www.isb-plus.de

HOW TO DETECT

PEGASUS SPYWARE AUF IOS GERÄTEN

01

Sysdiagnose Datei erstellen

- Folgende 3 Tasten gleichzeitig für 1,5s gedrückt halten: Laut-,Leise- und Sperrknopf, bis das Gerät kurz vibriert.
- Wenn ein Screenshot erstellt wird oder Ihr ins Notrufmenü kommt, Vorgang wiederholen.
- Nach ca. 30min ist die Datei erstellt.

02

Datei übertragen

- Die Datei liegt unter Einstellungen → Datenschutz → Analyse → Analysedaten
- Hier nach der sysdiagnose Datei suchen
- Diese Datei Teilen und in Downloads speichern
- Jetzt kann die Datei ebenfalls über Teilen bspw. in einen Cloud-Speicher hochgeladen werden, damit Ihr Sie anschließend auf dem Analysesystem herunterladen könnt.

03

Skripte und Befehle

- Unter folgendem Link findet Ihr die Ressourcen: https://github.com/KasperskyLab/iShutdown
- Hier den Code als zip-Archiv downloaden
- Auf der Seite findet Ihr die Abhängigkeiten für Python und die Befehle zur Analyse.

04

Analysesystem vorbereiten

- Python in einer Version >3.X installieren
- Damit Ihr die Abhängigkeiten installieren könnt, müsst ihr ein Paketmanager installieren bspw. pip
- Alternativ Kali Linux Image herunterladen, da ist Python und pip schon installiert
- Dann alle aufgeführten Abhängigkeiten mit pip installieren: pip install “Paketname“
- Falls einige Abhängigkeiten nicht installiert werden können, keine Sorge, diese sind dann schon in Python vorhanden.

05

Analyse durchführen

- Entpacken des zip-Archivs mit den Analyseskripten.
- Starten der Shell und in das Verzeichnis der Skripte wechseln.
- Skript iShutdown_detect.py mit Pfad zur Sysdiagnose Datei ausführen: python3 iShutdown_detect.py /Pfad-zu-Sysdiagnose
- Enter und die Analyse startet.

06

Ergebnis

- Nach dem die Analyse abgeschlossen ist, erhaltet ihr im gleichen Fenster das Ergebnis.
- Es wird angezeigt, wie viele Neustarts mit einer Verzögerung durchgeführt wurden.
- Darunter ist zu sehen, ob eine Manipulation im Verzeichnis /private/var/db vorliegt
- Bei “No suspicious processes detected“ ist das Gerät nicht infiziert.

ISB PLUS
IT-SICHERHEIT DURCH PRÄVENTION