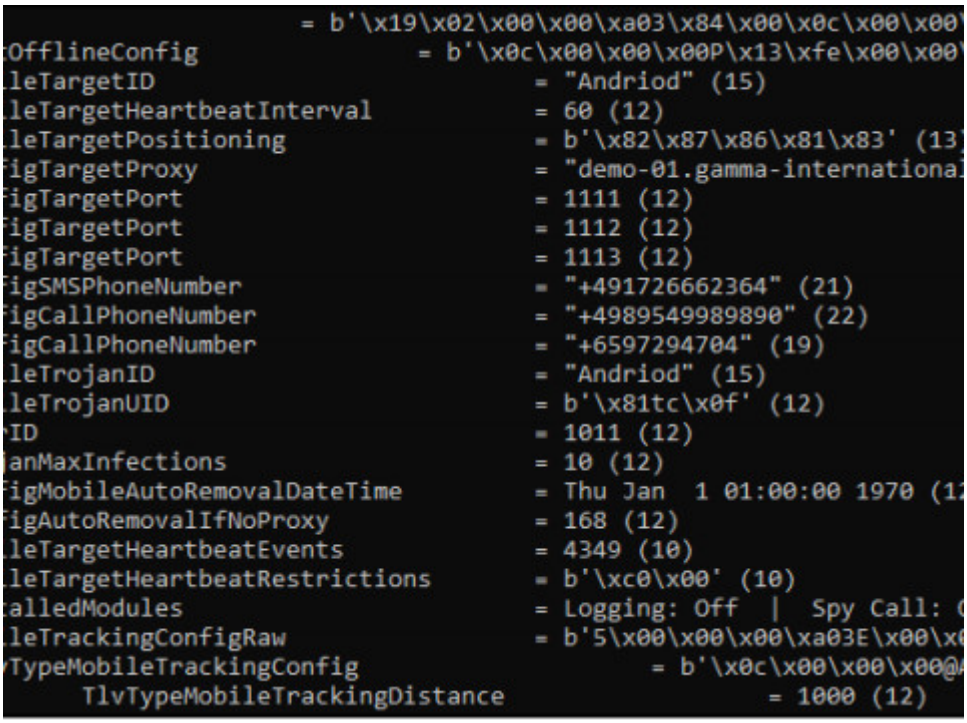
Bundestrojanische Gäule



Mit großem Interesse habe ich den Heise-Bericht über den „Spionage-Trojaner FinFisher“ gelesen. (Das heisst nicht „Trojaner“, sondern „Trojanisches Pferd“ – die Trojaner waren in Troja, und die Griechen saßen im Pferd.)

Schade, dass die Analyse des CCC „Evolution einer privatwirtschaftlichen
Schadsoftware für staatliche Akteure“ noch nicht erschienen war, als ich mein Buch veröffentlichte – es hätte Die Online-Durchsuchung gut ergänzt. Jetzt können wir „Butter bei die Fische“ tun. Kann die Frage: Wie fange ich mir so etwas ein? beantwortet werden?

Metzpolitik.org hatte schon vor vier Jahren geschrieben: „Die Begrenzung auf Windows 7 und Vista erscheint veraltet. Bereits vor zwei Jahren haben wir berichtet, dass FinSpy Mobile auch für alle mobilen Systeme (also iOS, Android, BlackBerry, Windows Mobile und Symbian) existiert. Und letztes Jahr haben interne Folien bestätigt, dass FinSpy alle großen Betriebssysteme (Windows, Linux und Mac OS X) infizieren

kann.“

Der wichtigste Satz: „Über den Infektionsweg sagt das Team um Morgan Marquis-Boire wenig. Nur: Falls die Trojaner die mobilen Betriebssysteme nicht direkt angreifen, **benötigen alle untersuchten Exemplare eine Interaktion des Nutzers, wie dem Klicken auf einen Mail-Anhang oder eine Webseite**.“

Genau das – und nur das! – habe ich immer behauptet, während fast alle Medienberichte entweder das Problem, wie die Spionage-Software zu installieren sei, vornehm ignorierten oder zu Magie – der Hacker hackt und ist irgendwann drin – greifen mussten.

Aber wie soll das funktionieren, wenn das Zielobjekt nicht total bekloppt ist? Klicken auf einen Mail-Anhang? Oha! Oder gar auf einer Website? Mit oder ohne Javascript erlaubt? Selbst wenn ein unerfahrener Windows-Nutzer Virustotal nicht kennt: Leben wir denn noch in Zeiten des Loveletter-Virus, als Outlook (wer nutzt das??) Anhänge nicht korrekt anzeigte?

Netzpolitik.org wies noch auf drei weitere Schwachstellen hin: Windows 7 SP1 – Acrobat Reader PDF Exploit, Windows 7 SP1 – Browsers Exploit, Windows 7 SP1 – Microsoft Office 2010 DOC-XLS Exploits. Schon klar. Das erinnert mich an 2003: „UK government gets bitten by Microsoft Word“.

Hilfe, jemand wollte einen Bundestrojaner bei mir installieren! (25.06.2011) Nur gut, dass ich immer wachsam bin und die zunehmende Radikalisierung und Extremismusierung der

E-Mail-Attachments bekämpfe!