uber basic check for kelogers.py

```
import psutil
import os
import sys

def find_suspicious_processes():
    suspicious_processes = []
    for process in psutil.process_iter(['pid', 'name', 'exe', 'cmdline']):
        try:
            if process.info['exe'] and process.info['cmdline']:
                exe_name = os.path.basename(process.info['exe']).lower()
                cmdline = ' '.join(process.info['cmdline']).lower()

                if 'keylogger' in exe_name or 'keylogger' in cmdline:
                    suspicious_processes.append(process)
        except (psutil.NoSuchProcess, psutil.AccessDenied, psutil.ZombieProcess):
            pass
    return suspicious_processes

def main():
    suspicious_processes = find_suspicious_processes()

    if not suspicious_processes:
        print("No suspicious processes found.")
    else:
        print("Suspicious processes found:")
        for process in suspicious_processes:
            print(f"PID: {process.info['pid']} - Name: {process.info['name']} - Exe: {process.info['exe']}
- Cmdline: {' '.join(process.info['cmdline'])}")

if __name__ == '__main__':
    main()
```

Revision #3
Created 28 April 2023 07:17:32 by naruzkurai
Updated 28 April 2023 11:35:04 by naruzkurai