Analýza phisingu z pohľadu honeypotov

Motivácia k výberu témy

Autor: Martin Glova

Vedúci: RNDr. JUDr. Pavol Sokol

Na svete existuje veľmi veľa zaujímavých a fascinujúcich vecí. Človek sa neustále snaží viac a viac preskúmať svet a prírodu, uľahčovať si prácu, zefektívniť svoju činnosť... To mu samozrejme (okrem iného) robí radosť, ktorá mu zároveň dáva zmysel žiť. V mnohých vedeckých odboroch, ktoré sú známe, je tu denne veľmi veľa pokrokov a vývoj ide stále dopredu. Väčšina vedcov si myslí, že práve ten ich odbor je ten najzaujímavejší. A áno, všetci ľudia, ktorí povedia: *"Môj odbor je najlepší!"* majú pravdu.

Človek by si mal pre svoju činnosť vyberať niečo, čo mu bude na osoh. Veď má zmysel robiť niečo, čo nikomu nikdy nebude treba? Má zmysel snažiť sa, investovať čas do vecí, ktoré sú nepodstatné? Kto ale vie povedať, čo je nepodstatné a čo je podstatné?

V niektorých odboroch je zjavné, že sú pre človeka veľmi užitočné. Príkladom môže byť medicína. Jej pokroky denne priamo zachraňujú mnohé životy. Sú ale odbory ako fyzika, chémia, geografia, matematika, dejepis, psychológia... a na neposlednom mieste informatika také užitočné ako medicína? Odpoveďou by mohla byť otázka: Môže ľubovoľný z odborov existovať bez ľubovoľného iného? Môže medicína fungovať napríklad bez informatiky alebo chémie?

Deti v škole sa dosť často môžu stretávať s pojmom medzi-predmetové vzťahy. Ak zrazu na fyzike treba upravovať matematický výraz po dosadení do nejakého fyzikálneho vzorca, už je to na chvíľu viac o matematike ako o fyzike. Dá sa tomu vyhnúť? Asi sotva. Dá sa navymýšľať ešte mnoho iných príkladov, ktoré dokazujú, ako sú jednotlivé vedné odbory poprepájané a vzájomne si pomáhajú.

Poďme sa ale bližšie pozrieť na informatiku. Čo je to za vedu?

Veľmi zjednodušene a stručne povedané, informatika je veda o spracovávaní informácií. Mnoho ľudí si mylne myslí, že informatika je veda o počítačoch. Známa a veľmi výstižná analógia, ktorú vyslovil informatik Edsger Wybe Dijkstra je, že *"Informatika nie je viac o počítačoch ako astronómia o teleskopoch."* Áno, je pravda, že informatika je veľmi úzko spätá s počítačmi, ale je to iba nástroj, ktorý sa veľmi často používa. Ak informatika poprosíte o opravu počítača, je to to isté ako by ste poprosili astronóma o opravu teleskopu. Neznamená to, že to infomatik nebude vedieť, väčšinou je to práve naopak, keďže sa infomatici zaoberajú informáciami, často ich vedia aj efektívne vyhľadávať a učiť sa - teda aj vedieť si rýchlo poradiť s rôznymi problémami ako je oprava počítača, ale (väčšinou) to nie je ich primárna oblasť záujmu.

Ak by človek chcel vedieť všetko, veľmi rýchlo by narazil na veľmi známe obmedzenie tohto sveta - čas. Keďže je tu toto obmedzenie a človek sa predsa len chce v svojom živote niečomu venovať, musí si vybrať. Veľmi šikovní ľudia by mohli namietať, že toho stihnú viac za svoj život, tak tí si minimálne musia určiť poradie, v akom sa daným veciam budú venovať.

Rovnako ako je samotná veda rozdelená na viaceré odbory, vieme, že aj tieto odbory majú svoje pododbory a tieto sa ďalej môžu členiť... Aj keď sa na prvý pohľad môže zdať, že niektoré pododbory nie sú také dôležité, všetky majú svoje miesto v nejakom odbore a o vážnosti daného pododboru by vedeli najlepšie povedať ľudia, ktorí sa mu venujú (všetko sa dá spochybniť, ale už v úvode je naznačené, že zrejme nie je veľký problém nájsť príklad ako sú jednotlivé odbory poprepájané, čo prideľuje aj každému pododboru určitú vážnosť). Takýmto pododborom informatiky je aj bezpečnosť.

A to je práve odbor, ktorému som sa rozhodol venovať v svojej bakalárskej práci. Ak niekto neverí, že je to dôležitý odbor, nech si spomenie napríklad na svoj e-mailový účet, ktorý by ako komunikačný prostriedok nemohol bez bezpečnosti fungovať (bezpečnosť zahŕňa aj autentifikáciu vlastníka účtu pomocou hesla, ak sa napríklad prihlasujete do svojho e-mailového účtu...).

Konkrétna oblasť, ktorej som sa rozhodol venovať je phishing - "lov údajov cez internet". Celé to chcem brať z pohľadu honeypotov, teda skúšať pozorovať útočníkov, ktorí phishing používajú na získavanie citlivých informácií, ako sú napríklad prihlasovacie údaje, a získané informácie analyzovať. Čo s tým útočník robí? Ako pristupuje k získaným informáciám? Ako je na tom momentálne výskum v tomto smere? Ako je možné sa proti phishingu brániť? Akým novým pohľadom by som vedel prispieť do tejto

problematiky ja?

Práve to sú otázky, ktoré budem rozoberať v mojej bakalárskej práci. Práve to sú otázky, ktorým by som sa chcel viac venovať nejaké obdobie s cieľom prispieť k výskumu v oblasti počítačovej bezpečnosti, čo ma zároveň veľmi baví, aj keď to chce často úsilie a námahu. Avšak, čo dobré, čo zároveň stojí za to, je v živote jednoduché?