

SHERLOG

Team :

Sonja Ebel MI7 Semester 4
Johannes Fischer MI7 Semester 4
Julian Beck MI7 Semester 4
Maya Palmer MI7 Semester 4
Polidefkis Dimoglidis MI7 Semester 4
Monika Pavic MMB Semester 4
Ronaldo Da Ros MI7 Semester 4

Motivation / Kontext :

Verstehen, wie Keylogger auf Linux-Systemen funktionieren
Angreiferperspektive verstehen,
um bessere Erkennungsmethoden zu entwickeln

Problemstellung:

- Klassische Antivirenprogramme erkennen nur leichte / unbekannte Varianten
- Mehr Schutz vor Keyloggern und Datendiebstahl
- Fokus auf IT-Sicherheit und Linux-Systeme

Was kann der Nutzer machen?

- Linux-System überwachen
- Verdächtige Prozesse erkennen
- Warnungen in Echtzeit erhalten
- Systemstatus über TUI einsehen



SHERLOG

Umsetzung / Lösung – Technologien :

- Go – Hauptprogrammiersprache
- Linux – Zielplattform und Entwicklungsumgebung
- /dev/input & Linux Input Subsystem – Erfassung von Tastatur-Events
- /proc-Dateisystem – Prozess- und PID-Analyse
- eBPF & C – Kernel-Level-Monitoring
- Bubble Tea – Terminal User Interface (TUI)
- Lip Gloss – TUI-Styling
- GitLab – Versionsverwaltung und Teamarbeit
- Virtuelle Maschinen – sichere Testumgebung



```
Suspicious Processes ..... 1 of 7
Type      Name      Risk
-----
dev/input secret-key-reader-demo 92%
dev/input code-editor             28%
dev/input loggylogger             98%
kernel    sherlog-keyboard-hook     100%
graphical secret-key-reader-demo  92%
graphical browser                 14%
graphical test-process            34%

Details .....
PID:      2345      Status: running
Name:     secret-key-reader-demo  Type: dev/input
Risk:     92%
Binary:   /tmp/secret-key-reader-demo
Command:  /tmp/secret-key-reader-demo --watch

Input:
/dev/input/event3
/dev/input/event5

Files:
write /tmp/secret-key-reader-demo.log inode(764221)
```

Probleme

- Go neu lernen
- Komplexe Kernel-Einarbeitung
- Umgang mit False Positives

Aha-Moment

- Wie mächtig und komplex der Linux-Kernel ist
- Verständnis von /proc und /dev/input
- Eigenen Keylogger bauen ⇒ besserer Detector möglich