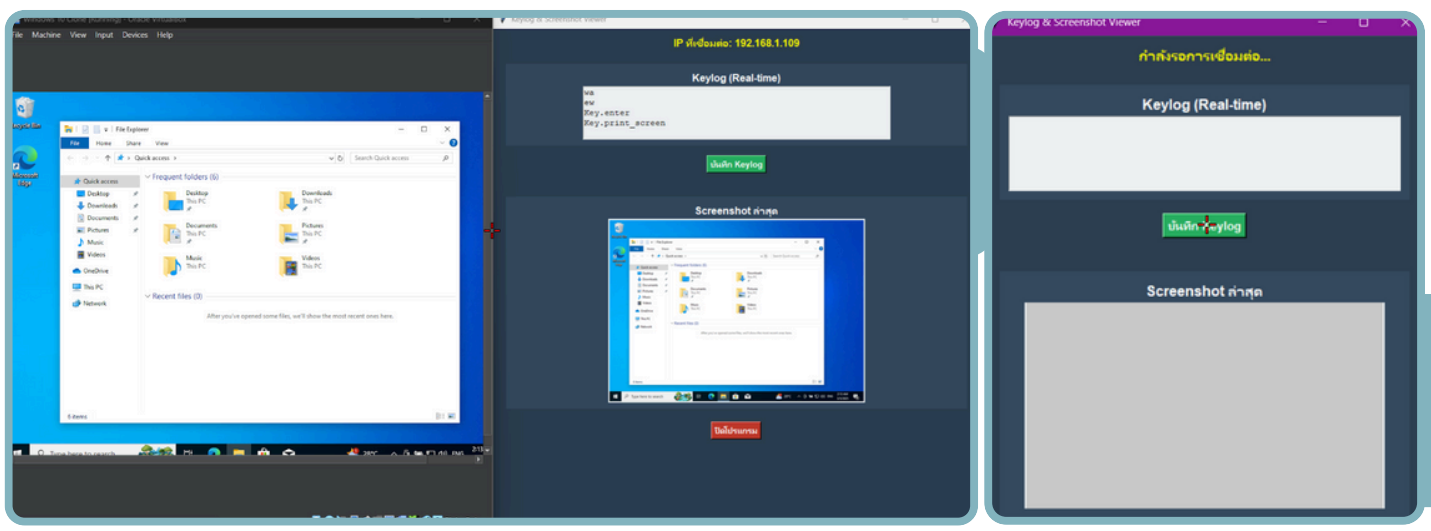


ขอบเขตของงาน

- บันทึกการกดแป้นพิมพ์ทุกครั้งและจัดเก็บข้อมูลในไฟล์
- จับภาพหน้าจอตามเวลาที่กำหนดและบันทึกลงไดเรกทอรี
- ตั้งค่าให้ทำงานเป็น Background Service
- เพิ่มฟังก์ชันบันทึกเวลา (Timestamp) ในไฟล์

จุดเด่น: ทำงานอัตโนมัติทันทีเมื่อเปิดเครื่อง

โปรแกรมของ สามารถทำงานขึ้นมาได้เองหากมีการกดใช้แล้วหนึ่งต่อให้ปิดเปิดเครื่องใหม่แล้ว ก็ยังทำงานอยู่ถ้าเคยกดไปแล้ว



สมาชิก
นายวจนะ ใต้ระหัน 663380360-3 นายฤทธิเดช สุขสมบูรณ์ 663380570-2 นางสาวเพ็ชรพริ้ง มะลิทอง 663380638-4
นายภูผา แก้วทอง 663380357-2 นายพงศ์พัฒน์ พิตรพิบูลผล 663380354-8
นายศุภชัย คนเพียร 663380576-0 นางสาวพลอยขวัญ อุปสัย 663380355-6

โปรแกรมที่ใช้ทดสอบ