ANALÝZA INTERNETOVÝCH HROZIEB A METÓD ÚTOČNÍKOV S VYUŽITÍM HONEYPOTOV A HONEYNETOV

Matej Zuzčák[1]

[1]*Katedra informatiky a počítačov, Prírodovedecká fakulta, Ostravská univerzita v Ostrave, 30. dubna 22, 701 03 Ostrava,*

+421914236610, R11265@student.osu.cz

Abstrakt. V posledných rokoch sa množstvo bezpečnostných incidentov a útokov v rámci internetu i lokálnych sieti neustále zvyšuje. Za účelom budovania efektívnej línie ochrany voči týmto hrozbám je potrebné získať o útočníkoch a ich postupoch čo najviac informácií. K tomuto cieľu efektívne dopomáhajú nástroje nazývané ako honeypot. Nasledujúci článok v stručnosti poukazuje na výsledky získané počas 3-mesačného výskumu. Počas tohto obdobia bol za výskumnými účelmi zriadený malý honeynet, skladajúci sa zo 4 honeypotov s nízkou mierou interakcie. Išlo o honeypot Dionaea určený pre analýzu malware smerovaného na systémy Microsoft Windows a o 1 honeypot Kippo, ktorý analyzoval útoky smerujúce na linuxové systémy. Text veľmi stručne sumarizuje najpodstatnejšie výsledky a závery.

Verejne publikované informácie vychádzajúce z použitia honeypotov a honeynetov sa v súčasnosti objavujú len veľmi sporadicky. Väčšina spomínaných projektov neposkytuje dáta o útokoch v miere umožňujúcej ďalšie analýzy, či v požadovanej aktuálnosti. Hlavným dôvodom marginálneho výskytu týchto informácií je najmä obava autorov projektov o zneužitie takto získaných dát, ale i finančný aspekt smerujúci skôr k ich komerčnému uplatneniu.

Hlavným cieľom výskumu tak bolo identifikovať najvhodnejšie implementácie honeypotov s nízkou mierou interakcie, ktoré je možné nasadiť v rámci vlastného honeynetu. Následne použité nástroje vhodne optimalizovať a získavať dáta, ktoré nie sú iným spôsobom dostupné. Tieto dáta tak vytvorili čiastočný pohľad na aktuálnu situáciu v oblasti trendov, ktoré prevládajú medzi útočníkmi. V poslednej fáze bolo možné z takto získaných dát vyvodiť určité závery a vyhodnotiť možnosti ďalšieho výskumu, dodatočnej optimalizácie, perspektívu následnej využiteľnosti dát, či možnosti efektívnejšieho spôsobu ochrany pred počítačovými útokmi.

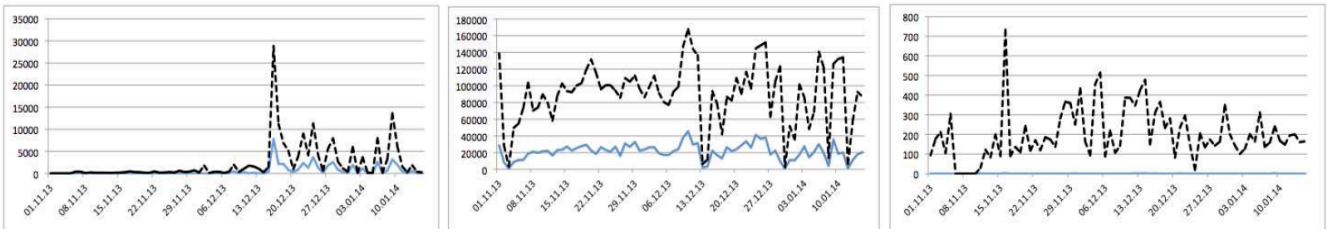
Honeypot predstavuje systém, ktorý slúži na prilákanie útočníka a následnú analýzu jeho správania. Možno ho klasifikovať v rámci niekoľkých kategórií. Na základe aktivity – ako pasívny (serverový), emulujúci zraniteľnosti systému, čakajúci na útok a aktívny (klientsky) simulujúci zraniteľný klientsky softvér, aktívne vyhľadávajúci hrozby. Z pohľadu interakcie môže ísť o systém s nízkou mierou interakcie – emulujúci konkrétnu zraniteľnosť a naopak o vysokú mieru interakcie, ktorá dáva útočníkovi k dispozícii celý systém. Okrem tu spomínanej klasifikácie existuje i celá rada ďalších rozdelení a pohľadov na túto problematiku. [1] [2]

Ako už bolo spomenuté v honeynete vytvorenom za účelmi tohto výskumu boli použité 2 typy riešení. Dionaea honeypot emuloval zraniteľnosti populárnych služieb ako SMB a pod. Honeypot Kippo emuloval pre útočníkov shell bežiaci na porte 22 – sprostredkovaný protokolom SSH. Skúmané boli i meta-dáta ako napríklad geografické informácie o útočníkoch, mená a heslá použité za účelom prihlásenia sa atď. Tieto informácie pomáhali vykresliť celkovú mozaiku poznatkov. Honeypoty (senzory) boli umiestnené nasledovne: prvý Dionaea honeypot v serverovom centre Ostravskej univerzity a pripojený do siete CESNET. Druhý Dionaea senzor bol umiestnený na VPS hostingu v Prahe. Tretí Dionaea senzor sa nachádzal na Spojenej škole

v Kysuckom Novom Meste pripojenej do siete SANET. Kippo senzor sa nachádzal na ďalšom VPS hostingu v Prahe.

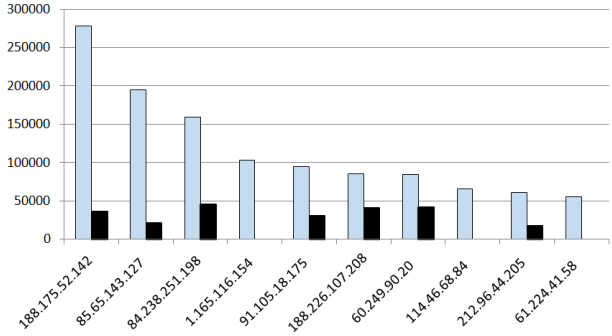
Výsledky plynúce z dát získaných senzormi zaradenými v honeynete sú rozdelené do dvoch sekcií podľa cieľového emulovaného systému na honeypote – Windows a Linux.

Na úvod sa pohľad na aktivitu troch vyššie spomínaných Dionaea senzorov za obdobie 3 mesiacov umiestnených v rôznych lokalitách, v poradí: senzor umiestnený na OSU, na VPS, v Prahe, na Spojenej škole.



Obrázok 1 - Čiarkovaná čierna čiara predstavuje všetky spojenia smerujúce na senzor, modrá čiara predstavuje počet stiahnutých binárnych súborov (zvyčajne vzoriek obsahujúcich malware).

Možno konštatovať, že najviac atakovaným senzorom bol honeypot umiestnený na VPS hostingu v Prahe. Akademické siete sa tak nejavia útočníkom ako dostatočne zaujímavé. Počas prevádzky bola zaznamenaná na Dionaea senzory nasledovná, čo sa spojení týka: Možno si povšimnúť, že počet spojení je značne vyšší ako počet spojení, kde došlo k distribúcií binárneho súboru – najčastejšie malware. Dôvody môžu byť rôzne od chyby pri spojení až po filtráciu na trase od útočníka k obeti.



Obrázok 2 - Modrá farba reprezentuje všetky spojenia smerujúce na honeynet, čierna spojenia, kde došlo i k distribúcií malware.

Najatakovanejším sieťovým portom sa stal port 445 (používaný protokolom SMB), nasledovaný portom 80 a 1443. Najrozšírenejšou infiltráciou, ktorá bola zachytená sa stal červ Conficker a jeho najrôznejšie varianty (3 najviac zachytené: Conficker AL, AE, AA). Z celkového počtu zachytených vzoriek – 9.3387 milióna len 665 nebolo identifikovaných ako Conficker. Tieto údaje o najrozšírenejšom malware však nemožno brať celkom objektívne. Honeypot Dionaea sa totiž vyznačuje v najlepšej miere emulácie práve pri protokole SMB, cez ktorý sa primárne najlepšie šíri červ Conficker. Rozšírenosť tohto červa však poukazuje na veľmi flagrantný prístup užívateľov k aktualizácií svojich operačných systémov a vysokú aktivitu botnetov.

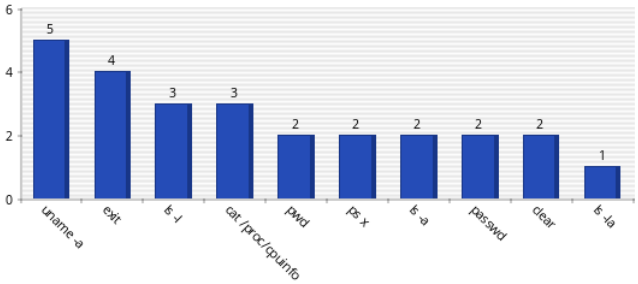
Ďalší pohľad na trendy v oblasti útokov bol získaný analýzou dát, ktoré poskytol Kippo senzor.

Nasledujúca tabuľka zobrazuje 4 najpočetnejšie kombinácie mien a hesiel, ktoré boli použité pri prieniku do emulovaného shellu.

Meno	Heslo	Počet útokov
root	123456	215
root	admin	190
root	root	85
root	1qaz2wsx	78

Tabuľka 1 - Najpoužívanejšie kombinácie prihlasovacích údajov.

Príkazy, ktoré boli najčastejšie vykonávané útočníkmi na emulovanom systéme:



Obrázok 3 - Najčastejšie používané príkazy.

Na základe získaných dát vysokou pravdepodobnosťou možno tvrdiť, že sa jednalo hlavne o automatizované útoky a počiny tzv. script-kiddies.

Celkovo výskum poukázal na aktuálne rozšírené trendy v oblasti internetových hrozieb. Ponúkol tiež dostatok dát, ktorých následná analýza prinesie udanie smerovania pre pokračovanie výskumu. Dáta môžu tiež poslúžiť pre účely zamedzenia útokov pomocou bezpečnostných nástrojov (napr. blacklisty firewallov). Tiež je možné vytvoriť si obraz atraktivity jednotlivých sietí na základe útočenia na jednotlivé honeypoty. V komplexnom aspekte možno povedať, že akýkoľvek systém pripojený na internet, vlastniaci verejnú IP adresu je ihneď pod značným tlakom útokov najmä zo strany automatizovaných robotov. Výskum ukazuje i podceňovanie aktualizácie systémov, čo umožňuje šírenie infiltrácií aj napriek faktu, že aktualizácie pre zraniteľnosti, ktoré používajú sú dostupné už niekoľko rokov.

Kľúčové slová: *počítačový útok, honeynet, honeypot, malware, internetová hrozba*

Poďakovanie

Poďakovanie za pomoc, zásadné rady a koordináciu práce patrí RNDr. Tomášovi Sochorovi CSc. Poďakovanie za poskytnutie technického zabezpečenia pre možnosť umiestnenia senzorov patrí Centre informačných technológií Ostravskej univerzity v Ostrave a Spojenej škole v Kysuckom Novom Meste. Za odborné konzultácie ďakujem pánovi Davidovi Vorelovi – vedúcemu českej kapitoly združenia The Honeynet.org a pracovníkom organizácie CZ NIC Labs.

Literatúra

[1.] **R.C. Joshi, Anjali Sardana.** Honeypots A New Paradigm to Information Security. USA: Science Publishers. 2011. 339 s. ISBN 978-1-57808-708-2.

[2.] Eric Peter, Todd Schiller, Raj Jain. A Practical Guide to Honeypots. Cs.wustl.edu. [online], [citované: 21. januára 2014]. Dostupné z WWW: http://www.cs.wustl.edu/~jain/cse571-09/ftp/honey/