Posudek bakalářské práce

Autor: **Marek Timr**

Název práce: **Framework for proof of concept implementations of C&C channels**

Posudek vypracoval vedoucí práce: Mgr. Jan Kohout

V bakalářské práci se student zabývá problematikou tzv. řídících (command and control, C&C) kanálů botnetů, zejména pak možnostmi zneužití známých a široce používaných internetových služeb jako např. Dropbox nebo Twitter pro předávání zpráv v rámci těchto kanálů. V rámci řešení se student seznámil s problematikou botnetů a jejich C&C kanálů, včetně několika konkrétních příkladů, které ve své práci detailněji analyzoval. Na základě této analýzy pak navrhl jednoduchý protokol simulující základní příkazy botnetu a otestoval možnosti jejich předávání pomocí několika internetových služeb. Pro účely tohoto testování pak student navrhl a implementoval framework v jazyku Java, který právě takovou simulaci předávání příkazů přes vybranou službu umožňuje.

Členění práce do jednotlivých kapitol je logické, práce začíná motivací, dále pokračuje obecnou charakteristikou botnetu následovanou třemi příklady konkrétních botnetů. Čtvrtá kapitola je pak věnována popisu implementovaného frameworku a návrhu realizace C&C komunikace přes služby Dropbox, Pastebin, Twitter a Google Documents. Popis každé služby je doplněn zhodnocením zneužitelnosti dané služby pro řízení botnetu a analýzou omezení, kterým by botmaster musel čelit. Framework je navržen účelně a díky modulární struktuře umožňuje snadné rozšíření o další implementace C&C komunikace přes další služby.

V průběhu zpracování práce student prokázal schopnost analyzovat problém a samostatně navrhnout vhodné řešení. Velký přínos práce vidím také v možnosti jejího využití v rámci výzkumu v síťové bezpečnosti pro testování detekce C&C kanálů zneužívajících např. sociální sítě. Velmi oceňuji experiment prověřující zneužití několika služeb pro C&C komunikaci současně, který student v rámci práce sám navrhl a realizoval. Přes občasný výskyt drobných gramatických nedostatků také kladně hodnotím fakt, že je práce zpracována v angličtině.

Předloženou bakalářskou práci hodnotím známkou: **A-výborně**.

12. 6. 2015