VŠB TECHNICKÁ UNIVERZITA OSTRAVA
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Spyware na mobilních zařízeních

Spyware on Mobile Devices

Bc. David Trebichalský

Diplomová práce

Vedoucí práce: prof. Ing. Ivan Zelinka, Ph.D.

Ostrava, 2023

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Č.j.VSB/22/078943
vsboee22026039

Zadání diplomové práce

Student: **Bc. David Trebichalský**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T025 Informatika a výpočetní technika

Téma: Spyware na mobilních zařízeních
Spyware on Mobile Devices

Jazyk vypracování: čeština

Zásady pro vypracování:

Práce se zabývá analýzou a tvorbou ukázkového spyware na mobilní platformě. Požadovaná funkcionalita spyware je záznam obrazovky, klávesnice a zvuku s aplikací šifrování a komprese na získaná data a jejich utajené odeslání na dané úložiště. Součástí práce je i otestování vytvořeného spyware proti známým antivirovým a obranným prostředkům. Spyware musí být naprogramován minimalistickým způsobem. Kód musí být strukturovaný a bohatě okomentovaný.

1.Aktualizace stavu na poli moderních technologií spyware.
2.Návrh řešení a volba vhodných technologií.
3.Realizace spyware.
4.Testování funcionality a odolnosti proti odhalení.
5.Tvorba ukázkových a plně opakovatelných příkladů použití.
6.Shrnutí výsledků a vyhodnocení

Seznam doporučené odborné literatury:

[1] Egele, M., Kruegel, C., Kirda, E., Yin, H. and Song, D., 2007. Dynamic spyware analysis.
[2] Kirda, E., Kruegel, C., Banks, G., Vigna, G. and Kemmerer, R., 2006, August. Behavior-based Spyware Detection. In Usenix Security Symposium (p. 694).
[3] Moshchuk, A., Bragin, T., Gribble, S.D. and Levy, H.M., 2006, February. A Crawler-based Study of Spyware in the Web. In NDSS (Vol. 1, p. 2).
[4]Stafford, T.F. and Urbaczewski, A., 2004. Spyware: The ghost in the machine. The Communications of the Association for Information Systems, 14(1), p.49.

17. listopadu 2172/15
708 00 Ostrava-Poruba
Česká republika

spojovatelka: +420 597 321 111
epodatelna: epodatelna@vsb.cz
ID datové schránky: d3kj88v

IČ: 61989100
DIČ: CZ61989100

email: studijni.fei@vsb.cz
www.fei.vsb.cz

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **prof. Ing. Ivan Zelinka, Ph.D.**

Datum zadání: 01.09.2022

Datum odevzdání: 30.04.2023

Garant studijního oboru: prof. RNDr. Václav Snášel, CSc.

V IS EDISON zadáno: 07.11.2022 11:59:22

Abstrakt

Tato diplomová práce se zabývá spywarem a jeho tvorbou pro mobilní zařízení. Je zde obecně popsána problematika malwaru a spywaru, včetně technik sociálního inženýrství. Dále se zabývá aktuálním stavem na poli moderních technologií spyware, a to jak pro systém Windows, tak i pro populární mobilní platformy. Hlavní důraz je kladen na implementace aplikací klienta a serveru, které mají simulovat reálný útok na mobilní zařízení. Pomocí frameworku Xamarin byla vyvinuta aplikace pro Android, která demonstruje jednoduchost získávání osobních informací oběti z mobilního zařízení. Všechna získaná data se odesílají na vzdálený server, který následně útočníkovi umožňuje data prohlížet, a popřípadě zneužít. Výsledná mobilní aplikace je následně testována proti odhalení populárními antivirovými programy, které jsou dostupné v obchodě s aplikacemi. Na závěr práce jsou předvedeny ukázkové příklady užití obou aplikací.

Klíčová slova

Spyware; Malware; Xamarin; Android; C#; diplomová práce

Abstract

This master thesis is focused on spyware and its creation for mobile devices. It describes the issue of malware and spyware in general, including social engineering techniques. The current state of the art in the field of modern spyware technologies is also analyzed, both for the Windows system and for popular mobile platforms. The main emphasis is placed on the implementation of client and server applications that are intended to simulate a real attack on mobile devices. Using the Xamarin framework, an Android application was developed to demonstrate the simple retrieval of a victim's personal information from a mobile device. All the obtained data are sent to a remote server, which allows the attacker to view the data and possibly abuse it. The final mobile application is then tested against detection by popular antivirus programs available in the app store. At the end of the thesis, examples of the use of both applications are presented.

Keywords

Spyware; Malware; Xamarin; Android; C#; master thesis

Poděkování

Rád bych na tomto místě poděkoval prof. Ing. Ivanovi Zelinkovi, Ph.D. za odbornou pomoc a konzultaci při zpracování této diplomové práce.

Obsah

Seznam použitých zkratek a symbolů

IP	–	Internet Protocol
RSA	–	Rivest–Shamir–Adleman
AES	–	Advanced Encryption Standard
WMI	–	Windows Management Instrumentation
URL	–	Uniform Resource Locator
SMS	–	Short Message Service
DNS	–	Domain Name System
APK	–	Android Application Package

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

V dnešní době proniká výpočetní technika do všech sfér našeho života. Málokdo si v moderní společnosti umí představit život bez internetu, počítače, nebo chytrého telefonu. Tato technika v současnosti patří do běžných potřeb každé domácnosti, instituce, nebo podniku. Jako příklad je třeba zmínit různé obchody a služby, kde při výpadku systému nelze obsloužit zákazníka, ani zaplatit kartou.

Na internetu lze najít nespočet důležitých informací, ale je třeba také dávat pozor na potenciální nebezpečí, které veřejná síť skýtá. Je třeba mít na paměti, že ne všichni uživatelé internetu se připojují za dobrými úmysly. Útočníci skrytě čekají na možnost způsobit uživatelům internetu škodu, a to většinou za účelem svého výdělku. Jejich malware se může soustředit na náhodné koncové uživatele, nebo přímo na celé firemní domény. Pro šíření jsou nejčastěji využity techniky sociálního inženýrství, kterými se útočník snaží získat důvěru oběti. Kyberzločinci se předhánějí ve vytváření nových útočných technik a taktik, přičemž v závěsu za nimi jsou vždy ti, kteří se snaží koncového uživatele ochránit. V průběhu let se stále objevují nové druhy škodlivého softwaru, které jsou čím dál tím víc sofistikovanější.

Spyware je speciální druh malwaru, který se snaží získat citlivá data, a tajně je odeslat útočníkovi. Obecně se snaží získat uživatelská hesla, osobní informace, navštívené webové stránky, nebo údaje ke kreditním kartám. Většinou se dobře skrývá a snaží se zůstat v systému co nejdéle, protože se tím zvyšuje šance získat velmi cenné informace. Nejefektivnější spyware dnešní doby míří na mobilní telefony, které obsahují velké množství cenných dat. Klasicky je větší riziko u takových aplikací, které nejsou z oficiálního obchodu pro danou platformu.

Tato práce se zabývá problematikou a tvorbou mobilního spywaru, která nemůže být v dnešní době více aktuální. Díky rychlému technologickému pokroku se staly mobilní telefony součástí našeho každodenního života. Časem přišel větší dotykový displej, kvalitní operační systém, a neustálé zvyšování výkonu. Toto způsobilo, že dnes již všichni mají chytrý telefon na dosah ruky, a ukládají si v něm všechny důležité informace. Mobilní aplikace tak mohou využívat integrované funkce, a obohatit operační systém o mnoho dalších nových funkcí. Ať už jde o zábavu, vzdělání, nebo ulehčení

každodenního života. Tyto funkce usnadnění mohou být ovšem nebezpečné, pokud se do systému dostane škodlivá aplikace. Na tento potenciál přístupu k cenným datům se v průběhu let snaží reagovat tvůrci škodlivého softwaru, kteří dokážou být velmi kreativní. V současném trendu bezpečnostních hrozeb se práce snaží poukázat na jejich známé varianty, typy útoků, a důležitost celkového povědomí o hrozbách u koncového uživatele. V praktické části dojde k implementaci ukázkového spywaru, který bude obsahovat běžné funkce moderního malwaru, a využívat základní techniky sociálního inženýrství. Následně dojde k testování proti odhalení, a na závěr k ukázkovým příkladům užití.

Kapitola 2

Seznámení s problematikou

2.1 Techniky sociálního inženýrství

Sociální inženýrství je jedním z nejúspěšnějších prostředků, jak mohou útočníci získat přístup k datům oběti. Tato metoda útoku spoléhá na lidskou chybu a nevědomost.

2.1.1 Phishing a Spear Phishing

Phishing je v dnešní době stále jeden z nejčastějších typů útoku sociálního inženýrství. Spoléhá na lidskou důvěru, a globální závislost na e-mailové komunikaci[1]. Útočník zkonstruuje podvržený e-mail a rozešle potenciálním obětem. Přičemž se vydává za důvěryhodný kontakt, aby zmanipuloval k předání citlivých údajů. Takto podvržený e-mail může například obsahovat odkaz na napodobeninu reálné webové stránky, nebo přihlašovacího formuláře. Tímto způsobem může oběť nevědomě předat své přihlašovací údaje na internetové bankovnictví, nebo jiné webové služby. Další příklad může být přesvědčení oběti, aby si stáhla přílohu se škodlivým kódem, a po spuštění se nainstaluje příslušný malware. Hromada pokusů o phishing cílí na tisíce uživatelů, a proto je většinou neosobní. Obsah takového e-mailu nebude pro příjemce vždy relevantní, takže útoky lze poměrně snadno odhalit.

Největší nárůst e-mailů využívající phishing v poslední době přišel během koronavirové krize v březnu 2020, kdy se organizace snažily zajistit svým zaměstnancům práci z domova. Na tohle období strachu a nejistoty hned zareagovali útočníci, a podle zprávy Barracuda Networks[2] počet phishingových e-mailů vzrostl o alarmujících 667 %.

U spear phishingu cílí útočník na jednoho uživatele. Před útokem je nutné vědět hodně informací o oběti, včetně pracovní role a lidech z jeho okolí. To umožňuje poslat velice personalizovaný důvěryhodný e-mail, který je velmi těžké odhalit. Tyto zprávy jsou tolik sofistikované, že se hodněkrát vyhnou tradičním způsobům filtrování e-mailů.

2.1.2 Vishing

Tento název vznikl spojením anglického slova voice, a phishing. Do češtiny to lze volně přeložit jako hlasový phishing. Vishing spoléhá na použití hlasové komunikace pro oklamání oběti. Prostřednictvím hlasového hovoru se snaží útočník donutit oběť k předání osobních informací, zatímco se vydává za nějakou pověřenou osobu. Tímto způsobem může z oběti dostat adresu, přihlašovací údaje, informace k platební kartě, a další data. Tento hovor většinou zahrnuje zmínění časové tísně, k vytvoření pocitu naléhavosti. V tomto případě má oběť pocit, že nemá jinou možnost než předat informace.

2.1.3 SMiShing

Další typ phishing útoku, který se snaží oklamat oběť k předání osobních informací prostřednictvím podvodných SMS zpráv. V této zprávě buď vyzývá k otevření odkazu URL, nebo zavoláním na specifické číslo. V prvním případě je odkaz přesměruje na falešnou stránku, kde jako v případě phishingu žádá o stažení software, nebo vyplnění přihlašovacích údajů. Druhý případ vede k telefonnímu hovoru, kde dojde k pokusu o vishing, nebo se jedná o číslo se zvýšenou sazbou hovoru, a oběti potom přijde tučný telefonní účet.

2.1.4 Whaling

Je využíváno spear phishingu pro získání informací o lukrativnějším cíli, jako je například ředitel, nebo jiný vysoce postavený zaměstnanec. Poté se z něj snaží dostat podvodem informace, nebo velké bankovní převody. Pro tento typ útoku je také možné se vydávat za nadřízeného oběti, a díky tomu z hlavního cíle dostat důležité informace, nebo dokonce peníze. Tato iluze nadřízeného je další úroveň sociálního inženýrství, a přitom využívá základní psychologii. Jednoduše se většina zaměstnanců bojí odmítnout požadavky výše postaveného subjektu.

2.1.5 Pharming

Poslední ze zmíněných je pharming, který nevyužívá e-mailovou komunikaci. Tato forma sociálního inženýrství využívá napodobeniny reálných webových stránek. Poté je nutné podvrhnout DNS server, aby přesměrovával všechny dotazující zařízení na tento web. Po zadání přihlašovacích údajů, nebo informací k internetovému bankovnictví, dojde hned k odeslání získaných dat útočníkovi. Pharming tedy neútočí na jednu osobu, ale na všechny, co se dotazují na DNS překlad v určité doméně.

2.2 Malware

Název vznikl kombinací anglických slov malicious a software. Přičemž slovo malicious může znamenat zlomyslný, či škodlivý. Takže toto slovní spojení můžeme volně přeložit jako škodlivý software. Jedná se o počítačový program nebo kus kódu, který byl vytvořen za účelem napadení koncového zařízení. Po infikování systému může docházet k jeho poškození, ovládnutí, sledování, nebo odcizení dat uživatele[3].

Cílem každého tvůrce takového softwaru je zisk, který lze získat přímo krádeží údajů pro internetové bankovnictví, nebo zajistit přeprodej cenných uživatelských dat. Útočníci jsou při hledání způsobu infikování zařízení velmi kreativní. Avšak největší úspěchy zajistili útokem na nejslabší článek zabezpečení, a to samotný uživatel. Pomocí různých technik sociálního inženýrství pokouší zvědavost oběti, a pro nakažení zařízení většinou pak stačí jedno kliknutí. Obecně jsou nejúspěšnější, a zároveň nejlevnější podvodné e-mailové kampaně.

2.2.1 Dělení

Malware se dělí na mnoho kategorií, a to například podle způsobu šíření, či funkcí. V dnešní době existuje mnoho speciálních kategorií tohoto softwaru, a proto budou níže popsány jen jeho nejčastěji objevující varianty[4]. Spyware, který je zároveň téma práce, je samostatně popsán v kapitole 2.3.

2.2.1.1 Adware

S tímto typem se setkalo velké množství uživatelů internetu. Jednoduché verze tohoto malwaru napadají internetové prohlížeče, a obtěžují uživatele nechtěnými reklamami. Pokročilejší druhy mohou sledovat internetovou aktivitu, odkazovat na phishing stránky, nebo měnit nastavení prohlížeče. Přítomnost adwaru lze poznat podle často objevujících vyskakovacích oken, přidáním nežádoucího doplňku do prohlížeče, pomalejší rychlost prohlížení, změna zobrazení stránek, nebo přesměrovávání na podezřelé stránky.[5]

Neškodný adware se také vyskytuje ve volně šířených bezplatných programech. V mnoho případech se lze tomuto vyhnout, a to odebráním souhlasu během procesu instalace. Doporučením je i číst licenční podmínky softwaru, protože je možné, že do zařízení pronikne adware legálním způsobem. Pro vývojáře je to často jediný zdroj příjmů pro financování vývoje.

2.2.1.2 Bezsouborový malware

Oproti tradičním typům malwaru nepoužívá spustitelné soubory, a nijak neovlivňuje souborový systém. Místo toho používá nesouborové objekty, jako makra Microsoft Office, Powershell, Windows Management Instrumentation (dále jen WMI), a další systémové nástroje. Do zařízení se mohou dostat prostřednictvím exploitu, kompromitovaného hardwaru, nebo spouštěním podezřelých aplikací a skriptů. Tento malware se dělí na tři typy[6]:

- **Typ I: Žádná souborová aktivita -** Do této skupiny patří instalace zadních vrátek do paměti jádra, nebo přidání škodlivého kódu do firmwaru. (BIOS, nebo síťová karta) Může přežít formátování disků, i přeinstalaci operačního systému.
- **Typ II: Nepřímá souborová aktivita -** Zapsání škodlivého skriptu do úložiště WMI, které je ve fyzickém souboru. I v tomto případě se jedná o útok bez souborů, protože úložiště WMI je datový kontejner, který nelze detekovat, nebo odstranit.
- **Typ III: Soubory jsou potřebné k provozu -** Dojde k využití souboru, který ale nelze detekovat jako hrozbu, protože jsou v něm náhodná data. Do registrů se uloží klíč, který obsahuje obslužnou rutinu systému pro náhodnou příponu souboru. Do dalšího klíče potom uloží příkaz ke spuštění takového souboru při startu systému. Následné otevření potom spustí škodlivý skript pomocí legitimního nástroje.

2.2.1.3 Počítačový virus

Program, který pro nakažení a šíření vyžaduje akci uživatele. Název byl odvozen kvůli podobnosti s biologickým virem, který se šíří vkládáním do živých buněk, a přenosem mezi lidmi[7]. Jinak řečeno, většinou se jedná o spustitelný soubor, který se po spuštění sám šíří do dalších aplikací. Dále také může být skrytý v systémových oblastech disku, dokumentech Microsoft Office, ve skriptech, nebo dalších místech. Tento typ může pro systém také mít destruktivní účinky, jako je mazání souborů, nebo poškození dat.

2.2.1.4 Červ

Tento speciální typ se oproti viru dokáže přenášet sám, a nepotřebuje žádnou asistenci. Při úspěšném nakažení koncového zařízení se provede kód červa, a poté se pokusí o jeho další šíření. Jako přenosové médium umí použít lokální sítě, e-mailovou komunikaci, nebo přenosných médií. U přenosu přes počítačovou síť se vkládá do síťových paketů, kde využívá zranitelnosti připojených zařízení. Může také využít sdílené síťové adresáře cílové domény, a vkládat zde infikované soubory. Takto může za krátký čas dosáhnout nakažení celé firemní, nebo školní sítě. Při šíření e-mailem se po nakažení červem odešle všem kontaktům oběti e-mail s nakaženou přílohou, a tento proces se u každé oběti opakuje.

2.2.1.5 Trojský kůň

Název tato skupina získala podle příběhu z řeckých bájí, kde Řekové tajně ukryli vojáky do dřevěného koně. Trójané se nechali přelstít, a vtáhli tento dar do města. Skrytí vojáci v noci vylezli a otevřeli bránu, což vedlo k dobytí města Trója.[8]

Tento kůň v softwarové podobě představuje legitimní software, jako vojáky si lze představit škodlivý kód a město Trója jako zařízení oběti. Z toho tedy vyplývá, že je hrozba zamaskována

do bezpečně vypadajících souborů nebo programů. Malware tohoto typu sám není schopen šíření jako vir nebo červ, kvůli tomu spoléhá na stažení a spuštění uživatelem. Útočník toho dosáhne často prostřednictvím taktik sociálního inženýrství. Po úspěšném nakažení pak provádí svůj kód v pozadí. Mezi jeho funkce může patřit například otevření zadních vrátek, převzetí kontroly zařízení, získání dat uživatele, nebo stažení a spuštění jiného malwaru.

2.2.2 Obrana a prevence

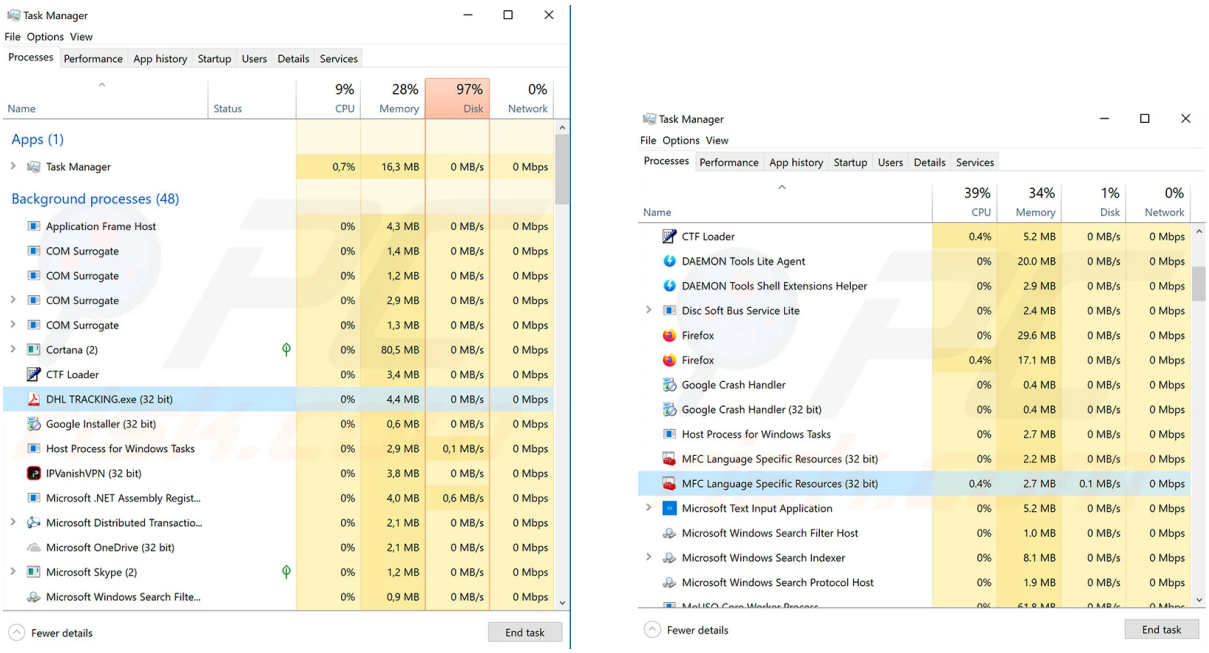
Pokročilé antivirové programy zvládnou odstranit malware z počítače, telefonu nebo internetových prohlížečů. Na riziko infekce vždy upozorní, a umístí podezřelý soubor do karantény. Tato akce znemožní malwaru provádět škodlivou činnost. Při selhání antivirového programu nebo nástroje pro odstranění škodlivého softwaru je nutné ruční odebrání. Toho lze dosáhnout spuštěním zařízení v nouzovém režimu, jak doporučuje oficiální podpora Microsoft[1].

Bez pomoci nástrojů se malware poznává velice těžko, jelikož většina symptomů může být velmi neurčitá. Někdy se stačí podívat na běžící procesy, kde si můžeme všimnout podezřelé aktivity, jak je vidět na obrázku 2.1. Jedním z typických příkladů je doporučení pro pozastavení antiviru u instalace, nebo jeho vypnutí bez vědomí uživatele. Malware se snaží v počítači schovat, a tyto programy mu práci komplikují. Další z příkladů může být zvláštní chování internetového prohlížeče, jako například velký počet nevyžádaných reklam, změna záložek, domovské stránky a podobně. Takové chování můžou způsobit typy browser hijacker nebo adware. Počítač může v případě nakažení i velmi zpomalit svoji práci, jelikož některé druhy malware využívají nemalou část operační paměti. V takovém případě může způsobit zamrzání, nebo dokonce přehřívaní, které vede k modré smrti. Navíc může zablokovat místo na disku, naistalovat doprovodné programy a podobně. Počítač taky někdy může upozorňovat na funkční chyby, poškozené soubory nebo adresáře, což může být výsledkem aktivity malware. Někdy totiž maže nebo nahrazuje reálné soubory, které potom chybí při funkcích legitimního softwaru.

Nelze popírat, že na internetu číhají zločinci a hackeři. Ve firemní sféře za rok 2022 se 82 % narušení bezpečnosti týkalo lidského selhání[10]. V této oblasti je nejlepší obrana odborné školení o povědomí možných útoků a bezpečnosti. Protože uživatelé jsou jak cílem, tak i poslední linií obrany proti všem útokům malwaru. Níže budou popsány způsoby, jak se lze obecně proti těmto hrozbám chránit[11]:

- **Aktualizace zařízení a softwaru -** Je žádoucí užívat aktualizovaný operační systém, prohlížeč, antivirový program a firewall. Softwarové společnosti často vydávají aktualizace svého softwaru, které obsahují opravy chyb a exploitů. Pokud zařízení běží na operačním systému, který již nemá průběžnou podporu výrobce, tak nemusí být odolný vůči novým hrozbám.

[1] https://support.microsoft.com/en-gb/topic/how-to-prevent-and-remove-viruses-and-other-malware-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5



(a) Proces DHL TRACKING.exe (b) Proces MFC Language Specific Resources

Obrázek 2.1: Podezřelé procesy spywaru ve správci úloh[9]

Pokud zařízení má všechny bezpečnostní aktualizace, tak se zlepší jeho obrana vůči možným útokům.

- **Nevyužívat profil administrátora -** Pro běžnou práci, nebo kdykoli je to možné, se doporučuje používat účet s omezenými právy. Účet správce má všechna práva, jako je například instalace nového softwaru, změna v registrech, a podobně. Použitím účtu s omezenými právy může zabránit tomu, aby se malware nainstaloval do počítače a měnil nastavení na úrovni celého systému.

- **Neklikat na podezřelé odkazy a nestahovat z nich -** Útočníci se snaží nalákat uživatele, a po kliknutí na odkaz nabízejí různé věci zdarma. O neznámých webových stránkách je nejlepší vyhledat informace nebo recenze předtím, než z nich hned něco stáhnout a nainstalovat. Stahování škodlivých souborů je nejčastější způsob, jak se do zařízení může dostat malware.

- **Neotevírat přílohy podezřelých e-mailů -** Důležité je, aby v žádném případě nedošlo k otevření přílohy e-mailu od neznámého odesílatele. Někdy může jít pouze o spam nebo reklamu, ale jindy o výplod technik sociálního inženýrství, který se snaží oběť donutit k otevření přílohy.

- **Nevěřit vyskakovacím oknům -** Jako obecný příklad můžou být případy, kdy stránka hlásí, že uživatel vyhrál něco zadarmo, nebo že jeho počítač byl infikován. Okno chce uživatele donutit k otevření nakaženého odkazu, nebo stažení škodlivého softwaru.

- **Omezení sdílení souborů -** Při stahování ze sdílených úložišť je před spuštěním souboru žádoucí kontrola antivirovým programem. Sdílené úložiště je často cílem počítačového červa, nebo jiného typu malwaru. Škodlivý software může být zamaskován jako fotka, video, dokument, hra, nebo program.

- **Používat antivirový software -** Ideální scénář je, že by uživatel měl pomocí tohoto softwaru zkontrolovat všechny stažené položky, a to ještě před jejich spuštěním. Podporují i kontrolu celého zařízení jako prevenci před nakažením. Tato kontrola by se měla provádět pravidelně, aby se malware podařilo odhalit včas, a zabránit jeho šíření.

2.3 Spyware

V dnešní době je jedním z nejnebezpečnějších typů malwaru, jelikož sbírá tu nejcennější věc - citlivá data. Samotný pojem spyware vznikl z anglického slova „spy“, tedy v překladu špehovat nebo špión. Může za to fakt, že spyware je škodlivý software, který tajně sbírá informace a následně je odesílá útočníkovi. Existuje hodně druhů tohoto malwaru, ale většinou se zaměřuje na data, která mají nějakou hodnotu. Může se jednat o přihlašovací údaje, informace o kreditních kartách, nebo další citlivá osobní data. Útočník získané informace může využít pro další kyberútoky, nebo je přeprodává třetí straně.

Spyware je pro nezkušené uživatele těžko odhalitelný, jelikož svou činnost úplně skrývá, nebo schovává za důvěryhodně vypadající procesy. Většinou nijak neovlivní chod systému, jen se snaží od uživatele získat cenné informace. Nejefektivnější spyware je ale v dnešní době mířený na mobilní telefony, kde uživatelé vkládají mnohem více osobních informací. Největší riziko skrytě implementovaného spywaru je u mobilních aplikací, které nejsou z jejich oficiálního obchodu pro danou platformu.

2.3.1 Historie spywaru

S pojmem „spyware“ se setkala většina uživatelů internetu. Tento název se poprvé veřejně objevil v říjnu 1995, na diskuzním fóru Usenet. Obsahoval ho článek, který se zaměřil na obchodní model Microsoftu. Název se nejdřív moc neuchytil, a proto bylo tomuto typu malwaru přezdíváno jako „vybavení pro slídění“[12].

Potom se oficiálně objevil až během roku 2000, kdy ho zakladatel Zone Labs - Gregor Freund[13] zmínil v tiskové zprávě pro produkt osobního firewallu, což způsobilo začátek používání tohoto termínu v praxi. Na začátku roku 2001 si Steve Gibson, zakladatel Gibson Research Corporation, všiml něčeho divného. Uvědomil si, že v jeho systému je nainstalován reklamní software, který tajně krade jeho osobní údaje. Na základě tohoto objevu se rozhodl proti tomu bojovat, a po nějaké době vydal v historii první anti-spywarovový nástroj - OptOut[2].

[2]https://www.grc.com/optout.htm

V říjnu roku 2004 provedly společnosti America Online a National Cyber-Security Alliance průzkum kvůli rozšiřující se aktivitě spyware[14]. Výsledek byl alarmující, protože přibližně 80 % uživatelů, kteří se zúčastnili tohoto průzkumu mělo svůj systém nakaženo tímto typem malwaru. A přibližně 95 % přiznalo, že pro jejich instalaci neudělili povolení.

Od počátku 21. století je tento termín používán všemi společnostmi zabývající se kyberbezpečností. Tedy druh nežádoucího softwarového programu, který je určen pro špehování aktivity počítače a získání osobních údajů. V minulosti byl obecně pro útoky preferován systém Windows, a to kvůli jeho velkému rozšíření. Nicméně v posledních letech útočníci obrátili svou pozornost i na mobilní zařízení. Kvůli tomu se nyní vývojáři věnují zabezpečení více než kdy dřív. Například společnost Apple během minulého roku zareagovala na množící se počet útoků spywaru Pegasus, který je detailně popsán v kapitole 4.3.2. A vydala bezpečnostní funkci zvanou „Lockdown Mode“[15], kterou může zapnout napadený uživatel. Jednoduše dojde k omezení určitých funkcí, čímž sníží dopad útoku spywaru. Háček je ale v tom, že uživatel si musí být vědom probíhajícího útoku.

2.3.2 Typy spywaru

Tento specifický malware má mnoho podob. Může se například chovat jako jednoduchý keylogger, který zachytává stisknutí kláves. Více pokročilé varianty jsou schopny monitorovat obrazovku, odposlouchávat síťový provoz, přeposílat soubory útočníkovi a nebo můžou obsahovat různé kombinace již zmíněných funkcí. Kvůli tomu je dle mého názoru těžké tuto skupinu rozdělit na specifické druhy. V dnešní době je pravidlem, že jsou velmi komplexní a skoro vždy kombinují větší počet funkcí. Některé obecné typy spywaru jsou zmíněny níže[16]:

- **Adware -** Popsán v kapitole 2.2.1.1. Mezi spyware patří pouze pokročilejší varianty, které sledují historii vyhledávání, navštívené webové stránky a posílají tyto informace útočníkovi. Jednoduché verze tohoto malwaru, které pouze zobrazují nevyžádané reklamy a neodesílají žádné data útočníkovi, se mezi spyware neřadí. Patří mezi ně i browser hijacker, který může mít podobné funkce, ale navíc dokáže měnit nastavení prohlížeče.
- **Systémový monitoring -** Představují vážné riziko pro soukromí, protože tajně sledují aktivitu uživatele. Do této skupiny patří například keylogger nebo sniffer. Zástupci této kategorie mohou sledovat nainstalované programy, navštívené webové stránky, ovládat zařízení, monitorovat všechny stisknutí kláves, nebo informace o síťové komunikaci.
- **Trojský kůň -** I tento typ malwaru může mít funkce pro získávání osobních informací, pokud je tak navržen. Po nakažení může získávat uživatelské údaje pomocí funkcí podobných systémovému monitoringu, nebo uživatele přesměrovávat na podvodné stránky. Detailní popis tohoto malwaru je v kapitole 2.2.1.5. Do této kategorie může například patřit falešný anti-spyware software, který se může tvářit jako bojovník proti spywaru, který ho ale ve skutečnosti instaluje.

Kapitola 3

Aktualizace stavu na poli moderních technologií spyware

I přes neustálé vylepšování ochrany uživatele a povědomí společnosti o kybernetických hrozbách, je toto téma pořád aktuální. Na začátku roku 2023 se v České republice zvýšil počet detekovaných výskytů spyware. Nejčastěji se šíří prostřednictvím e-mailového spamu, kde se útočník snaží přimět oběť k otevření infikované přílohy. Jako zástěrka je v mnoha případech použita skutečná společnost, a tyto infikované e-maily obsahují firemní loga a legitimně vypadající podpisy fiktivních, nebo i skutečných osob. Tyto e-maily mohou být nejen v angličtině, ale i v češtině. Útočníci se snaží lokálně přizpůsobit a využít českých překladů, které ale někdy mohou obsahovat chyby. Díky tomu si může uživatel všimnout, že je něco v nepořádku. V ideálním případě by takové kybernetické hrozby měly být zastaveny již v rané fázi, a to detekcí škodlivého e-mailu ze strany poštovního serveru. Statistiky detekovaných hrozeb od společnosti ESET za leden 2023 jsou v tabulce 3.1.

Nejčastěji se útočníci snaží získat přihlašovací údaje, které později využijí na napadení konkrétních online služeb. Nejcennější určitě jsou v tomto případě údaje k internetovému bankovnictví, nebo platebních karet. Důležité je taky, aby uživatel nepodcenil složitost svých hesel. V běžném případě se může útočníkům podařit získat hodnotu hash uživatelských hesel. A čím je heslo složitější, tím bude pro útočníka těžší prolomit. Obecně silné heslo by mělo být dlouhé aspoň 10 znaků, a obsahovat velká a malá písmena, číslice, a nejlépe i speciální znaky.

Tabulka 3.1: Tabulka nejčastěji detekovaných hrozeb v České republice za leden 2023[17]

Název	Procento výskytu
MSIL/Spy.AgentTesla trojan	15,14 %
Win32/Formbook trojan	9,61 %
Win32/PSW.Fareit trojan	1,96 %
Win32/Shafmia trojan	1,43 %
BAT/Runner trojan	1,22 %

Obrázek 3.1: Phishing e-mail spywaru Agent Tesla[18]

3.1 Agent Tesla

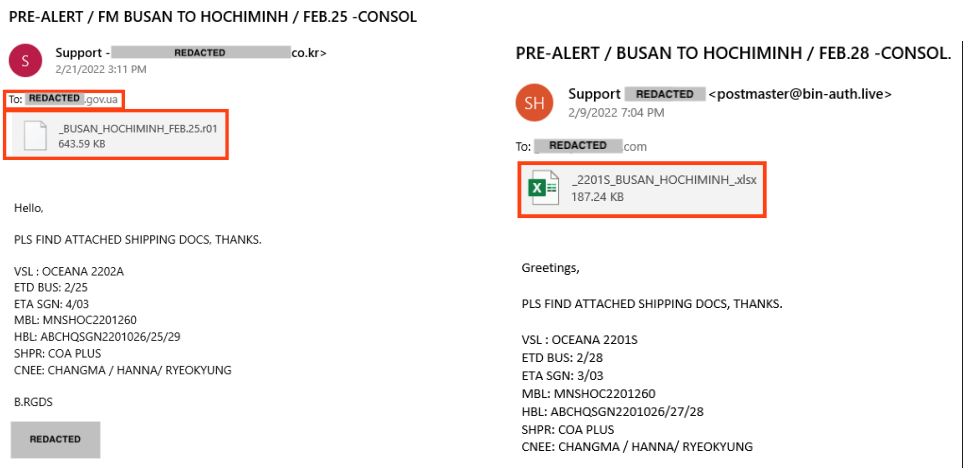
Tento spyware je statisticky největším rizikem pro českého uživatele, i když je známý už od roku 2014[1]. Objevil se v 15,14 % případů detekovaných hrozeb v České republice, jak je znázorněno v tabulce 3.1.

Agent Tesla je .NET trojský kůň pro vzdálený přístup, který je klasifikován jako Malware-As-A-Service (MaaS). Svůj vzdálený přístup může pak útočník využít pro instalaci dalších malware hrozeb. Jedná se o agresivní typ škodlivého softwaru, který napadá systém Windows a zaměřuje se na odcizení hesel. Obsahuje funkce, které umí prohledat internetové prohlížeče, e-mailové klienty, databáze, VPN aplikace, nebo nástroje pro vzdálenou zprávu. Z těchto programů vytáhne důvěrné informace, jako třeba přihlašovací údaje, které pak odešle útočníkovi. Dále je ještě schopen krást zkopírovaná data ze schránky, zaznamenávat stisky kláves, nebo pořizovat snímky obrazovky[18]. Šíří se jako spustitelná e-mailová příloha, přičemž její nejčastější název v lednu byl „PAYMENT SLIP_002_JPEG.exe“[17], který svou indikací neprovedené platby pokouší zvědavost oběti. Příklad e-mailu, kde útočník používá skutečnou společnost jako zástěrku, je na obrázku 3.1.

3.2 Formbook

Funguje na principu prohledávání procesů, kde z paměti vytahuje určité řetězce a následně je krade. Formbook dokáže ukrást přihlašovací údaje z webových prohlížečů, pořizovat snímky obrazovky,

[1]https://cofense.com/blog/the-rise-of-agent-tesla-understanding-the-notorious-keylogger/



(a) Komprimovaná příloha (b) Příloha typu Microsoft Office

Obrázek 3.2: Typy příloh při šíření spywaru Formbook[21]

zaznamenávat stisknutí kláves, stahovat a spouštět soubory podle instrukcí útočníka, čímž může dojít k infikování jiným druhem malwaru.

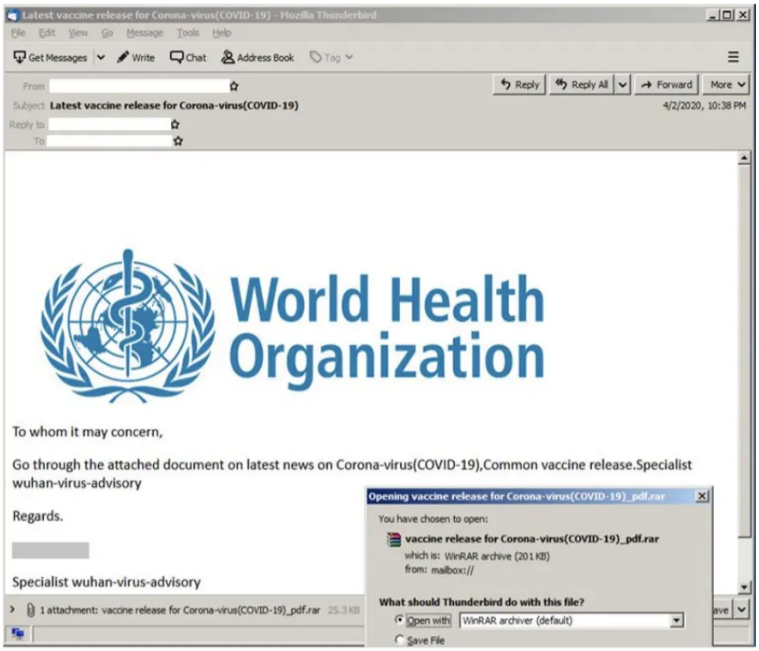
Poprvé byl detekován v roce 2016 a dodnes je prodáván na nelegálních fórech. Když dojde ke spuštění infikovaného souboru, vloží svůj obfuskovaný kód do legitimních procesů, aby se skryl před detekcí a zkomplikoval jeho odstranění ze zařízení[19]. Na začátku roku 2022 byl během války mezi Ruskem a Ukrajinou použit při kybernetickém útoku na ukrajinské cíle[20]. Během dubna téhož roku byl nejvíce detekovaný spyware u nás[2]. V lednu 2023 je tato hrozba stále aktuální, a u nás se nejčastěji v e-mailech objevoval jako příloha s názvem „RFQ-HKSCAN.exe“[17].

Pro šíření využívá techniky sociálního inženýrství, a to většinou phishing. V každém případě se snaží uživatele donutit ke stažení e-mailové přílohy. Příloha může mít podobu dokumentu Microsoft Office, spustitelného souboru, nebo komprimovaný soubor. Podoby infikovaného e-mailu jsou na obrázku 3.2.

3.3 Fareit

Fareit pracuje hlavně jako password stealer. Na přelomu roku se objevil jen v jednotkách procent, ale v průběhu minulého roku byl stabilně v českých e-mailových schránkách[3]. Útočníci vylepšili Fareit českým překladem, který se snaží získat důvěru uživatelů. Využívají manipulativní komunikaci a zajímavé názvy příloh, které mají pokoušet zvědavost oběti. Jednalo se například o přílohy se jmény „Objednávka TR04_ B004-V021_Patrem S.R.O.exe“, „Unicredit_SVX5700736_Elektronická platební.exe“, nebo „Objednávek(P.O_R6790074)_INTERCOM_Bohemia.exe“. Názvy obsahují překladatelské chyby, takže více zkušenější uživatel si může všimnout, že něco není v pořádku. Ale

[2]https://www.dvojklik.cz/spyware-formbook-odcizi-hesla-a-ovladne-pocitac/
[3]https://mobilenet.cz/clanky/pozor-na-malware-fareit-utoci-v-cr-na-uzivatelska-hesla-ve-windows-45500



Obrázek 3.3: Kampaň spywaru Fareit využívající vakcíny proti onemocnění COVID-19[22]

stačí troška nepozornosti uživatele, a už je zařízení nakaženo. Do budoucna se určitě útočníci zaměří na vylepšení českých překladů a vymýšlení lstivých způsobů, jak donutit oběť otevřít přílohu.

Fareit byl během vlny onemocnění COVID-19 šířen pomocí falešných výzev k vakcinaci. Tento podvodný e-mail byl zasílán pod jménem Světové zdravotnické organizace (WHO), a obsahoval i legitimní logo a podpis. Příklad reálného e-mailu šířící Fareit je na obrázku 3.3. Škodlivé přílohy byly zabaleny jako formáty .arj nebo .rar, a obsahovaly názvy jako „Corona-virus vaccine.arj“ nebo „vaccine release for Corona-virus(COVID-19)_pdf.rar“.[22]

Kapitola 4

Mobilní spyware

Mobilní telefony v průběhu tohoto století staly důležitou součástí každodenního života. Bylo to způsobeno hlavně nástupem chytrých telefonů, kdy máme všechny informace a aplikace na dosah ruky. Tyto zařízení obsahují většinou více osobních informací, než stolní počítače. Uživatelé v nich mají uložené fotky, zprávy, čísla, přihlašovací údaje, bankovnictví, nebo dokonce i své tělesné míry. Provází nás celý den, a to od vstávání, práci, či večerní odpočinek. Moderní útoky se kvůli množství informací zaměřují na tyto zařízení.

Dnes již existuje spyware na oba nejrozšířenější mobilní operační systémy, a to iOS i Android. Vývoj pro méně oblíbené platformy se většinou nevyplatí, a to kvůli poměru nákladů a potenciálních obětí. Většina škodlivých aplikací se tváří jako legitimní, a snaží se dostat do zařízení mimo oficiální obchody s aplikacemi. Ale pozor, můžou ale být i případy, které jsou k mání i v oficiálním obchodu, a obsahovat falešné spokojené recenze zákazníků. Existuje mnoho způsobů, jak se může spyware do zařízení dostat. Například pomocí phishing stránek a odkazů, instalací neznámých souborů APK, falešné doporučení na fórech, kliknutím na reklamu s malwarem, a dále. Nejdůležitější část je při spuštění, kdy je nutné si přečíst povolení, které aplikaci dáváme. Proč by například měla aplikace pro cvičení mít přístup do galerie, foťáku a telefonním kontaktům?

4.1 Spyware pro Android

U operačního systému Android je hrozba určitě vyšší než u jeho protějšku iOS. Může za to otevřenost systému, to přináší možnost nahlížet do kódu platformy, a hledat potenciální slabiny. Takový spyware se může do zařízení dostat jak stažením aplikace třetích stran, tak i instalací z oficiálního obchodu. Google Play zveřejněné aplikace sice kontroluje, ale ne tak do hloubky jako konkurence.

V poslední době přišlo velké odhalení, že někteří výrobci do svých zařízení vědomě dávají spyware. Píše se to ve studii, kterou zveřejnili výzkumníci z University of Edinburgh a Trinity College Dublin[23]. Tato studie se zatím týká jen zařízení prodávaných v Číně, ale po jejich exportu se budou takto přednastavené telefony chovat stejně. Toto je velmi závažné zjištění, jelikož Čína je jedním

z největších světových výrobců chytrých telefonů. U zkoumaných modelů Xiaomi Redmi Note 11, OnePlus 9R a Realme Q3 Pro je ve výchozím nastavení předinstalováno velké množství systémových aplikací, které mají povolené nebezpečné práva. Toto jim umožňuje shromažďovat a odesílat informace o poloze, používání aplikací, historie hovorů a SMS, čísla kontaktů a další osobní data.

4.2 Spyware pro iOS

Obchod AppStore má velmi striktní postupy schvalování nových aplikací, a proto je velmi malá šance, že na něm uživatel stáhne škodlivý software. Publikace takové škodlivé aplikace je v tomto obchodě velmi obtížná, ale nikoliv nereálná. Při neúspěchu publikace je potřeba dostat škodlivou aplikaci do zařízení jinak, a k tomu je potřeba povolení instalace aplikací třetích stran. Pro tuto funkci je nutné nejdřív donutit uživatele, aby ji povolil přes nastavení iCloudu[1]. V největším nebezpečí jsou uživatelé neoficiální verze iOS se jménem „jailbreak“[24], která má tuto funkci v základním nastavení povolenou.

4.3 Příklady mobilního spywaru

Na trhu existuje mnoho nabízených mobilních spywarů. Některé se tváří jako pomůcka pro hlídání aktivity dítěte, nebo firemních zařízení zaměstnanců. Jiné pomáhají k nelegálním činnostem a sledováním.

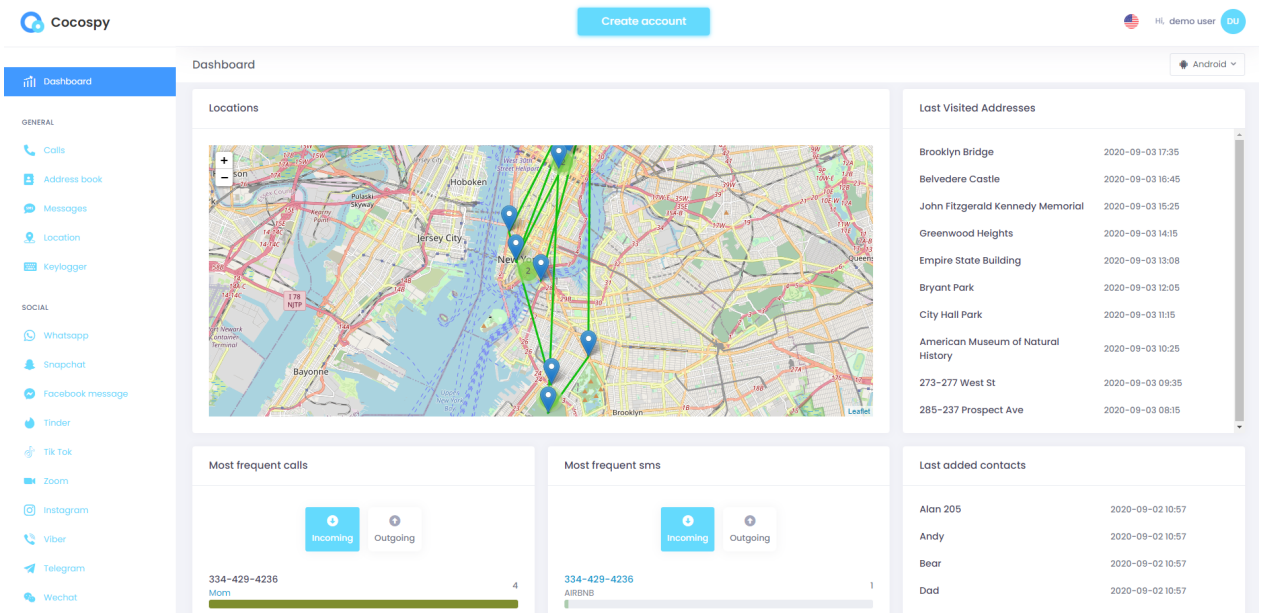
4.3.1 Komerční spyware

Zde jsou zmíněny příklady spywaru, které jsou komerčně nabízené, a platí si dokonce reklamu ve vyhledávači Google. Takové sledovací aplikace jsou vyvíjeny pouze kvůli zisku, a proto jsou všechny zpoplatněny.

4.3.1.1 Cocospy

Cocospy slibuje sledování zařízení v reálném čase, a podporuje operační systémy Android a iOS. Tváří se jako legální software určený pro dohled dětí, nebo zaměstnanců. Má přístup ke kontaktům, všem konverzacím na sociálních sítích, historii hovorů, sledování polohy a historie prohlížeče[2]. Obsahuje také keylogger, a může nahlížet do galerie fotek a videí. Obsahuje také tajný mód, který neupozorní uživatele o jeho sledování. Díky tomu může být použit pro nelegální činnost, a monitorovat uživatele bez jeho souhlasu. Po úspěšné instalaci na zařízení má útočník všechny důležité informace na webové nástěnce, jejíž demo verze je na obrázku 4.1.

[1] https://support.apple.com/cs-cz/guide/icloud/mmfeb236a772/icloud
[2] https://www.cocospy.org/



Obrázek 4.1: Webová nástěnka monitorovacího nástroje Cocospy

4.3.1.2 FlexiSpy

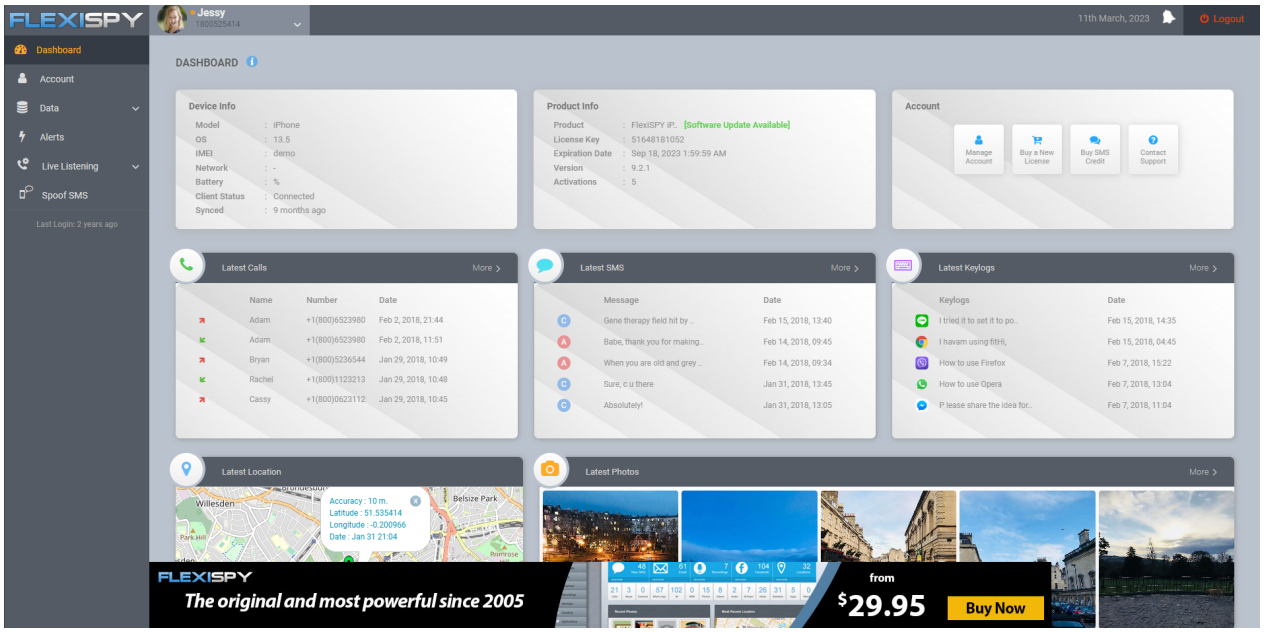
Podporuje operační systémy Android, iOS, Windows a MacOS[3]. Dá se říct, že neskrývá svou skutečnou podstatu. I když se tváří, že je určen pro monitorování dětí a zaměstnanců, tak tento spyware je populární mezi lidmi, co chtějí někoho nelegálně špehovat. Většinou je distribuován prostřednictvím webových stránek třetích stran, kde se snaží dostat do cílového zařízení. Tento spyware umožňuje poslouchat mikrofon, používat kameru, zaznamenávat stisknuté klávesy a sledovat konverzace. Je to plnohodnotný spyware, ale o jeho šíření se musí postarat útočník sám. Opět obsahuje webovou nástěnku, a její demo verze je na obrázku 4.2.

4.3.2 Pegasus

Tento spyware je považován za nejlepší, a zároveň za nejnebezpečnější z mobilních variant. Byl vyvinut společností NSO Group, která spadá pod izraelskou vládu. Byl použit jako nástroj pro sledování osob, které byli považovány jako nebezpečí pro židovský stát. Mezi ně patří i aktivisti, novináři, politici a ředitelé. Dále jako nástroj pro hon na válečné zločince, a další nežádoucí osoby.

Pegasus je multiplatformní malware, který lze nainstalovat na operačních systémech Android, iOS, BlackBerry OS, Windows Phone, nebo dokonce i na Linuxu. Pro šíření využívá techniky tradičního malwaru, a to konkrétně exploity nebo spear phishing, který je popsán v kapitole 2.1.1. Exploity dokážou využít odborní a dobře financovaní útočníci, přičemž Pegasus dostávají do zařízení útoky „nulového kliknutí“[25], které využívají zranitelnosti běžného softwaru. Útoky s nulovým

[3]https://www.flexispy.com/



Obrázek 4.2: Webová nástěnka spywaru FlexiSpy

kliknutím jsou velmi nebezpečné, a je velmi těžké se jim vyhnout. Nevyžadují žádnou akci uživatele, jelikož využívají bezpečnostní mezery, které se můžou vyskytnout v jakémkoliv softwaru. Útočník tak pošle škodlivý kód přes e-mail, v dokumentu, nebo v textové zprávě. Po přijetí klientské aplikace oběti se automaticky aktivuje škodlivý kód, a využije mezery v procesu ověřování dat. V minulosti bylo pro tiché proniknutí do zařízení využito exploitu aplikací Apple Messages, nebo WhatsApp[26]. Pegasus obsahuje funkce pro čtení textových zpráv, e-mailů, přístup do galerie, seznamu kontaktů, nebo nahrávání hovorů. Může také tajně v reálném čase odposlouchávat mikrofon, nebo snímat obraz z kamery.

Tento „vládní spyware“ byl v posledních letech využíván mnoho zeměmi pro vlastní zájmy. Obecně pro potřeby zahraniční zpravodajské služby, armády, nebo dokonce vnitřní sledování. Poslední ze zmíněných potřeb se většinou týkala diktatur, nebo zemí se silnou cenzurou. Časem se zjistilo, že Pegasus využilo až 27 zemí z celého světa. Mezi ně patří například USA, Polsko, Spojené království, Španělsko, Ukrajina, nebo Spojené arabské emiráty. Dodnes je tento spyware aktivně používán.

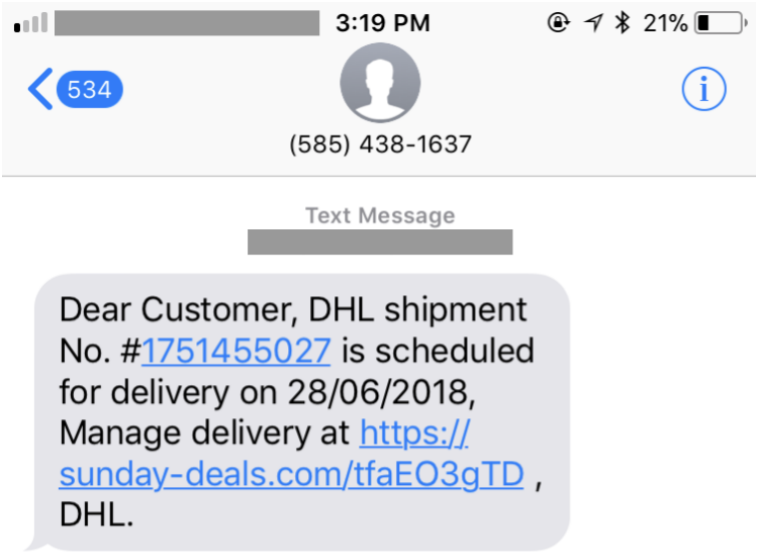
4.3.3 Obrana

Metody obrany proti spywaru Pegasus, a dalších moderních mobilních malwarů, se liší podle používané platformy. Níže budou rozebrány doporučené akce společnosti Kaspersky[27], které můžou snížit riziko nakažení.

- **Každodenní restart -** Zajistí, že útočníci budou muset zařízení znovu infikovat, jelikož tento typ pokročilých mobilních hrozeb pracuje pouze v operační paměti. Časem to zvyšuje šance na odhalení, nebo zachycení nakažené zprávy a útočného vektoru.
- **Aktualizace systému -** Udržujte zařízení aktuální, aby obsahovalo nejnovější bezpečnostní záplaty. Mnoho takových útoků využívá exploity, které jsou v novějších verzích systému opraveny.
- **Neotevírat odkazy v podezřelých textových zprávách -** Velká část útočníků si nemůže dovolit kupovat nově nalezené exploity, a proto pro šíření využívají techniky sociálního inženýrství. Tyto odkazy přijdou prostřednictvím SMS, e-mailu, nebo jiných komunikačních aplikací. Příklad takové zprávy je na obrázku 4.3.
- **Nepoužívat integrovaný prohlížeč -** Útoky nulového kliknutí mohou mířit i na výchozí prohlížeče platforem.

Následující příklady jsou relevantní pouze pro systém iOS.

- **Zakázání iMessage a Facetime -** Tyto služby jsou integrovány do systému iOS, a ve výchozím nastavení jsou povoleny. Což z nich činí velmi atraktivní cíle. Po mnoho let jsou na černém trhu exploity těchto aplikací velmi žádané a odměňované, takže se doporučuje tyto služby zakázat.



Obrázek 4.3: SMS zpráva obsahující škodlivý odkaz, který byl použit v roce 2018 pro nakažení telefonu spywarem Pegasus[28]

Kapitola 5

Návrh řešení

Cílem této práce je také naprogramovat mobilní aplikaci, která bude klasifikována jako spyware. To znamená, že musí splnit podmínky nepovoleného sbírání informací od uživatele, a posílat je útočníkovi na vzdálené úložiště. Testování a vývoj aplikace bude proveden v uzavřeném prostředí, a v žádném případě nebude nikdy využit pro nelegální sběr informací. Finální aplikace se bude řadit mezi spyware typu trojský kůň. To znamená, že se bude tvářit jako legitimní software, který ale bude tajně provádět škodlivou aktivitu.

5.1 Volba vhodných technologií

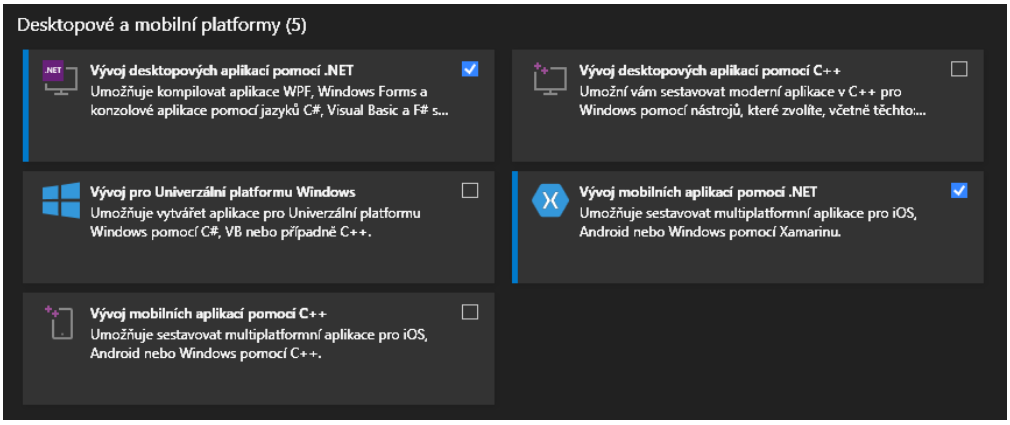
Vývoj mobilního spywaru bude realizován v jazyce C# a vývojové platformy Xamarin, která je spravována Microsoftem. Využitím Xamarinu má vývojář přístup k většině funkcím Androidu, které lze v našem případě zneužít pro tvorbu škodlivého softwaru. Dalším důvodem pro volbu této platformy je personální preference autora, protože ve vývoji v ní má už zkušenosti z bakalářské práce.

5.1.1 Xamarin

Xamarin je open source platforma využívající .NET, která umožňuje nativní vývoj aplikací pro operační systémy Android, iOS, Windows, Mac a další. Principiálně se při kompilaci projekt překládá do konkrétních nativních jazyků, a každá aplikace vypadá a chová se, jako by byla napsána nativně. Je to způsobeno abstraktní vrstvou, která se stará o komunikaci sdíleného kódu s nativním kódem platformy. Při použití Xamarinu že je možné většinu back-end kódu napsat pouze jednou, a v konkrétních podprojektech pro dané platformy upřesnit, přepsat, nebo rozvést potřebné funkce. V případě použití klasického Xamarinu je nutné uživatelské rozhraní definovat pro každou platformu zvlášť. To se změnilo příchodem Xamarin.Forms, který přišel s aktualizací Xamarin 3. Xamarin.Forms vyřešil dlouhodobý problém nepřenositelnosti kódu uživatelského rozhraní. Pokud chce vývojář aplikaci pro více operačních systémů, tak při použití rozšíření Xamarin.Forms pro uživatel-

Tabulka 5.1: Tabulka požadavků pro sestavení projektu u Visual Studio pro Mac a Windows[29]

	macOS	**Windows**
Vývojové prostředí	Visual Studio pro Mac	Visual Studio
Xamarin.iOS	Ano	Ano (s počítačem Mac)
Xamarin.Android	Ano	Ano
Xamarin. Forms	pro iOS a Android	Android, Windows (iOS s počítačem Mac)
Xamarin.Mac	Ano	Pouze kompilace



Obrázek 5.1: Sady funkcí pro desktopové a mobilní platformy ve vývojovém prostředí Visual Studio 2019

ské rozhraní je možné sdílet až 90% kódu napříč platformami. Díky Xamarinu můžeme dosáhnout nativního výkonu, vzhledu, i chování aplikací.

5.1.1.1 Vývojové prostředí a instalace

Vývoj podporují vývojové prostředí Microsoft Visual Studio, Xamarin Studio, nebo placená verze JetBrains Rider. Vývoj v Xamarin Studio se již nyní nedoporučuje, kvůli absenci nových aktualizací. JetBrains je nejnovější konkurence .NET vývojových prostředí, a již delší dobu podporuje i vývoj Xamarin aplikací. Visual Studio je dle mého názoru nejlepší volba pro potřeby každého Xamarin vývojáře. Toto vývojové prostředí je dostupné nejen na Windows, ale i MacOS, a to ve verzi Visual Studio for Mac. Vývojář může být v při sestavování projektu omezen, a to při konkrétní kombinaci cílové platformy a svého operačního systému. Přehled podporovaných kombinací je znázorněn v tabulce 5.1.

V rámci praktické části byl vývoj realizován ve vývojovém prostředí Visual Studio 2019 Community, v operačním systému Windows. Všechno potřebné pro začátek vývoje lze přidat již u instalace prostředí, nebo lze později doinstalovat ve Visual Studio Installer. V průběhu instalace je v sekci výběru sady funkcí na výběr „Vývoj mobilních aplikací pomocí .NET“, jako je na obrázku 5.1.

5.2 Typ služby

Foreground Service, neboli služba na popředí, je speciální typ spuštěných služeb v systému Android. Zpravidla má vyšší prioritu než běžná služba, a taky více možností přístupu ke zdrojům. Tento typ služby musí mít speciální notifikaci, která je viditelná po celou dobu jejího běhu.

Android v posledních letech zapracoval na zabezpečení, hlavně u běžících procesů na pozadí. U novějších verzí tohoto systému už není možné přistupovat k hardwaru a službám dle potřeb, jak tomu bylo dřív. Od verze Android 8.0 služby na pozadí dostaly mnoho omezení, jako třeba automatické vypínání těchto procesů po několika minutách práce[30]. Taková služba může být na pozadí pouze v tom případě, pokud jde například o správu paměti, či jinou triviální funkci. Pokud je ale na popředí, tak může volně vytvářet a spouštět jiné služby, a to na popředí i pozadí. Tato funkcionalita je pro vývoj spywaru klíčová, i když riskujeme odhalení uživatelem. Proto je žádoucí službu vydávat za legitimní, a to použitím názvu a oficiálního loga systému Android. Díky tomu je možné využít nevědomosti oběti k získání potřebných povolení pro běh spywaru, který bude implementován jako Foreground Service. Výsledná aplikace bude tajně sbírat informace o uživateli a jeho zařízení, které následně pošle na vzdálené úložiště. Implementované funkce budou záznam obrazovky, klávesnice a zvuku, doplněné o aktualizaci polohy a získání základních informací o zařízení. Na data před odesláním bude aplikována komprese, a hned poté šifrování.

5.3 Šifrovací algoritmy

Při implementaci byly pro šifrování dat použity algoritmy RSA a AES. Všechny odesílané data jsou zašifrovány symetrickým algoritmem AES. Oproti asymetrickým šifrováním je velmi rychlý, a i při šifrování velkého počtu bajtů není tolik náročný na hardware a software. Jediné negativum je to, že AES, a obecně symetrické algoritmy, používají stejný klíč pro zašifrování i dešifrování dat. Při odchytu předávání tohoto klíče mezi klientem a serverem může dojít k odhalení aktivity spywaru a získání ukradených dat. Tomuto lze předejít tak, že klíč AES je před odesláním na server zašifrován asymetrickým šifrováním RSA.

RSA je asymetrická šifra, která je vhodná nejen pro šifrování, ale i podepsání dokumentů prostřednictvím digitálního podpisu. Asymetrické algoritmy jsou specifické v tom, že pro zašifrování a dešifrování je potřeba jiný klíč. Potřebná data jsou zašifrována veřejným klíčem, který sám příjemce, nebo certifikační autorita poskytne. Po úspěšném zašifrování je možné tyto data získat jen pouze privátního klíče, který má jen cílový server. Nemůže proto dojít k žádnému úspěšnému odposlechu na cestě mezi odesílatelem a příjemcem.

Kapitola 6

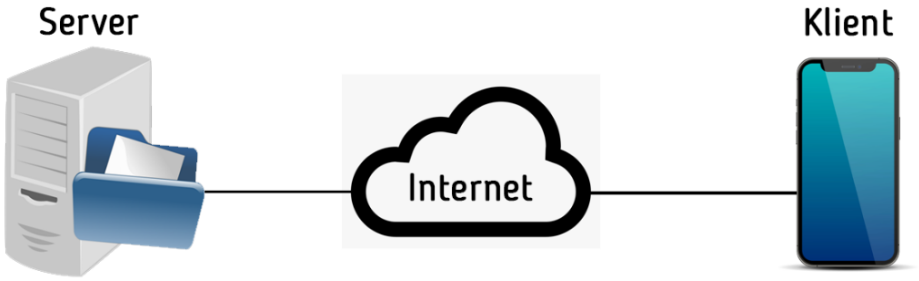
Implementace

V této kapitole bude popsána implementace dvou aplikací, které spolu budou navzájem komunikovat. Jedná se o simulaci scénáře, kde se spyware dostal do zařízení oběti a již komunikuje se serverem útočníka. Funkce spywaru je zcela automatická, a útočník se v tomto scénáři stará jen o využití získaných dat. Pro jednoduchost byl tento spyware navrhnut pouze pro jedno cílové zařízení.

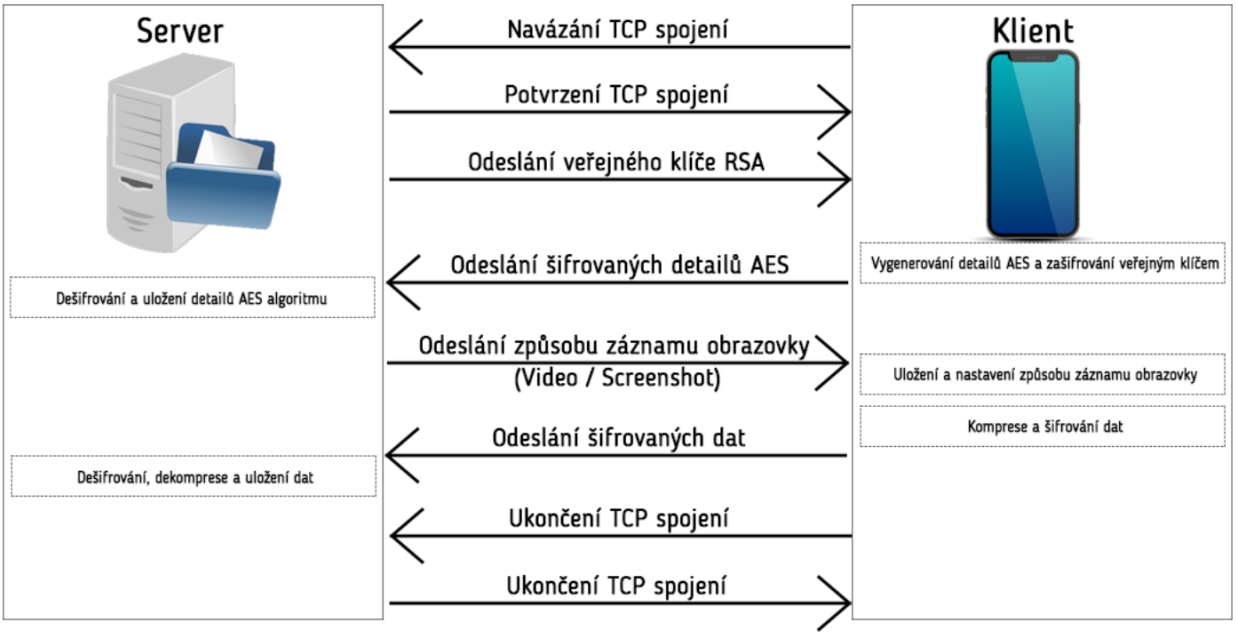
6.1 Síťová komunikace

Nejdůležitější část implementace je samozřejmě síťová komunikace, protože je potřeba získaná data dostat k útočníkovi, aby mohlo dojít k jejich dalšímu zneužití. Jako architekturu jsem zvolil jednoduchý klient-server, základní schéma komunikace je na obrázku 6.1. Před odesláním citlivých dat od klienta je na ně aplikována komprese a šifrování. Na straně serveru je proto před čtením informací nutné provést dešifrování a hned poté následovat dekompresí.

Spojení navazuje klient, zatímco server naslouchá na portu 13000. Před každým odesíláním dat se zkontroluje, jestli je server dostupný. Pokud není, tak se získaná videa a obsah keylogger souboru



Obrázek 6.1: Základní schéma síťové architektury klient-server, která je v implementaci použita



Obrázek 6.2: Časové schéma implementovaného přenosu mezi serverem a klientem (posloupnost shora)

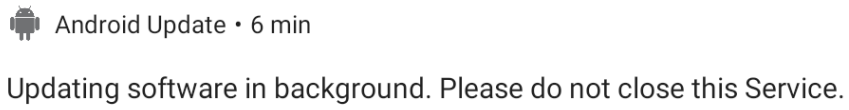
pošlou později. Výjimka je lokace, která se nikde neukládá pro pozdější odeslání, a při zpřístupnění serveru se odešle aktuální poloha.

6.1.1 Šifrování

Hned po navázání spojení je jako první nutné získat veřejný klíč serveru pro asymetrické šifrování. Tento klíč je pro každé spojení náhodně generovaný a klientovi ho odesílá server. Veřejný klíč serveru je použitý pro zašifrování detailů symetrického šifrování AES pomocí algoritmu RSA na straně klienta. Jinak řečeno, samotné data jsou šifrovány symetrickým algoritmem AES, a jeho detaily pro odšifrování jsou zašifrovány veřejným klíčem serveru. Tím pádem server nejdřív použije svůj soukromý klíč pro dešifrování AES klíče a inicializačního vektoru, pomocí kterých následně dojde k dešifrování získaných dat. Přehledné schéma přenosu je na obrázku 6.2.

6.1.2 Komprese

Komprese je aplikována na bytové pole, a to ještě před začátkem šifrování. V opačném pořadí by došlo k nenávratné ztrátě dat. Pro tento proces byla použita třída DeflateStream, která poskytuje metody pro kompresi bytového toku typu MemoryStream. Implementované funkce CompressByteArray a DecompressByteArray jsou v příloze B.1.



Obrázek 6.3: Notifikace implementované služby na popředí

6.2 Klient

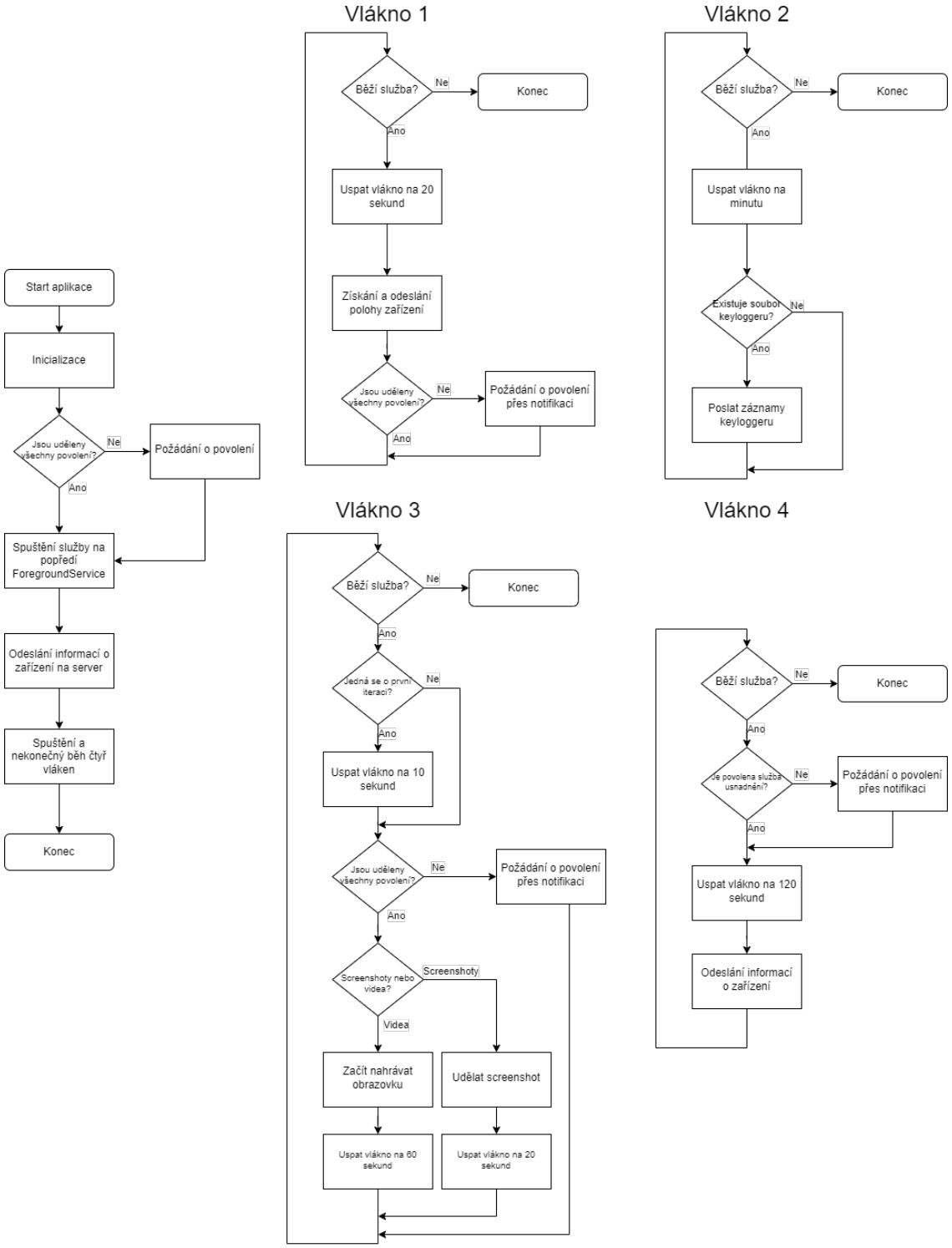
Klientská část byla implementována prostřednictvím již zmíněného frameworku Xamarin, a to konkrétně jako služba na popředí, anglicky Foreground Service. Implementovaný spyware se snaží zneužít neznalosti oběti tak, že se tváří jako oficiální aplikace od Androidu. Její název „Android Update“ napovídá, že slouží pro aktualizaci softwaru zařízení. Žádnou takovou funkci ale nemá, jde jen o zástěrku a známou techniku útočníků.

Jedna z nejdůležitějších částí Android aplikací je třída Activity. Každá aplikace, bez ohledu na její složitost, musí mít aspoň jednu takovou třídu. Při vývoji mobilních aplikací není vstupním bodem metoda *main()*, jak je zvykem u většiny programovacích jazyků, ale hlavní aktivita. Většinou je tato třída nazvána jako „MainActivity“, a inicializují se zde potřebné instance, nebo se volají specifické metody, které jsou potřebné pro sestavení Xamarin aplikace. U vyvíjeného spywaru tomu není jinak, kde se tato třída stará o inicializaci, získání potřebných povolení, a spuštění služby na popředí. Příklad funkce, která se provede při vytvoření hlavní aktivity, je v příloze B.2. Vývojový diagram klientské aplikace je na obrázku 6.4.

6.2.1 Finální služba

Služba, která je definovaná ve třídě ForegroundService.cs, se spustí po vytvoření hlavní aktivity spywaru. Tento specifický typ služby vyžaduje vlastní notifikaci, která informuje uživatele o jejím běhu, jak již bylo zmíněno v kapitole 5.2. Výsledná notifikace hlavní implementované služby, která je vidět po celý běh spywaru, je na obrázku 6.3. Samotný kód spuštění služby na popředí se změnil příchodem Android 8.0 Oreo, kde se již rozlišuje klasická služba a její alternativa v popředí. Ukázka kódu spuštění takové služby, který je funkční na všech verzích Androidu je v příloze B.3.

Po restartu zařízení, které mělo spuštěnou službu ForegroundService, dojde k jejímu opětovnému zapnutí. O tuto funkci se stará třída BootReciever.cs, která dědí z třídy BroadcastReciever. BootReciever obsahuje IntentFilter, který zachytává akci „Intent.ActionBootCompleted“, a při jejím zachycení opět spustí službu spyware. Kód této třídy zajišťující neustálý běh spywaru je v příloze B.4.



Obrázek 6.4: Základní vývojový diagram aplikace

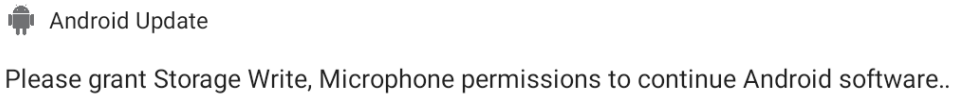
6.2.1.1 Potřebné povolení

Služba ForegroundService, která se stará o veškerou aktivitu spywaru, je v hlavičce třídy definovaná jako typ *ForegroundService.TypeMediaProjection*. Tato definice přišla s verzí Android 8.0 Oreo, a bez této definice není možné přistupovat k softwaru nahrávání médií. Pro naplnění potenciálu vyvinutého spywaru je potřeba získat od uživatele pár povolení. Jaké, a proč jsou potřeba, je uvedeno níže:

- Poloha zařízení - sledování polohy oběti v intervalu dvaceti vteřin
- Přístup k úložišti - pro uložení videa obrazovky a souboru keyloggeru před odesláním
- Mikrofon - pro nahrávání zvuku

O tyto povolení aplikace požádá hned v momentu startu spywaru, a snaží se získat plnou důvěru uživatele nainstalovaného softwaru. Při ideálním scénáři by mohl mít útočník fyzický přístup k zařízení, a tyto povolení, a další potřebné věci by nastavil sám. U jiného scénáře by bylo nutné zapracovat na oklamání uživatele, a to třeba vytvoření falešných stránek s aplikacemi pro zrychlení telefonu. Samozřejmě je třeba zmínit i povolení, ke kterým není potřeba souhlas uživatele. Stačí je pouze přidat do souboru „AndroidManifest.xml“, který popisuje základní informace o aplikaci pro nástroje sestavení Androidu. A to například navázání služby usnadnění přístupu nebo služby na popředí, přístup k internetu, a další.

V případě zamítnutí se spyware tyto povolení snaží získat později, a to pomocí notifikací. Při kliknutí na notifikaci se objeví nastavení aplikace, kde musí uživatel dodat chybějící povolení. Při zavření takové notifikace uživatelem se objeví znovu, a to přibližně za dvacet sekund, takový interval je pro zjištění lokace zařízení a kontrolu povolení. Ukázka takové notifikace, která chce oběť navést ke spolupráci, je na obrázku 6.5.

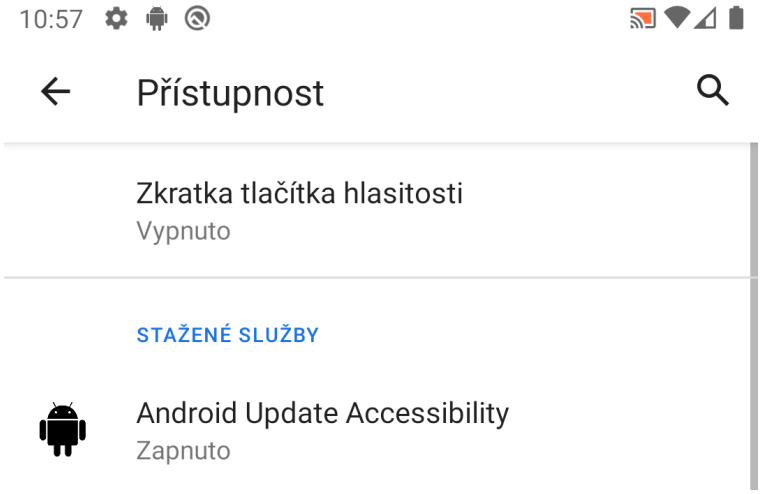


Obrázek 6.5: Notifikace, která žádá oběť o povolení přístupu k úložišti a mikrofonu

6.2.2 Keylogger

Keylogger je software, který snímá stisky kláves. Slouží hlavně pro získání hesel, nebo citlivých informací oběti. V této praktické části byl implementován přes službu usnadnění přístupu, která může snímat stisknuté klávesy, změny oken, a další události v operačním systému. U novějších iteracích Androidu, které již obsahují bezpečnostní záplaty, není jiný způsob jak snímat stisky kláves. Pro spuštění této funkce je nutné povolení uživatele v nastavení, tím pádem se spyware hned

Obrázek 6.6: Notifikace, která vyvolá otevření služby usnadnění přístupu



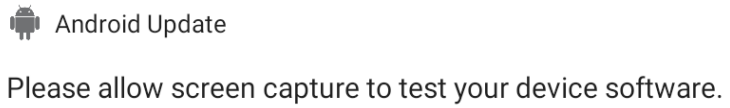
Obrázek 6.7: Nastavení služeb usnadnění přístupu

po startu snaží oklamat oběť notifikací. Pokud dojde k zavření notifikace uživatelem a služba stále není povolena, tak se zapnutí služby zkontroluje opět za dvě minuty, a případně se tato notifikace objeví znovu. Takto spyware naléhá na uživatele, že bez jeho svolení nemůže pokračovat ve falešné aktualizaci softwaru. Notifikace, která nabádá uživatele pro povolení služby usnadnění přístupu, je na obrázku 6.6.

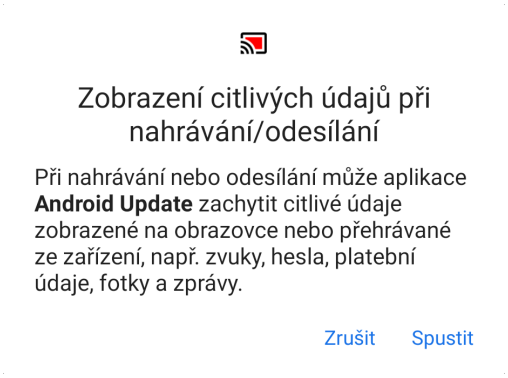
Kliknutím na notifikaci se otevře nastavení, kde je přehled všech dostupných služeb usnadnění přístupu, jak je vidět na obrázku 6.7. Zde musí oběť povolit službu „Android Update Accessibility“, která je vlastně přestrojený keylogger. Po povolení lze nenápadně sbírat informace, jako jsou uživatelská jména a hesla, nebo otevření určitých aplikací, webových stránek a oken.

6.2.3 Záznam obrazovky a zvuku

Nahrávání obrazovky a zvuku je implementováno pomocí třídy MediaRecorder, která je součástí knihovny *android.media*. Snímky obrazovky se pořizují co 20 sekund, a videa se nahrávají v intervalu jedné minuty. U obou případů spyware získává obraz díky služby MediaProjectionManager, a u videa zvuk z mikrofonu zařízení. Interval videí byl zvolen kvůli rychlejšímu přenosu dat, a aby videa nezabíraly tolik místa v úložišti. Toho je docíleno taky tím, že po pořízení média se hned pošle na vzdálený server, a následně se v zařízení smaže.



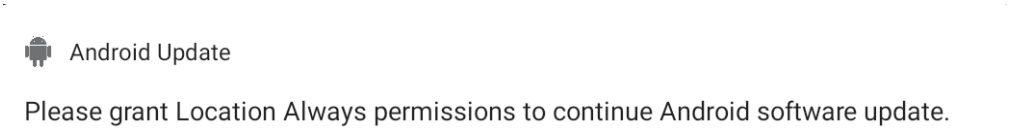
Obrázek 6.8: Notifikace, která po kliknutí vyvolá aktivitu ScreenCapture



Obrázek 6.9: Žádání o nutné povolení pro nahrávání obrazovky

Aby došlo k úspěšnému spuštění obou typů záznamu obrazovky, tak je nejdřív potřeba zkontrolovat oprávnění aplikace. U videa je pro MediaRecorder nutné zajistit povolení přístupu k úložišti a mikrofonu, jinak se instanci této třídy nepodaří inicializovat. Od verze Android 11 a vyšší tento systém zapracoval na zabezpečení svých uživatelů, a pro přístup k mikrofonu z pozadí je povinné nejdřív získat povolení usnadnění přístupu. Jinak řečeno, spyware se musí pokusit nejprve získat povolení pro funkce keyloggeru, jak je popsáno v kapitole 6.2.2, a poté až pro záznam obrazovky.

Pokud služba výše zmíněné povolení získá, tak požádá prostřednictvím notifikace o spuštění nové aktivity ScreenCapture, jak je vidět na obrázku 6.8. Tato aktivita se stará o vyvolání integrované služby Androidu, která umožňuje zachycení obrazovky. Tato služba se jmenuje MediaProjectionManager, a pro její funkce je opět potřeba potvrzení uživatele, jak je vidět na obrázku 6.9. Bez použití této služby už není v moderních verzích systému Android jiné řešení, jak zachytávat obrazovku zařízení. V tento moment útočník musí doufat v důvěru oběti, která si v ideálním scénáři může myslet, že jde o kontrolu softwaru. Při úspěchu dojde nejdříve ke zjištění a uložení rozlišení obrazovky, získání instance třídy MediaProjection, a u videí dojde navíc k nastavení konfigurace nahrávání. Ukázka použitých parametrů videa pomocí třídy MediaRecorder je v příloze B.5. Poté díky zmíněným parametrům dojde k inicializaci virtuálního displeje. Pak už spywaru nebrání nic v začátku získávání osobních informací oběti.



Obrázek 6.10: Notifikace pro Android 11 a vyšší, která žádá o nepřetržitý přístup k lokaci

6.2.4 Testování u různých verzí Androidu

Spyware byl testován na verzi Android 8, 9, 10, 11 a 12. Přičemž u novějších verzí bylo potřeba aplikovat změny v zabezpečení a získávaní povolení.

U vývoje aplikace pro novější verze Androidu je třeba počítat s malými změnami v zabezpečení. Například u Androidu 12 je jiné definování PendingIntent, které se vkládá do notifikace. Intent je zpráva nebo instrukce, která lze přenášet mezi komponenty Androidu. Jeho nejvýznamnější využití je při spouštění aktivit, nebo služeb. Je to v podstatě datová struktura, která obsahuje abstraktní popis akce, která má být provedena. Rozdíl mezi Intent a PendingIntent je ten, že pokud dostane jiný komponent Intent od naší aplikace, tak instrukce v něm provede pomocí vlastních oprávnění. Naopak u PendingIntent komponent může využít získané povolení od aplikace, který tento vyvolal. Další výhoda použití tohoto typu je, že můžeme iniciovat různé akce komponentů pomocí notifikací, což bylo použito při praktické části této práce.

Od verze Android 11 přišlo několik bezpečnostních záplat, které zabraňují přístup k poloze zařízení, nebo mikrofonu z pozadí. Kvůli přístupu k lokaci bylo nutné implementovat notifikaci, která uživatele žádá o povolení přístupu k poloze z pozadí. Tato specifická notifikace pro Android 11 a vyšší je na obrázku 6.10. Postup pro získání přístupu k mikrofonu z pozadí je již popsán v kapitole 6.2.3.

```
//vytvoření intentu pro povolení accessibility kvůli keyloggeru
Intent i = new Android.Content.Intent(Android.Provider.Settings.
    ActionAccessibilitySettings);
PendingIntent resultPendingIntent = null;
if (Android.OS.Build.VERSION.SdkInt >= Android.OS.BuildVersionCodes.S) //Android
    12 potrebuje jinak definovat PendingIntent
{
   resultPendingIntent = PendingIntent.GetActivity(this, 0, i, Android.App.
       PendingIntentFlags.Mutable); //Mutable místo Oneshot
}
else
{
   resultPendingIntent = PendingIntent.GetActivity(Android.App.Application.Context
       , 0, i, PendingIntentFlags.OneShot);
```

```
}
```

Listing 6.1: Definování struktur Intent a PendingIntent, a jeho změna atributu u verze Android 12

6.3 Server

Strana serveru je implementována pomocí jazyka C# a frameworku .NET. Jedná se o projekt typu Windows Forms, což je knihovna tříd, která slouží pro tvorbu uživatelského rozhraní. Umožňuje vytvořit formulářovou aplikaci pomocí grafického designéru, který obsahuje velké množství ovládacích prvků, nebo komponentů. Skládá se z dvou oken, a to z konzole a formuláře. Konzolová část slouží hlavně jen pro výpis, a přehlednost příchozích TCP spojení. Zatímco formulář hlavně pro vizualizaci získaných dat oběti. Obecně na serveru běží jen jedno vlákno, jehož úkolem je naslouchat příchozím spojením, a předání dat do formuláře, který je vizualizuje. Start tohoto vlákna a jeho nekonečná smyčka je k vidění ve výpisu kódu B.6. Vývojový diagram aplikace serveru je na obrázku 6.11.

Server slouží pro shromažďování dat oběti, a jako přístupový bod útočníka. Použitý protokol pro komunikaci je TCP, přičemž server stále naslouchá na portu 13000. IP adresa serveru se automaticky nastaví podle IP adresy počítače, na kterém běží. Pro komunikaci mimo lokální síť by byla potřeba zajistit počítač s veřejnou IP adresou.

6.3.1 Formulář

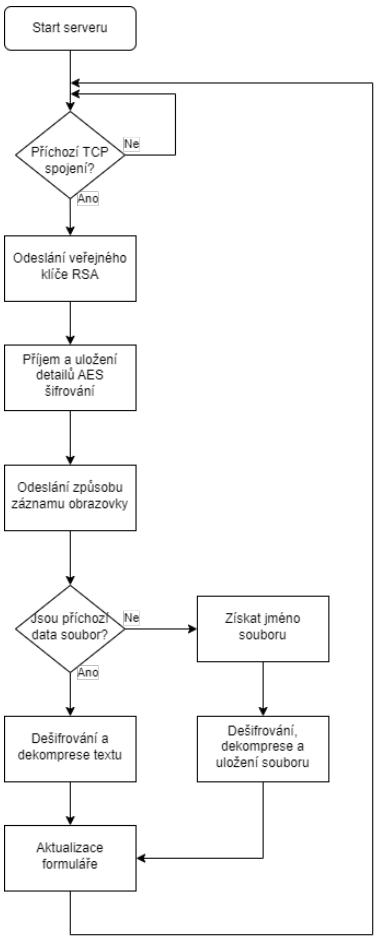
Formulář na straně serveru pro útočníka slouží jako prohlížeč získaných dat. Obsahuje záložky s názvy Location, Device Info, Keylogger a Screen Capture, Screenshots a Settings.

První ze zmíněných slouží pro zakreslení přesné pozice zařízení v mapě. Mapa je do formuláře vykreslena pomocí NuGet balíčku GMap.NET.WinForms, který podporuje mnoho typů map, jako například Google Maps, Bing, OpenStreetMap, Mapy.cz a mnoho dalších. Po instalaci balíčku se u návrhu formuláře v sadě nástrojů objeví prvek GMap.NET.WindowsForms.GMapControl, který byl v aplikaci použit. Vzhled záložky s polohou zařízení je na obrázku 6.12.

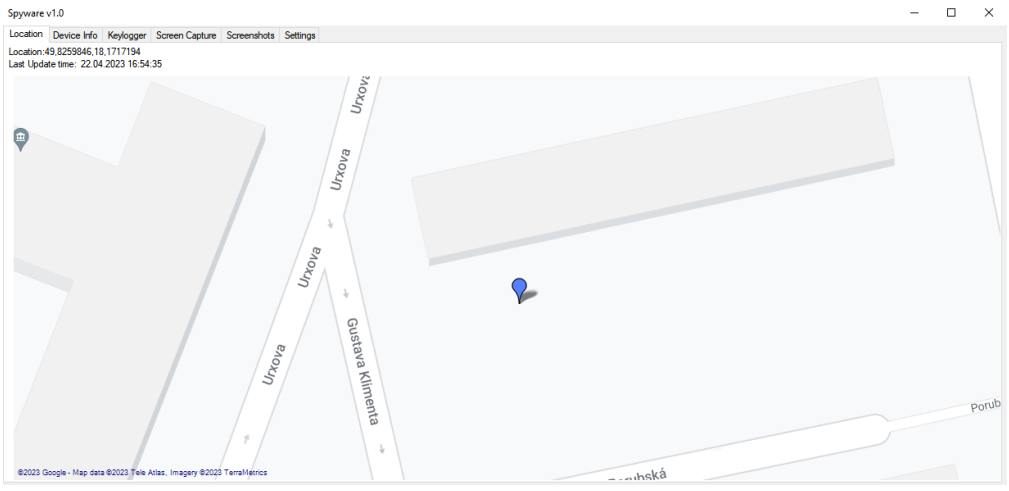
Uvnitř záložky Device Info se útočníkovi zobrazí obecné informace o nakaženém zařízení. Jako například verze operačního systému, model telefonu, mobilního operátora oběti a dále. Výpis těchto dat, získaných z Android emulátoru, je na obrázku 6.13. Pro zápis do formuláře byl použit jednoduchý komponent Label.

Jako třetí v pořadí je Keylogger, kde si útočník může prohlédnout všechny získané logy z konkrétního dne. Na obrázku 6.14 je konkrétní případ, kdy oběť vyplňuje přihlašovací údaje. I když je na webové stránce heslo skryto, Android ukazuje uživateli poslední napsaný znak. Toho lze zneužít, a pouhým okem si lze heslo přečíst.

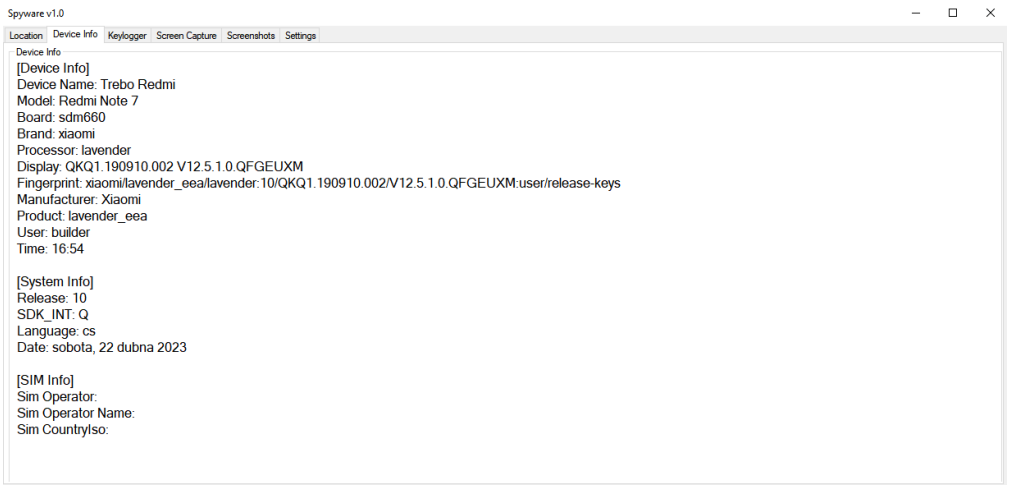
Záložky Screen Capture a Screenshots obsahují list, který zobrazuje všechny získané záznamy obrazovky. Snímky i videa jsou pojmenovány podle data a času, kdy byly pořízeny. Při výběru



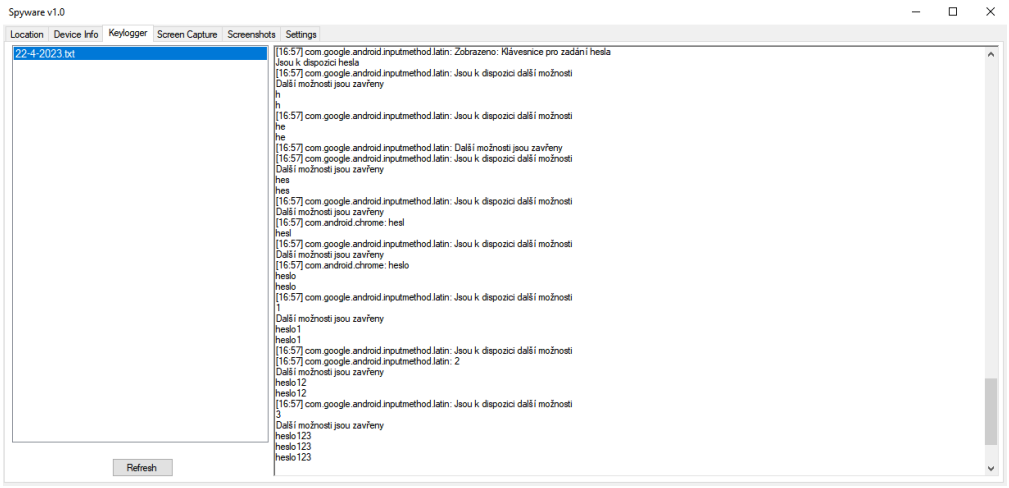
Obrázek 6.11: Vývojový diagram serveru



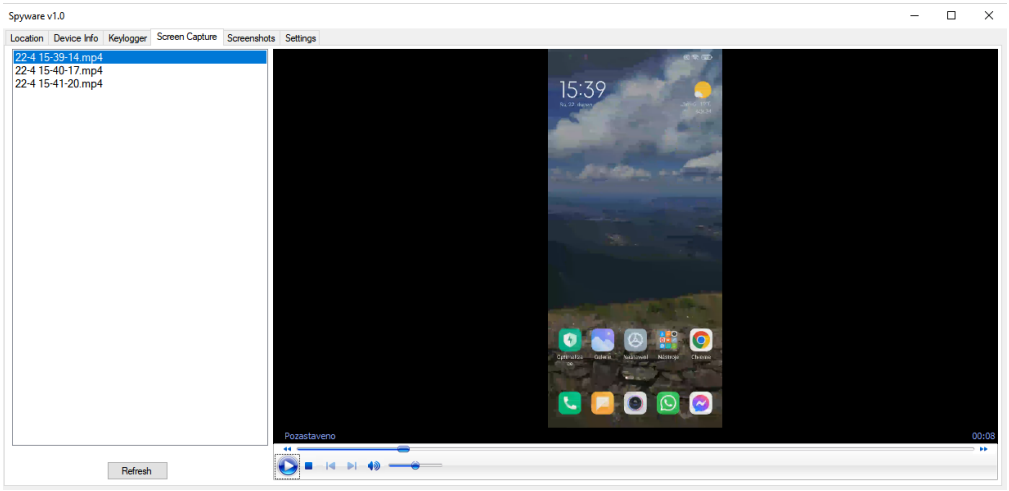
Obrázek 6.12: Záložka Location ve formuláři s polohou oběti



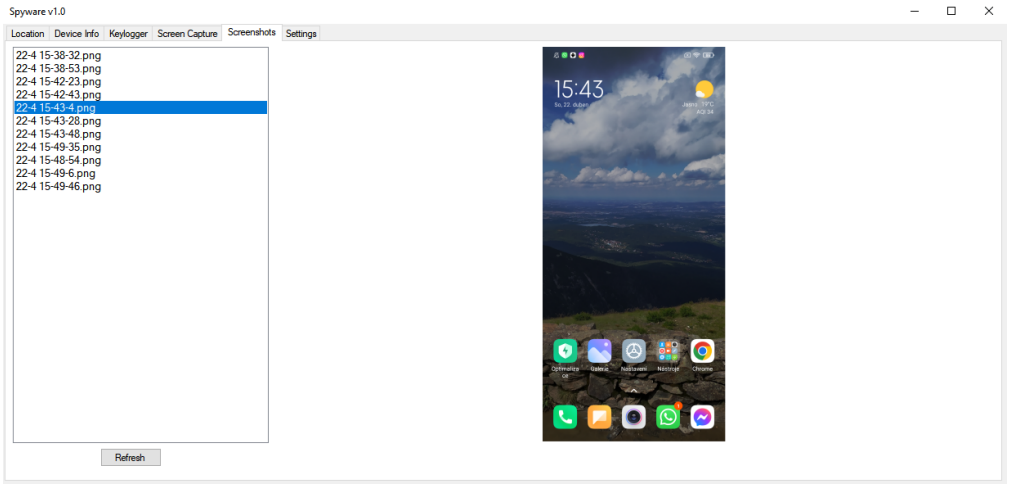
Obrázek 6.13: Záložka Device Info na straně serveru, s informacemi z emulátoru s verzí Android 11



Obrázek 6.14: Záložka Keylogger a zobrazení výpisu ze dne 22. 4. 2023, kde oběť vyplňuje přihlašovací údaje



Obrázek 6.15: Záložka Screen Capture a přehrávání získaného videa



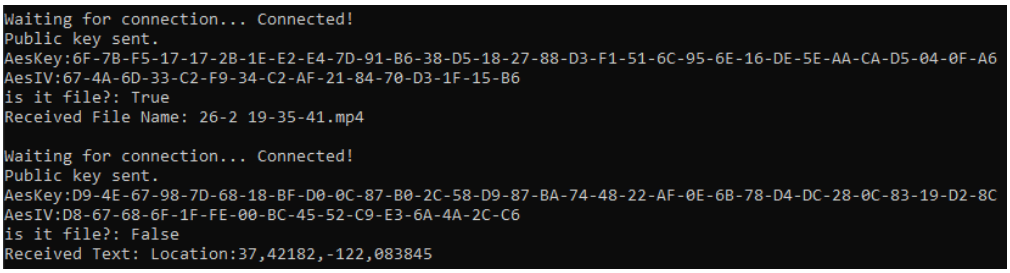
Obrázek 6.16: Záložka Screenshots a zobrazení snímku obrazovky

záznamu se fotka vykreslí v prohlížeči obrázků, který se nachází na pravé straně formuláře. U videa se začne ihned přehrávat v integrovaném přehrávači Windows Media Player. Tento přehrávač lze do sady nástrojů ve Visual Studiu přidat podle jednoduchého návodu, který je dostupný v oficiální dokumentaci.[1] Zobrazení snímku obrazovky je na obrázku 6.16. Konečný vzhled a přehrávání konkrétního videa v integrovaném přehrávači Windows Media Player, je na obrázku 6.15.

6.3.2 Konzole

Konzolové okno slouží pouze pro sledování příchozích spojení a monitorování, jestli aktivně probíhá komunikace mezi serverem a klientem. Pokud server naslouchá a čeká na spojení, tak je v okně

[1] https://learn.microsoft.com/en-us/windows/win32/wmp/using-the-windows-media-player-control-with-microsoft-visual-studio



Obrázek 6.17: Serverový výpis v konzoli u dvou příchozích spojení, první se záznamem obrazovky a druhé s polohou zařízení

přítomna hláška: „Waiting for connection...“. Při příchozím spojení se vypíšou některé důležité informace, jako úspěšné odeslání veřejného klíče, dešifrované detaily pro AES algoritmus, a jaké data útočník získal. Na praktické ukázce v obrázku 6.17 nejdříve server přijal video se záznamem obrazovky, a následně polohu zařízení oběti.

Kapitola 7

Testování proti odhalení

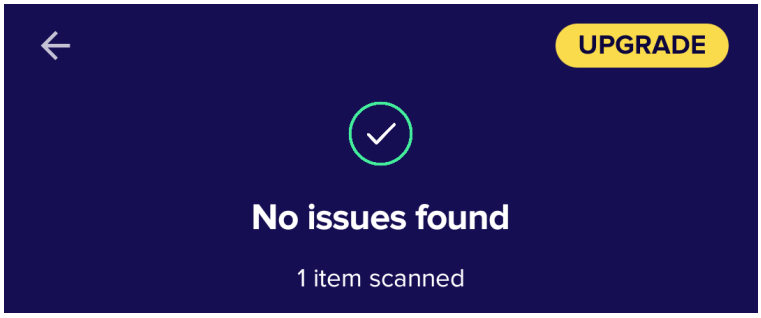
Výběr antivirové aplikace pro Android je důležitá, protože většina je k ničemu. Toto tvrdí rozsáhlá studie od společnosti AV Comparatives, která v roce 2019 otestovala 250 typů tohoto softwaru[31]. Pouze 23 produktů detekovalo všechny vzorky malwaru, což nebyla ani desetina celkově testovaných. Alarmující informace je, že 170 antivirů dostupných na oficiálním obchodě Google Play, nezvládlo odhalit ani třicet procent škodlivých aplikací. Tato informace by měla hlavně motivovat uživatele alternativních ochran, kteří by měli přejít na spolehlivější produkt. Mezi úspěšnými se samozřejmě objevily produkty od společností Avast, AVG, ESET, Kaspersky, McAfee a další. Z toho vyplývá, že se obecně vyplatí vsadit na známější dodavatele antivirového softwaru, kteří svou ochranu pravidelně aktualizují.

U nejnovějšího testu této společnosti, který proběhl v květnu roku 2022, se vybraly pouze nejpopulárnější produkty. Mezi testované patřily například Avast Mobile Security 6.48, AVG AntiVirus Free 6.48, ESET Mobile Security Premium 7.3, Google Play Protect & OS Features 30.4, nebo Kaspersky Standard for Android 11.84. V tabulce 7.1 jsou výsledky tohoto průzkumu. Celkově bylo prokázáno, že většina opravdu své aplikace aktualizuje proti všem novým hrozbám. Jediným případem co u testování selhal, je Google Play Protect. Tato antivirová aplikace přímo od Googlu nezvládla správně identifikovat malware až u 13,1 % případů, z toho důvodu se tento antivir nedoporučuje. Všechny výsledky testů dostaly i testované subjekty, takže má Google do příštího testu co dělat.[32]

Během následujících testů byly použity bezplatné verze mobilních antivirů, které jsou volně dostupné v obchodě s aplikacemi. Výjimkou je Google Play Protect, který je integrován ve službách Google, a je aktivován ve výchozím nastavení všech verzí Androidu.

Tabulka 7.1: Tabulka ochrany nejznámějších antivirových aplikací pro Android[32]

Název	Procento ochrany	Počet falešných poplachů
Bitdefender, G Data, Kaspersky, Trend Micro	100 %	0
AVG	100 %	3
Avast	100 %	4
Avira, ESET, Securion	99,9 %	0
Malwarebytes	99,3 %	7
Google Play Protect	87,9 %	11



Obrázek 7.1: Test instalačního APK spywaru programem Avast Mobile Security 6.56.1

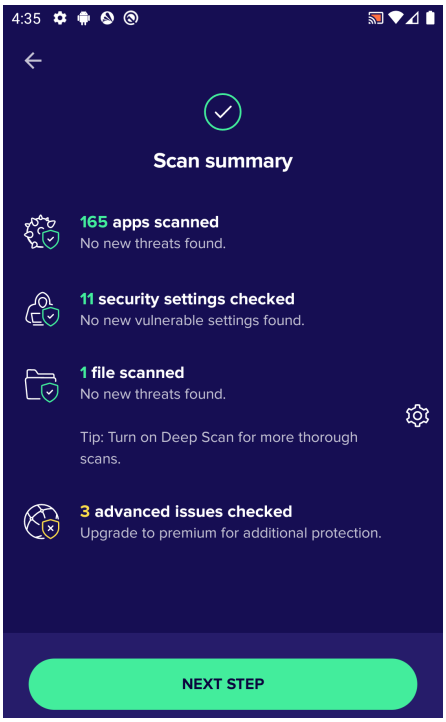
7.1 Avast

Velmi známý antimalware program, který vyvíjí Avast Software s.r.o. sídlící v Praze. V současnosti využívá nějakou verzi tohoto antiviru přes 435 milionů uživatelů[1]. Pro testování byl použit Avast Mobile Security 6.56.1, a to konkrétně neplacená varianta této ochrany. Skenování instalačního souboru APK programem Avast nenašlo žádné hrozby, jak je vidět na obrázku 7.1. Poté přišel čas na zkoušku instalace spywaru, při spuštěné ochraně Avast. Během tohoto kroku nebylo žádné upozornění o škodlivosti aplikace, ani během jejího spuštění. I po získání a odeslání citlivých informací nebyla žádná reakce od tohoto antiviru. Při běžícím spywaru byl poté spuštěn běžný test zabezpečení, který opět nenašel žádnou hrozbu. Výsledek testu při běžícím spywaru je na obrázku 7.2.

7.2 Bitdefender

Bitdefender je rumunská společnost, která se zabývá kyberbezpečností[2]. Byla použita aktuální verze mobilní ochrany této firmy, a to Bitdefender Mobile Security 3.3.201.2198. Tento antivir neumožňuje skenování jednoho souboru, a proto bylo nutné provést sken celého zařízení. Před instalací, kdy byl

[1] https://www.avast.com/cs-cz/
[2] https://www.bitdefender.com/



Obrázek 7.2: Výsledek běžného testu Avast při aktivitě spywaru, jehož ikona jde vidět na horní liště zařízení

pouze APK soubor ve složce stažených souborů, se opět nenašla žádná hrozba. Po spuštění spywaru byl opět proveden test, který byl znovu negativní. Oba výsledky testů jsou na obrázku 7.3.

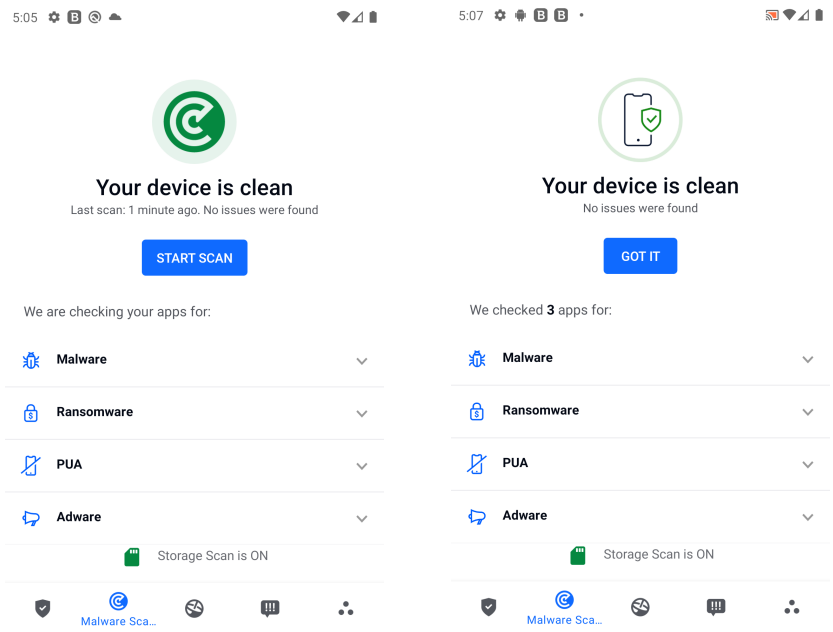
7.3 Malwarebytes

Malwarebytes Inc. je společnost sídlící v Americe, která se také zabývá ochranou před malware hrozbami[3]. U Malwarebytes trval první celkový test zařízení o hodně déle, než tomu bylo u ostatních aplikací. Zatímco u předchozích to byla otázka několika vteřin, tak u tohoto naopak pár minut. Další test už byl hotov za 16 vteřin, a proto se asi u prvního případu jednalo o podrobnější vstupní prohlídku zařízení. Výsledky testů jsou na obrázku 7.4.

7.4 ESET

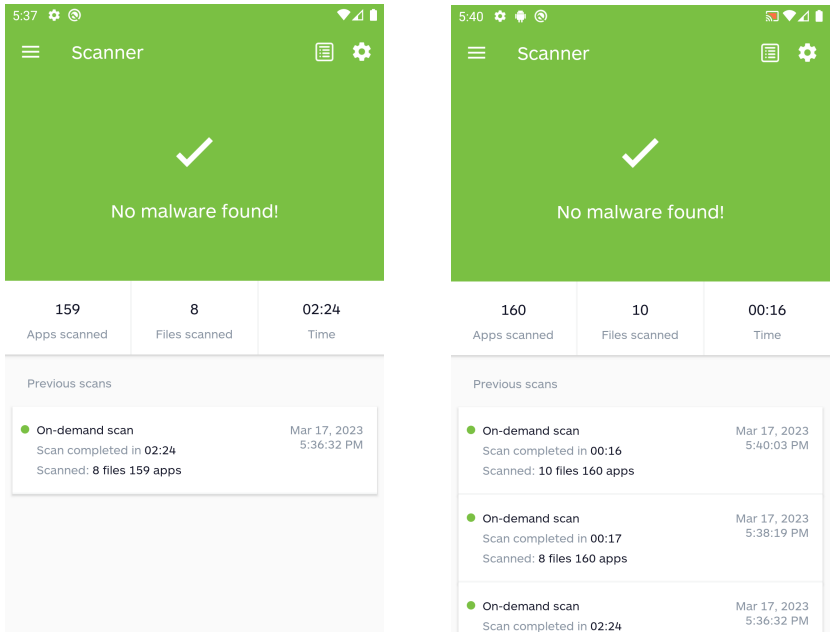
ESET spol. s.r.o. se specializuje na kybernetickou bezpečnost, a poskytuje svoje produkty po celém světě[4]. ESET Mobile Security jako jediný správně označil implementovanou škodlivou aplikaci jako spyware, a to hned po přesunu souboru APK do zařízení. Nebylo nutné ani aplikaci instalovat,

[3]https://www.malwarebytes.com/
[4]https://www.eset.com/



(a) Před instalací (b) Po spuštění

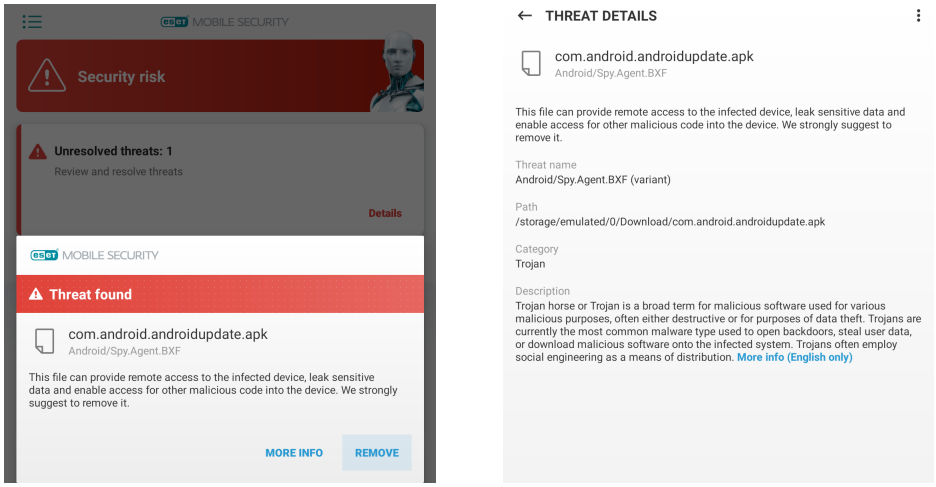
Obrázek 7.3: Výsledek testování antivirem Bitdefender před instalací, a po spuštění spywaru



(a) Před instalací (b) Po spuštění

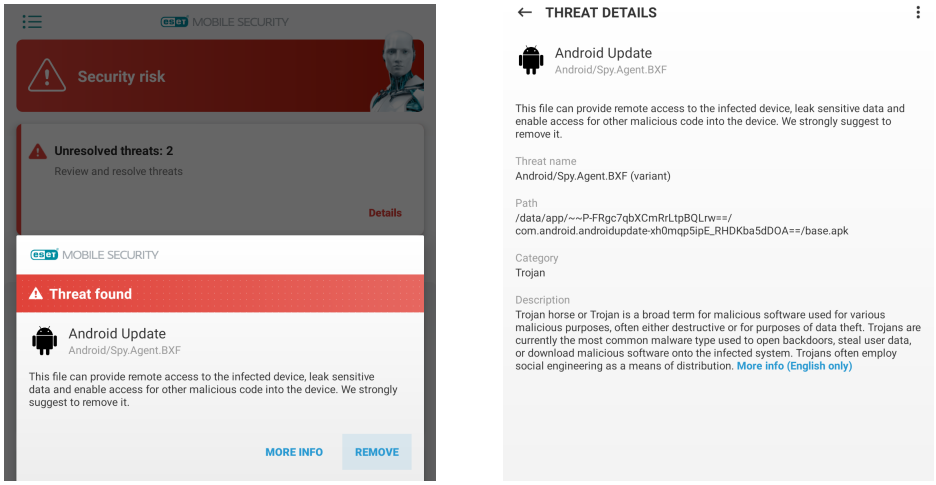
Obrázek 7.4: Výsledek testování antivirem Malwarebytes před instalací, a po spuštění spywaru

a ESET již z instalačního balíčku varoval o jeho hrozbě, jak je vidět na obrázku 7.5. Navíc ji označil jako variantu Spy.Agent.BXF, a správně zařadil do kategorie trojských koní. I po instalaci škodlivé aplikace antivir nepřestal varovat uživatele, a poukazuje přímo na instalovanou aplikaci, jak je vidět na obrázku 7.6.



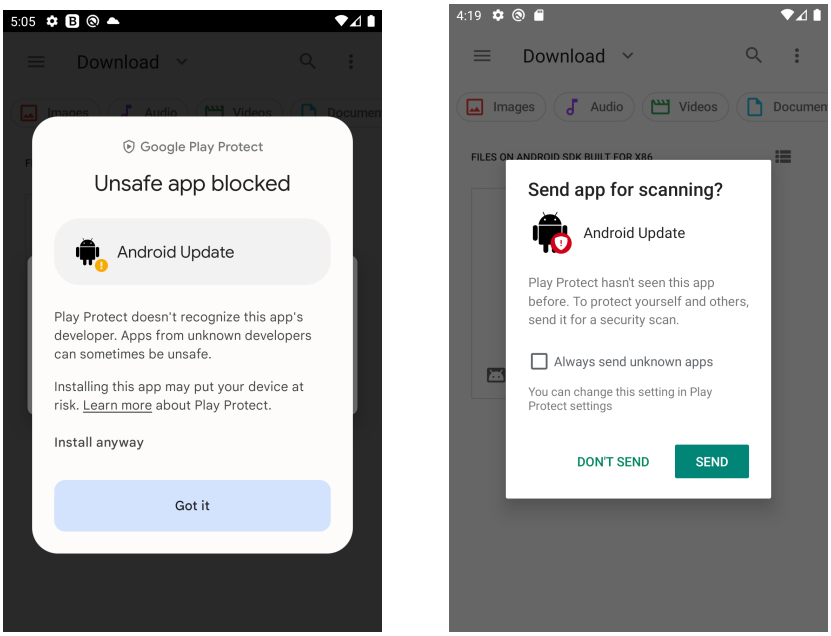
(a) Oznámení o hrozbě (b) Detail hrozby

Obrázek 7.5: Oznámení antiviru ESET o hrozbě před instalací APK balíčku



(a) Oznámení o hrozbě (b) Detail hrozby

Obrázek 7.6: Oznámení antiviru ESET o hrozbě nainstalované aplikace Android Update



(a) Zablokování instalace (b) Nabídka poslání k přezkoumání

Obrázek 7.7: Varování integrovaného antiviru Google Play Protect při instalaci softwaru třetích stran

7.5 Google Play Protect

Google Play Protect je již od roku 2017 integrován do služeb Google Play, a je v základním nastavení povolena. Tato služba neustále skenuje a kontroluje nejen aplikace, které jsou publikovány v obchodě Google, ale i lokální instalace. Tento antivir pouze varuje uživatele před instalací neznámého softwaru třetí strany. Toto varování se ale ukazuje u všech případů instalace aplikací třetích stran, takže jej uživatel v ideálním scénáři může po předchozí zkušenosti ignorovat. Po instalaci nabídne poslání aplikace pro přezkoumání, což je pro útočníka špatná zpráva. Vyskakovací hlášky od Google Play Protect jsou na obrázku 7.7.

7.6 Závěr testování

Po těchto testech se dá konstatovat, že implementovaný spyware se pro většinu komerčních antivirů tváří jako bezpečný. Jediný ESET Mobile Security správně označil aplikaci za spyware. Ale například Google Play Protect varuje před instalací neznámé aplikace, a nabídne ji poslat pro přezkoumání. Z tohoto testování tedy vyplývá, že pokud uživatel nemá spolehlivý antivirus, tak stačí využít sociálního inženýrství pro získání jeho důvěry. Uživatel si potom do zařízení vědomě nainstaluje zdánlivou aplikaci pro aktualizaci softwaru. Po tomto kroku může útočník nepozorovaně získat hodně citlivých informací.

Kapitola 8

Ukázkové příklady užití

V této kapitole budou demonstrovány plně opakovatelné příklady užití implementovaného spywaru. A to postup instalace, nastavení IP adresy, nebo vypnutí spywaru na straně klienta.

8.1 Instalace

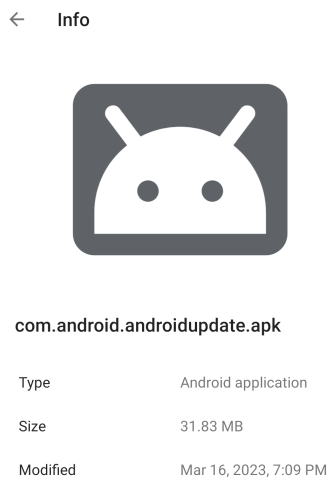
8.1.1 Klient

Aplikace klienta má nastavenou cílovou verzi Android 12 (API 31-S), a minimální verzi Android 8 (API 26-Oreo). Jakákoliv verze v tomto rozsahu podporuje implementovaný spyware. Mimo tento rozsah nebylo provedeno testování správné funkčnosti. Pro instalaci klientské aplikace je nejdříve nutné do cílového zařízení dostat APK, jehož podoba je na obrázku 8.1. Tento instalační soubor se společně s Androidem postará o všechnu práci. Teda pouze v případě, pokud dostane zařízení povolení instalace aplikace třetí strany, která již byla ukázána na obrázku 7.7.

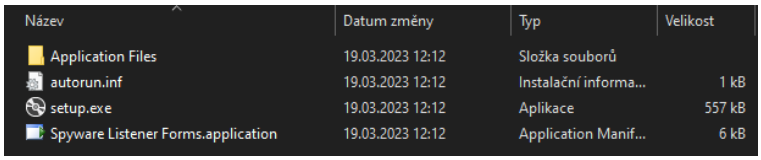
Spuštění aplikace lze provést i ve vývojovém prostředí Visual Studio, které má správně nastavené všechny potřebné nástroje. Mezi ně patří například integrovaný Android Emulator, uvedení cesty k SDK a JDK v možnostech tohoto vývojového prostředí, a dále.

8.1.2 Server

U serveru stačí buď projekt Windows Forms spustit ve vývojovém prostředí Visual Studio, nebo využít již připravené spustitelné verze, která je přiložena k práci. U prvního případu je potřeba spustit projektový soubor Spyware Listener Forms.sln ve složce Spyware Listener Forms. U druhého stačí spustit setup.exe ve složce Spyware Listener Forms Publish, což je publikovatelná instalační verze, kterou z projektu vygenerovalo Visual Studio. V tomto případě se aplikace nainstaluje do AppData, konkrétně cesta „C:/Users/Username/AppData/Local/Apps/2.0/...“. Do této složky se také ukládají všechny získané data. Obsah instalačního adresáře serverové aplikace je na obrázku 8.2.



Obrázek 8.1: Instalační balíček APK spywaru Android Update



Obrázek 8.2: Instalační a spouštěcí adresář serverové aplikace

8.2 Nastavení IP adresy

Ve výchozím nastavení poslouchá server na portu 13000, a IP adresu si nastaví podle počítače, na kterém je spuštěn. Ukázka funkce pro získání IP adresy počítače je v ukázce 8.1. Většinou se bude jednat o adresu ze třídy C, které jsou pouze privátní. Domácí routery můžou jako adresu výchozí brány použít jakoukoliv soukromou IP, ale 192.168.0.1 je pro tento účel jedna z nejčastěji používaných adres. Proto byla výchozí IP adresa, která je nastavena v aplikaci klienta, zvolena 192.168.0.129. Při jiné adrese serveru je po spuštění proto třeba změnit hodnotu v souboru „IPconfig.txt“, který se nachází v cestě „/Internal Storage/Android/data/com.android.androidupdate/files“. Textové soubory lze na Androidu editovat pomocí jakéhokoliv textového editoru, nebo některé telefony tuto funkci umožňují nativně. Po změně této hodnoty hned aplikace zareaguje a naváže spojení.

Druhý způsob je změna ip adresy počítače, který hostuje server, ještě před spuštěním serverové aplikace. Ale tato možnost se naskytuje pouze pokud router poskytuje síť s adresou 192.168.0.0/24. Změna IP adresy lze provést v ovládacích panelech, konkrétně „Ovládací panely/Síť a internet/Síťová připojení“.

Port 13000 byl vybrán z toho důvodu, protože nepatří do pevně definované skupiny dobře známých portů, takže na něm nebude běžet žádná běžná služba. Z historického hlediska na tomto

portu operovalo již pár druhů malwaru[1], a proto to je ta správná volba.

```
public string GetLocalIPAddress()
{
    var host = Dns.GetHostEntry(Dns.GetHostName());
    foreach (var ip in host.AddressList)
    {
        if (ip.AddressFamily == AddressFamily.InterNetwork)
        {
            return ip.ToString();
        }
    }
    return "Can't get IP address";
}
```

Listing 8.1: Získání IP adresy počítače, který spouští aplikaci serveru

8.3 Spuštění a sledování uživatele

Výsledky základního sledování uživatele už byly ukázány v kapitole 6.3. Během následující kapitoly bude popsán postup pro úspěšné sledování oběti.

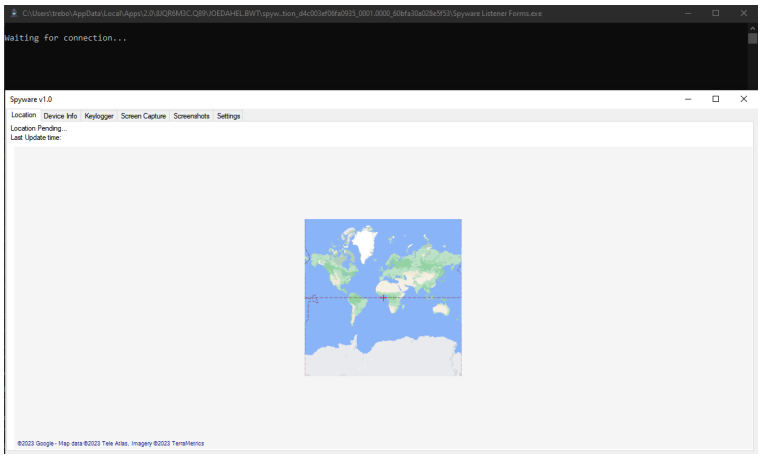
8.3.1 Server

Pro útočníka je důležité nejdřív nainstalovat a zapnout server, obě tyto se provedou automaticky při spuštění souboru setup.exe ve složce Spyware Listener Forms Publish. Tato akce lze samozřejmě provést i po nakažení zařízení oběti, protože se získané informace z keyloggeru a nahrávání obrazovky můžou poslat zpětně až po navázání spojení. Úspěšný start serverové aplikace, kdy už se čeká na první spojení s obětí, je na obrázku 8.3. Tímto je strana serveru nachystána na sledování oběti.

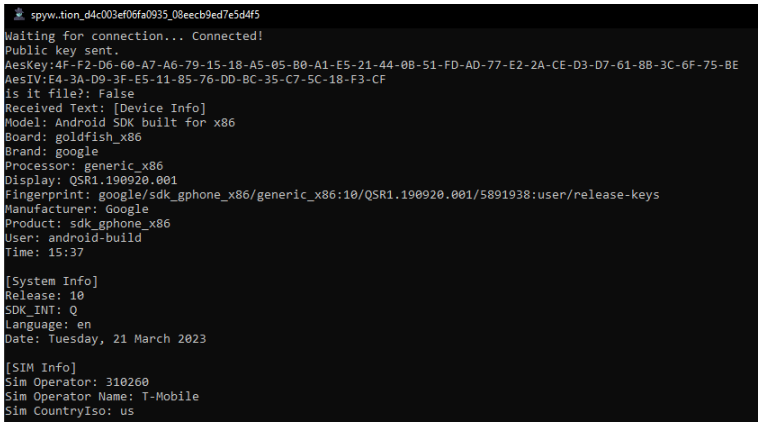
8.3.2 Klient

V mobilním zařízení oběti je po instalaci nutné spuštění škodlivé aplikace Android Update. Start spywaru nabídne sám systém, nebo je pro tento účel k dispozici zástupce na domovské obrazovce. Pokud adresa serveru je jiná než 192.168.0.129, tak je nutná změna, jak je zmíněno v kapitole 8.2. Pro správné fungování všech funkcí spywaru je nutné udělit povolení z kapitoly 6.2.1.1, na které se hned aplikace zeptá. V případě zamítnutí se sama o tyto povolení přihlásí, pomocí implementované notifikace. Aplikace totiž v intervalu 20 vteřin ověřuje povolení a zasílá polohu zařízení.

[1] https://www.adminsub.net/tcp-udp-port-finder/13000



Obrázek 8.3: Konzole a formulář serveru, který čeká na spojení se zařízením oběti

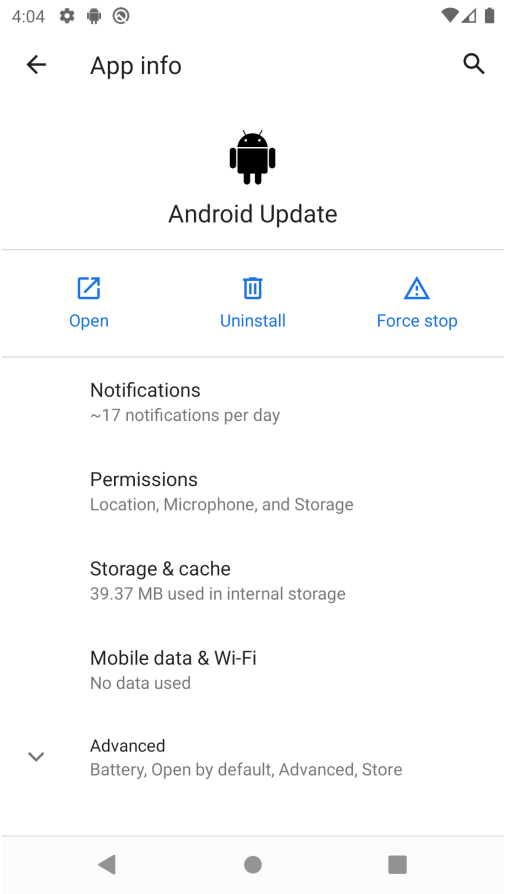


Obrázek 8.4: Příchozí spojení s informacemi o zařízení oběti v konzoli

Hned po startu aplikace se pošlou na server informace o nakaženém zařízení. V případě nedostupnosti serveru se tyto data získají později, jelikož jsou pravidelně posílány co 2 minuty. Příchozí spojení v konzoli, s informacemi o zařízení oběti, je na obrázku 8.4. Všechny získané data se poté automaticky vloží do formuláře serveru, kde je může prohlížet útočník. Jak již bylo zmíněno, tak poloha oběti lze sledovat v reálném čase, a aktualizuje se co 20 vteřin. Pro její funkčnost je potřeba pouze povolení o přístupu k lokaci. Naopak pro keylogger a záznam obrazovky jsou potřeba další akce uživatele, jako je povolení služby usnadnění nebo promítání. Všechny funkce a jejich zapnutí je popsáno v kapitole 6.2.

8.4 Vypnutí klienta spywaru

Implementovanou službu na popředí nikdy nevypne sám systém, a zapne se automaticky po každém restartu zařízení. Proto jsou jediné způsoby jejího vypnutí odinstalace, nebo vynucené zastavení.



Obrázek 8.5: Detail nainstalovaného spywaru Android Update

Obě tyto možnosti jsou k dispozici v nastavení, když si uživatel pod položkou „Nainstalované aplikace“ rozklikne detail spywaru Android Update. Podrobnosti nainstalované aplikace jsou v ukázce 8.5, kde se kromě možných akcí zobrazují poskytnuté povolení, nebo využití úložiště.

Kapitola 9

Závěr

Na začátku práce bylo seznámení se sociálním inženýrstvím, jehož techniky se běžně používají pro šíření škodlivého softwaru. Byly popsány všechny jeho druhy, jako například phishing, spear phishing, vishing, whaling a další. V následující sekci byla rozebrána problematika malwaru, a to například jak tento název vznikl, nebo jaký má obecně tento software cíl. Poté je zmíněno, do jakých kategorií se dělí podle funkčnosti, nebo způsobu šíření. Na konci podkapitoly jsou rozebrány možnosti obrany a prevence před útoky všeho druhu malwaru, a zmíněny konkrétní způsoby a postupy, jak dosáhnout nejvyššího zabezpečení. V závěru kapitoly se práce dostala k hlavní problematice, a to k popisu spywaru. V této poslední sekci kapitoly je hned po popsání tohoto typu malwaru krátce vyložena jeho historie, následovaná obecným dělením spywaru.

Další dvě kapitoly se zaměřují na aktuální stav škodlivého spywaru, a to nejdříve v České republice, kde dominují varianty pro systém Windows. Toto téma pokračuje v kapitole mobilní spyware, kde jsou nejprve rozvedeny možnosti pro Android nebo iOS, a poté konkrétní příklady mobilních špionů. Nejdůležitějším zástupcem je spyware Pegasus, který je nejlepší a nejnebezpečnější z mobilních variant, protože pro šíření využívá exploitů integrovaných, nebo populárních aplikací. Možností obrany proti takovým pokročilým útokům je málo, ale existují jednoduché akce, které mohou snížit riziko nakažení. Tyto akce jsou popsány na závěr čtvrté kapitoly.

V praktické části této diplomové práce došlo k implementaci mobilního spywaru pro Android, a serverové aplikace pro Windows. Obě tyto části jsou celé v jazyce C#. Pro vývoj mobilní aplikace byla využita open source platforma Xamarin, která poskytuje přístup k většině potřebným funkcím. Během návrhu řešení je tato platforma popsána, a navíc i vývojové prostředí a postup instalace. Následuje popis služby na popředí, která byla vybrána jako řešení pro realizaci spywaru, a použité šifrovací algoritmy u přenosu dat. Popis implementace síťové komunikace, dvou aplikací a jejich funkcí je v kapitole 6. Finální mobilní aplikace obsahuje funkce jako keylogger, záznam obrazovky, mikrofonu, nebo sledování lokace.

Součástí práce je i testování implementované spyware aplikace proti odhalení mobilními antiviry. Rozsáhlé testy odhalily, že spyware Android Update se pro všechny antivirové nástroje tváří

jako bezpečný. Pokud uživatel nerespektuje varování proti instalaci aplikací třetích stran od integrovaného Google Play Protect, tak může spyware nepozorovaně sbírat citlivé informace o oběti.

V poslední kapitole jsou demonstrovány plně opakovatelné příklady užití, a to od klientské, tak od serverové aplikace. Byla zde popsána instalace aplikací, změna IP adresy, konkrétní případ spuštění a sledování oběti, a na konec jak dosáhnout vypnutí mobilního klienta.

Možností implementace mobilního spywaru jsou v dnešní době velké, jelikož všechny zařízení obsahují nespočet integrovaných funkcí. Většina dnešních aplikací komunikuje se serverem, a proto lze tato nežádoucí aktivita schovat v tom velkém shluku důležitých informací. Uživatel si nikdy nemůže být jistý, jestli o něm aplikace sbírá pouze potřebné informace, nebo si taky bere něco navíc. Pro označení za spyware stačí posílání nějaké informace, která například nebyla schválena uživatelem, není nutná pro běh, nebo řešení určitého problému. Většina malwaru dnešní doby spoléhá na lidskou chybu, a proto je důležité se rozmyslet, jestli je nutné stahovat a spouštět danou přílohu, soubor, nebo aplikaci.

Literatura

1. *Phishing, Vishing, SMiShing, Whaling And Pharming: How To Stop Social Engineering Attacks* [online]. [cit. 2023-03-08]. Dostupné z: https://expertinsights.com/insights/phishing-vishing-smishing-whaling-and-pharming-how-to-stop-social-engineering-attacks/.
2. *Threat Spotlight: Coronavirus-related phishing* [online]. 2020-03-26. [cit. 2023-03-08]. Dostupné z: https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/.
3. *Co to je malware?* [online]. [cit. 2023-03-07]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/co-to-je-malware/.
4. *10 Most Common Types of Malware Attacks* [online]. 2022-10-25. [cit. 2023-03-07]. Dostupné z: https://arcticwolf.com/resources/blog/8-types-of-malware/.
5. *Adware* [online]. [cit. 2023-03-07]. Dostupné z: https://www.eset.com/cz/adware/.
6. *Fileless threats* [online]. 2023-02-07. [cit. 2023-03-07]. Dostupné z: https://learn.microsoft.com/en-gb/microsoft-365/security/intelligence/fileless-threats?view=o365-worldwide.
7. *Počítačový virus* [online]. [cit. 2023-03-07]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus.
8. *The myth of the Trojan War* [online]. 2019-06-18. [cit. 2023-03-08]. Dostupné z: https://www.britishmuseum.org/blog/myth-trojan-war.
9. MESKAUSKAS, Tomas. *What is Agent Tesla?* [online]. 2022-10-26. [cit. 2023-03-14]. Dostupné z: https://www.pcrisk.com/removal-guides/14767-agent-tesla-rat.
10. *2022 Data Breach Investigations Report* [online]. [cit. 2023-03-07]. Dostupné z: https://www.verizon.com/business/en-sg/resources/reports/dbir/.
11. *Ochrana proti malwaru* [online]. [cit. 2023-03-08]. Dostupné z: https://support.google.com/google-ads/answer/2375413.
12. *The History of Spyware* [online]. [cit. 2023-03-08]. Dostupné z: https://supportnex.zendesk.com/hc/en-us/articles/4408057264020-The-History-of-Spyware.

13. *Spyware* [online]. [cit. 2023-03-08]. Dostupné z: https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/s/Spyware.htm.

14. *Online risks for US web users* [online]. 2004-10-25. [cit. 2023-03-08]. Dostupné z: https://www.theguardian.com/technology/2004/oct/25/security.internet.

15. *Apple expands industry-leading commitment to protect users from highly targeted mercenary spyware* [online]. 2022-07-06. [cit. 2023-03-08]. Dostupné z: https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/.

16. *What Is Spyware? Definition, Types, Removal, and Prevention Best Practices in 2022* [online]. 2022-07-27. [cit. 2023-03-09]. Dostupné z: https://www.spiceworks.com/it-security/security-general/articles/what-is-spyware/.

17. *ESET: Spyware od začátku roku opět posílil, útočníci budou investovat do vylepšení svých strategií* [online]. 2023-02-17. [cit. 2023-02-23]. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-spyware-od-zacatku-roku-opet-posilil-utocnici-budou-investovat-do-vylepseni-svych-strategii/.

18. *Trojan-stealer discovered in spam mailouts to businesses* [online]. 2022-09-23. [cit. 2023-02-23]. Dostupné z: https://www.kaspersky.com/blog/agent-tesla-spam-mailout/45621/.

19. *What is FormBook Malware?* [online]. [cit. 2023-02-23]. Dostupné z: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/what-is-formbook-malware/.

20. *FormBook spam campaign targets citizens of Ukraine* [online]. 2022-03-09. [cit. 2023-02-23]. Dostupné z: https://www.malwarebytes.com/blog/threat-intelligence/2022/03/formbook-spam-campaign-targets-citizens-of-ukraine.

21. PALAZOLO, Gustavo. *New Formbook Campaign Delivered Through Phishing Emails* [online]. 2022-03-11. [cit. 2023-03-14]. Dostupné z: https://www.netskope.com/blog/new-formbook-campaign-delivered-through-phishing-emails.

22. OSBORNE, Charlie. *Pandemic threats: The common threads in COVID-19 scams and criminal schemes* [online]. 2021-03-31. [cit. 2023-03-14]. Dostupné z: https://www.zdnet.com/article/pandemic-threats-the-common-threads-in-covid-19-scams-criminal-schemes/.

23. *Android OS Privacy Under the Loupe – A Tale from the East* [online]. 2023-02-03. [cit. 2023-03-11]. Dostupné z: https://arxiv.org/pdf/2302.01890.pdf.

24. *Jak je na tom jailbreak v roce 2022 a má vůbec ještě smysl?* [online]. 2022-02-08. [cit. 2023-03-09]. Dostupné z: https://jablickar.cz/jak-je-na-tom-jailbreak-v-roce-2022-a-ma-vubec-jeste-smysl/.

25. *What is zero-click malware, and how do zero-click attacks work?* [online]. [cit. 2023-03-11]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-zero-click-malware.

26. *Pegasus Spyware and Citizen Surveillance: Here's What You Should Know* [online]. 2022-07-19. [cit. 2023-03-11]. Dostupné z: https://www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance-what-you-need-to-know/.

27. *Staying safe from Pegasus, Chrysaor and other APT mobile malware* [online]. [cit. 2023-03-11]. Dostupné z: https://www.kaspersky.com/blog/how-to-protect-from-pegasus-spyware/43453/.

28. *How Saudi-Linked Digital Espionage Reached Canadian Soil* [online]. 2018-10-01. [cit. 2023-03-11]. Dostupné z: https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/.

29. *Xamarin System requirements* [online]. 2022-09-21. [cit. 2023-02-25]. Dostupné z: https://learn.microsoft.com/en-us/xamarin/cross-platform/get-started/requirements.

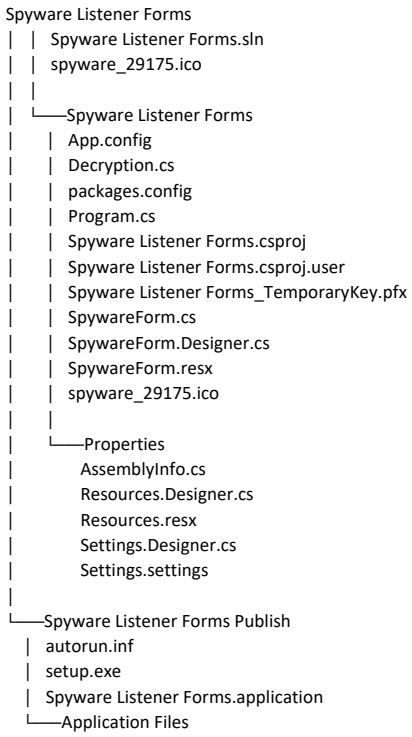
30. *Background Execution Limits* [online]. 2021-03-11. [cit. 2023-02-25]. Dostupné z: https://developer.android.com/about/versions/oreo/background#services.

31. *Android Test 2019 – 250 Apps* [online]. 2019-03-12. [cit. 2023-03-14]. Dostupné z: https://www.av-comparatives.org/tests/android-test-2019-250-apps/.

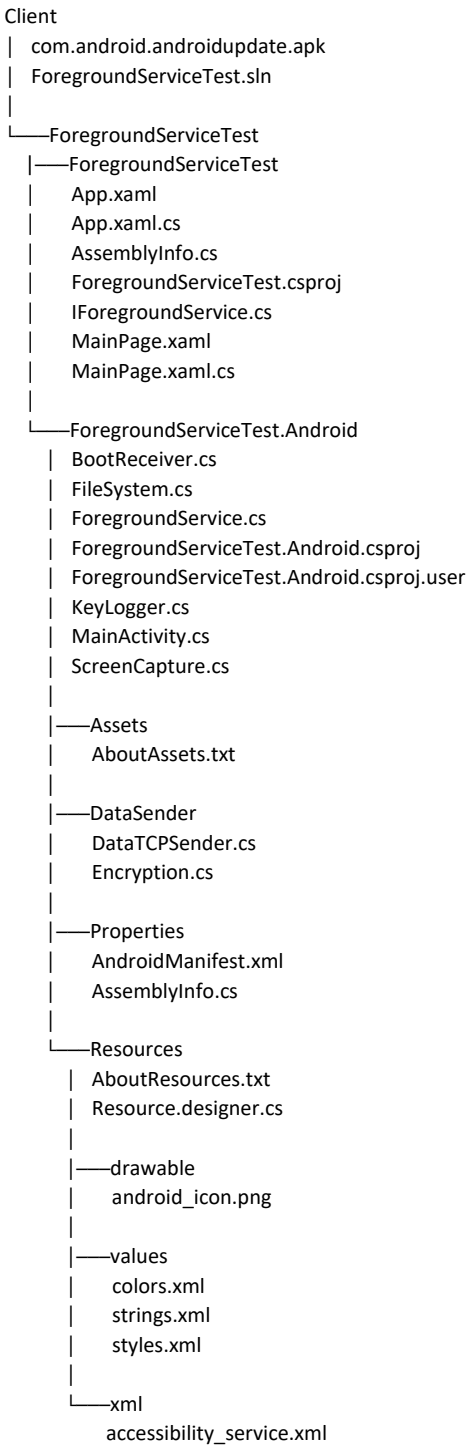
32. *Mobile Security Review 2022* [online]. 2022-06-20. [cit. 2023-03-14]. Dostupné z: https://www.av-comparatives.org/tests/mobile-security-review-2022/.

Příloha A

Struktury projektů



Obrázek A.1: Struktura projektu serverové aplikace



Obrázek A.2: Struktura projektu klientské aplikace - pro přehlednost byly vynechány složky pro mipmap ikony ve složce Resources

Příloha B

Ukázky kódu

```
//komprese dat
byte[] CompressByteArray(byte[] data)
{
   MemoryStream output = new MemoryStream();
   using (DeflateStream dstream = new DeflateStream(output, CompressionLevel.
       Optimal))
   {
      dstream.Write(data, 0, data.Length);
   }
   return output.ToArray();
}

//funkce pro dekompresi bytoveho pole
byte[] DecompressByteArray(byte[] bytedata)
{
   MemoryStream input = new MemoryStream(bytedata);
   MemoryStream output = new MemoryStream();
   using (DeflateStream dstream = new DeflateStream(input, CompressionMode.
       Decompress))
   {
      dstream.CopyTo(output);
   }
   return output.ToArray();
}
```

Listing B.1: Funkce CompressByteArray z klientské aplikace, a DecompressByteArray ze serveru

```
protected override void OnCreate(Bundle savedInstanceState)
{
   base.OnCreate(savedInstanceState);

   Xamarin.Essentials.Platform.Init(this, savedInstanceState);
   global::Xamarin.Forms.Forms.Init(this, savedInstanceState);
   //LoadApplication(new App()); nechceme zobrazit forms

   MainActivityInstance = this;
   GetPermissionsAndHide(); //ziska potrebne opravneni a schova aplikaci

   DependencyService.Resolve<IForegroundService>().StartMyForegroundService();
}
```

Listing B.2: Funkce OnCreate, která se provede po vytvoření MainActivity

```
   public void StartMyForegroundService()
   {
      var intent = new Intent(Android.App.Application.Context, typeof(
          ForegroundService));
      if (Build.VERSION.SdkInt >= BuildVersionCodes.O) //u Androidu Oreo se změ
          nilo startování služby na popředí
      {
         Android.App.Application.Context.StartForegroundService(intent);
      }
      else
      {
         Android.App.Application.Context.StartService(intent);
      }
   }
```

Listing B.3: Funkce StartMyForegroundService, která spustí službu na popředí

```
[BroadcastReceiver(Enabled = true,Exported = false)]
[IntentFilter(new[] { Intent.ActionBootCompleted }, Priority = (int)
    IntentFilterPriority.HighPriority)]
public class BootReceiver : BroadcastReceiver
{
   public override void OnReceive(Context context, Intent intent)
```

```
    {
        Intent i = new Intent(context, typeof(ForegroundService));
        i.AddFlags(ActivityFlags.NewTask);
        if (Build.VERSION.SdkInt >= BuildVersionCodes.O)
        {
            context.StartForegroundService(i);
        }
        else
        {
            context.StartService(i);
        }
    }
}
```

Listing B.4: Třída BootReciever, která se stará o opětovné spuštění služby při restartu

```
//připravení nahrávání a nastavení parametrů
public void PrepareRecordingObject()
{
    try
    {
        fileName = DateTime.Now.Day + "-" + DateTime.Now.Month + " " + DateTime.Now.
            Hour + "-" + DateTime.Now.Minute + "-" + DateTime.Now.Second + ".mp4";
        string path = Path.Combine(MainActivity.filepath, fileName);
        mMediaRecorder.SetAudioSource(AudioSource.Mic); //na emulatoru nutne
            pripojit virtualni sluchatka v nastaveni, Android 11+ je nutne mit
            povoleny accessibility service první, jinak nejde použít mikrofon v pozad
            í
        mMediaRecorder.SetVideoSource(VideoSource.Surface);
        mMediaRecorder.SetOutputFormat(OutputFormat.Mpeg4);
        mMediaRecorder.SetAudioEncoder(AudioEncoder.Aac);
        mMediaRecorder.SetVideoEncoder(VideoEncoder.H264);
        mMediaRecorder.SetVideoSize(WidthPixels, HeightPixels);
        mMediaRecorder.SetVideoFrameRate(16); //16fps kvuli velikosti
        mMediaRecorder.SetOutputFile(path);
        mMediaRecorder.SetVideoEncodingBitRate(512000); //512Kbps kvuli velikosti
        mMediaRecorder.Prepare();

    }
```

```
    catch (Exception e)
    {
        //error
        Console.WriteLine(e.Message);
    }
}
```

Listing B.5: Funkce PrepareRecordingObject, která nastaví parametry nahrávání videa

```
    //Vlákno co bude naslouchat
    Thread workerThread1 = new Thread(new ThreadStart(Listen));
    //Start vlákna
    workerThread1.Start();

    void Listen()
    {
        // Začátek nekonečné smyčky, kde se čeká na spojení a přenos dat
        while (true)
        {
            Console.WriteLine();
            Console.Write("Waiting for connection... ");
            client = listener.AcceptTcpClient(); //přijmout příchozí spojení
            Console.WriteLine("Connected!");

            //získání streamu TCP klienta pro komunikaci (čtení a zápis dat)
            stream = client.GetStream();

            //poslání druhé straně veřejný klíč serveru pro asymetické šifrování
            SendPublicKey();

            try
            {
                //získání klíče a IV pro AES
                GetAESDetails();

                //poslání druhé straně instrukce screenshots/video
                SendWantedMediaType();
```

```
            isFileBool = isFile();
            if (isFileBool)
            {
               fileName = GetString();
               GetFile(fileName);
            }
            else
            {
               GetString();
            }
         }
         catch (Exception e)
         {
            Console.WriteLine(e.Message);
         }
      }
   }
```

Listing B.6: Kód spuštění vlákna a metoda Listen, která běží v nekonečné smyčce