Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Výskyt počítačových červů ve veřejné síti

Jan Haluza

© 2020 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jan Haluza

Systémové inženýrství a informatika
Informatika

Název práce

Výskyt počítačových červů ve veřejné síti

Název anglicky

Presence of computer worms in the public network

Cíle práce

Hlavním cílem bakalářské práce je stanovit postupy pro zabezpečení počítačové sítě před počítačovými červy. Dílčí cíle jsou analyzovat výskyt tohoto typu malware ve veřejné síti a analyzovat současné přístupy k ochraně.

Metodika

Bakalářská práce je založena na průzkumu veřejné sítě a studiu odborné a vědecké literatury. Na základě poznatků z pozorování, analýzy dat a odborných zdrojů bude syntetizován závěr práce.

Doporučený rozsah práce

40 – 50stran

Klíčová slova

Bezpečnost počítačových sítí, malware, počítačoví červi

Doporučené zdroje informací

ANBAR, Mohammed, Rosni ABDULLAH, Alhamza MUNTHER, Mohammed AL-BETAR a Redhwan SAAD. NADTW: new approach for detecting TCP worm. Neural Computing [online]. 2017, 28, 525-538 [cit. 2019-06-09]. DOI: 10.1007/s00521-016-2358-9. ISSN 09410643.

Basic definitions for discrete modeling of computer worms epidemics. Ingeniería e Investigación [online]. 2015, 35(1), 79-85 [cit. 2019-06-09]. DOI: 10.15446/ing.investig.v35n1.44323. ISSN 01205609.

OCHIENG, Nelson, Waweru MWANGI a Ismail ATEYA. Optimizing Computer Worm Detection Using Ensembles. Security and Communication Networks [online]. 2019, 2019 [cit. 2019-06-09]. DOI: 10.1155/2019/4656480. ISSN 19390114.

SHAHZAD, Khurram, Steve WOODHEAD a Panayiotis BAKALIS. An investigation of mechanisms to mitigate zero-day computer worms within computer networks [online]. 2015 [cit. 2019-06-09]. ISSN edsble.

ZHANG, Changwang, Shi ZHOU a Benjamin m. CHAIN. Hybrid Epidemics—A Case Study on Computer Worm Conficker. PLoS ONE [online]. 2015, 10(5), 1-17 [cit. 2019-06-09]. DOI: 10.1371/journal.pone.0127478. ISSN 19326203.

Předběžný termín obhajoby

2019/20 LS – PEF

Vedoucí práce

Ing. Alexandr Vasilenko, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 11. 10. 2019

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 14. 10. 2019

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 23. 03. 2020

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Výskyt počítačových červů ve veřejné síti" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 23.3.2020 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Alexandru Vasilenkovi, Ph.D. za odborné vedení, za pomoc a rady při zpracování této práce.

Výskyt počítačových červů ve veřejné síti

Abstrakt

Předmětem této bakalářské práce je ochrana před počítačovými červy a jejich výskyt ve veřejné síti. Hlavním cílem bakalářské práce je stanovit postupy pro zabezpečení počítačové sítě před počítačovými červy. Dílčí cíle jsou analyzovat výskyt tohoto typu malware ve veřejné síti a analyzovat současné přístupy k ochraně. Ke zkoumání výskytu počítačových červů ve veřejné síti byl využit program Wireshark, k sestavení vyhledávacích filtrů byl využit uživatelský manuál za účelem kontroly syntaxe samotného programu, která je k vyhledávacím filtrům stejná jako u *tcpdump, WinDump, Analyzer* a jakýkoliv další program, který využívá knihovny libpcap/WinPcap a řídí se syntaxí *libpcap filter language*. Dále také studium odborné literatury a dalších zdrojů k definici způsobu šíření jednotlivých červů, převážně jejich využívání konkrétních síťových protokolů a portů. Ke stanovení postupů k zabezpečení vycházel autor dle metodiky z vlastního průzkumu sítě a studia literatury. Postupy k zabezpečení počítačové sítě před počítačovými červy byly stanoveny, současné přístupy k ochraně analyzovány a proběhl průzkum veřejné sítě s následným odhalením počítačových červů.

Klíčová slova: Bezpečnost počítačových sítí, malware, počítačoví červi

Presence of computer worms in the public network

Abstract

This bachelor thesis is focused on computer worm prevention and their presence in the public network. Main objective of this bachelor thesis is to define procedures to secure computer network from computer worms. Partial objectives are to analyse the presence of this malware in the public network and to analyse current protection approaches. For computer worm investigation in the public network was used Wireshark, for setting capture filters was used user guide to control the program syntax, which uses the same syntax for capture filters as tcpdump, WinDump, Analyzer, and any other program that uses the libpcap/WinPcap library and commands are written in libpcap filter language. Then also studying scholarly literature and other resources to define the way of how certain computer worm spread, mainly by their usage of specific network protocol and ports. To define procedures to secure the network, author proceeded based on methodology and own research of the network and study of literature. Procedures to secure computer network from computer worms were defined, current protection approaches analysed, and public network has been explored, with subsequent disclosure of computer worms.

Keywords: Computer network security, malware, computer worms

Obsah

Seznam obrázků

1 Úvod

V dnešní době si člověk život bez počítače a internetu zvládne jen stěží představit. Informační technologie se staly nedílnou součástí nejen našich pracovních, ale také osobních životů. Spolu s vývojem každé technologie ovšem přichází i její zneužívání, což pro všechny uživatele představuje konstantní riziko. Vývojáři software na jednu stranu jejich systémy neustále zdokonalují, stejně se ovšem zdokonalují i kybernetičtí útočníci a nacházejí nové mezery v zabezpečení, které by mohli zneužít ke krádeži osobních dat, finančních prostředků, výpočetního výkonu, či v nedávných případech k uzamčení dat a požadování výkupného za jejich odemčení. Zároveň je třeba být na pozoru i před hrozbami známými. Určité druhy malware, jako jsou počítačoví červi, je obtížné zcela eliminovat a podobně jako lidské nemoci se vrací ve vlnách, či neustále parazitují na určitém množství počítačové populace, a to s jediným cílem – další reprodukce. Původně šlo o pouhou myšlenku kódu, který by se sám replikoval. Časem se však z myšlenky stal pokus a z pokusu zbraň. V minulosti se několikrát stalo, že počítačový červ napáchal škody za miliony dolarů, paralyzoval výrobu či fungování nemocnice, nebo i v přes původně dobrý záměr zahltil síť. Nutno také dodat, že červi samotným šířením nemusí nutně napáchat až takové škody, mohou ovšem udělat prostor dalším, destruktivnějším typům malware. Z toho důvodu je potřeba dodržovat různá opatření a aplikovat postupy k zabezpečení našich počítačových sítí před tímto typem malware. Právě těmi se tato práce zabývá. Dále byl zkoumán výskyt počítačových červů na veřejné síti. K tomu byl využit program Wireshark, který používá stejnou syntaxi k vyhledávacím filtrům jako *tcpdump, WinDump, Analyzer* a jakýkoliv další program, který využívá knihovny libpcap/WinPcap, jde tedy o *libpcap filter language.*

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem bakalářské práce je stanovit postupy pro zabezpečení počítačové sítě před počítačovými červy. Dílčí cíle jsou analyzovat výskyt tohoto typu malware ve veřejné síti a analyzovat současné přístupy k ochraně.

2.2 Metodika

Bakalářská práce je založena na průzkumu veřejné sítě a studiu odborné a vědecké literatury. Na základě poznatků z pozorování, analýzy dat a odborných zdrojů bude syntetizován závěr práce.

3 Teoretická východiska

3.1 Počítačová síť

Pojmem počítačová síť se rozumí zejména spojení dvou a více počítačů tak, aby mezi sebou mohli komunikovat a navzájem sdílet své prostředky. Nezáleží přitom zda se jedná o prostředky hardwarové nebo softwarové. Před nástupem počítačových sítí musel mít každý počítač, ze kterého se chtělo tisknout, vlastní tiskárnu. Případně se musel dokument k tisku nahrát na disketu a odnést k počítači s tiskárnou a poté dokument vytisknout. Horší však situace nastala, pokud s jedním dokumentem nebo jednou databází pracovalo více osob. V takovém případě se totiž nedalo zaručit, že všichni mají ve stejném okamžiku stejnou verzi s úpravami, které provedl kolega před hodinou. Tyto dva příklady nám ukazují práci v samostatném prostředí. Význam počítačových sítí neustále roste. Sítě se uplatňují jak ve firmách, tak i při výuce na školách. I doma má dnes mnoho lidí svoji malou síť – nemluvě o připojení k internetu. Počítačová síť je tedy systém, který vzniká komunikačním propojení počítačů, případně další IT techniky. Aby mohla vzniknout počítačová síť je zapotřebí dvou základních věcí. Síťový HW, který umožňuje vlastní fyzické propojení (síťová karta, přenosové médium, propojovací síťové prvky) a síťový SW, který se stará se o přesuny dat, komunikaci, navazování spojení a další služby jako např. zabezpečení apod. (firmware, ovladače, síťový OS, aplikace …)

3.1.1 LAN – lokální síť

Zpočátku se používaly malé sítě, s asi deseti navzájem propojenými počítači a tiskárnou. Velikost sítě, včetně počtu počítačů, omezovala dostupná technologie. Dnes už je možné dosáhnou podstatně větších sítí. Takovým sítím (na jednom podlaží budovy nebo v jedné malé firmě) se říká lokální síť (LAN z anglického „*Local Area Network*“).

Většina moderních sítí LAN podporuje širokou škálu počítačů a jiných zařízení. Každé zařízení musí používat vlastní fyzické protokoly a protokoly datového spojení pro konkrétní síť a všechna zařízení, která chtějí komunikovat se všemi ostatními v síti, musí používat stejný komunikační protokol. Ačkoliv jednotlivé sítě LAN jsou prostorově omezeny, mohou být propojeny do větších sítí. Podobné sítě LAN se

propojují pomocí mostů (*bridge*), které slouží jako body přenosu mezi sítěmi, rozdílné sítě LAN se spojují bránami (*gateways*), které přenášejí data a zároveň je konvertují podle protokolů používaných sítí příjemce.

Sítě se rozdělují podle poměru doby vysílání a přijímání dat. U LAN sítí je doba vysílání t_v vyšší než doba šíření signálu t_s po přenosovém médiu ($t_v > t_s$).

3.1.2 MAN – metropolitní síť

Veřejná síť pracující vysokou rychlostí a schopná přenášet data na vzdálenost až několika desítek km. Většinou podporuje data i hlas. Tato síť je menší než WAN ale větší než LAN. Klasifikačně pro ni platí přibližně to stejné, co v síti LAN (viz výše).

Síť MAN má přibližně stejnou dobu vysílání jako šíření signálu ($t_v \approx t_s$).

3.1.3 WAN – rozlehlá síť

S růstem geografického dosahu sítí připojováním uživatelů v různých městech nebo státech přerůstá síť LAN a MAN do sítě WAN (*Wide Area Network*). Sítě WAN jsou tedy obecně rozlehlé a mohou propojovat obrovské množství uživatelů na rozloze do asi 1000 km. V tomto ohledu existuje i pojem GAN (*global area network*), taková globální síť pak vlastně propojuje jednotlivé WAN sítě. Veřejnou globální sítí je např. internet.

Doba vysílání je menší než doba šíření ($t_v < t_s$) [1].

3.2 Internet

Koncepční základ k vytvoření Internetu byl převážně vytvořen třemi jedinci a jednou výzkumnou konferencí. Zasadili se o změnu našeho pohledu na technologii a důvěrně předpověděli její budoucnost.

- Vannevar Bush sepsal první vizionářský popis potencionálního využití informačních technologií s jeho popisem automatického systému knihoven memex.
- Norber Wiener vynalezl vědní obor kybernetika a inspiroval budoucí vědce k zaměření technologie na rozšíření lidských schopností.
- Marshall McLuhan přišel s myšlenkou globální obce propojené elektronickým nervovým systémem jako součást naší populární kultury.

- *The 1956 Dartmouth Artificial Intelligence conference*, tedy konference o umělé inteligenci na univerzitě Dartmouth v roce 1956 ukázala, že se technologie exponenciálně vyvíjí a poskytla první vážné zvážení důsledků.

V roce 1957 Sovětský svaz vypustil první satelit Sputnik I, což přimělo někdejšího prezidenta Spojených států amerických Dwighta Eisenhowera k založení vládní agentury ARPA, s cílem znovuzískání technologického náskoku v závodu ve zbrojení. ARPA jmenovala hlavou nové organizace IPTO J.C.R. Licklidera s pověřením k dalšímu výzkumu programu SAGE a ochraně Spojených států před vesmírným jaderným útokem. Licklinder v rámci IPTO uvažoval také nad potencionálními přínosy celostátní komunikační sítě a přiměl své nástupce k zaměstnání Lawrence Robetrse, který jeho vizi realizoval.

Roberts byl v čele vývoje sítě založené na nové myšlence *packet switching* (přepojování packetů) vynalezené Paulem Barandem v RANDu a o pár let později Donaldem Daviesem v *UK National Physical Laboratory* (Národní fyzikální laboratoř Spojeného království). Tento návrh byl realizován vývojem speciálního počítače zvaném *Interface Message Processor* (IMP) a fungoval jako uzel přepínání paketů, začátkem října 1969 byl zprovozněn ARPANET. První komunikace proběhla mezi výzkumným centrem Leonarda Kleinrocka na Kalifornské univerzitě v Los Angeles a centrem Douglase Engelbarta na Stanfordském výzkumném ústavu.

První síťový protokol, který se používal na ARPANETu byl *Network Control Program* (Program řízení sítě). V roce 1983 byl nahrazen *TCP/IP* protokolem, vytvořen Robertem Kahnem, Vintonem Cerfem a dalšími, který se brzy stal nejrozšířenějším síťovým protokolem na celém světě.

V roce 1990 byl ARPANET převeden na NSFNET. Ten byl brzy následně připojen k CSNETu, který spojoval univerzity v severní Americe a později k EUnetu, který propojoval výzkumná zařízení v Evropě. Díky správě NSF a popularitě webu používání internetu v roce 1990 explodovalo, což následně roku 1995 přimělo vládu USA k přenesení řízení na nezávislé organizace. A tak jsme se dostali do stavu, který trvá dodnes [2].

3.3 World Wide Web

Od jeho založení v roce 1989 *World Wide Web* (celosvětová síť) ovlivnil životy miliard lidí po celém světě a zásadně změnil způsob, jakým mezi sebou komunikujeme, podstatu našich prací, jak objevujeme a sdílíme nové nápady, jak se zabavujeme a jak se tvoří a fungují komunity. *World Wide Web* byl projekt CERNu (Evropská organizace pro jaderný výzkum) s názvem ENQUIRE, který zahájil britský vědec Tim Berners-Lee. V úvahu byly také kupříkladu názvy jako *The Information Mesh* (Informační síť) či *The Mine of Information* (Důl informací). V téže roce společnost AOL (americký poskytovatel internetových služeb) spustila instantní chatovou službu a začala uživatele vítat ikonickým pozdravem *"You've got mail!"*, čili „Máte mail!".

V roce 1990 již počítač používalo 42 % dospělých Američanů. Byla také vytvořena první webová stránka a server *go life at CERN*, který běžen na počítači NeXT Tima Bernerse-Lee, z toho důvodu na něm bylo napsáno *"This machine is a server. DO NOT POWER DOWN!"*, tedy „Tento stroj je server. NEVYPÍNAT". Tim Barnes-Lee zároveň vyvinul první webový prohlížeč *WorldWideWeb.* První internetový vyhledávač Archie byl vyvinut studentem univerzity McGill Alanem Emtagem.

V roce 1991 vědečtí pracovníci sestavili živý záběr kávové konvice, aby mohli ze svých počítačových obrazovek vidět, kdy se čerstvá káva dovaří. Následným připojením k *World Wide Webu* vznikla první web kamera.

V roce 1992 se objevil pojem „surfovat na internetu". Tim Berners-Lee zveřejnil na webu první fotku, šlo o kapelu *"Les Horribles Carnettes".* Spustil se *Line Mode Browser.* Jde o první jednoduchý univerzální textový webový prohlížeč.

V roce 1993 CERN umístil *World Wide WEB* technologii na veřejnou doménu a daroval ji tím světu. Národní centrum pro superpočítačové aplikace (NCSA) vydalo Mosaic 1.0, první prohlížeč, který se stal populárním u široké veřejnosti. „Web, jak ho známe, začíná vzkvétat", píše Wired [3].

3.4 Malware

Označení malware vzniklo spojením dvou anglických slov *malicious software*, tedy škodlivý či zákeřný software. Jde o termín používaný pro označení škodlivé aplikace a kódu který může poškodit zařízení a přerušit jeho běžné užívání. Malware může umožnit neautorizovaný přístup, využívat zdroje systému, krást hesla, odstřihnout uživatele od počítače a žádat výkupné a další. Kybernetičtí zločinci, kteří rozesílají malware jsou často motivování penězi a použijí infikované počítače k dalším útokům, získávají bankovní údaje, sbírají informace, které mohou být prodány, prodávají přístup k výpočetním zdrojům, nebo oběti vydírají [4]. V průzkumu od [5], se *malware event*, tedy pokus o napadení malwarem, v podniku objeví každé 3 minuty a útoky míří na mnoho oblastí. Výsledkem jsou znepokojující ztráty intelektuálního vlastnictví, záznamů o zákaznících anebo dokonce i zničením dat [6].

3.4.1 Virus

Počítačový virus můžeme označit jako sadu programových instrukcí, kus kódu, která napadne soubor nebo program a stane se tedy jeho součástí. Pomocí lidského zásahu se dále replikuje se a šíří i do ostatních souborů [7].

3.4.2 Trojský kůň

Trojský kůň je program, který se sám nereplikuje. Místo toho předstírá užitečnou funkcionalitu a při instalaci či spuštění souběžně vykonává škodlivou činnost. Například zapojí napadený stroj do tzv. botnetu (síť infikovaných strojů, které lze na dálku ovládat), krade uživatelská data a instaluje další škodlivý software. Během své instalace může využít bezpečnostních děr daného systému (např. díky chybějícím aktualizacím) a získat vyšší oprávnění než běžný software. Často také bývá připojen k žádoucímu programu, který si uživatel chce nainstalovat [7].

3.4.3 Počítačoví červi

Počítačový červ je program, jehož hlavní vlastností je schopnost se šířit skrz datovou síť bez přímé účasti uživatele. Jakmile je jeho tvůrcem vypuštěn, kód sám sebe automaticky replikuje a zneužívá chyb v operačních systémech a síťových zabezpečovacích protokolech, podle účelu, za jakým byl vytvořen. Využívá

automatické procesy OS, aby pro uživatele zůstal neviditelným a těžko detekovatelným. Poškození způsobené červy je značné, především jde o velkou destabilizaci systému a sítě [7] [8]. Jejich šíření je velmi rychlé, dokáží nakazit až 359,000 počítačů za méně než 14 hodin [6]. Základními druhy jsou e-mailový a internetový červ.

E-mailoví červi začínají jako emailová příloha, která při otevření nakazí počítač. Vyžadují tedy akci ze strany uživatele. Červ hledá v nakaženém počítači soubory obsahující e-mailové adresy, jako jsou například adresáře nebo dočasné webové stránky. Červ pak tyto adresy použije k rozesílání nakažených e-mailových zpráv a často napodobuje (nebo falšuje) adresu odesílatele v těchto e-mailových zprávách tak, aby to vypadalo, že původcem nakažené zprávy je někdo, koho daný uživatel zná. Červ se pak automaticky šíří díky chybám zabezpečení e-mailových zpráv [9].

O internetových červech pojednává kapitola 3.5.

3.4.4 Zero day worms

Zero day worms, neboli červi nultého dne jsou speciálním případem počítačových červů. Odhalit chybu v zabezpečení systému, která by se dala využít k šíření počítačového červa, není snadné. Proto je běžné, že samotnou chybu objeví autor softwaru, vydá aktualizaci, která tuto chybu opravuje, čímž jí ovšem zároveň zveřejní. Útočníci poté využijí tuto chybu ke tvorbě a šíření malware a spoléhají přitom na pomalou reakci ze strany uživatelů. Červ se tedy začne šířit až několik dní poté, co proti němu již existuje ochrana. Červi nultého dne jsou tedy takoví červi, u kterých jejich autor využívá k šíření dosud neznámou zranitelnost systému a žádná ochrana při počátku šíření není dostupná. Příkladem je Stuxnet. [10]

3.4.5 Spyware

Spyware se může nainstalovat do počítače bez povědomí uživatele. Tyto programy mohou měnit konfiguraci počítače nebo sbírat reklamní data a osobní údaje. Spyware může také sledovat zvyky uživatele při hledání v internetu a rovněž přesměrovat uživatele na jiný web, než na který chtěl přejít [9].

3.4.6 **Adware**

Jako adware označujeme software, který se zaměřuje na zobrazování reklamy uživateli. Po napadení počítače pozměňuje obsah zobrazovaných webových stránek, kde nahrazuje a přidává vlastní reklamní bannery, vyskakující reklamní okna a další [7].

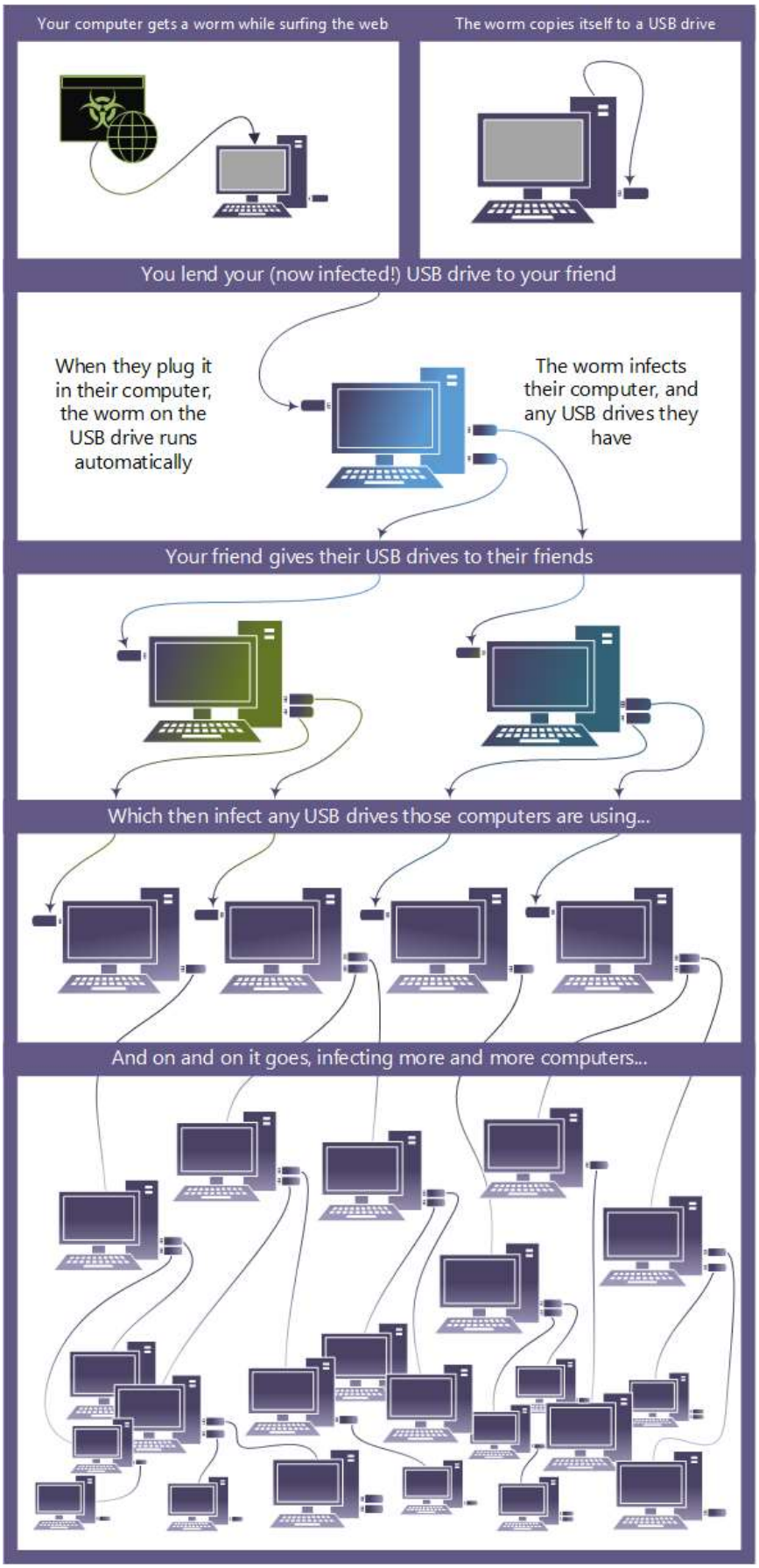
3.4.7 **Keylogger**

Keylogger je software pro zachytávání, záznam a odeslání znaků psaných na klávesnici. Takto lze od uživatelů bez jejich vědomí získat hesla, obsah osobní a obchodní korespondence, či důvěrných dokumentů vytvořených na infikovaném počítači. Jedná se o velmi oblíbenou a nebezpečnou formu útoku právě díky možnosti získání hesel k dnes velmi rozšířeným webovým službám (email, internetové bankovnictví, ...) [7].

3.4.8 **Podvodný bezpečnostní software**

Podvodný bezpečnostní softwarový program se uživatele pokusí přesvědčit, že jeho počítač je nakažen virem, a zpravidla vyzývá ke stažení nebo nákupu produktu, který tento virus odstraní. Názvy těchto programů často obsahují slova jako antivirus, *shield* (ochranný štít), *security* (zabezpečení), *protection* (ochrana) nebo *fixer* (opravy). To má vzbudit zdání legitimity. Tyto programy se často spustí ihned poté, co je stáhnete, nebo při příštím spuštění počítače. Podvodný bezpečnostní software může rovněž bránit některým aplikacím, například aplikaci Internet Explorer, ve spuštění. Podvodný bezpečnostní software může rovněž zobrazit legitimní a důležité soubory systému Windows jako nakažené [9].

Obrázek 1: Rychlost šíření červa přes sdílený USB disk [10]



3.5 Taxonomie internetových červů

Počítačové červy lze klasifikovat různými způsoby dle schéma hledaní svých cílů, schéma přenosu, datového obsahu, záměru vývojáře a dle výskytu, následovně:

3.5.1 Dle schéma hledání cílů

Hledáním cílů se myslí mechanismy, kterými červ objevuje nové cíle k napadení. Schémata se dají rozdělit na: skenovací, hit-list, warhol, flash a další. Internetoví červi jsou zpravidla skenující a používají různé způsoby (náhodný, sekvenční, permutační atd.) k šíření. Skenováním se myslí proces prozkoumávání sady IP adres k rozpoznání zranitelných hostitelů. Například, SQL slammer, Nimda, Code Red, jsou náhodně skenující červi. Toto jsou různé základní způsoby skenování, jaké může červ použít:

- **Sekvenční**: Pracuje skrz adresový blok a používá uspořádanou sadu IP adres.
- **Náhodný**: Generuje IP adresy z bloku pseudo-náhodným způsobem
- **Permutační**: Toto je způsob skenování kde se jednotlivé instance červa se koordinují navzájem tak, aby každá instance skenovala oddělenou část adresního prostoru.

Tyto základní způsoby skenování mohou být spojeny tak, aby vytvořily následná komplexnější schémata:

- **Skenování dle důležitosti**: Červ používající tuto techniku se šíří ve dvou fázích: v první fázi je k vytvoření počátečnímu rozdělení zranitelných hostitelů použito náhodné nebo směrovací skenování. Ve druhé fázi je poté využita „technika vzorkování důležitosti“ (angl. *Importance sampling technique*) ke snížení počtu skenů a rychlému útoku na velký počet zranitelných hostitelů.
- **Topologický**: Topologický skenovací červ používá interní seznam cílů, který je vytvořen na základě hledání lokálních informací v síti, jako /etc/hosts soubor u Unixových hostitelů, nebo topologické informace použitím ARP tabulky mezi paměti a netstat (síťových statistik).

- **BGP skenování**: BGP (*Border Gateway Protocol*) směrovací červ využívá BGP skenovací techniky, které používají BGP směrovací tabulky k zúžení skenovaného adresního prostoru. Tento typ červa je schopný zaměřit konkrétní hostitele ve specifické geografické lokaci, jako například v konkrétním státě, ISP (poskytovatel internetového připojení) nebo samosprávný systém a může se šířit 2krát až 3krát rychleji než tradiční náhodně skenující červ.
- **Meta-server**: Meta-server červi používají externě generovaný seznam cílů, zranitelných hostitelů, který je udržován na odděleném serveru.
- **Pasivní**: Pasivní červ nehledá potencionální oběti, místo toho čeká na to, až se cílové zařízení připojí k zařízení, na kterém je umístěn. Příklady jsou Gnuman a CRClean.
- **Hit-list**: Červ šířící se tímto způsobem využívá před-generovaný seznam zranitelných IP adres. Příkladem je Witty, který využívá mimo náhodné skenování a botnet k šíření také Hit-list.
- **Warhol**: Jde o hypotetický, velmi rychle se šířící typ červa, který využívá kombinaci hit-listu, který pomáhá k počátečnímu rozšíření, a permutačního skenování, které je účinnější než náhodné skenování.
- **Flash**: Svým způsobem jde o rozšíření Warholova červa. Obsahuje počáteční hit-list globálního rozsahu. Autoři předpokládali, že červ založený na UDP (*User Datagram Protocol*) by mohl infikovat 95 % z milionu zranitelných hostitelů během 510ms, zatímco červ založený na TCP (*Transmission Control Protocol*) by mohl infikovat tu samou populaci za 1,3s [11, s. 22-26].

3.5.2 Dle schéma přenosu

Schéma přenosu je mechanismus, který červ používá k přenosu sebe sama do cílových hostitelů. Může použít výše zmíněné protokoly, tedy TCP nebo UDP.

- **TCP**: Červ šířící se pomocí tohoto protokolu mívá větší odezvu, jelikož k vytvoření spojení používá *3-way handshake* (trojcestné potvrzení). Příkladem je Code Red.
- **UDP**: Červi šířící se pomocí tohoto protokolu jsou limitováni šířkou pásma a jsou zpravidla schopni rychlejšího šíření. Příkladem je SQL Slammer [11, s. 22-26].

3.5.3 Dle datového obsahu

Datovým obsahem (*payload*) se myslí samotný kód nesený červem, tedy kromě propagačních rutin. Může být používán pro vykonávání různých funkcí, jako používání cílového hostitele ke spamu, jeho zaměstnání jako HTML proxy server, vytváření DOS (*Denial Of Service*) útoků, útoky na servery 911, nebo v rámci kybernetické války útočí na fyzické cíle, jako Stuxnet, jehož cílem bylo sabotovat Íránský jaderný program přeprogramováním programovatelných logických ovladačů. Na základě typu datového obsahu můžeme červy rozdělit na tři kategorie:

- Monomorfní: Datový obsah monomorfních červů se během šíření nemění a vykazuje neměnný podpis. Díky tomu může být snadno detekován systémem založeným na podpisy. V některých případech se u jednotlivých instancí může velikost obsahu lišit, a to kvůli přidávání odpadu – kód který nemá žádnou funkcionalitu. I přesto je však většinou podpis stejný.
- Polymorfní: Datový obsah polymorfních červů se během šíření mění, zachovává však stejnou funkcionalitu.
- Metamorfní: U metamorfních červů se datový obsah také mění, spolu s tím se ovšem upravuje i jejich chování [11, s. 22-26].

3.5.4 Dle záměru vývojáře

Červy lze také klasifikovat na základě záměru jeho autora a to následovně:

- Škodlivý červ: Červ se považuje za škodlivého, jsou-li záměry jeho autora škodlivé, tedy přerušení internetových služeb, fyzická újma ve světě, DOS útoky, ekonomická sabotáž, terorismus, kybernetická válka atd. Příklady jsou Slammer, Code Red, Witty, Stuxnet.
- Prospěšný červ: Někdy takzvaní obranní červi či anti-červi, mohou být vypuštěni se záměrem „zalepování děr“ které zneužívají škodlivé červi pomocí instalování záplat (*patches*). Jsou ovšem také považováni za nelegální, poněvadž tak činí bez svolení uživatele a bez ohledu na svůj záměr zatěžují síť což může vést až k jejímu kolapsu. Příklady jsou Welchia a CRClean [11, s. 22-26].

3.5.5 Dle výskytu

Červy můžeme také následně klasifikovat na základě jejich výskytu:

- Skuteční: Jedná se o existující, implementované počítačové červy. Příklady jsou SQL Slammer, Witty, Code Red.
- Hypotetičtí: Hypotetičtí červi byli pouze navrženi, ale ne vypuštěni. Příklady jsou Flash a Warhol [11, s. 22-26].

3.6 Wireshark

Wireshark je přední a široce používaný program analyzující síťové protokoly na světě. Umožňuje sledovat co se ve vaší síti děje na mikroskopické úrovni, a to je de facto (a často i de jure) standard v mnoha komerčních a neziskových podnicích, vládních agenturách a vzdělávacích institucích. Vývoj Wiresharku se daří díky dobrovolným příspěvkům síťových expertů po celém světě a je pokračováním projektu, který zahájil Gerald Combs v roce 1998 [12].

3.7 Současné přístupy k ochraně

Vývojáři software se pochopitelně snaží, aby v jejich produktech žádné mezery v zabezpečení nebyly. I přes to se čas od času nějaké najdou a každý z těchto vývojářů má rozdílný přístup k řešení takového problému. Z pravidla se jedná o aktualizace, i ty se ovšem dají pojmout více způsoby.

3.7.1 Microsoft

Co se týče počítačových červů, je na tom Microsoft statisticky nejhůře. Většina počítačových červů napadá právě operační systém Windows. I z toho důvodu byli nuceni změnit svou politiku v rámci zabezpečovacích aktualizací.

Pokud se dnes podíváme na stránky Microsoftu [13], najdeme tam ke stažení řadu aktualizací, většinu z těch nejnovějších ovšem pro Windows 7 a 8 a to z toho důvodu, že přešli na automatické aktualizace pomocí Windows Update. V minulosti bylo několik případů, kdy se nejen počítačoví červi ale i další typy malware rozšířili pomocí mezery v zabezpečení, která již byla opravená, ale lidé si neaktualizovali počítač. I přes to je třeba podotknout, že i tyto, pro mnoho lidí otravné automatické aktualizace, se dají vypnout či přinejmenším odložit.

Microsoft obecně podporuje každou řadu Windows jen omezenou dobu a to zpravidla 10 let. V případě potřeby ovšem vydají doplňující aktualizace i pro starší verze, především pokud se objeví kritická chyba v systému.

Mimo výjimečné případy při odhalení mezery v zabezpečení vydává Microsoft aktualizace na *Patch Tuesday*, tedy každé druhé úterý v měsíci [14].

Novější řady Windows také disponují zabudovaným zabezpečovacím softwarem Windows Defender. Zabezpečovací software ať již z důvodu ceny či zkrátka nutné akce ne každý musel dříve využívat.

3.7.2 Linux

Apparmor, no antivirus

Na Linux ve srovnání s Windows neexistuje takové množství malware. Zároveň se díky komunitě a otevřenému zdrojovému kódu neustále testuje a svým způsobem si ho uživatelé mohou neustále upravovat.

I přes to má vlastní způsob ochrany, a to v podobě AppArmoru [15]

3.7.3 **Apple**

Stejně jako v případě Linuxu, kybernetický útok na zařízení s macOS od Applu nelze vyloučit. Část zabezpečení řeší aktualizace a stahování softwaru jen přes ověřený Mac App Store, kde jsou jednotliví vývojáři identifikováni a registrováni, a také pomocí bezpečnostního nastavení. Z hlediska aktualizací se zařízení snaží updatovat na aktuální verzi každý den, automaticky. Uživatel se ovšem může i pojistit komerčním bezpečnostním softwarem [16].

4 Vlastní práce

4.1 Výskyt ve veřejné síti

Na základě výše zmíněné definice počítačových červů je zřejmé, že dokud bude existovat nějaké nakažené zařízení, červ se bude snažit dále šířit. Dají se tedy, stejně jako lidské nemoci, jen stěží zcela vymýtit. Například počítačový červ Conficker, poprvé zaznamenán v roce 2008 byl v roce 2017 zaznamenán na 2564618 počítačích [17] a autor článku se k tomuto objevu vyjadřuje jednoduše. Kdokoliv, kdo používá starý, neaktualizovaný stroj, zůstává zranitelným. Za zmínku stojí, že Microsoft nabídl 250000$ za informace vedoucí k dopadení autora toho to červa, nikdy však nebyla uplatněna. Pokud chceme zkoumat výskyt počítačových červů na veřejné síti, je třeba nejdříve zjistit a pochopit, jak se jednotliví červi šíří a na základě toho vytvořit správné vyhledávací filtry.

4.1.1 Vyhledávací filtry

Při používání tak detailního nástroje jako je Wireshark je nezbytné nějak získávaný záznam omezit na informace, které nás opravdu zajímají. Tento způsob jednak značně usnadňuje práci se získanými daty, dále také šetří místo na disku – záznamy se mohou během několika hodin dostat až na jednotky GB. Wireshark má svůj portál, kde lidé sdílí všemožné filtry, které vymysleli. [18] Z hlediska počítačových červů konkrétně nám sdílené filtry stačit nebudou, dají se ovšem vzít jako příklad a zkombinovat je s žádoucím rozšířením, jak učinil autor této práce. Blaster a Welchia červi se dají najít dle těchto konkrétních příkazů:

```
(dst port 135 and tcp port 135 and ip[2:2]==48)
(icmp[icmptype]==icmp-echo and ip[2:2]==92 and icmp[8:4]==0xAAAAAAAA).
```

Tento filtr hledá *icmp echo* žádost, která je 92 B dlouhá a má icmp náklad, který začíná čtyřmi bajty písmene A (hex). Což je podpis Welchia červa předtím, než se pokusí infikovat systém. Mnozí červi se snaží šířit kontaktováním hostů na konkrétních portech.

SQL Slammer – UDP 1434

Code Red – HTTP GET 80

Rammen – TCP 21, UDP port 111, TCP port 515

Sasser – TCP 445, 139

Conficker – TCP 445

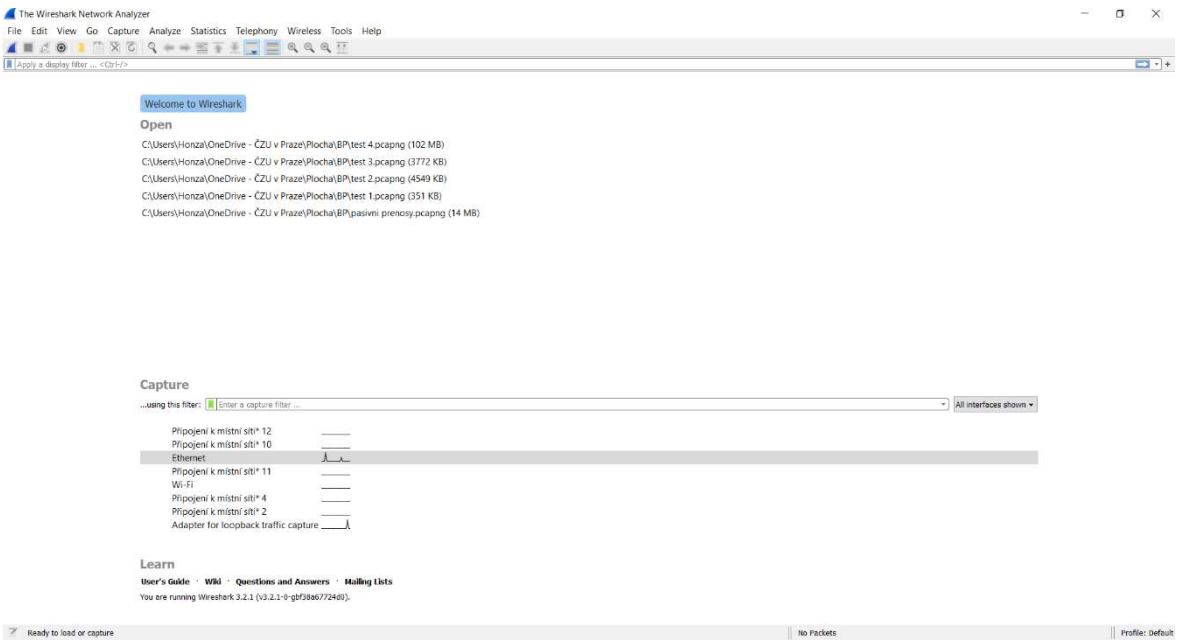
V kombinaci s hledáním SYN paketů lze červy najít následovně:

(port 80 and tcp[((tcp[12:1] & 0xf0) >> 2):4] = 0x47455420) or (tcp dst port 21 or udp dst port 111 or tcp dst port 139 or tcp dst port 445 or tcp dst port 515 or udp dst port 1434 or dst port 135 or dst port 1433 and tcp[tcpflags] & (tcp-syn) != 0 and tcp[tcpflags] & (tcp-ack) = 0) or (dst port 135 and tcp port 135 and ip[2:2]==48) or (icmp[icmptype]==icmp-echo and ip[2:2]==92 and icmp[8:4]==0xAAAAAAAA)

4.1.2 **Analýza výskytu**

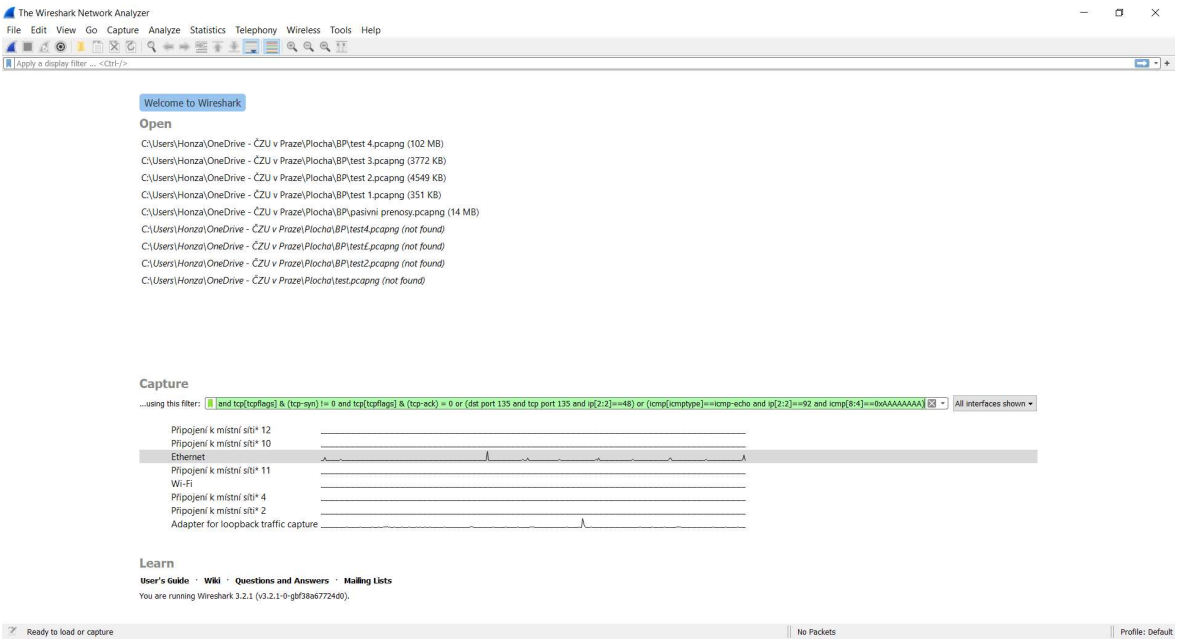
S vytvořeným filtrem jsme tedy připraveni na samotný průzkum sítě. Stáhneme a nainstalujeme Wireshark dle instrukcí z [12]. Po spuštění si vybereme zdroj dat. Z pravidla chceme takový zdroj, u kterého vidíme nějakou činnost. V našem případě tedy Ethernet:

Obrázek 2: Wireshark výběr zdroje dat



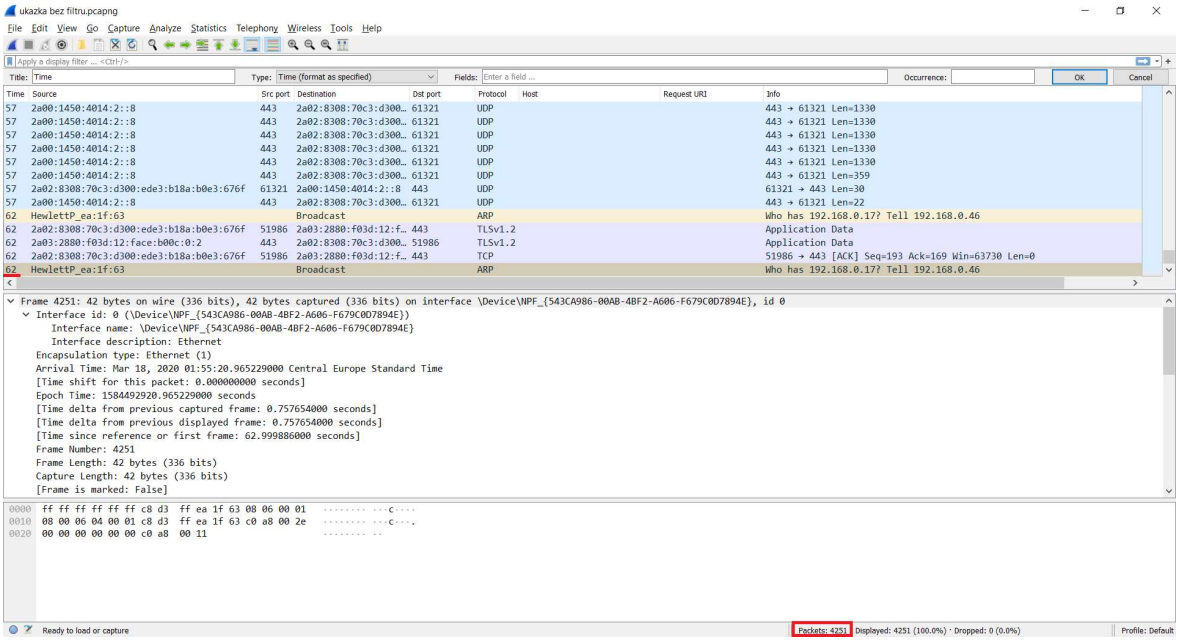
A následně vložíme žádaný filtr do Capture:

Obrázek 3: Wireshark vložení filtru



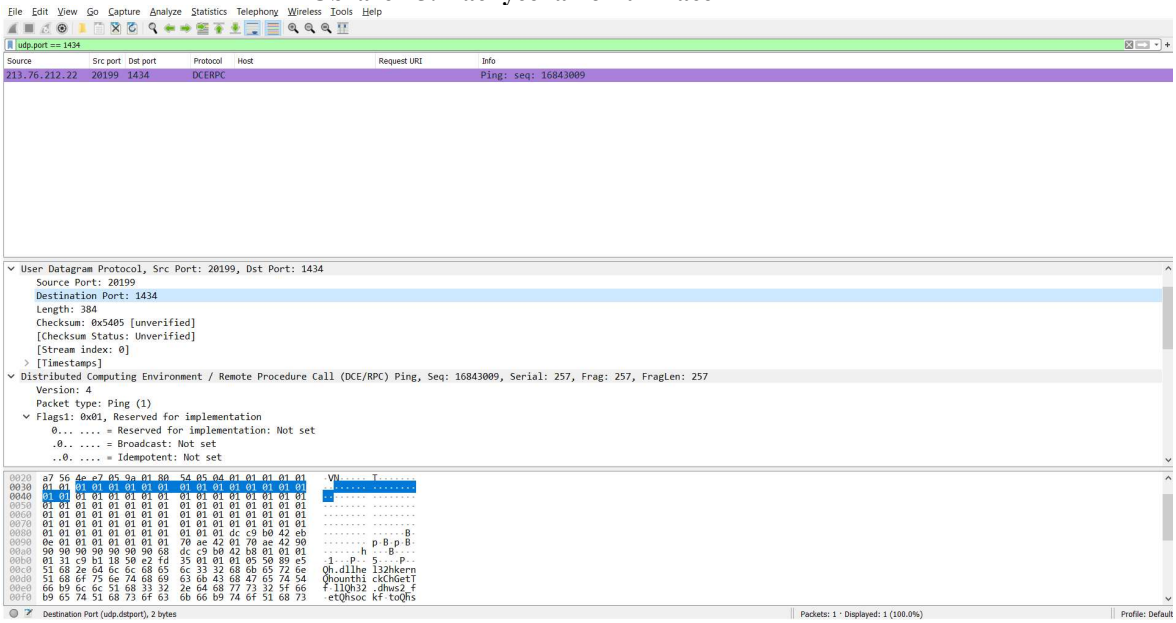
Zelené podbarvení svědčí o správné syntaxi, tedy platném příkazu. V případě chyby by bylo podbarvení červené. Zde můžeme vidět, proč filtry používáme:

Obrázek 4: Wireshark minuta záznamu



Jak je z obrázku vidět, za pouhých 62 vteřin Wireshark zaznamenal 4251 paketů.

Obrázek 5: Zachycená komunikace



Dle portu a protokolu můžeme definovat tuto komunikaci jako Slammer worm.

4.2 Stanovení postupů k zabezpečení

Celkový proces ochrany zařízení nebo sítě před počítačovými červy lze rozdělit na tři základní kroky a má mnoho společného s ochranou proti malware obecně. V první řadě aplikujeme různé postupy a opatření, které v ideálním případě zabraní nákaze. Ve druhém kroku kontrolujeme fungování počítače či sítě a zkoumáme, zda na nás nemíří nějaký útok, případně se může stát že i přes předchozí opatření k nákaze dojde. Posledním krokem je tedy odstranění nežádoucího softwaru, případně důsledků, které přinesl.

4.2.1 Prevence

Základem kvalitní ochrany sítě či zařízení před počítačovými červi je správná prevence. Tu lze následovně rozdělit na několik částí:

4.2.1.1 Aktuální software

Nejdůležitější součástí prevence je užívání aktuálního softwaru. Útočníci nejčastěji používají slabiny v softwaru, ať již v aplikacích či operačních systémech, na kterou

již existuje záplata (*patch*). Ne všichni uživatelé ji ovšem nainstalují okamžitě a jsou tedy možným terčem útoků – výjimkou je pochopitelně malware, který se začne šířit ve chvíli kdy na něj vývojáři ještě nestihli zareagovat, nebo o zranitelnosti ani neví, tedy *Zero day worms*. Viz kapitola 3.4.4.

Ne vždy jde ovšem o pouhé aktualizace v rámci jedné vývojové řady. Problém nyní nastává například se zastaralými verzemi Microsoft Windows jako Windows 7, kterým 14.1.2020 po více než deseti letech skončila podpora systému [19]. To především znamená, že Microsoft přestal vydávat zabezpečovací aktualizace a v případě že kdokoliv věděl o nějaké mezeře v zabezpečení, ale bál se, že by kvůli rychlé odezvě nemusela být plně využita, se takové situace již bát nemusí a počet útoků na tato zařízení se bude nejspíš zvyšovat. I přes to Microsoft ke konci února 2020 zaznamenal jen nízký pokles počítačů stále využívajících operační systém Windows 7 na 25 % [20], což znamená miliony zařízení a potencionálních cílů.

Na problémy s laxností uživatelů vůči zabezpečovacím aktualizacím Microsoft sám reagoval 30.5.2019 článkem *A Reminder to Update Your Systems to Prevent a Worm*, tedy *Připomínka k aktualizaci Vašich systémů k zabránění nákazy červem* [21] kde upozorňují na opravu kritické chyby v *Remote Code Execution*, tedy vzdálené spuštění kódu, která by podle nich v případě mohla zapříčinit podobné rozšíření malware využívajícího tuto zranitelnost, jako například WannaCry ransomware který se rozšířil v roce 2017. Za zmínku stojí časová osa ohledně zranitelnosti EternalBlue, tedy chyby, díky které se právě WannaCry ransomware rozšířil:

- 14.3.2017 Microsoft vydal *„security bulletin MS17-010“* který spravuje řadu SMBv1 zranitelností.
- 14.4.2017 ShadowBrokers zveřejnili sadu chyb, součástí které je *wormable exploit* (zranitelnost napadnutelná počítačovými červi) jménem EternalBlue, kterou o měsíc dříve vydaná aktualizace řeší
- 12.5.2017 Tato chyba je využita k uskutečnění ransomware útoků známých jako WannaCry. Stovky tisíc zařízení po celém světě jsou napadeny

Je tedy vidět, co může způsobit odkládání často „otravných“ automatických aktualizací. Proto je potřeba mít tyto odstrašující případy jako uživatel na paměti a v případě firmy školit zaměstnance z hlediska zodpovědného užívání počítače.

4.2.1.2 Bezpečnostní software

Z hlediska užívaného softwaru je také důležité dodat, že ne všechny operační systémy mají předem zabudovaný antivirový program. Člověk se tak může snadno uchýlit k jeho nepoužívání, což velmi zvyšuje šanci nákazy a zároveň snižuje pravděpodobnost zaznamenání a odstranění infekce. Běžnou praxí je dále používání neplacených verzí, které nemusí mít všechny funkce, ale na běžný provoz uživatele stačí. Nejhorším případem je ilegální stahování plných verzí, často jde totiž o podvodný bezpečnostní software, který nadělá více škody než užitku. Antivirové programy mají zpravidla rozsáhlé pravomoce, které mohou být zneužity. Optimálním řešením je pochopitelně užívání profesionálního, často placeného, bezpečnostního softwaru a dodržovat pokyny jeho vydavatele, jako pravidelné kontroly a aktualizace. Dále je také důležité využívat firewall.

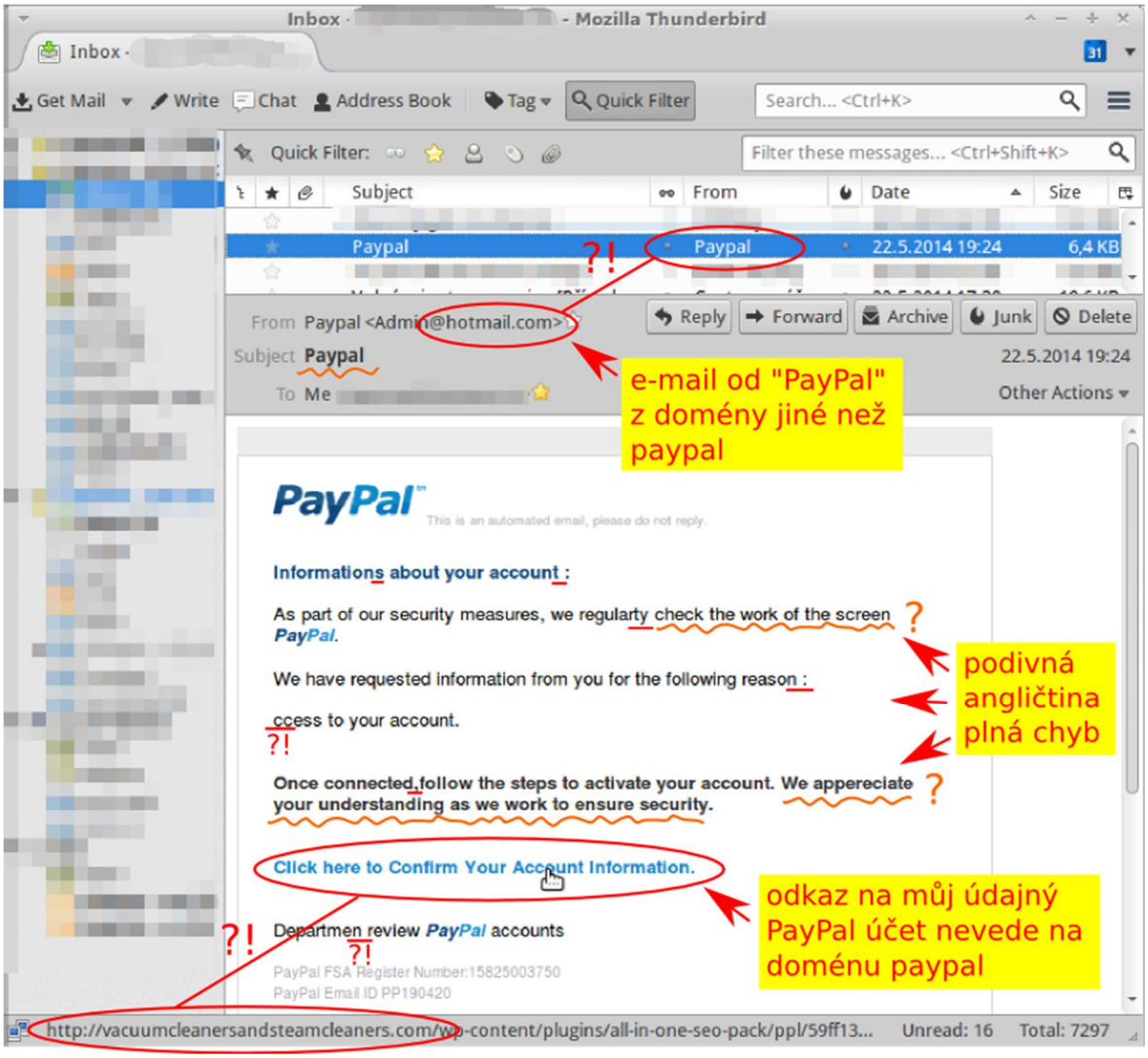
4.2.1.3 Sociální inženýrství

Dalším typickým způsobem šíření počítačových červů je s pomocí akce ze strany uživatele. Respektive samotné šíření je automatizováno, ale uživatel je původním impulzem a zapříčiní infekci prvního zařízení v síti. Pro útočníky může být mnohem jednodušší než prolamovat složitá a komplexní zabezpečení systému zkrátka přimět uživatele k otevření přílohy u zprvu nevinně vypadajícího emailu.

4.2.1.3.1 Phishing

K účinné ochraně před tímto typem útoku je třeba pochopit, jak funguje. Jde o způsob útoku, jehož cílem je ukrást citlivé informace přes emaily, webové stránky, textové zprávy, nebo další způsoby elektronické komunikace, které často vypadají jako oficiální komunikace od legitimní společnosti či jedince. Cílem těchto útoků jsou uživatelská jména a hesla, detaily kreditních karet a bankovní či jiné údaje. Ty jsou následně využívány škodlivými způsoby, jako hackování, krádež identity, krádež peněžních prostředků přímo z bankovních účtů a kreditních karet. Získané informace mohou být případně prodávány na černém trhu. Přímo v kontextu počítačových červů může jít o spam či automatickou zprávu od emailového červa, ale také cílený propracovaný útok, který přiměje uživatele ke stažení červa, který poté napadne jeho síť. Vzorový phishing email může vypadat například takto:

Obrázek 6: Vzorový phishing email [22]



Jak je vidět na základě výše uvedeného příkladu, základní složkou ochrany před tímto typem útoku je obezřetnost a informovanost. Především jde v rámci prevence o neotevírání příloh či klikání na odkazy u nevyžádaných zpráv, a to i v případě, že pochází ze známého zdroje. Neznamená to pochopitelně neotvírat žádné přílohy a neklikat na žádné odkazy, ale především u nečekaných zpráv je třeba být opatrný a v případě odkazů si ověřovat URL (*Uniform Resource Locator)* tedy jednotnou adresu zdroje. Jedním ze způsobů, jak poznat phishing email je, že odkaz „míří“ na jinou adresu. Běžná je také přímá žádost o sdělení citlivých údajů – V rámci oficiální komunikace není běžné osobní údaje sdělovat ve formě emailu. Další věcí, která by měla upoutat naši pozornost, je žádost o jakoukoliv změnu v zabezpečení, instalování

aplikací či povolování maker – Normální zprávy Vás o toto žádat nebudou. Případná rozdílnost v adrese a podpisu je také podezřelá, tedy pokud se odesílatel podepíše jako Václav se společnosti Příklad, ale adresa odesílatele je jana@korporace.com. Časté je také velké množství příjemců zprávy, které se zají jako náhodné adresy. Zprávy v rámci jedné organizace se zpravidla posílají přímo jednotlivým uživatelům. S tím souvisí také oslovení. Pokud Vás autor zprávy přímo neosloví jménem, například napíše vážený zákazníku, kolego, případně použije špatné jméno nebo se pokusí „vytáhnout“ vaše jméno z emailové adresy, může jít o zprávu se škodlivým záměrem [23].

4.2.1.3.2 Přenosná média

Některé počítačové červy se mohou také šířit pomocí kopírování z a do USB flash disků, či jiných výměnných disků. Útočníci tak úmyslně připravují a rozmísťují infikované disky a nechávají je na veřejných místech pro nic netušící oběti.

Příkladem takového červa je dříve zmíněný Stuxnet, který se údajně rozšířil v Iránu pomocí USB flash disku, který Izraelský dvojitý agent zanesl do jaderného zařízení Natanz [24]. Tento útok se stal již v roce 2010 a kód Stuxnetu je lidem volně dostupný. To přináší veřejnosti mnohá rizika, útočníci se tímto profesionálním malwarem mohou inspirovat a zaměřit se na další cíle.

Používejte tedy jen výměnné disky, se kterými jste obeznámeni, nebo přijdou od důvěryhodného zdroje [25].

4.2.1.4 Zálohování

Přes všechna preventivní opatření vždy existuje určitá šance, že naše zařízení či celá síť zařízení bude infikována počítačovými červi, což například u ransomwaru může znamenat ztrátu mnoha důležitých dat. Ta pochopitelně může nastat i z jiných důvodů, jako například živelné pohromy a další. Pro všechny případy je rozumné mít veškerá podstatná data uložena. Jednak na odděleném fyzickém uložišti – červi se mohou k připojenému cloudovému uložišti či sdíleným souborům dostat, tak zmíněná virtuální záloha – především pro případné znehodnocení fyzických dat, ale také pro jejich dostupnost.

4.2.2 Detekce

Z hlediska počítačových červů jde detekci rozdělit následovně na dva základní druhy. Detekování pokusu o útok a samotné šíření v rámci sítě po infikaci některého ze zařízení. V obou případech je základem mít přehled o tom, co se v naší síti odehrává a schopnost adekvátně reagovat. V dnešní době k tomu pochopitelně lze používat všemožný software, jako například v kapitole 4.1. Z hlediska automatizované detekce na bázi behaviorálních metod se z pravidla používá detekce dle počtu skenů za určitý čas. V případě infekce se počítač především snaží dále šířit, a proto skenuje své okolí a hledá další zranitelná zařízení. V takovém případě lehce dosáhne na tisíce takových skenů během krátké doby, zároveň se tím dá předejít zbytečnému izolování a následným finančním ztrátám v případě chybného označení počítače. V průměru totiž počítači trvá dostat se na takové množství skenů třeba i týdny.

4.2.3 Odstranění

Pokud se nám podaří detekovat infikovaný počítač, základem je ho co nejdříve izolovat a předejít rychlému rozšíření. To se pochopitelně zajistí odpojením zařízení od sítě, následné odstranění infekce je v lepším případě zařízeno antivirovým programem, v horším případě je nutná přeinstalace a následná obnova dat ze zálohy.

4.3 Výsledky

Na základě teoretických východisek, průzkumu sítě, odborné literatury a dalších zdrojů byly stanoveny výše uvedené postupy k zabezpečení sítě, které snižují hrozbu a případné následky napadení sítě počítačovými červi. V rámci průzkumu sítě byl nalezen jen červ Slammer, nutno však podotknout, že s velkou pravděpodobností není jedinou stávající hrozbou. Většina zdrojů je v anglickém jazyce, autor překladem přibližuje téma i části české populace, jež tento jazyk neovládá.

5 Závěr

Cílem této bakalářské práce bylo stanovit postupy pro zabezpečení počítačové sítě před počítačovými červy, dále analyzovat současné přístupy k ochraně a analyzovat výskyt tohoto typu malware ve veřejné síti. Práce byla rozdělena na dvě základní části. Teoretická východiska zabývající se problematikou související s druhou částí, tedy vlastní prací. Teoretická východiska se zaměřují zprvu na samotnou infrastrukturu umožňující mimo jiné také šíření tohoto typu malware, čili počítačové sítě, Internet který se zasadil o propojení zařízení po celém světě a World Wide Web, jež přinesl nový rozměr virtuální komunikace, spolu s ním ovšem také nástroj na šíření škodlivého softwaru. Spolu se stále rozšířenějším využíváním počítačů ve všech oblastech našich životů jsme nejen zranitelní, zároveň jsme na těchto technologiích závislí, což může útočníky o to více lákat.

Další kapitoly jako malware a taxonomie internetových červů jsou kritické pro sestavení vyhledávacích filtrů ve Wireshark v *libpcap filter language* bylo nutné zkombinovat stávající dostupné příkazy se znalostí, jak konkrétně se internetoví červi šíří. Tyto příkazy mohou být dále využity jako příklady pro další tvorbu podobných vyhledávacích filtrů, nebo k samotnému vyhledávání v lokálních či veřejných sítích a tím podpořit zabezpečení. Stanovené postupy jsou výsledkem analýzy stávajících přístupů, průzkumu sítě, odborné literatury a dalších zdrojů. Stanovené postupy jsou využitelné jak pro jednotlivé uživatele, malé podniky, tak velké firmy. Počítačoví červi se totiž šíří, kam jen mohou, a zanesou v krátkém okamžiku i rozsáhlou síť. Z hlediska firmy je také ovšem důležité nejen zabezpečovat systém jako takový, ale opravdu věnovat čas a prostředky na školení řadových zaměstnanců, jelikož jsou pro útočníky mnohdy podstatně snazším vstupním bodem.

Je tedy vidět, že počítačoví červi jsou minulostí, ale aktuální hrozbou pro nás všechny. Počítačoví červi se jako skuteční paraziti vyvinuli a stále vyvíjejí z původních zábavných pokusů studentů přes život znepříjemňující spamy až k profesionálně vytvořeným cíleným útokům na důležitou infrastrukturu.

Nutno upozornit také na to, že díky zveřejnění takového kódu může dojít k jeho replikaci a modifikaci za nové cíle. Co se týče ochrany, víme již, že základem je prevence. Zároveň, především u cíleného útoku, ne vždy prevence stačí a je nutné přejít k dalším krokům. Základním prvkem je v efektivní ochraně také z důvodu

exponenciálního růstu včasná reakce. Na závěr tedy hlavní rada, aktualizujte si software.

6 Seznam použitých zdrojů

[1] *Počítačové sítě* [online]. b.r. [cit. 2020-03-02]. Dostupné z: http://www.ped.muni.cz/wtech/03_studium/avt2/avt2-04.pdf. Masarykova univerzita.

[2] STEWART, William. Internet History. *This Living Internet* [online]. 2000 [cit. 2020-03-22]. Dostupné z: https://www.livinginternet.com/i/ii_summary.htm

[3] PEW RESEARCH CENTER, . World Wide Web Timeline. *Internet & Technology* [online]. Pew Research Center [cit. 2020-03-20]. Dostupné z: https://www.pewresearch.org/internet/2014/03/11/world-wide-web-timeline/

[4] MICROSOFT, . Microsoft Docs: Understanding malware & other threats. *Microsoft Docs: Understanding malware & other threats* [online]. 2020 [cit. 2020-03-03]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/understanding-malware

[5] FIREEYE, Inc,. *The Need for Speed: Incident response survey* [online]. In: . 2018 [cit. 2020-03-04]. Dostupné z: https://www2.fireeye.com/ismg-incident-response-survey.html

[6] OCHIENG, Nelson, Waweru MWANGI a Ismail ATEYA. Optimizing Computer Worm Detection Using Ensembles. *Security and Communication Networks* [online]. vol. 2019. 2019, **2019**, 1-10 [cit. 2019-06-09]. DOI: 10.1155/2019/4656480. ISSN 1939-0114. Dostupné z: https://www.hindawi.com/journals/scn/2019/4656480/

[7] HLADKÁ, Eva a Jan FOUSEK. *Základy IT gramotnosti: Malware* [online]. 2020 [cit. 2020-03-04]. Dostupné z: https://is.muni.cz/do/1492/el/sitmu/law/html/malware.html. Masarykova univerzita.

[8] GUEVARA, P., G. DELGADO, J. VALDEZ a H. PÉREZ. *Basic definitions for discrete modeling of computer worms epidemics: Ingeniería e Investigación* [online]. 2016, 79-85 s. [cit. 2020-03-04]. ISSN 0120-5609 DOI: https://doi.org/10.15446/ing.investig.v35n1.44323. Dostupné z: https://revistas.unal.edu.co/index.php/ingeinv/article/view/44323/54679. Universidad Nacional de Colombia.

[9] MICROSOFT, . *How to prevent and remove viruses and other malware* [online]. [cit. 2020-03-08]. Dostupné z: https://support.microsoft.com/en-us/help/129972/how-to-prevent-and-remove-viruses-and-other-malware

[10] IMPERVA, . *Zero-day (0day) exploit* [online]. [cit. 2020-03-18]. Dostupné z: https://www.imperva.com/learn/application-security/zero-day-exploit/

[11] SHAHZAD, Khurram, Steve WOODHEAD a Panayiotis BAKALIS. *An investigation of mechanisms to mitigate zero-day computer worms within computer networks* [online]. University of Greenwich, 2015 [cit. 2019-06-09]. ISSN edsble.732824. Dostupné z: https://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.732824

[12] *Wireshark* [online]. b.r. [cit. 2020-03-01]. Dostupné z: https://www.wireshark.org/

[13] MICROSOFT, . *Stažení softwaru* [online]. [cit. 2020-03-20]. Dostupné z: https://www.microsoft.com/cs-cz/download/windows.aspx

[14] FISHER, Tim. *Patch Tuesday* [online]. [cit. 2020-03-23]. Dostupné z: https://www.lifewire.com/patch-tuesday-2625783

[15] ASKUBUNTU, . *What is the Ubuntu "built in virus protection"* [online]. [cit. 2020-03-20]. Dostupné z: https://askubuntu.com/questions/42284/what-is-the-ubuntu-built-in-virus-protection

[16] SUPPORT APPLE, . *Protect your Mac from malware: macOS User Guide* [online]. [cit. 2020-03-23]. Dostupné z: https://support.apple.com/en-gb/guide/mac-help/mh40596/10.15/mac/10.15

[17] O'NEILL, Patrick. *Conficker worm still spreading despite being nearly 10 years old* [online]. [cit. 2020-03-17]. Dostupné z: https://www.cyberscoop.com/conficker-trend-micro-2017/

[18] WIRESHARK, . *CaptureFilters* [online]. 2016 [cit. 2020-03-18]. Dostupné z: https://wiki.wireshark.org/CaptureFilters

[19] MICROSOFT, . Windows 7 support ended on January 14, 2020. *Microsoft Support* [online]. [cit. 2020-03-15]. Dostupné z: https://support.microsoft.com/en-us/help/4057281/windows-7-support-ended-on-january-14-2020

[20] KEIZER, Gregg. *Windows by the numbers: Remaining Windows 7 users in no rush to move on* [online]. [cit. 2020-03-15]. Dostupné z: https://www.computerworld.com/article/3199373/windows-by-the-numbers-remaining-windows-7-users-in-no-rush-to-move-on.html

[21] MICROSOFT SECURITY RESPONSE CENTER, . *A Reminder to Update Your Systems to Prevent a Worm: MRSC blog* [online]. [cit. 2020-03-15]. Dostupné z: https://msrc-blog.microsoft.com/2019/05/30/a-reminder-to-update-your-systems-to-prevent-a-worm/

[22] ZAHRADNÍK, Martin. Ukázka typického phishing e-mailu s vysvětlením. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2014 [cit. 2020-03-16]. Dostupné z: https://cs.wikipedia.org/wiki/Phishing#/media/Soubor:Jak_snadno_poznat_phishing.png

[23] MICROSOFT, . *Phishing* [online]. [cit. 2020-03-17]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing

[24] TERDIMAN, Daniel. *Stuxnet delivered to Iranian nuclear plant on thumb drive* [online]. © CBS Interactive Inc. All Rights Reserved. [cit. 2020-03-17]. Dostupné z: https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

[25] MICROSOFT, . *Microsoft Docs: Prevent malware infection* [online]. 2019 [cit. 2020-03-08]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/prevent-malware-infection