Acta Informatica Pragensia, 2015, 4(3): 288–301
DOI: 10.18267/j.aip.75
Peer-reviewed paper

Využitie komunikácie na báze zvuku v distribúcii škodlivého softvéru bez prístupu k sieťovým službám

Using of Sound-Based Communication in the Process of Malware Distribution without Connectivity to Network Services

Ján Hurtuk*

Abstrakt

V dnešnej dobe, založenej na širokom spektre využívaných technických a výpočtových zariadení, sa otvára široký priestor pre zneužitie slabých miest obsluhujúceho softvéru pre deštrukčné alebo obohacujúce účely. Denne sú vyvíjané a nasadzované čoraz sofistikovanejšie škodlivé softvéry umožňujúce ovládnutie napadnutého systému, alebo zneužitie citlivých informácií, ktoré napadnutý systém uchováva. Jednu z neprebádaných oblastí predstavujú neštandardné formy komunikácie takýchto softvérov, mimo sieťových služieb, ktoré môžu do budúcna predstavovať za istých podmienok reálnu hrozbu. Tento článok popisuje návrh a následnú implementáciu špeciálneho typu škodlivého softvéru, ktorého komunikačná zložka je založená na IRC (Internet Relay Chat) a v prípade nedostupnosti sieťového pripojenia zohľadňuje možnosti komunikovania infikovaných počítačových systémov pomocou generovaných zvukových vĺn. Skúma jeho jednotlivé vetvy správania sa, založené na pretrvávajúcich podmienkach, jeho slabé stránky, a v závere poukazuje na najdôležitejšie ukazovatele efektivity jeho činnosti. Druhá časť článku sa venuje experimentálnym metódam komunikácie prostredníctvom zvukových vĺn s kmitočtami mimo počuteľné spektrum. V poslednej časti článku sú uvedené výsledky dotazníka, ktoré jednoznačne poukazujú na rozšírené používanie zariadení potrebných na spustenie vetvy vírusu, ktorá je úzko spojená s generovaním signálov za pomoci zvukových vĺn, a tým poukazujú na hrozbu možného využitia podobne zameraných vírusov v reálnej prevádzke. V závere je poukázané na fakt, že podobný druh škodlivého softvéru je za istých splnených podmienok plne schopný fungovať v reálnej prevádzke.

Klíčová slova: Škodlivý software, komunikácia, experiment, zvukové vlny.

Abstract

Nowadays, in today's society based on a wide range of the technical and computing devices, it opens wide scope for misusing vulnerabilities of managing software, for destructive or enriching purposes. Daily are developed and deployed increasingly sophisticated malicious software, enabling the controlling of contested system or misusing sensitive information that infected system stores. One of the yet unexplored areas represent non-standard forms of communication used by such software, without access to network services, which could in the future represent a real threat to certain conditions. This article describes the design and

* Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Letná 9, 042 00 Košice, Slovak Republic
✉ jan.hurtuk@tuke.sk

subsequent implementation of a special type of malicious software that communications components are based on IRC (Internet Relay Chat) and in case of unavailability of the network connection takes into account the possibility of communicating infected computer systems by generating sound waves. It examines the various branches of behavior, based on ongoing conditions, its weaknesses, and finally points out the most important indicators of the effectiveness of its activities. The second part of the article is devoted to experimental methods of communication using sound waves with frequencies outside the audible range. The last part of the article presents the results of a questionnaire, which clearly point to the widespread use of equipment needed to run the branches of the virus, which is closely associated with the generation of signals with the help of sound waves, and thus point to the threat of the possible use of similarly based viruses in real operation. In conclusion, it is pointed out to the fact that a similar type of malware is fully usable under certain conditions, and it can be fully deployed in real environment.

Keywords: Malware, Communication, Experiment, Sound waves.

1 Úvod do problematiky

Otázka škodlivého softvéru je v súčasnosti veľmi diskutovanou témou, a to pre užívateľov ako aj pre samotných vývojárov alebo iných odborníkov v oblasti informačných technológií. Pokiaľ ide o pokrok, prichádzajú čoraz sofistikovanejšie a viac efektívne spôsoby, ako vytvoriť takzvaný exploit, a tým poškodiť používateľa. Tiež boj proti tomuto druhu trestnej činnosti je veľmi náročný, z hľadiska časového i vedomostného, pretože, kým sa útočník sústredí len na jeden konkrétny typ zraniteľnosti, spoločnosti zapojené do boja proti tejto trestnej činnosti musia spravovať zabezpečenie mnohých súčastí rôznych systémov z hľadiska softvéru i hardvéru.

Tento článok je pokračovaním výskumu z práce Hurtuk et. al (2015), opiera sa o dosiaľ publikované znalosti a vrhá nové svetlo na túto tému, pričom poukazuje na väčší potenciálny prístup k zneužívaniu všetkého druhu. Výsledok analýzy sa skladá zo základných bodov, ktoré sú charakteristické pre každý resp. všeobecný model škodlivého softvéru a ich plnením by sa mala zaručiť vysoká účinnosť a efektívnosť daných výsledných škodlivých operácií. Nastoľuje otázku, ktorá stavia do popredia oblasť komunikácie, pričom je kontrola a oblasť riadenia určená ako počiatočná podmienka a vyvodzovanie záverov je otázkou najvyššej priority. Účelom tejto práce je teda vyvinúť nový spôsob komunikácie zložiek navrhovaného vírusu založenej na neštandardnom prístupe za pomoci generovaného zvuku a za pomoci zariadení bežne používaných v reálnej prevádzke. Z hľadiska operačných systémov ako testovacie prostredie zvolený systém Windows, pre jeho všeobecné rozšírenie.

V snahe simulovať pôsobenie škodlivého softvéru a jeho šírenie bola implementovaná a do programových jednotiek pridaná komunikácia medzi klientom a serverom, aby bolo možné zvážiť účinnosť komunikácie za štandardných podmienok, z pohľadu útočníka. Ako ďalšie možné modely boli zvažované témy spracovania a šírenia zvukového nízkofrekvenčného signálu ako zdroja priameho útoku na používateľa.

2 Spoločné záchytné body správania sa škodlivého softvéru

Pôvodné počítačové vírusy a ďalší škodlivý softvér boli vyvinuté pre vysoko špecializované sieťové aplikácie, ktoré sa neustále menia a ovplyvňujú vývoj ohľadom počítačovej bezpečnosti. Samotná problematika škodlivých aplikácií je veľmi široká a autori týchto

aplikácií sú veľmi motivovaní v ich úsilí. Je tiež možné mnohých z nich klasifikovať ako časť organizovanej skupiny. Stratégia pre útoky škodlivého softvéru sa vyvinula na natoľko odlišné metódy, ktoré môžu byť popísané ako multi-procesné kroky, ktoré využívajú celý rad systémových zraniteľností a tým je samotný škodlivý softvér zložený s niekoľkých stupňujúcich sa koordinovaných útokov na firemné či iné siete, Schrittwieser a Katzenbeisser (2011).

Medzi kľúčové spoločné kroky modernej stratégie útoku patria:

- schopnosť infikovať cieľový systém,
- schopnosť perzistencie,
- komunikácia,
- možnosť riadenia a kontroly.

Z predchádzajúcich viet je možné vyvodiť, že tvorba a využívanie vírusov, sa neustále vyvíja smerom dopredu a neustále prináša nové hrozby a výzvy. Je možné tiež vidieť pravidlo, podľa ktorého vírusy vytvorené pomocou pokročilých techník sú ťažko zistiteľné a sledovateľné. To isté platí aj pre boj proti tejto hrozbe. Čím viac sofistikované a účinné metódy škodlivý softvér používa, tým vyššie percento hrozieb nie je možné včas odhaliť.

Súčasný stav dnešnej problematiky vírusov je diametrálne odlišný od stavov v minulosti. Škodlivý softvér slúži ako nástroj aktu zvaného kybernetická vojna. Je stále sofistikovanejší a pokročilejší a nachádza sa na miestach, ktoré pred niekoľkými rokmi ešte neboli k dispozícii. Preto je potrebné pochopiť a analyzovať ich rozvoj do stavu, ktorý nám umožní pochopiť budúce generácie škodlivého softvéru a jeho orientáciu, analýzou existujúcich najrozšírenejších hrozieb. Po preskúmaní vybraných vzoriek nastáva otázka, ako triediť a bojovať s vírusmi v dnešnej dobe. Prihliadnuc na predchádzajúce zistenia, sa ako jedno z možných riešení ukazuje použitie zariadení v zabezpečenej sieti, ktorá bude schopná (dočasne) znemožňovať alebo obmedzovať aktivity vírusu tak, že autor nebude schopný vzorku riadiť, vírus nebude schopný komunikovať s jeho kópiami v sieti, nebude schopný sa aktivovať alebo aktualizovať, a tým prestane byť aktívny.

3 Analýza spoločných bodov životného cyklu škodlivého softvéru

Z predchádzajúcich zistení je možné poukázať na niekoľko nedostatkov v životnom cykle škodlivého softvéru na základe bližšieho pohľadu na štyri hlavné atribúty, ktoré charakterizujú jeho činnosť: infekcia, perzistencia, komunikácia, riadenie a kontrola Hurtuk et al. (2014).

Schopnosť prieniku do systému

Táto funkcia je silno závislá na interakcii a činnosti používateľa, jej najsilnejším nástrojom je takzvané sociálne inžinierstvo, ktorý využíva podiel ľudskej interakcie a človeka ako najrizikovejší faktor ohľadom bezpečnosť. Podľa CSIRT (2014) je sociálne inžinierstvo druh útoku využívajúci priamu interakciu s človekom za účelom vykonania určitej akcie (napr. spustenie súboru), alebo získania určitých informácií. Sociálne inžinierstvo môže prebiehať osobne alebo prostredníctvom prostriedkov komunikácie (telefón, mail...), alebo úpravou prostredia (ako je opustenie médií na verejne prístupnom mieste).

Perzistencia

Definuje schopnosť škodlivého softvéru byť videný operačným systémom, čo sa v danom prípade rovná jeho neodhaleniu a tým a schopnosti zotrvania v danom hostiteľskom systéme. Využíva pokročilé techniky a rôzne druhy slabých miest umožňujúcich priamy zásah do systému a jeho častí.

Komunikácia

Snahou komunikácie je zabezpečiť, aby sa informácie získané od obetí dostali späť k útočníkovi. V prípade, že komunikácia neprebieha, činnosť útočníka je zameraná iba na samotné poškodenie systému alebo zneužitie jeho súčastí v rámci krokov komplexnejšieho útoku Vokorokos et al. (2014).

Kontrola a manažment

Ide o jeden z najviac kritických bodov. Dôvodom je, že hoci je škodlivý softvér schopný úspešne sa rozšíriť a skryť v systéme, ale nie je možné riadiť ho, veľmi rýchlo sa stáva nekontrolovateľný a ľahko detekovateľný a neschopný ďalšej činnosti. Z pohľadu útočníka musí existovať forma kontroly nad jeho činnosťou, najmä ak ide o vyspelejšie vírusy, kde môže akcia byť variabilná v závislosti na infikovanom systéme a jeho ochranách. Strata kontroly môže teda viesť k plytvaniu útočníkových zdrojov, alebo v prípade, že je softvér zameraný na zber dát, stratu a znehodnotenie celých blokov údajov potrebných pre ďalšiu činnosť. Existuje mnoho rôznych možností pre komunikáciu, ktoré útočník môže využiť vo svoj prospech. Pre zvýšenie úspešnosti daného škodlivého softvéru je z hľadiska útočníka potrebné zaviesť opatrenia na zlepšenie vytrvalosti, optimalizovať kód a implementovať polymorfizmus, Ennert et al. (2014) alebo založiť útok na niekoľkých spolu prepojených a spolupracujúcich vírusových vzorkách a použiť pokročilé techniky, ako je sociálne inžinierstvo a inžinierstvo sociálnych sietí.

Je však nevyhnutné nastoliť otázku, čo v prípade odpojenia sa používateľa zo siete. Z pohľadu útočníka je preto vhodné pokúsiť sa nájsť nový spôsob komunikácie medzi zariadeniami, ktorý bude schopný zastúpiť konvenčné metódy ak tie konvenčné nebudú k dispozícii. Jedným z takýchto návrhov je jednosmerná komunikácia tranzitného zvukového vysielania a jeho následnej analýzy, ktorá bude opísaná v nasledujúcich kapitolách.

3.1 Výhody a nevýhody jednosmernej komunikácie

Aby bolo možné používať zvuk pre účely komunikácie škodlivého softvéru, je potrebné stanoviť kľúčové faktory ovplyvňujúce komunikáciu. Jedná sa o:

- Aký druh komunikácie sa použije (centralizovaná / P2P),
- V akom zvukovom spektre bude komunikácia prebiehať,
- Ako budú signály dekódovať a prekladať potrebné inštrukcie,
- Aký bude dopad a využitie tohto druhu komunikácie a jeho obmedzenia.

Najväčším obmedzením jednosmernej komunikácie je, že je schopná len prijímať pokyny a nie je schopná potvrdiť príjem inštrukcií, čo značne obmedzuje jej spoľahlivosť. Vytvorenie spätnej väzby by bolo možné, ale v takom prípade by bolo potrebné pracovať s presne časovanou formou komunikácie alebo nájsť vhodnejšiu alternatívu kódovania a vysielacích frekvencií. Rovnako je pri bližšom skúmaní možné naraziť na hardvérové obmedzenia týkajúce sa pripojeného mikrofónu, ktorým musí byť prijímajúce zariadenie vybavené.

4 Návrh komunikačnej schémy nového typu škodlivého softvéru

Zmysel operácie spočíva v nekonečnej slučke, ktorá je prvým krokom funkcionality škodlivého softvéru v danom zariadení. Najskôr sa overí pripojenie k internetu, prípadne so serverom C & C (command-and-control server). V prípade možnosti takéhoto pripojenia by do navrhovaného vírusu mala byť pripojená riadiaca inštrukcia pre túto operáciu. Následne sú vykonávané inštrukcie, ktoré pochádzajú buď zo správcovského kanála, alebo pasívne čakajú na príjem ich riadiacej inštrukcie mimo počuteľné rozmedzie. Následne prebehne aktualizácia niekoľkých súčastí ako aktualizácia zdrojového kódu (jednoduchý polymorfizmus).

C&C server

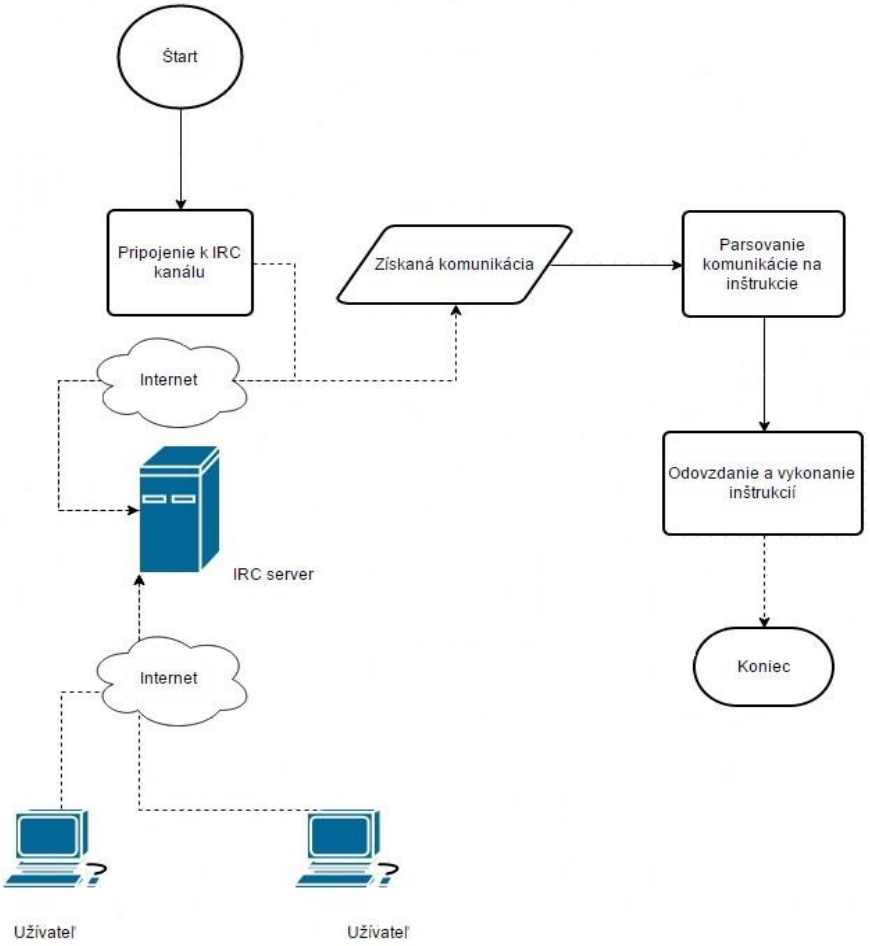
Predstavuje centralizovaný počítač, ktorý je špeciálne nastavený na kontrolu a rozdeľovanie príkazov pre vírusové vzorky pasívne sediace v infikovanom prostredí, tzv. zombies. Tie s vonkajším prostredím komunikujú pomocou utajovaných kanálov na základe protokolu IRC (vytvorených napr. trójskym koňom).

IRC protocol

Je protokol aplikačnej vrstvy, ktorý umožňuje komunikáciu vo forme textu. Pracuje systémom na sieťovom modeli klient / server. IRC klienti predstavujú počítačové programy, ktoré je možné nainštalovať v danom systéme. Klienti komunikujú so serverom, ktorý následne distribuuje správy cieľovej stanici. IRC je určený predovšetkým pre skupinovú komunikáciu ale umožňuje i one-on-one komunikáciu prostredníctvom súkromných správ vo forme chatu a taktiež prenos dát, vrátane zdieľania súborov.

IRC komunikácia

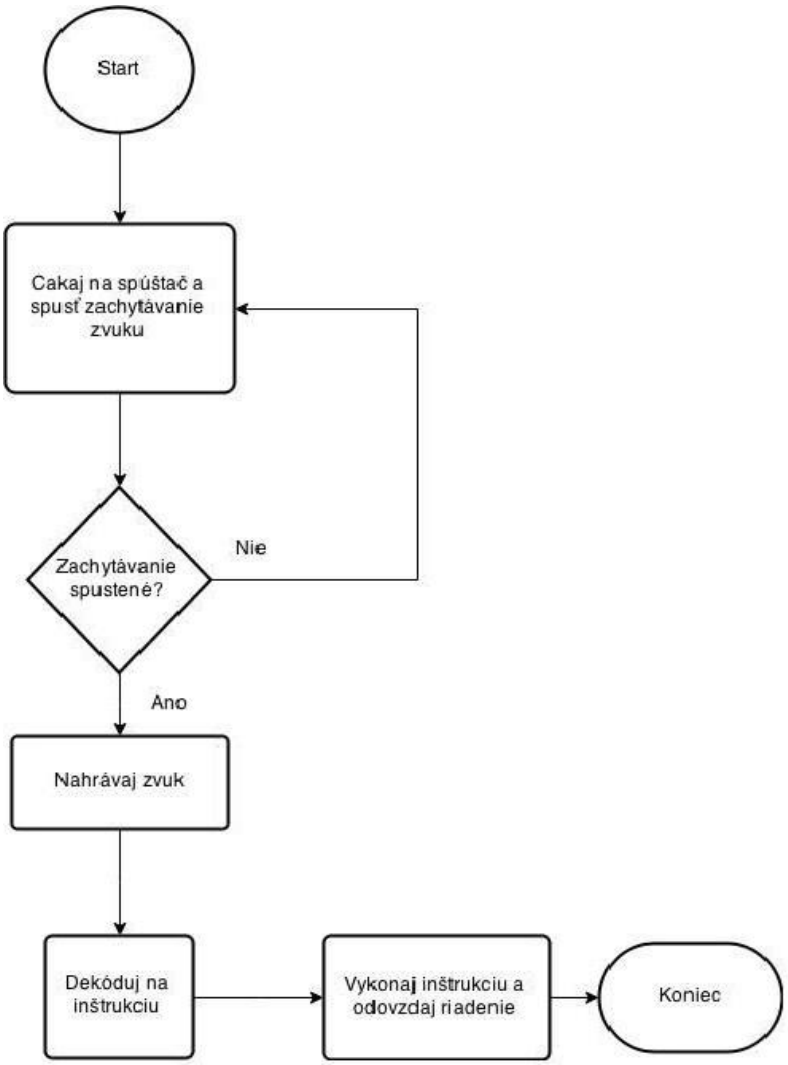
Tento typ komunikácie je základným typom komunikácie so správou servera C & C, kde sa vírus prikladá ku konkrétnemu IRC kanálu a odtiaľ "číta" komunikáciu a funguje ako bežný používateľ Vokorokos et al. (2012). Okrem toho, však prekladá inštrukcie, ktoré riadia jeho činnosť. Je dôležité zároveň zabezpečiť, aby komunikácia pomocou IRC prebiehala na základoch vzorovej dokumentácie IRC podľa CSIRT (2014) pre správne spracovanie prichádzajúcich správ a správne formátovanie odchádzajúcich správ. Priebeh komunikácie ilustruje Obr.1.



Obr. 1. *Priebeh IRC komunikácie. Zdroj: Autor*

Uskutočnenie vetvy využívajúcej zvuk a jeho preklad na inštrukcie

Základné rutiny prekladu inštrukcií závisia na vyššie uvedených skutočnostiach, a teda straty prístupu k sieti a neschopnosti komunikácie so serverom pre správu, čo znemožňuje fungovanie celého modelu. V tejto štúdií sa spomínaný problém obchádza pomocou inicializácie bloku vedenia kódu pomocou zvuku Vokorokos et al. (2015). Spiace inštrukcie čakajú v tzv. spúšťacej fáze, ktorá môže niesť určitý časový interval vypnutia, časovú pečiatku, alebo byť spustená mimoriadnou udalosťou v systéme. Dekódovanie sa skladá z odfiltrovania zvukových vĺn, ktorých škála nespadá do rozsahu definovaným v danom bloku. Spracovanie by malo byť schopné počítať s hlukom, disperziou a skreslením. Výsledný interval teda nie je filtrovaný iba ako zvuk priamo zodpovedajúci 16kHz, ale ponecháva zvuk v rozmedzí 15,5 - 16,5 kHz. Po filtrácii sa do istej miery určuje doba trvania každej sekvencie, ktorá priamo zodpovedá ako kľúč inštrukcie v strome inštrukcií. Kľúče inštrukcií sú v strome definované ako približné hodnoty a teda ako intervaly. Výsledný preklad inštrukcií je tiež závislý na nastavení zvukovej karty, kvalite zvuku prijímaného mikrofónom a vzorkovacej frekvencii. Schematicky to znázorňuje Obr.2.

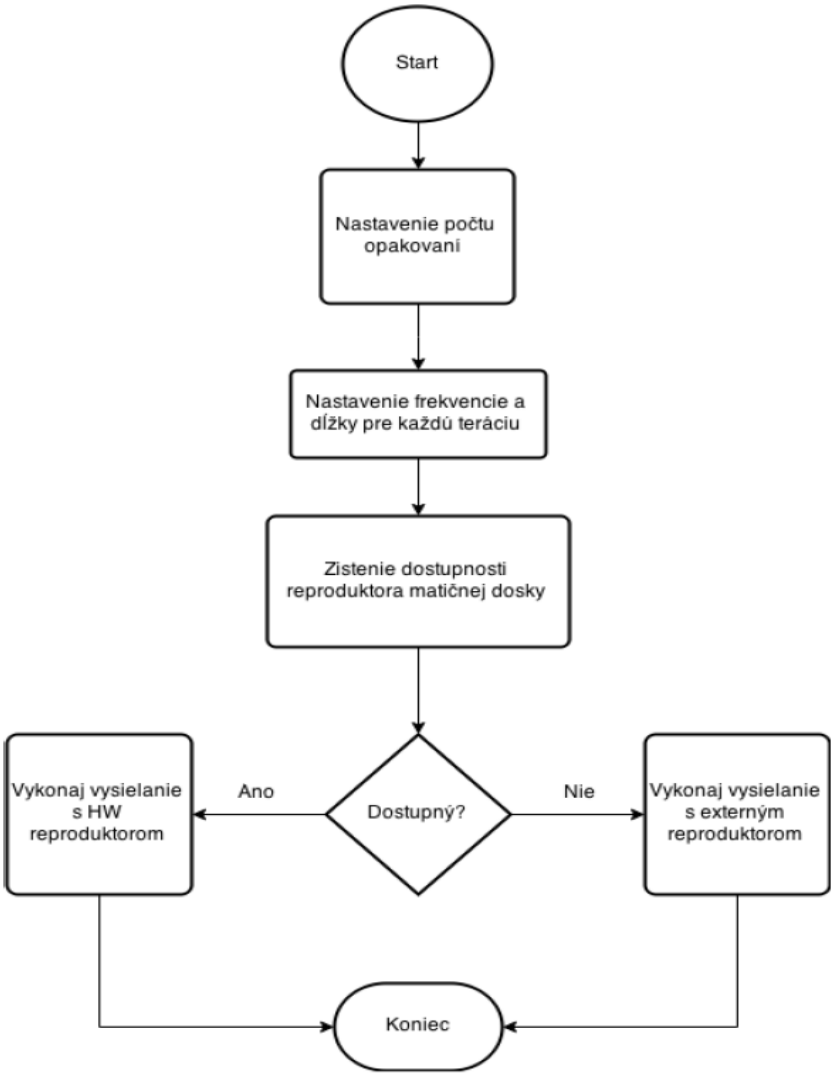


Obr. 2. *Preklad zvuku na inštrukcie. Zdroj: Autor*

Po odfiltrovaní nepotrebného rozsahu sa zistí dĺžka trvania jednotlivých sekvencií, poprípade trvanie jednej konkrétnej z nich a tej sa na základe jej dĺžky priradí jej kód pre konkrétnu inštrukciu v strome. Do algoritmu sú zahrnuté aj odchýlky a preto sa pri čase, pre ktorý sa priradí konkrétna inštrukcia uvažuje len o približných hodnotách. Výsledný preklad inštrukcie závisí aj od nastavenia zvukovej karty, kde si používateľ mení nastavanie kvality a vzorkovacej frekvencie a taktiež od nastavenia mikrofónu, ktorý zvuk nahráva.

Zvukový broadcast

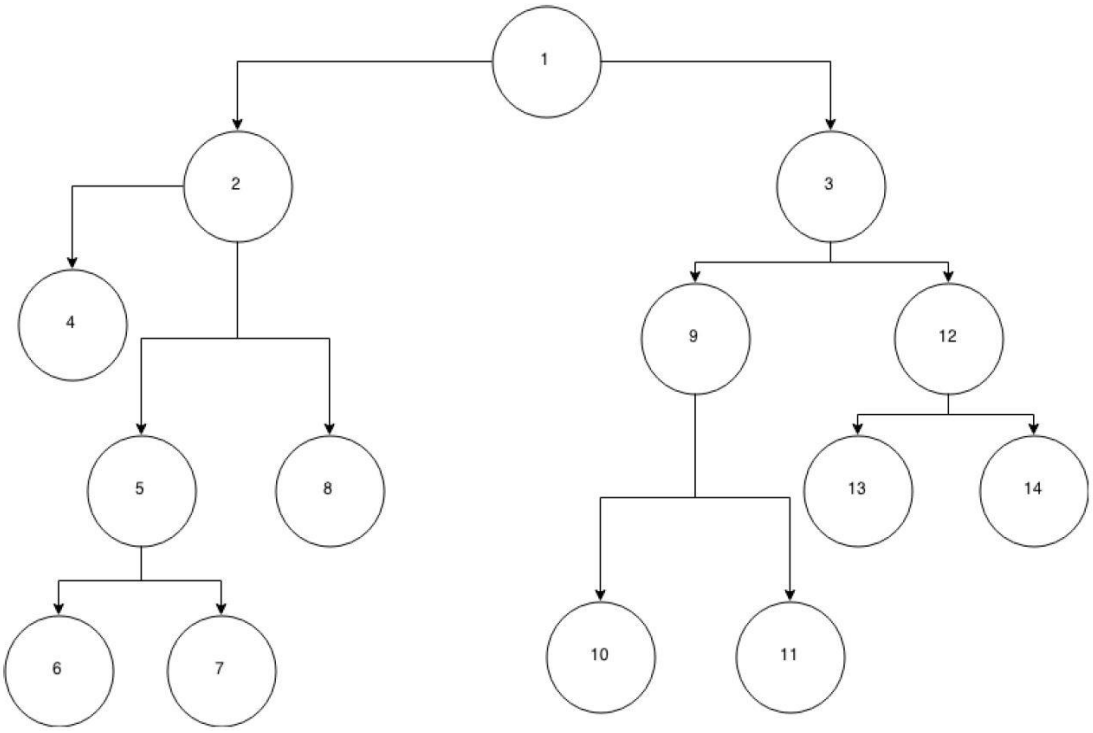
Zvukové vysielanie prebieha nasledovne. Nastaví počet iterácií vysielania, t.j. počet signálov, ktoré sú prenášané. Nastavuje frekvenciu, pri ktorej sa bude vysielať. Potom nastaví dĺžku, t.j. kľúč kódu pre každú iteráciu, tzn. signál pre každú inštrukciu. Potom sa zisťuje, či je k dispozícii hardvérovo vstavaný reproduktor na základnej doske zariadenia, pokiaľ nie je, je možné vysielať za pomoci externých reproduktorov. Tu sa nerozlišuje medzi reproduktormi pripojenými cez konektor, alebo reproduktormi vstavanými do notebooku. Výber možností prehrávacieho zariadenia ilustruje Obr.3.



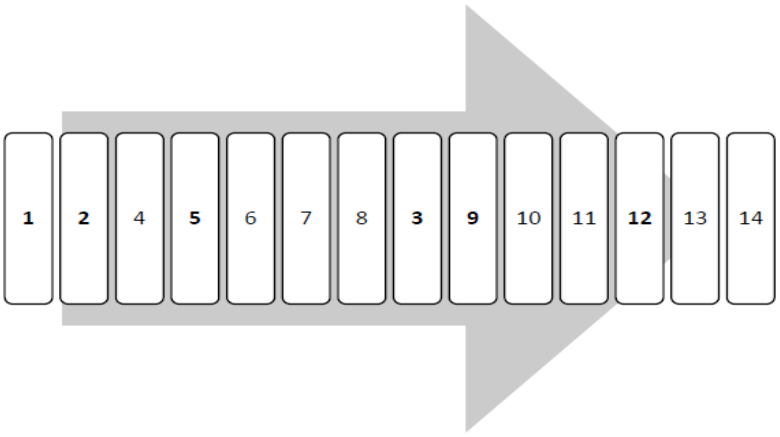
Obr. 3. *Výber možnosti prehrávacieho zariadenia. Zdroj: Autor*

Funkcia prechodu stromom inštrukcií definovaných pre zvuk

Strom inštrukcií je strom, ktorý nám umožňuje, ako už bolo spomínane spúšťať nielen konkrétne inštrukcie, ale aj celé vetvy inštrukcií. Obsahuje inštrukcie, sú vopred dané, nemenné a opakujúce sa. Strom znázorňuje Obr.4. Spúšťanie jednotlivých inštrukcií bolo popísané v predošlých kapitolách. Avšak je nutné poznamenať, že daný strom inštrukcií umožňuje pre inštrukciu 2 spustiť celý pod strom inštrukcií a tieto sa vykonávajú v poradí zhora nadol od ľavej vetvy k pravej. Pre konkrétny strom z Obr.4 je definované poradie vykonávania ilustrované na Obr.5.



Obr. 4. *Prechodový inštrukčný strom. Zdroj: Autor*



Obr. 5. *Poradie vykonania inštrukcií pre strom z Obr.4. Zdroj: Autor*

Hrubo zvýraznené sú body, kde sa tento strom vetví a kam prechádza riadenie vykonávania z ľavej vetvy do pravej. V programe sa toto správanie odrazí ako interpretácia pomenovaného stromu, ktorý si stále zachováva informáciu o aktuálnom umiestnení, o pôvodnom znení inštrukcie a o budúcom smerovaní, pre každý list.

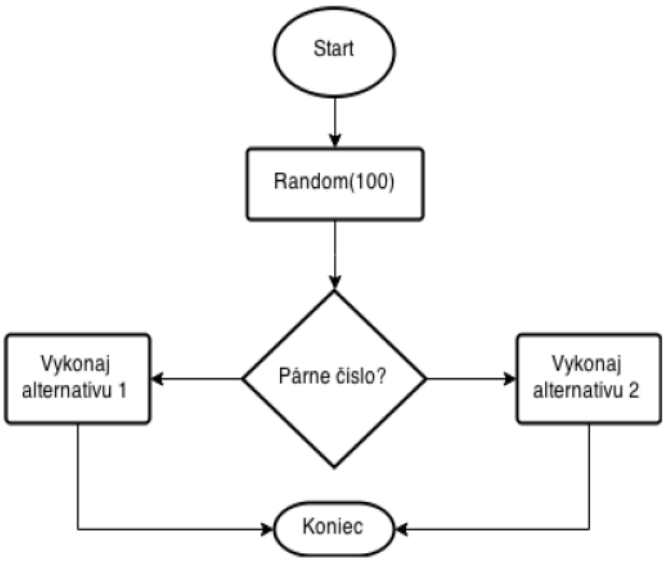
Analýza zvuku a filtrovanie konkrétnych frekvencií

Pre tento krok spracovávania je nutné zachytený zvuk s inštrukciami mimo počuteľné spektrum spracovať tak, aby bolo možné zistiť aký dlhý úsek, poprípade koľko tých úsekov sa nachádza v zachytenej vzorke. Na dosiahnutie tohto výsledku sa využívajú filtre s priepustnosťou v nízkych, vysokých frekvencii a s priepustnosťou v bežnom pásme. Pre účely tejto práce je najvhodnejšie využiť vysokofrekvenčný filter, ktorý prepúšťa nami požadovanú výšku zvuku a všetko pod touto hranicou zahodí. Pre túto zmenu v zvukovej vzorke sa používa diskrétna

Furierová transformácia, ktorá spracováva signál v závislosti od času. Na spracovanie signálu bolo využitá knižnica FIR-filter, ktorej dokumentácia a použitie je podrobne zdokumentovaná Perkins (2013).

Využitie oligomorfizmu

V tomto príklade sa jedná o pseudonáhodné generovanie inštrukcií, ktoré vykonajú totožnú, poprípade takmer zhodnú činnosť. Pre ilustráciu je uvedený diagram tejto funkcie a jednotlivé inštrukcie s vysvetlením, Obr.6.



Obr. 6. *Náhodné rozhodovanie pre oligomorfické inštrukcie. Zdroj: Autor*

Využité príkazy aj ich alternatívy sa nachádzajú v Tab. 1. Tieto príkazy slúžia pre ilustráciu škodlivej činnosti. V tabuľke sa nachádza aj popis ich činnosti.

Príkaz	Vysvetlenie	Alternatíva príkazu	Vysvetlenie
DEL /F *.dll	Vymazanie všetkých dostupných dll súborov z disku. Príznak /F umožňuje zmazanie súborov určených len pre čítanie.	DEL /a:R *.dll	Vymazanie všetkých dostupných dll súborov určených na čítanie.
		DEL *.dll	Vymazanie ostatných dll súborov
SHUTDOWN /s /t /d P:2:17	Vypnutie počítača s nastavenými príznakmi na upozornenie o vypnutí, na prednastavený čas vypnutia do 30s, a s výpisom chybového hlásenia o plánovanom vypnutí.	SHUTDOWN /f /d P:2:17	Okamžité vypnutie počítača s rovnakým chybovým hlásením, avšak bez odloženia a oznámenia.
Beep (16000, 2)	Funkcia pre vysielanie zvukového signálu ktorá ako parameter berie frekvenciu a čas.	Beep (0x3E80, 2)	Tá istá funkcia, avšak parameter frekvencie je prerátaný do sústavy so základom 16.

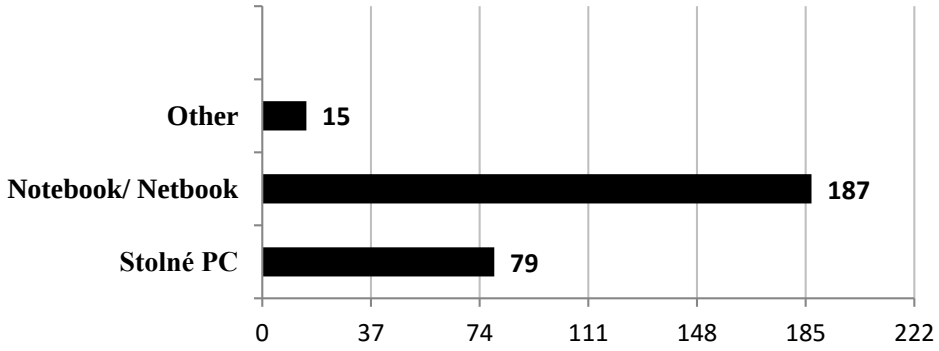
Tab. 1. *Ilustratívny príklad škodlivé činnosti. Zdroj: Autor*

5 Analýza podmienok nasadenia prezentovaného modelu v reálnej prevádzke

Jednou zo zásadných podmienok využitia špeciálnych vlastností vyššie navrhovanej schémy je prítomnosť zariadení schopných emitovať a prijímať kódované signály v podobe zvukových vĺn. Zistenia sú prezentované dotazníkom, na ktorý odpovedalo 190 respondentov. Dokazovaní boli vysokoškolskí študenti, pričom pri vypĺňaní bol uvedený ako predmet dotazníka prieskum o počte vlastnených a využívaných multimediálnych zariadení a technológií s nimi spojených. Jednotlivé podkapitoly zodpovedajú položeným otázkam.

Aké typy zariadení a koľko kusov vlastní domácnosť v ktorej žijete?

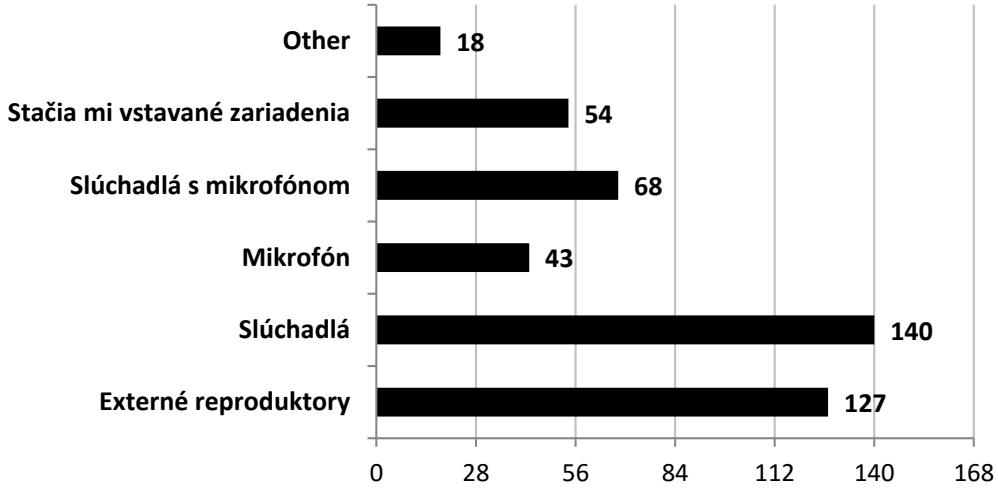
Z odpovedí vyplýva, že na jedného užívateľa, teda potenciálnu obeť pripadá viac ako jedno zariadenie v domácnosti. Toto zistenie je zásadné, keďže ako obmedzenie pre fungovanie vírusu je nutnosť vlastniť aspoň dva zariadenia, poprípade mať dva zariadenia pripojené zároveň. Výsledky reprezentuje Obr. 7.



Obr. 7. *Graf výsledkov otázky: Aké typy zariadení a koľko kusov vlastní domácnosť v ktorej žijete? Zdroj: Autor*

Aké príslušenstvo vlastníte k svojmu zariadeniu?

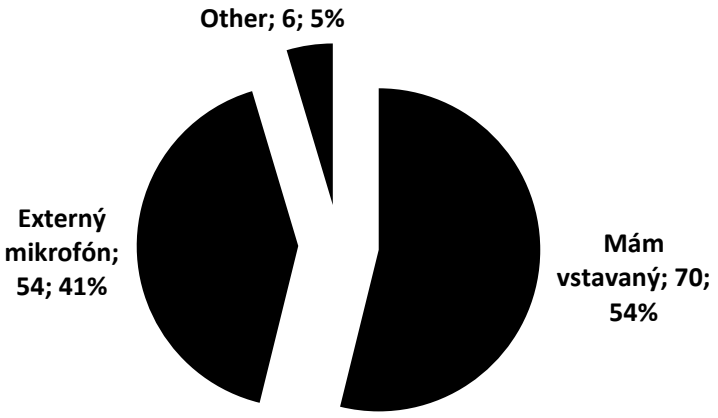
Zistením vyplývajúcim z týchto odpovedí je jednoznačná odpoveď na otázku, či je v bežnej domácnosti možné danú komunikáciu, ktorej obmedzením je vlastníctvo nahrávacieho a prehrávacieho zariadenia, uskutočniť. S príchodom nových technológií sa zariadenia ako mikrofón a reproduktory, či slúchadlá stali samozrejmosťou vo veľkom počte prípadov. Taktiež z tohto prieskumu vyplýva, že aj užívatelia so stolným počítačom, ktorý neobsahuje vstavaný mikrofón a reproduktory majú potenciál na to, aby sa stali buď vysielačom alebo prijímačom pri komunikácii toho vírusu. Výsledky reprezentuje Obr.8.



Obr. 8. *Výsledky odpovedí otázky: Aké príslušenstvo vlastníte k svojmu zariadeniu? Zdroj: Autor*

Aký druh mikrofónu pripojený k počítaču?

Pri zodpovedaní tejto otázky je možné vidieť, že využívanie nahrávacích zariadení je pomerne rozšírené. Podľa dotazníka 95% opýtaných používa mikrofón. Pričom pre naše potreby, kedy je najvhodnejšie využívať mikrofón vstavaný, či prípadne mikrofón je pripojený neustále je to až 54%. Možnosť, ktorú zaškrtlo 5% opýtaných zhruba zodpovedá možnosti, kedy nie je využívaný mikrofón. Výsledok odpovedí na túto otázku ukazuje, že použitie mikrofónu ako nahrávacieho zariadenia je vo všeobecnosti rozšírené, čo je pre potreby fungovania vírusu viac než dostačujúce. Výsledky reprezentuje Obrázok 9.



Obr. 9. *Výsledky odpovedí otázky: Aký druh mikrofónu pripojený k počítaču? Zdroj: Autor*

Považujeme za smerodajné, že vybraná vzorka respondentov pre tento dotazník bola dostatočná a taktiež aj na základe zistení je možné tvrdiť, že tieto zistenia dostatočne odrážajú aktuálnu situáciu, ktorá bola očakávaná. Vďaka zisteným informáciám je taktiež možné potvrdiť, že navrhnutý spôsob komunikácie bude nielen realizovateľný, ale taktiež v mnohých prípadoch aj veľmi efektívny.

6 Zhodnotenie navrhovaného riešenia

Navrhnuté riešenie pre komunikáciu zvukovými vlnami medzi jednotlivými zariadeniami nakazenými týmto druhom vírusu by za predpokladu, že výsledky z dotazníka je možné brať ako reprezentatívnu vzorku, sa ukázalo ako veľmi výhodné. Je možné ho teda považovať za správnu alternatívu ku komunikácii cez internetovú sieť.
V prípade reálneho nasadenia do prevádzky, teda za predpokladu schopnosti nakaziť väčšiu homogénnu oblasť tak, aby bolo možné ďalšie šírenie, máme za to, že takýto vírus by bol úspešný a dokázal reálne prežiť v bežnom užívateľskom prostredí. Výsledky, ktoré sme sa snažili dosiahnuť by sa dali zhrnúť v nasledujúcich bodov:

- Zabezpečiť komunikáciu zvukovými vlnami mimo počuteľné spektrum,
- Zabezpečiť základnú funkcionalitu vírusu,
- Využiť pokročilé techniky ako polymorfizmus, poprípade jemu podobné.

Ďalšie smerovanie výskumu

Ďalšie smerovanie výskumu by sa dalo zhrnúť do niekoľkých krokov:

- Nasadenie prezentovanej schémy do prostredia obsahujúceho viac ako dva počítačové systémy,
- Zameranie sa na viac komplexnejšie inštrukcie, resp. bloky inštrukcií a ich preklad do zvukových vzoriek,
- Implementácia vzorky do menej homogénneho prostredia,
- Skúmanie správania sa vzorky v prípade hlučného prostredia,
- Implementácia interaktívnej komunikácie pomocou zvuku so štandardnými formami sieťovej komunikácie s cieľom zmenšiť frekvenciu posielania správ pomocou sieťových kanálov, čo bude mať za následok vyššiu schopnosť perzistencie prezentovanej vzorky.

7 Záver

Navrhnuté riešenie pre komunikáciu za pomoci zvukových vĺn medzi zariadeniami, infikovanými týmto typom vírusu, môže byť považované za alternatívu ku komunikácii prostredníctvom siete Internet. Táto analýza a následný návrh týmto poukazuje na možné spôsoby a cesty vývoja škodlivého softvéru a tým otvára témy možnej ochrany proti podobne orientovaným schémam. V prípade reálneho nasadenia v prevádzke, za splnenia potrebných podmienok, by sa takýto vírus by bol schopný úspešne rozšíriť a mohol by prežiť v súčasnom používateľskom prostredí.

Zaujímavým zistením pri spracovaní problematiky audio frekvencie mimo rozsah ľudského vnímania bolo to, že pri použití vlny v spodnej hranici sluchovej počuteľnosti, ktorá patrí do infrazvuku, môže spôsobiť fyziologické zmeny vo fungovaní ľudského tela vrátane psychických problémov. Jedná sa o zvuk o vlnovej dĺžke 20 Hz a pod. V tomto prípade je však nutné dlhodobé pôsobenie na ľudský organizmus. Žiaran (2013), skúma vplyv rutinných zvukov podobných zvukom z otvoreného okna v aute pri jazde a ich podiel na zmenách vo fyziológii. Najznámejšie efekty hluku na ľudské telo zahŕňajú vplyv hluku na krvný tlak a v dlhodobom efekte následnej tvorby hypertenzie (t.j. zvýšenie krvného tlaku), ktoré sa môžu vyvinúť do chronických problémov. Žiaran vychádza z akustického tlaku, ktorý vzniká v dôsledku šumu, a pre každú hodnotu popisuje úroveň poškodenia, ktorá vplýva priamo na srdce. Hluk spôsobený nízkou frekvenciou má oveľa väčší vplyv než hluk na stredných a vysokých frekvenciách. So znižujúcou sa intenzitou nízkofrekvenčného zvuku úmerne stúpa čas nevyhnutný na dosiahnutie fyziologických zmien.

Zoznam použitej literatúry

CSIRT. (2014). Retrieved from https://www.csirt.org

Ennert, M., Madoš, B. & Dudláková, Z. (2014). Data visualization of network security. *Acta Electrotechnica et Informatica*, 14(4), 62-65. doi: 10.15546/aeei-2014-0034

Hurtuk, J., Copjak, M., Dufala, M., & Drienik, P. (2014). The malicious code hiding techniques, code obfuscation problem. In *Proceedings of the 12th IEEE International Conference on Emerging eLearning Technologies and Applications* (pp. 181-185). New York: IEEE. doi: 10.1109/ICETA.2014.7107581

Hurtuk, J., Madoš, B. & Halčín, Š. (2015). Sound-Based Communication in the Process of Malware Distribution. *Acta Electrotechnica et Informatica*, 15(2), 62-65. doi: 10.15546/aeei-2015-0020

Perkins, M. (2013). Retrieved from http://www.cardinalpeak.com/blog/a-c-class-to-implement-low-pass-high-pass-and-band-pass-filters

Schrittwieser, S., & Katzenbeisser, S. (2011). Code Obfuscation against Static and Dynamic Reverse Engineering. In *Proceedings of the 13th International Conference on Information Hiding* (pp. 270-284). doi: 10.1007/978-3-642-24178-9_19

Vokorokos, L., Baláž, A., & Madoš, B. (2012). Intrusion Detection Architecture Utilizing Graphics Processors. *Acta Informatica Pragensia*, 1(1), 50-59. doi: 10.18267/j.aip.5

Vokorokos, L., Hurtuk, J., & Madoš, B. (2014). Malware categorization and recognition problem. In *Proceedings of the 18th IEEE International Conference on Intelligent Engineering Systems* (pp. 105-108). New York: IEEE. doi: 10.1109/INES.2014.6909350

Vokorokos, L., Baláž, A., & Madoš, B. (2015). Application Security through Sandbox Virtualization. *Acta Polytechnica Hungarica*, 12(1), 83-101.

Žiaran, S. (2013). Low Frequency Noise and Its Assessment and Evaluation. *Archives of Acoustics*, 38(2), 265–270. doi: 10.2478/aoa-2013-0032