



Netzwerk-Architektur & Konzept

Keylogger-Funktionalitäten

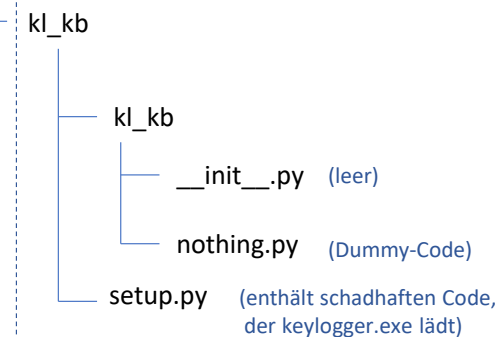
- ✓ Aufzeichnen von Tastatur-Eingaben und Maus-Klicks
- ✓ Erkennen von Sonder-Zeichen
- ✓ Aufzeichnung der Zwischen-Ablage bei STRG+V
- ✓ Screenshot bei Fensterwechsel
- ✓ Code-Obfuskation
- ✓ TLS-verschlüsselter Daten-Austausch via FTP
- ✓ Installation mittels „pip install“ eines manipulierten Python-Paketes
- ✓ Warten auf Start-Signal & „Stiller Start“
- ✓ Löschen der übermittelten Aufzeichnungen beim Opfer
- ✓ Automatische Ordner-Struktur beim Server

Dokumentation
in keylog.txt

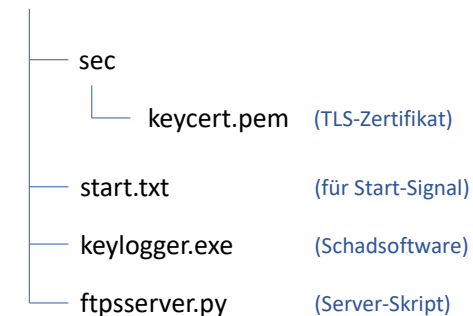
Relevante Files & Ordner-Struktur

Client

Manipuliertes Python-Package „kl_kb“,
das per „pip install .“ auf dem Opfer-Rechner installiert wird



Server





Netzwerk-Architektur & Konzept

