Université Catholique de Lille 1875

Pass the SALT
Open-source & Security Conference

DesktopRanger Blocks Keystroke Spying: Hardening Windows Desktop Isolation

Igor Korkin

Lille, France
Université Catholique de Lille
July, 2 2026

WHO AM I

Igor Korkin, PhD (05.13.19), MEPhI alumni

Academic & Practical security researcher

- Windows & Linux Security · OS Internals · AI-Driven Attacks
- Speaker: Black Hat x3 · ADFSL x7 · IEEE S&P
- Author: 50+ papers · Huawei patent · Monograph
- Scientific Advisor
- Software Developer

AGENDA

- Under Keylogger Attacks
- Keyloggers vs Password Managers
- Windows Desktop vs. High-Privilege Keyloggers
- DesktopRanger: Open-source Project & Testing Results
- Conclusion & Discussion

SENSITIVE INFORMATION

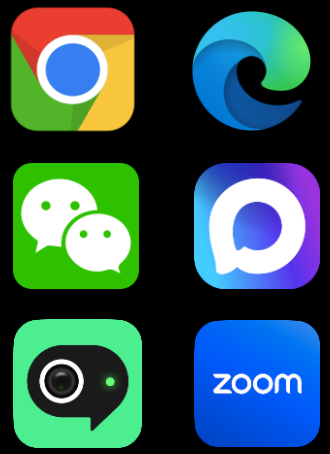
Web Browsing & Communication

Office & Documents

Passwords & Secrets

SENSITIVE INFORMATION

Web Browsing & Communication



Office & Documents

Passwords & Secrets

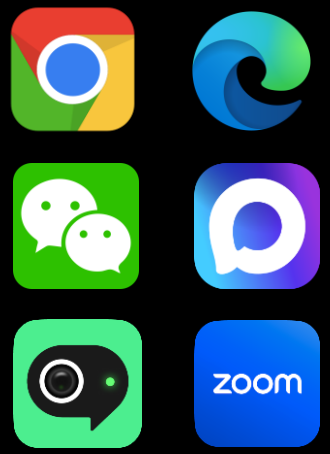
1Password

VeraCrypt

KeePass

SENSITIVE INFORMATION

Web Browsing & Communication



Office & Documents

Passwords & Secrets

1Password

VeraCrypt

KeePass

SENSITIVE INFORMATION

Web Browsing & Communication

Office & Documents

Passwords & Secrets

1Password

VeraCrypt

KeePass

Keyloggers

KEYLOGGERS = WINAPI-BASED + HIGH-PRIVILEGED

- Software keyloggers
  - User-level keyloggers
    - Based on Windows functions:
      - Hooking-based
      - Polling-based
      - Raw Input
      - Direct Input
    - ETW-based techniques
  - Kernel-level keyloggers

KEYLOGGERS = WINAPI-BASED + HIGH-PRIVILEGED

- Software keyloggers
  - User-level keyloggers
    - Based on Windows functions:
      - Hooking-based
      - Polling-based
      - Raw Input
      - Direct Input
    - ETW-based techniques
  - Kernel-level keyloggers

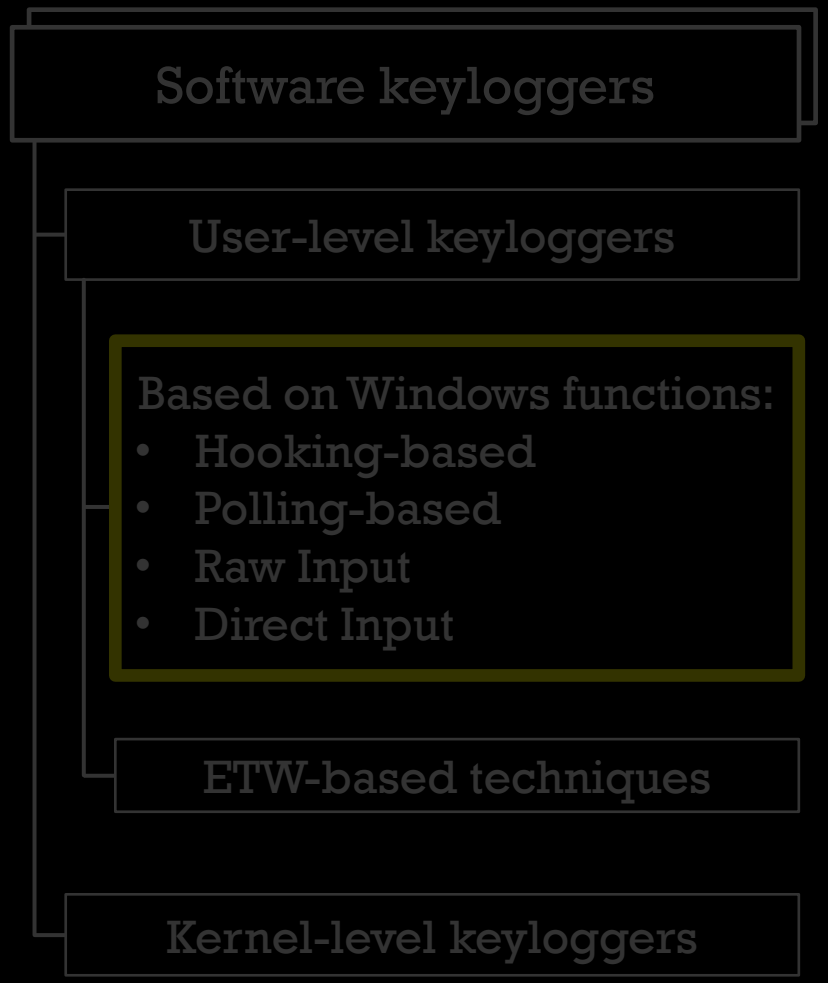
KEYLOGGERS = WINAPI-BASED + HIGH-PRIVILEGED

- Software keyloggers
  - User-level keyloggers
    - Based on Windows functions:
      - Hooking-based
      - Polling-based
      - Raw Input
      - Direct Input
  - ETW-based techniques
  - Kernel-level keyloggers

1 – Top Keyloggers based on WinAPI

WinAPI functions	Malware\Keyspy
SetWindowsHookEx	Snake
	Gurcu
GetAsyncKeyState	WarzoneRAT
	KLogExe
RegisterRawInputDevices GetRawInputData	Rhadamanthys
	RAT (3.3a), APT 31
DirectInput8Create GetDeviceState	EggStreme
	FusionCore

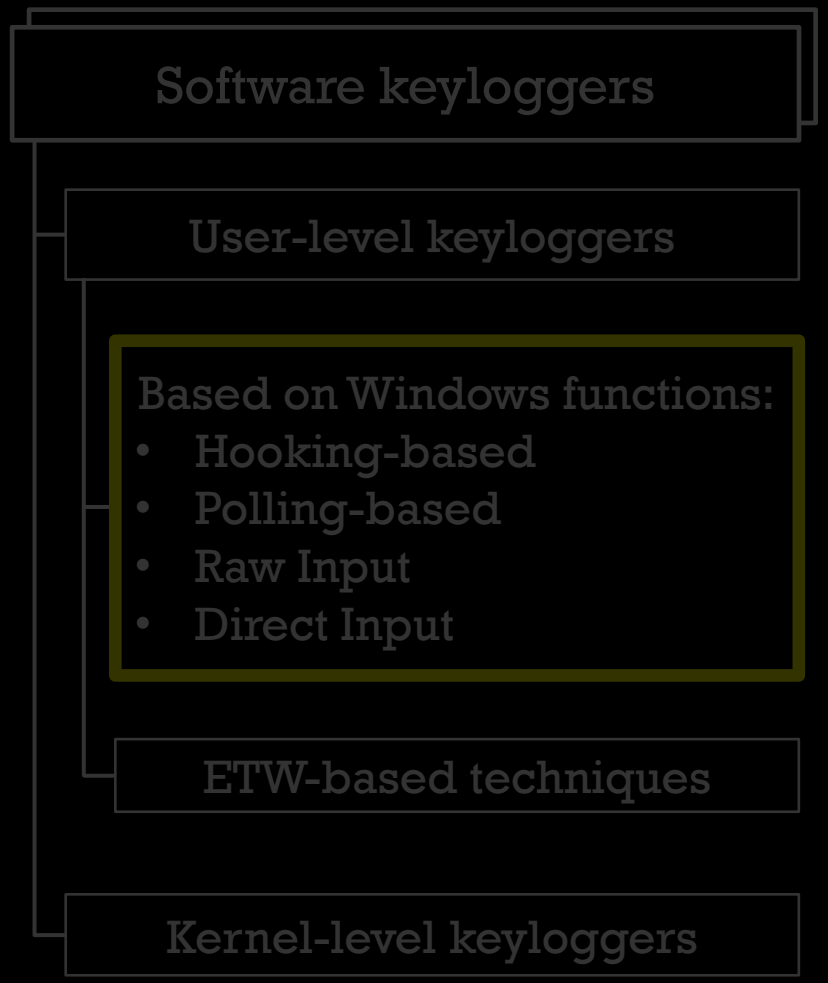
KEYLOGGERS = WINAPI-BASED + HIGH-PRIVILEGED



1 – Top Keyloggers based on WinAPI

WinAPI functions	Malware\Keyspy	Year
SetWindowsHookEx	Snake	2025
	Gurcu	2025
GetAsyncKeyState	WarzoneRAT	2025
	KLogExe	2024
RegisterRawInputDevices GetRawInputData	Rhadamanthys	2025
	RAT (3.3a), APT 31	2023
DirectInput8Create GetDeviceState	EggStreme	2025
	FusionCore	2023

KEYLOGGERS = WINAPI-BASED + HIGH-PRIVILEGED



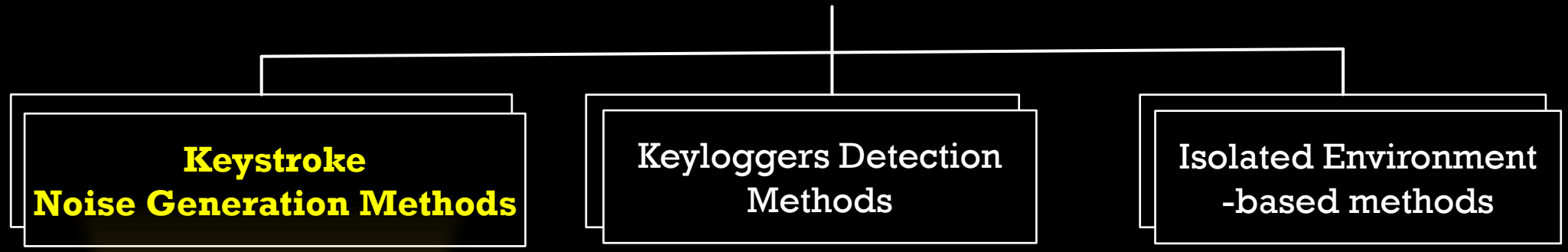
1 – Top Keyloggers based on WinAPI

WinAPI functions	Malware\Keyspy	Year
SetWindowsHookEx	Snake	2025
	Gurcu	2025
GetAsyncKeyState	WarzoneRAT	2025
	KLogExe	2024
RegisterRawInputDevices GetRawInputData	Rhadamanthys	2025
	RAT (3.3a), APT 31	2023
DirectInput8Create GetDeviceState	EggStreme	2025
	FusionCore	2023

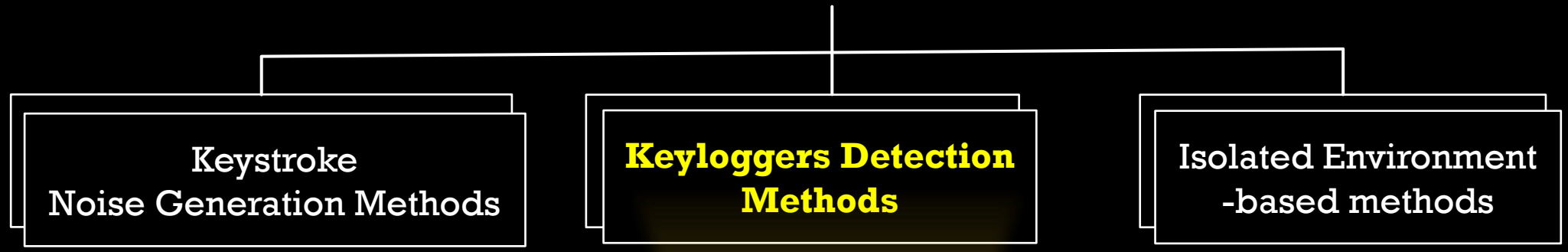
2 – High-privileged attackers

- MATE (Man-At-The-End) — a **highly privileged** local attacker who can **remain in user-mode** and interact with software and OS.
- CheckMATE 2025 @ ACM CCS

FIGHTING KEYLOGGERS



FIGHTING KEYLOGGERS



FIGHTING KEYLOGGERS

- Keystroke Noise Generation Methods
- Keyloggers Detection Methods
- **Isolated Environment -based methods**

FIGHTING KEYLOGGERS

- Keystroke Noise Generation Methods
- Keyloggers Detection Methods
- Isolated Environment -based methods
  - **Windows Desktop Technology**

Password Managers:

KeePass

FIGHTING KEYLOGGERS

Keystroke
Noise Generation Methods

Keyloggers Detection
Methods

Isolated Environment
-based methods

Windows Desktop
Technology

Attackers can bypass
protection technologies

FIGHTING KEYLOGGERS

Keystroke
Noise Generation Methods

Keyloggers Detection
Methods

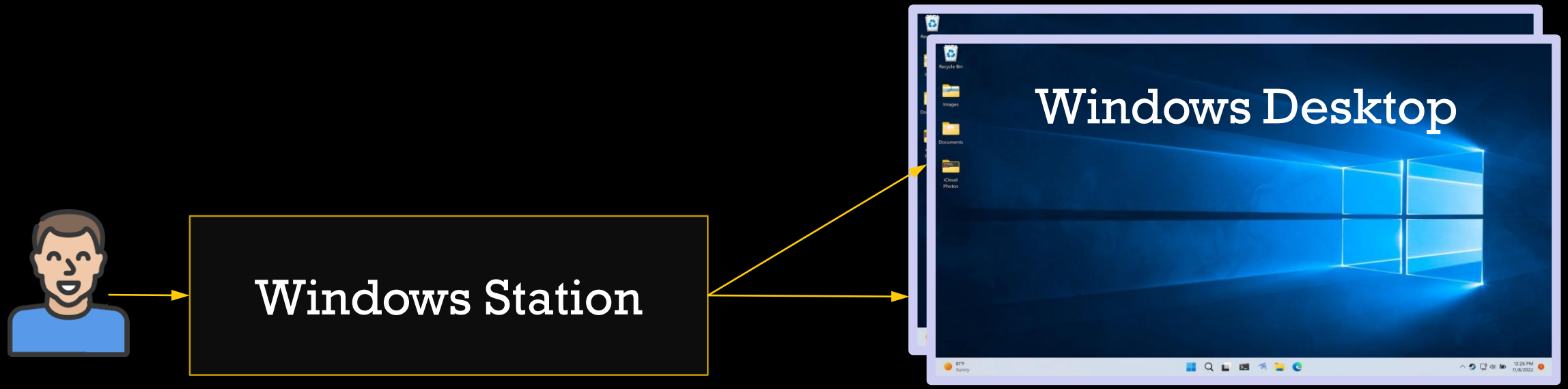
Isolated Environment
-based methods

Windows Desktop
Technology

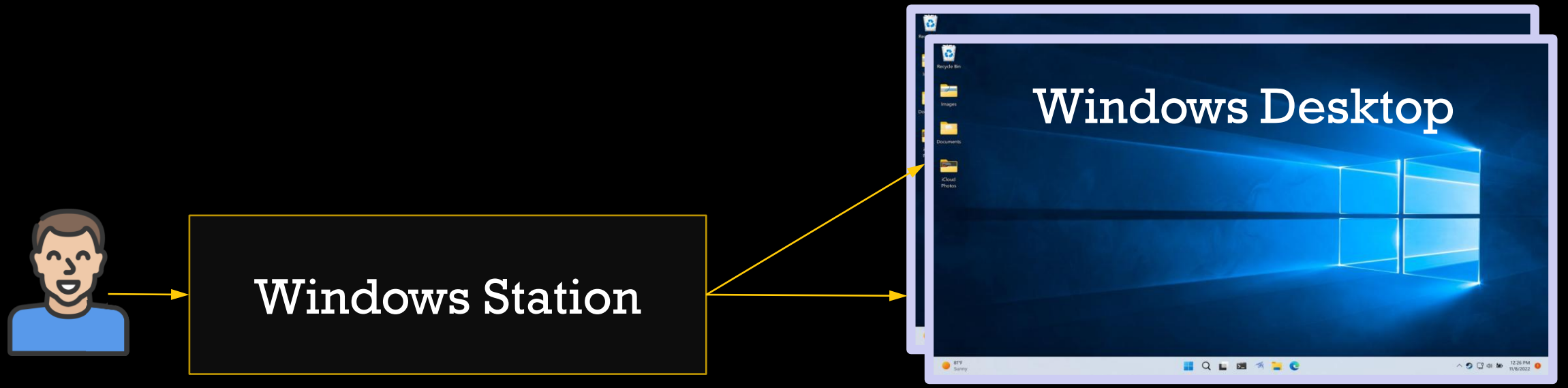
**Desktop
Ranger**

WINDOWS DESKTOP TECHNOLOGY

LOGIN → WINDOWS STATION → WINDOWS DESKTOP



LOGIN → WINDOWS STATION → WINDOWS DESKTOP



- Window station contains one or more desktop objects.

- **Windows desktop** contains windows, menus and **System Message Queue** shared among all apps running on the same desktop

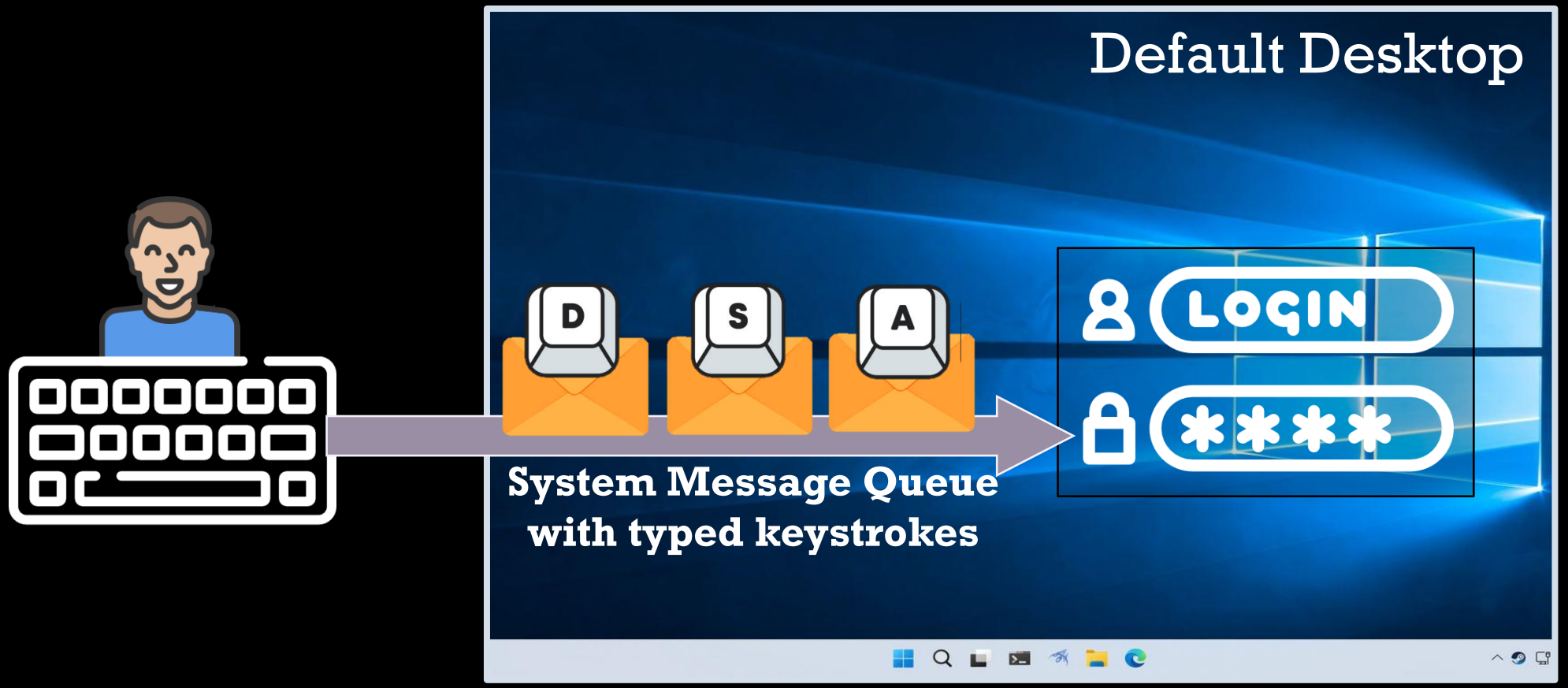
Station and Desktops are securable OS objects with access-rights

Access-rights:

- Create a desktop
- Enumerate desktops
- Read attributes
- etc

- Create windows
- Install hooks
- Read desktop's objects
- etc

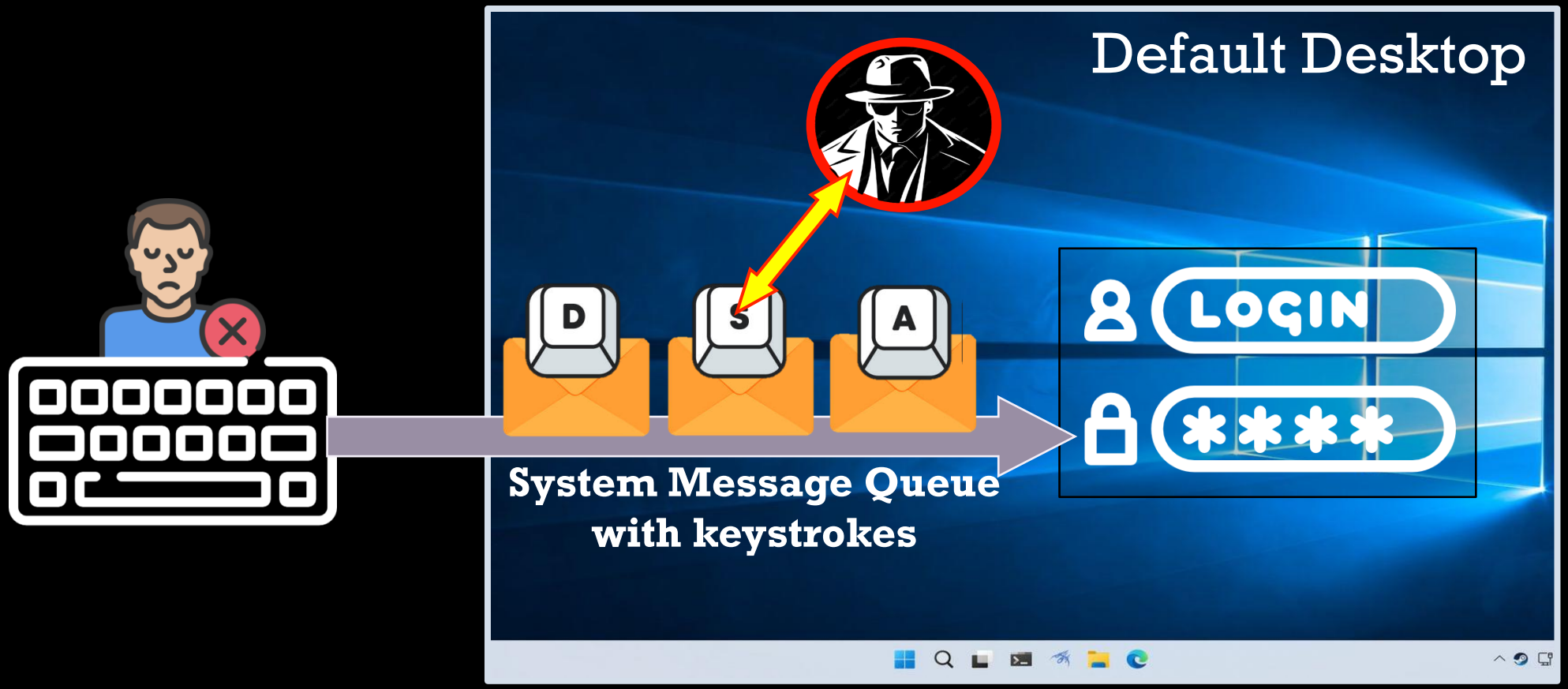
SAME DESKTOP = NO ISOLATION



A. Sensitive App is running on the Default Desktop

B. Keyspy gets keystrokes by reading System Queue shared among all apps running on the same desktop

SAME DESKTOP = NO ISOLATION



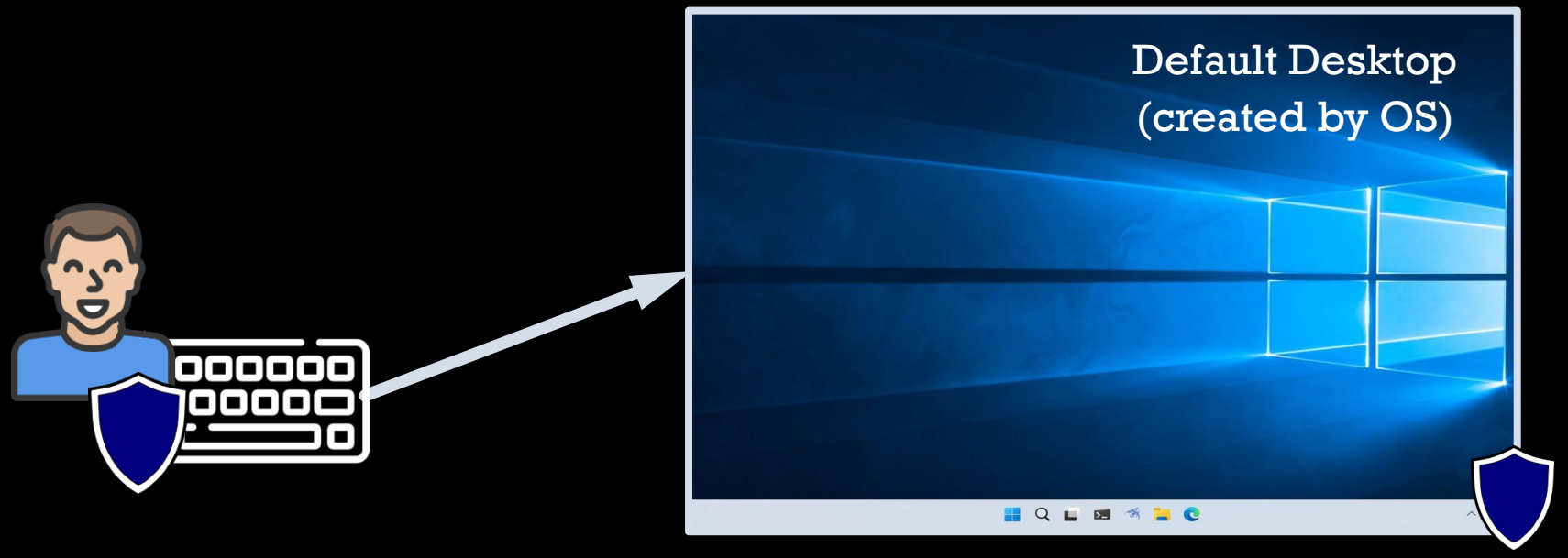
A. Sensitive App is running on the Default Desktop

B. Keyspy gets keystrokes by reading System Queue shared among all apps running on the same desktop

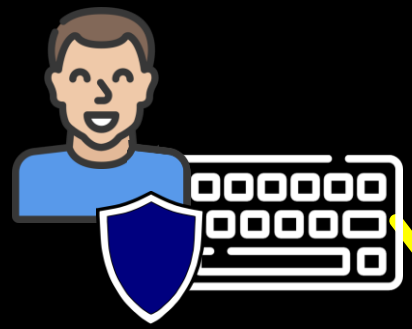
How to get an isolated message queue ??

Let's create a new Desktop!!

WINDOWS DESKTOP AS A SECURE OBJECT



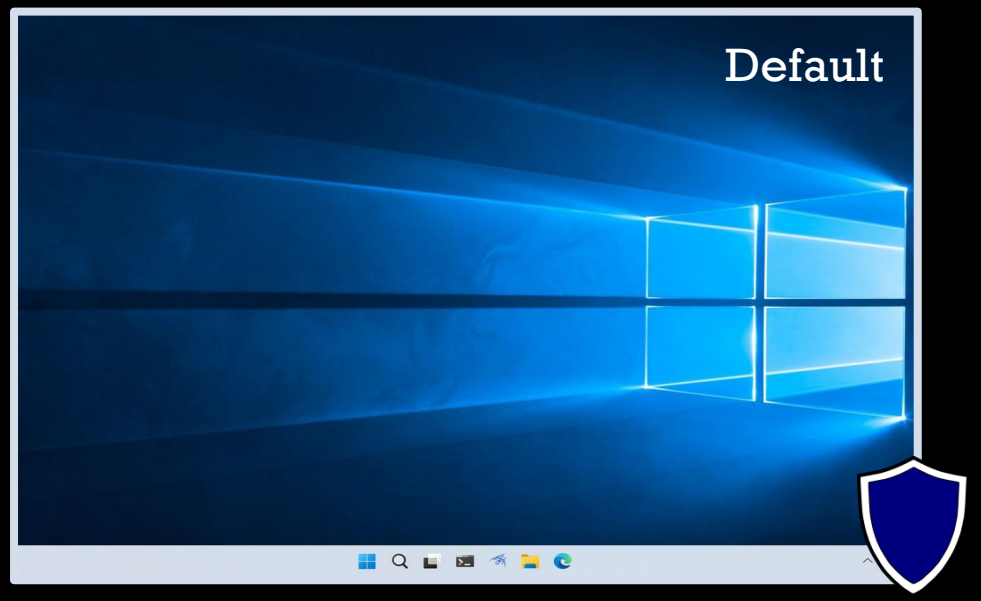
WINDOWS DESKTOP AS A SECURE OBJECT

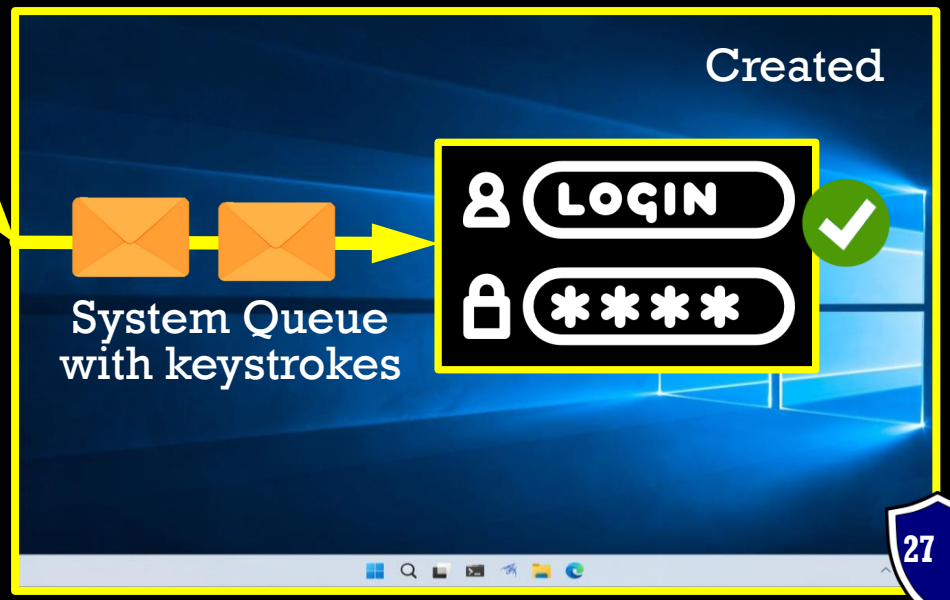


A. Password manager: creates a new desktop and relaunches its app on it
B. A desktop created with default SD inherits the creator's DACL

Password Managers:

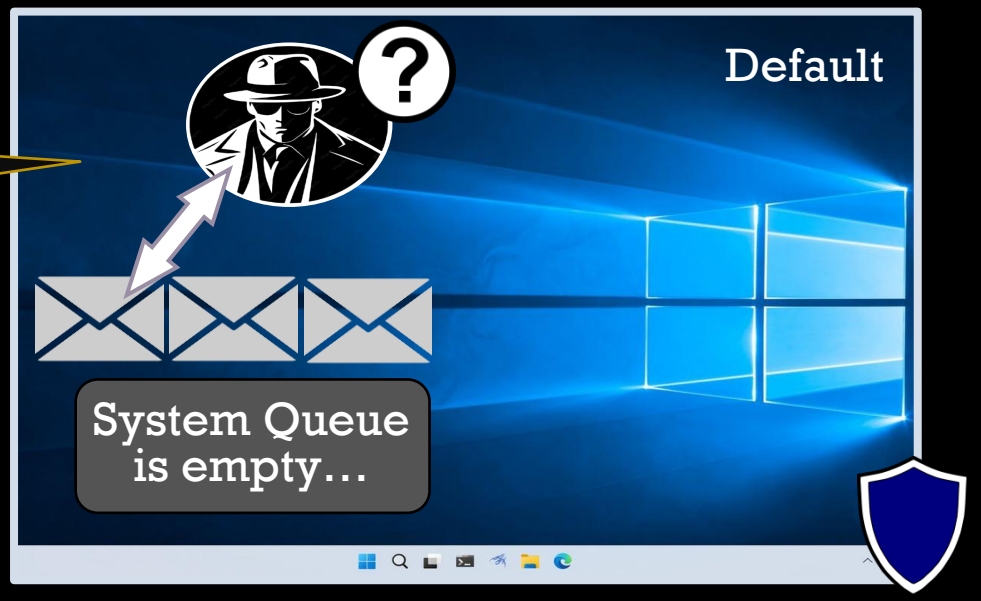
KeePass 1Password VeraCrypt



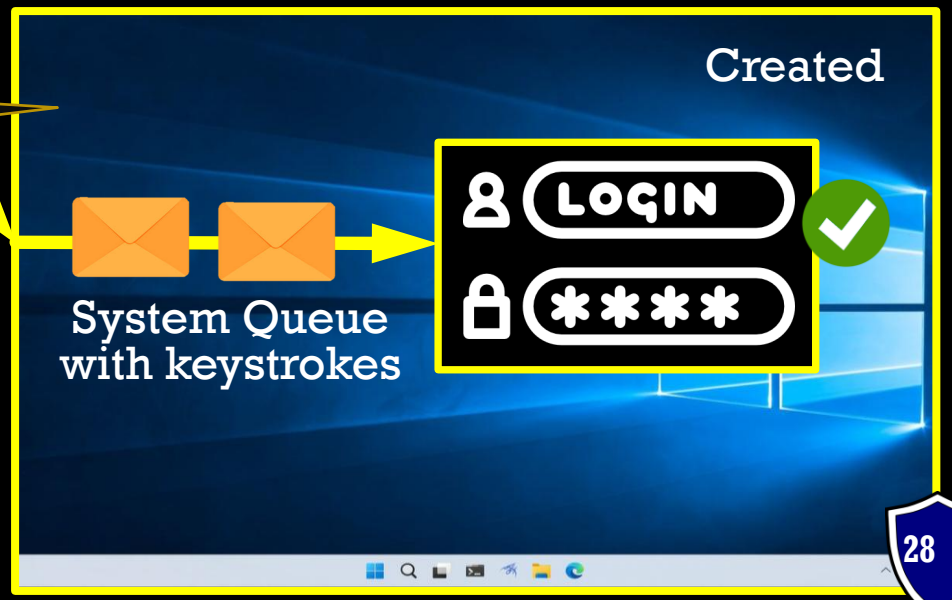


WINDOWS DESKTOP AS A SECURE OBJECT

A. Keylogger from Default Desktop cannot get any keystrokes typed on newly created Desktop



B. New Desktop has its own **isolated** System Msg Queue



Password Managers:

KeePass 1Password VeraCrypt

Can 2nd Desktop be infected?

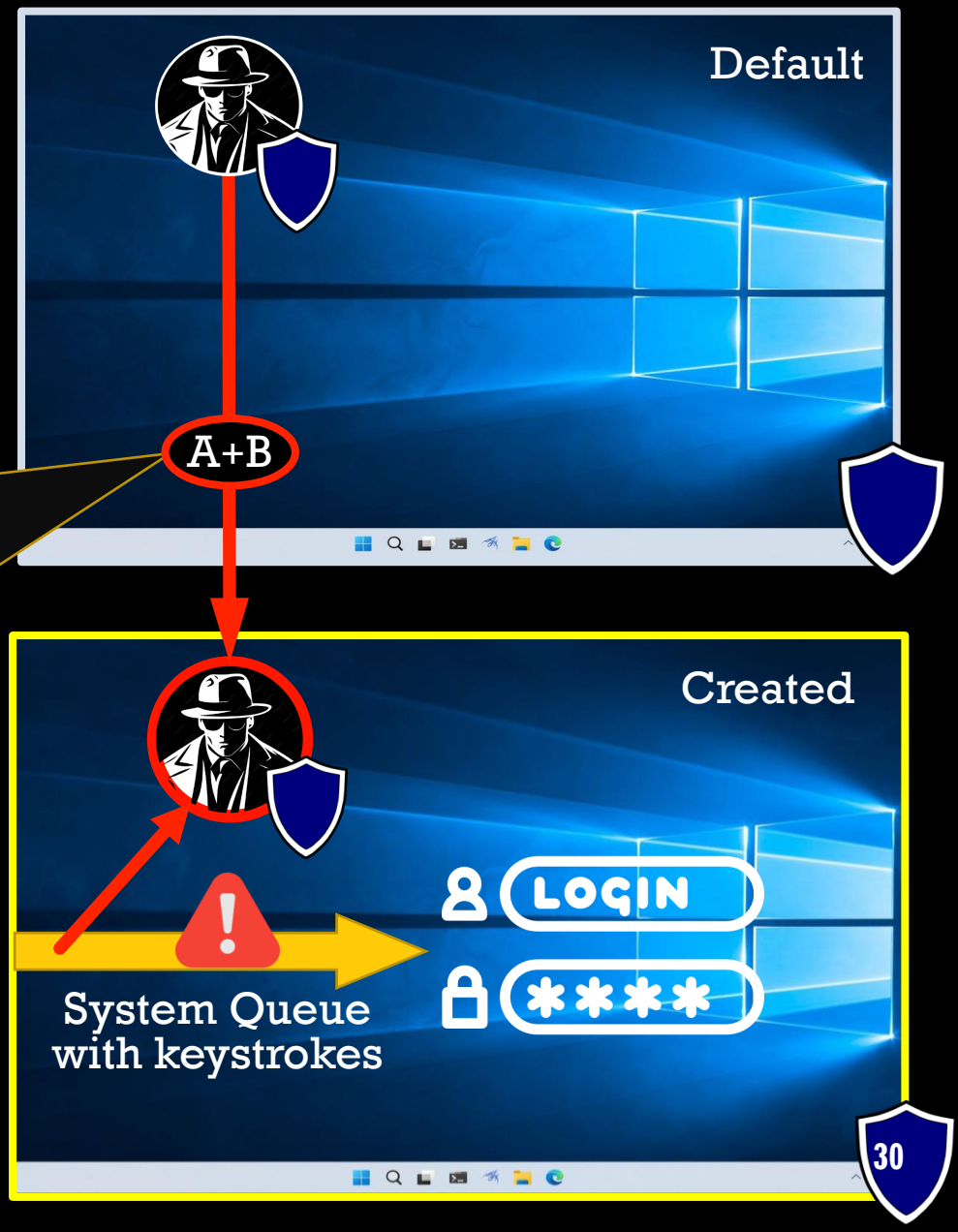
Yes, it can be infected 😮

2ND DESKTOP = NO ISOLATION

Attacker using the same user privilege can infect all the desktops:

Steps	WinAPI
A. Getting a list of all desktops	EnumDesktops
B. Launching its own app on each of desktop	OpenDesktop(name)

→ Now attacker can read all the keystrokes



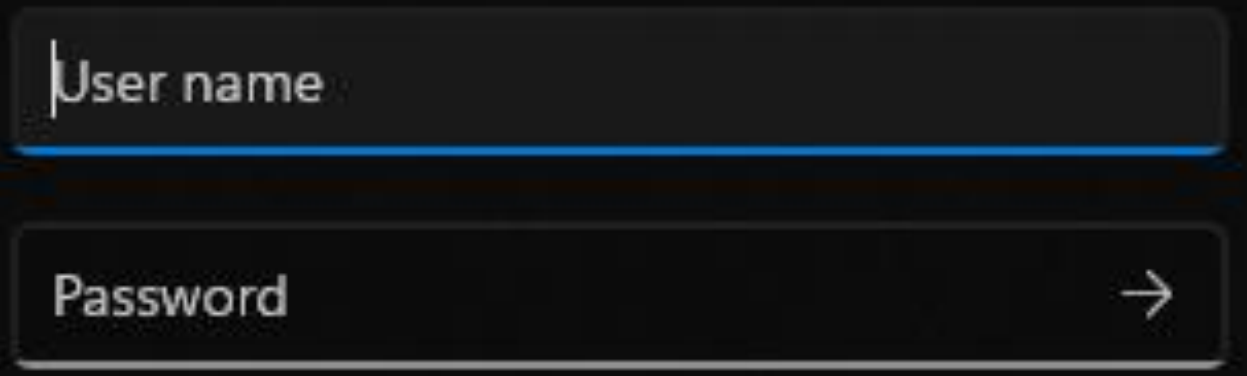
Keyloggers against KeePass Manager:

KeepassKeylogger shows that Master Password can be easily keylogged from "Secure desktop“

https://github.com/adenkiewicz/KeepassKeylogger

Winlogon desktop seems protected……

Actually, it can be infected too 😨

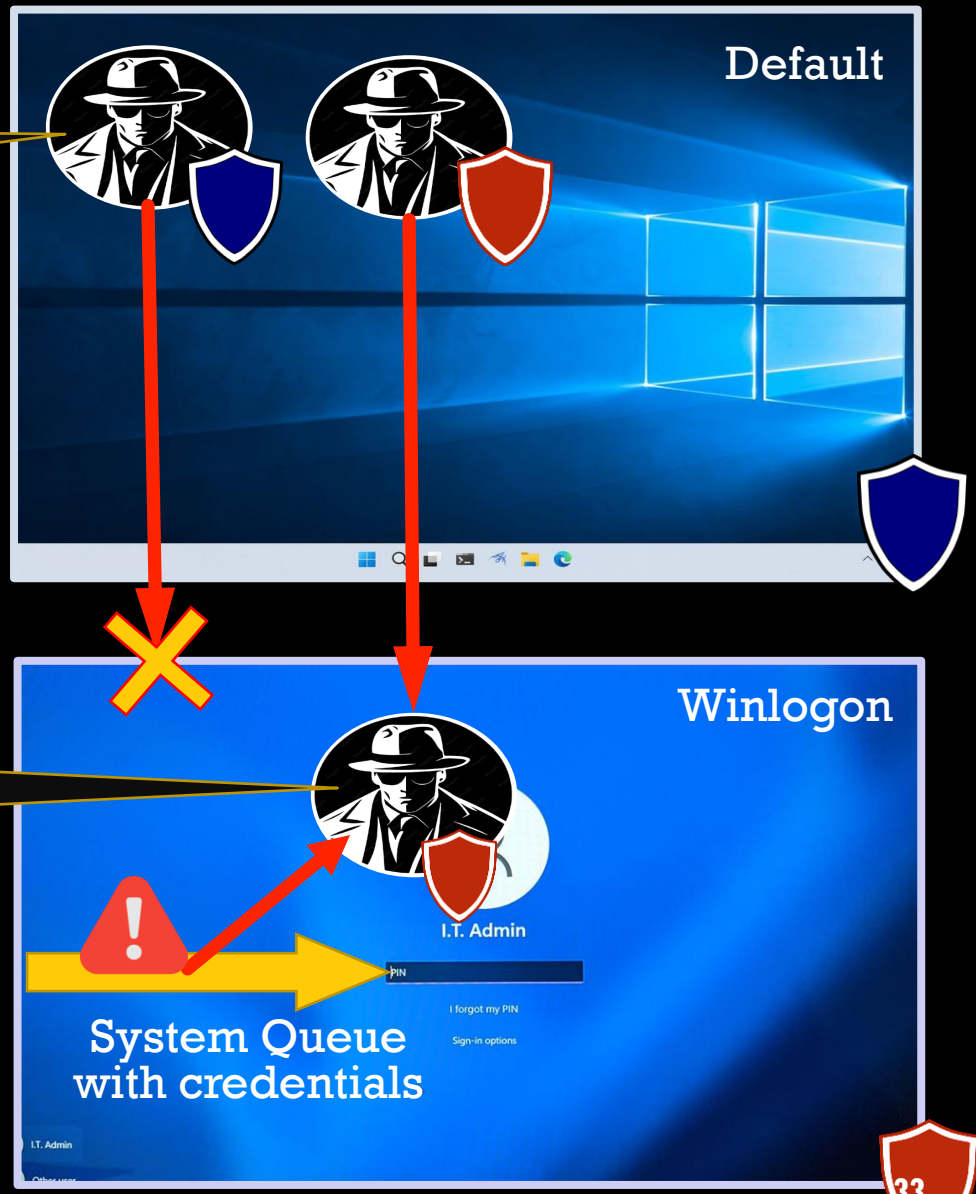


WINLOGON DESKTOP = NO ISOLATION

A. User-privileged keylogger cannot access Winlogon

WINLOGON DESKTOP = NO ISOLATION

A. User-privileged keylogger cannot access Winlogon



B. High-privileged keylogger can get access to Winlogon Desktop (e.g. via PsExec)

Keyloggers against Winlogon:

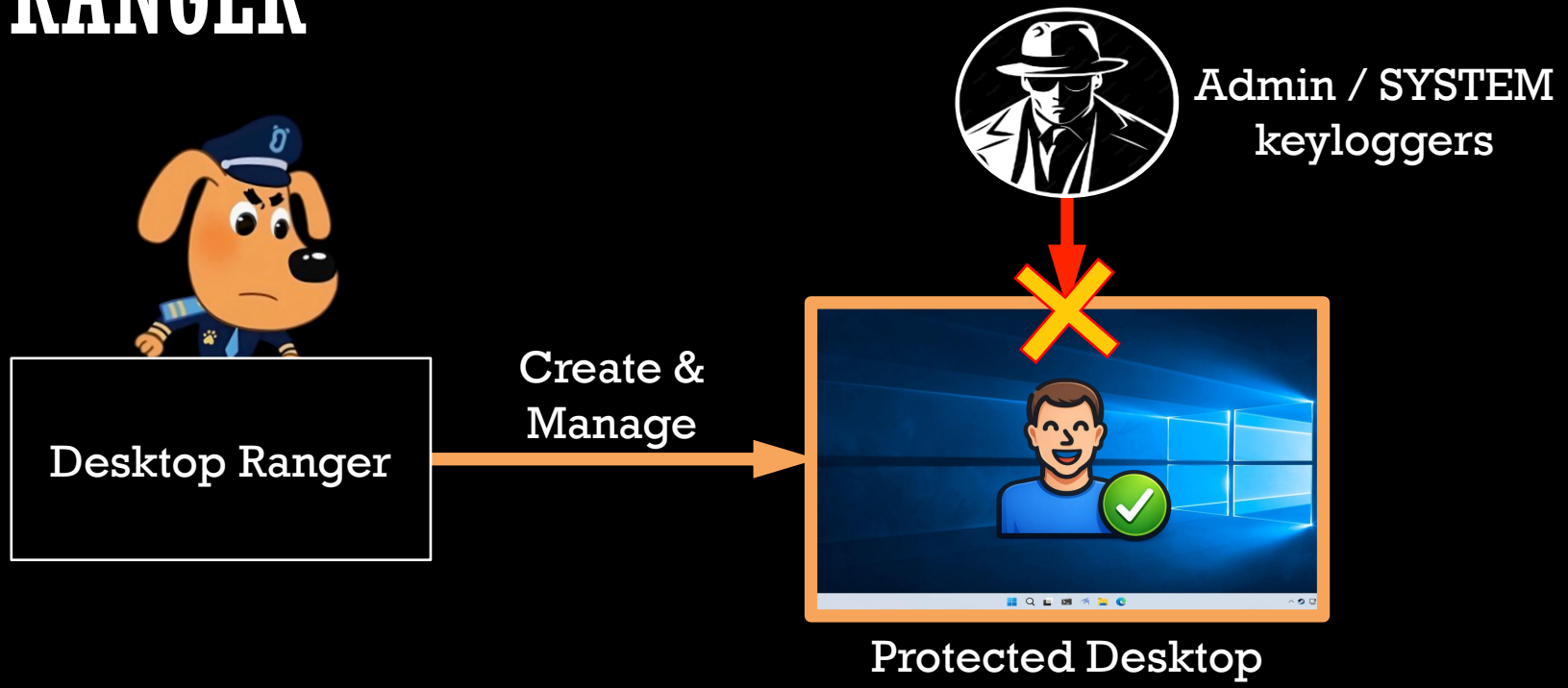
1. AdvanceLogger
2. AlmightyKeyLogger

https://github.com/Daniel-Ayz/AdvancedTopicsInMalware/tree/main/AlmightyKeyLogger
https://github.com/yuval2017/AdvanceLogger

Is possible to create a Desktop protected from high-privileged keyloggers?

Actually, yes

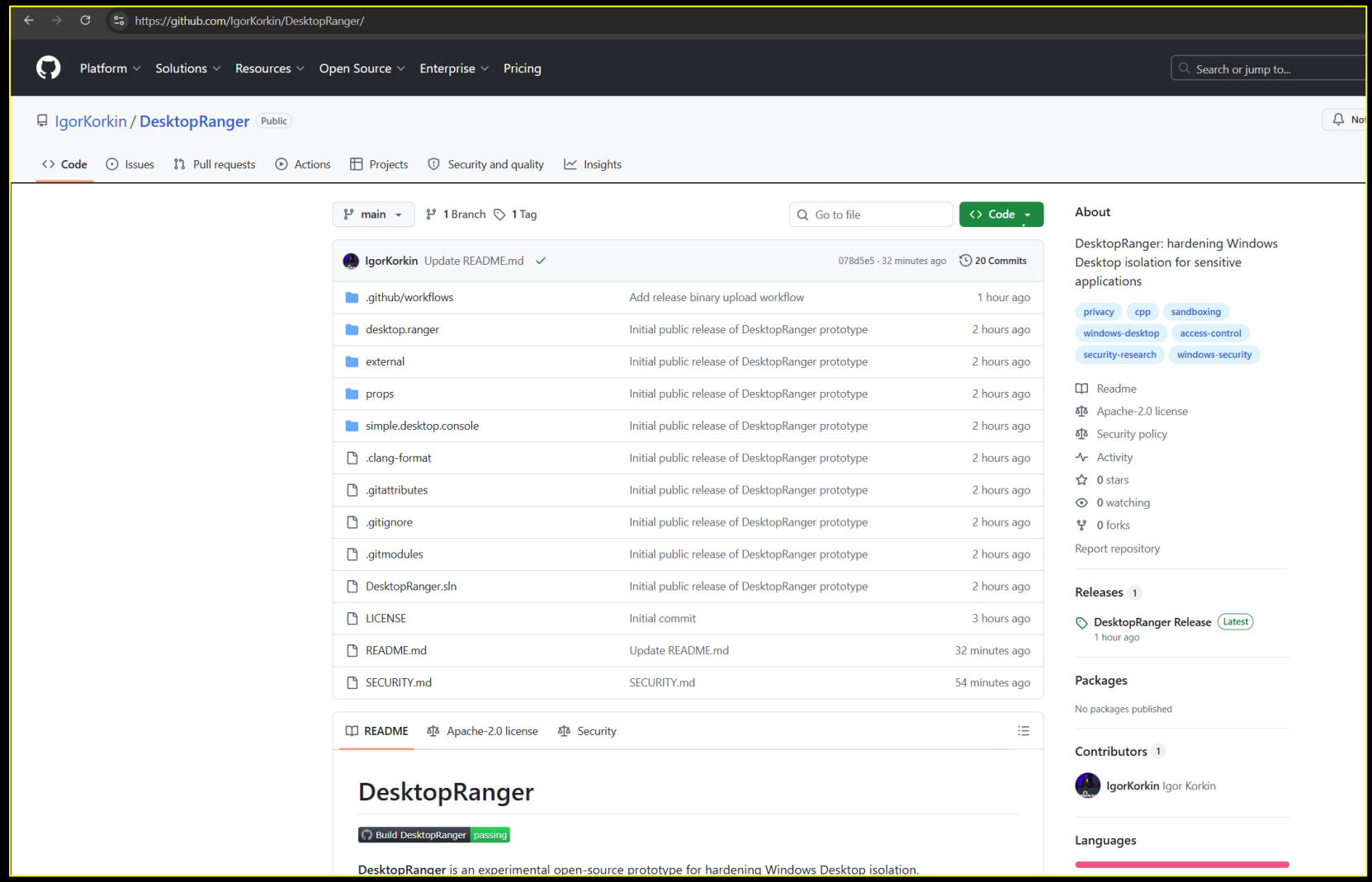
DESKTOP RANGER



- User-mode utility to create a secret desktop for private work
- Blocks attempts to enumerate, open, or attach to the protected desktop.
- Protects against high-privilege user-mode keyloggers.
- WinAPI + WIL / C++26 / ~2500 SLOC / Windows 11 26H1

DesktopRanger: Open-source repository

- Public repo: https://github.com/IgorKorkin/DesktopRanger



Step 1 – Create a desktop with an empty DACL

```
CreateDesktopW(RandomName, "D:P")
```

`"D:P"` – protected empty DACL: no ACEs, no inherited access

Step 1 – Create a desktop with an empty DACL

`CreateDesktopW(RandomName, "D:P")`

`"D:P"` – protected empty DACL: no ACEs, no inherited access

WinAPI	Result
EnumDesktops	RandomName is not returned
OpenDesktop	Access denied
CreateProcess(RandomName)	Access denied

WinAPI	Result
SwitchDesktop/CloseDesktop	☑
CreateProcess	see Step 2

Step 2 – Temporarily allow access in a secure way to run the app

1. Window Station: Revoke WINSTA_ENUMDESKTOPS
2. SetDesktopSD(“allow access”)
3. CreateProcess(UserApp) & Wait App initialization
4. SetDesktopSD(“restrict access”)
5. Restore WINSTA_ENUMDESKTOPS

Step 2 – Temporarily allow access in a secure way to run the app

1. Window Station: Revoke WINSTA_ENUMDESKTOPS
2. SetDesktopSD("allow access")
3. CreateProcess(UserApp) & Wait App initialization
4. SetDesktopSD("restrict access")
5. Restore WINSTA_ENUMDESKTOPS

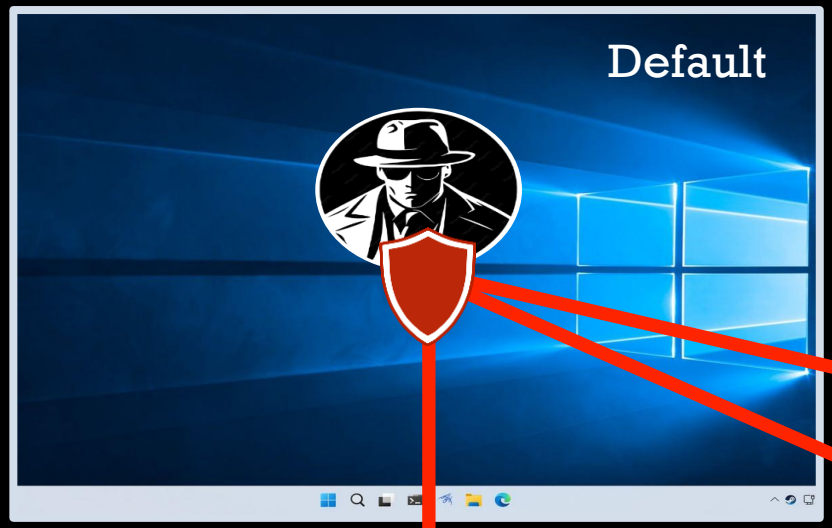
WinAPI	Result
EnumDesktops	Empty list (Step 1)
OpenDesktop(name)	name is random + not enumerable

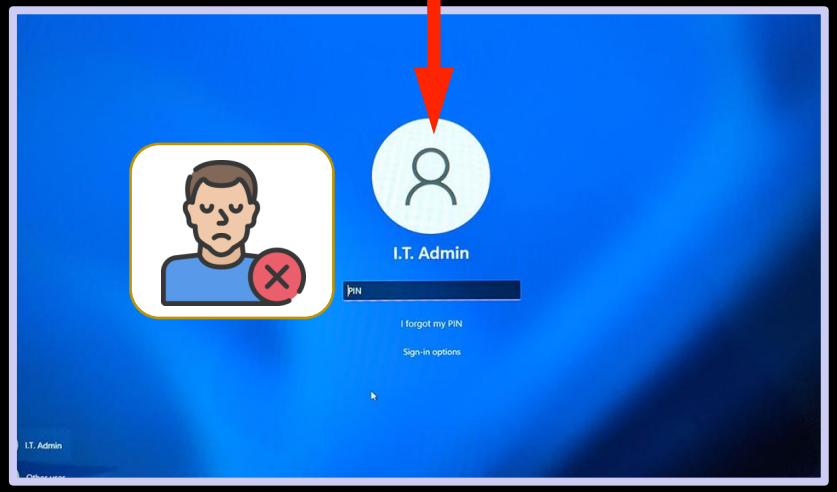
WinAPI	Result
CreateProcess	☑

TESTING SCENARIO

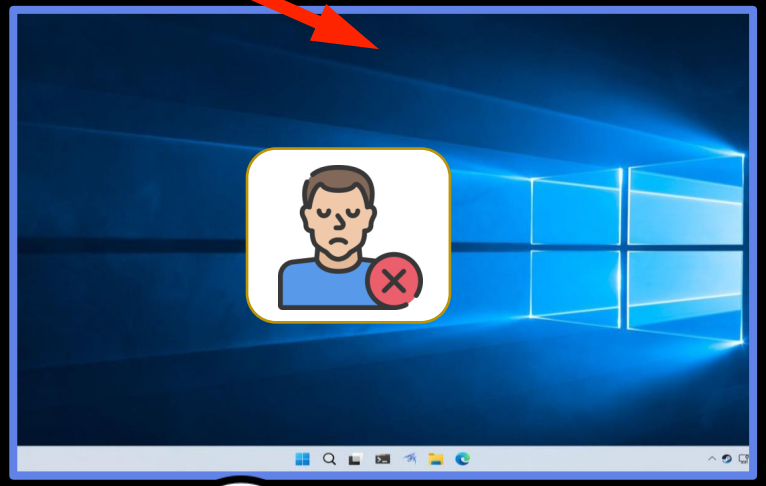
Experimental Keylogger:

1. WinAPI + WIL / C++26 / ~3000 SLOC
2. Implements 4 key intercepting techniques
3. Running with SYSTEM privileges
4. Monitoring desktops entities
5. vs Winlogon, KeePass & DesktopRanger





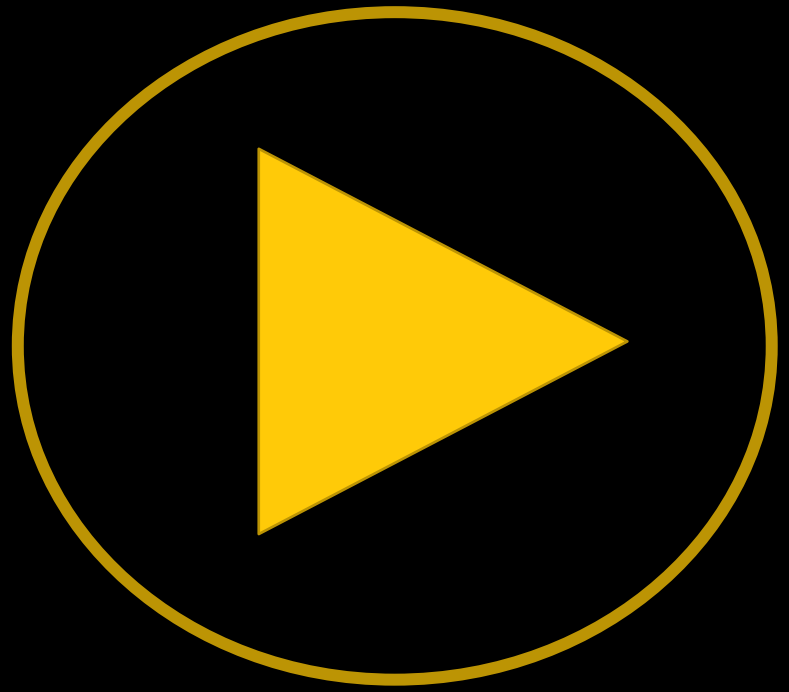
Winlogon



KeePass

Desktop Ranger

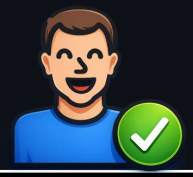
Demo: Advanced Keylogger vs Security Tools



The online version is here – https://igorkorkin.github.io/

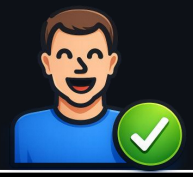
PROTECTION AGAINST HIGH-PRIVILEGE KEYLOGGERS

Testing Results:

		KeePass	Winlogon	Desktop Ranger 
	Default User	⛔	☑	☑
	Admin (via UAC)	⛔	☑	☑
	System (via PsExec)	⛔	⛔	☑
	Launch users apps	⛔	⛔	☑

PROTECTION AGAINST HIGH-PRIVILEGE KEYLOGGERS

Testing Results:

		KeePass	Winlogon	Desktop Ranger 
	Default User	⛔	☑	☑
	Admin (via UAC)	⛔	☑	☑
	System (via PsExec)	⛔	⛔	☑
	Launch users apps	⛔	⛔	☑

THANK YOU

- Igor Korkin
- igor.korkin@gmail.com
- github.com/IgorKorkin/DesktopRanger