UNIVERZITA OBRANY

Fakulta vojenských technologií

Metodologie

Týmová práce

svob. Roman BRÁTEL
svob. Tomáš HUJŇÁK
svob. Vojtěch POMAZAL
svob. Tomáš VÁVRA
svob. Tomáš VYSLOUŽIL
svob. Valerie UNGERSBÖCKOVÁ

BRNO 2021

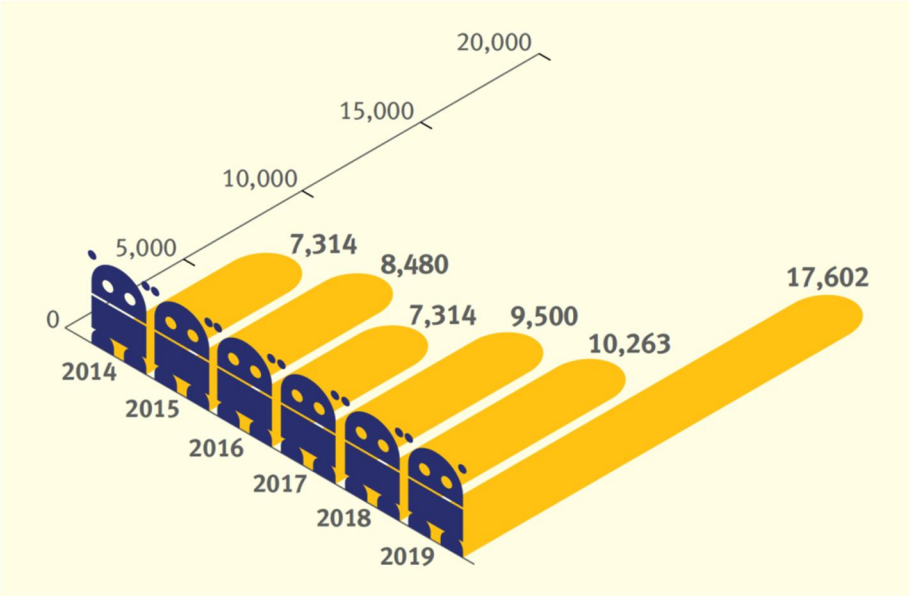
OBSAH

1 Návrh experimentu 2
1.1 Definice problému 2
1.2 Ohraničení problému 3
1.3 Návrh řešení 3
1.4 Definování hypotéz 5
1.5 Definování metrik a indikátorů 5
1.6 Forma experimentu 5
1.7 Analýza zainteresovaných stran 5
1.8 Vlastní návrh experimentu 6
2 Experiment 8
2.1 Parametry experimentu 8
2.1.1 Prototyp 1 8
2.1.2 Prototyp 2 9
2.1.3 Prototyp 3 9
2.1.4 Prototyp 4 10
2.2 Zhodnocení prototypů 10
2.3 Vyhodnocení hypotéz 11
2.3.1 Hypotéza č. 1 11
2.3.2 Hypotéza č. 3 11
3 Závěr 11
4 Zdroje obrázků 11

1 Návrh experimentu

1.1 Definice problému

Pro téma naší teamové práce jsme si vybrali problematiku nízké efektivity rozšiřování botnetu a to především v rámci nižších investičních možností. Použití botnetu je dnes stále velmi oblíbenou metodou, jak můžeme vidět například ze studie SpamhausBotnetLab.



Samotná tvorba botnetu vyžaduje především získání přístupu k co největší síti počítačů, jež následně mohou provádět řízenou činnost. V tento moment nám přichází „na pomoc“ samotný uživatel, jelikož získání přístupu od uživatele je ve většině případů mnohonásobně jednodušší, než technologické obcházení nejrůznějších zabezpečovacích systémů, tudíž vytvoření cesty, která přiměje uživatele postupovat tak, jak potřebujeme, je pro nás daleko efektivnější v mnoha směrech, než jiná řešení. Proto v rámci experimentu chceme testovat vybraná řešení a zpětné porovnání jejich efektivity a selektovat nejvhodnější skupinu uživatelů.

Vyřešením tohoto problému si zodpovíme především otázku pro způsob co možná nejefektivnějšího šíření botnetu, při co nejnižším úsilí a minimálních investicích.

1.2 Ohraničení problému

Experiment se bude zabývat nalezením řešení pro co nejefektivnější šíření botnetu, při minimální náročnosti a to ve formě porovnávání několika předem zvolených variant/tématik.

Samotné tématiky jsme vybrali v rámci co nejvyššího potencionálního trafficu, což má za účel zvýšení úspěšnosti, přičemž opomíjíme samotný technologický faktor tvorby botnetu a problém zjednodušujeme na měření lákavosti vstupu a potencionálu prokliku.

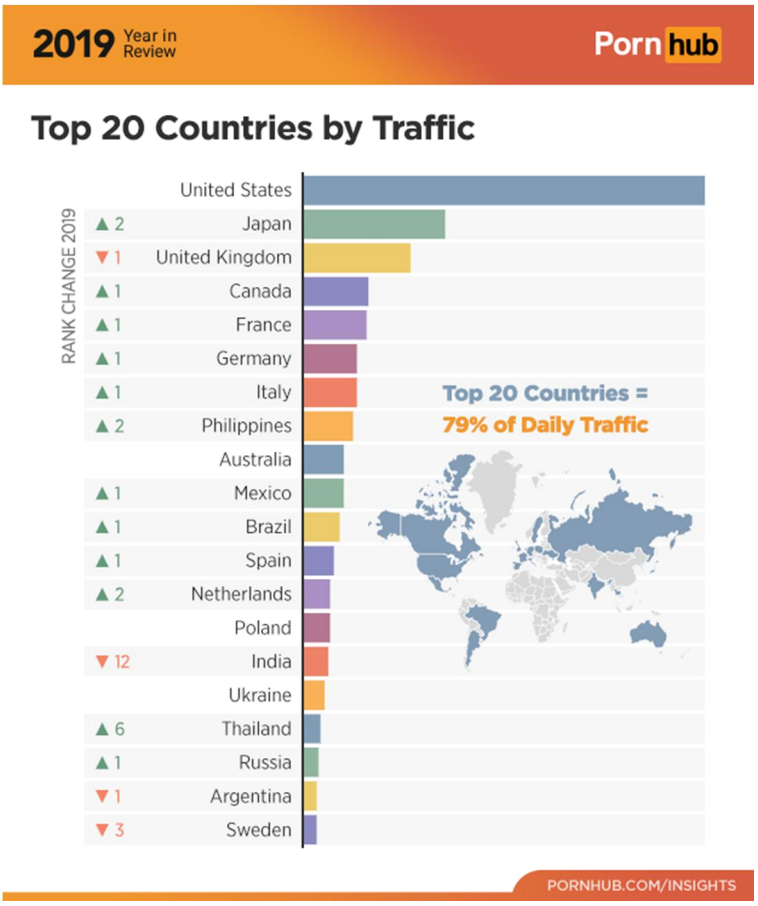
Tyto limitace jsou způsobeny několika faktory, počínaje amorální stránkou tvorby botnetu a omezeným množstvím naších schopností v této problematice konče.

1.3 Návrh řešení

Řešení pro tento problém je dle naší úvahy několik, s tím že byly vybrány 4 s největším potenciálem, které budeme dále rozvádět.

1. Šíření přes erotické stránky
   Tato možnost nám ihned nabízí obrovské množství potenciálních obětí. Samotné prostředí nám dále nahrává pro tvorbu nejrůznějších motivů, které limituje pouze naše

fantasie. Taktéž je velká část této skupiny poměrně náchylná k prokliku. Ze statistického hlediska se budeme taktéž zaměřovat na anglicky mluvící část populace, především z důvodu rozložení trafficu podle zemí.



2. Ilegální a podpůrné programy třetích stran do počítačových her
   Řešení, mířené především na mladší uživatele a hráče počítačových her. Podpůrné programy do her jsou v dnešní době nedílnou součástí a mnoho uživatelů si na ně nedá dopustit. Na druhou stranu ilegální programy jako například hacky jsou v herním a hlavně eSport průmyslu velkým problémem.
3. Fenomény
   U této volby jsme si vybrali velice populární a aktuální téma a to pandemii Covid, konkrétně očkování proti této nemoci. Domníváme se, že v dnešní pandemické době bude stránka s tímto tématem velmi navštěvována, jelikož jsme soubor pojmenovali „Petice proti očkování na Covid-19“. Je spoustu lidí v České republice, kteří nesouhlasí s očkováním, proto si myslíme, že tento soubor s tímto názvem bude stažen mnohokrát. Samozřejmě bude číslo návštěvnosti a stažení souboru nižší, protože tohle konkrétní téma může zaujmout pouze lidi z ČR.
4. Clickbaitové reklamy
   Na internetu se pohybují řady clickbaitových reklam. Od reklam na prohlížečové hry přes slevy v e-shopech až po úžasné způsoby jak nabrat svalovou hmotu nebo zhubnout několik kilogramů v rozmezí pár týdnů. Vybrali jsme si proto několik typů

těchto reklam. Tímto způsobem jsme zajistili zaměření jednoho řešení na více potencionálních cílových skupin.

1.4 Definování hypotéz

1. Domníváme se, že správnou volbou cílové skupiny je možné zefektivnit tvorbu botnetu.
2. S největší pravděpodobností bude taktéž záležet na momentálním vývoji jednotlivých řešení, kdy krátkodobý peak jednoho řešení může v omezeném časovém horizontu zastínit dlouhodobý trend jiného řešení, tudíž je volbu vždy potřeba zvážit a ne jen slepě sledovat tabulku.
3. Cílení na nezletilé → větší úspěšnost

V rámci experimentu chceme ověřit všechny hypotézy až na 2., jelikož nejsme schopni vygenerovat dostatečné množství spolehlivých dat v našem časovém horizontu.

1.5 Definování metrik a indikátorů

Jako hlavní metriku pro tento experiment jsme zvolili potenciál stažení, který představuje prosté množství úspěšných stažení stažení .exe souboru. Tímto způsobem je možné provádět měření nekomplikovanou cestou

1.6 Forma experimentu

Jako formu experimentu jsme zvolili mutaci prototypování a to formou vytvoření zmíněných 4 tématik/prototypů, jejichž následným vzájemným porovnáním chceme vyselektovat ten s největším potencionálem podle předem stanovených metrik a indikátorů.

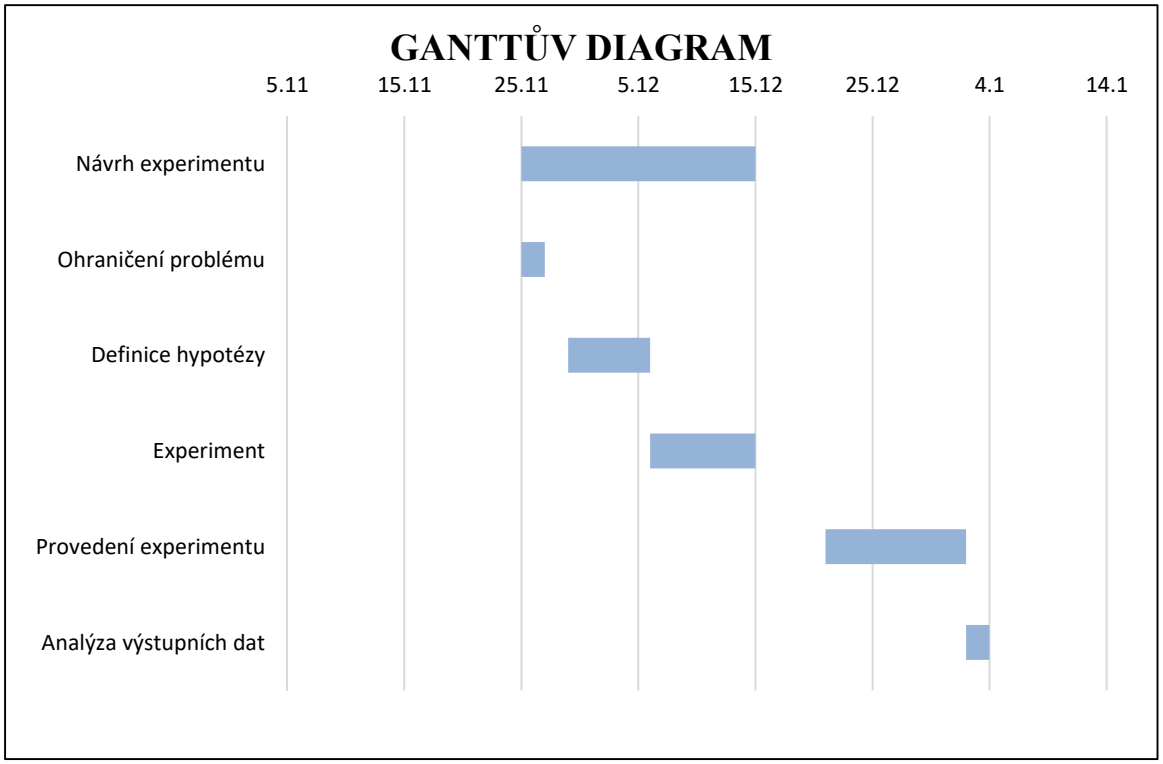
1.7 Analýza zainteresovaných stran

Pro co možná nejúspěšnější realizaci experimentu je potřeba zvážit všechny důležité zainteresované strany, jelikož jejich vnitřní či vnější vliv může pozměnit úspěšnost šíření, která je pro tento experiment velmi důležitá.

1. Oběti
2. Tvůrci botnetu
3. Majitelé inzerčních prostředí
4. Add-block
5. Psychologický aspekt reklamy
6. Znalý uživatel
7. Moderátoři komentářových sekcí
8. Správci reklamních panelů a herních modů

1.8 Vlastní návrh experimentu

Pomocí nejrůznějších nástrojů v závislosti na dané tématice prototypu jsme vytvořili 4 prototypy pro vytvoření neškodného .exe souboru (samospustitelné video). Tudíž v rámci této části práce budeme popisovat především tvorbu a funkci jednotlivých prototypů.



1. **Prototyp 1 → Šíření přes erotické stránky**

   Pro tento systém jsme zvolili metodu phishingu, kdy nabízíme službu rozpoznávání obličeje pornoherců/hereček za pomoci linku přesměrovávající na předem vytvořenou webovou stránku, z níž je možné stáhnout již zmiňovaný .exe soubor, který vydáváme za add-on rozšíření pro PornHub, jelikož je to nejpoužívanější a zároveň

nejrozšířenější stránka s erotických obsahem. Samotná webová stránka byla poměrně jednoduše vytvořena za pomoci služby Weebly, kde jsme dostali pro studijní účely i 14 denní hosting zdarma. Samotný frontend stránky je poměrně jednoduchý s tím, že na pozadí je měřena celková návštěvnost, jenž je zapisována v 24h úsecích stejně jako celkový počet stažení .exe souboru. Pokud jde o samotný link a případný přístup uživatele na náš web, tak jsme místo nejrůznějších vyskakovacích oken, apod. zvolili metodu rozšíření linku s krátkým popiskem do komentářových sekcí přibližně 500 nejpopulárnějších PornHub videí. Velkou výhodou tohoto systému je obejití add-blocku, naopak poměrnou nevýhodou je relativně rychlé zapadnutí komentáře s linkem, tudíž pro dlouhodobé fungovaní nemusí být v této verzi ideálním způsobem.
Desing webové stránky:

2. **Prototyp 2 → Ilegální a podpůrné programy třetích stran do počítačových her**

   Pro tento prototyp jsme vytvořili webovou stránku, kde jsme herním uživatelům nabízeli zdarma falešné podpůrné programy, které jim usnadní samotnou hru, ať už legální, nebo nelegální cestou. Webovou stránku jsme za pomoci nových falešných účtů rozhodili po velkém množství stránek zaměřujících se na herní tématiku, především herní fóra. Na naší stránce měli uživatelé možnost si stáhnout podpůrné programy do mnoha populárních počítačových her. Přestože se download link tvářil vždy jinak, odkazoval na jeden totožný soubor. Počet stáhnutí tohoto souboru jsme měřili každý den.

3. **Prototyp 3 → Šíření přes sociální síť Facebook**

   Zde jsme zvolili metodu, kde nabízíme petici proti očkování Covid-19 za pomoci linku, který odkáže na .exe soubor, vložený na webshare.cz. Jednoduše jsme vytvořili pár fake profilů na sociální síti Facebook a připojili se do různých skupin s covid tématikou. Aktivně jsme každý den sdíleli „petici“ ve všech skupinách a zapisovali počty stáhnutí.

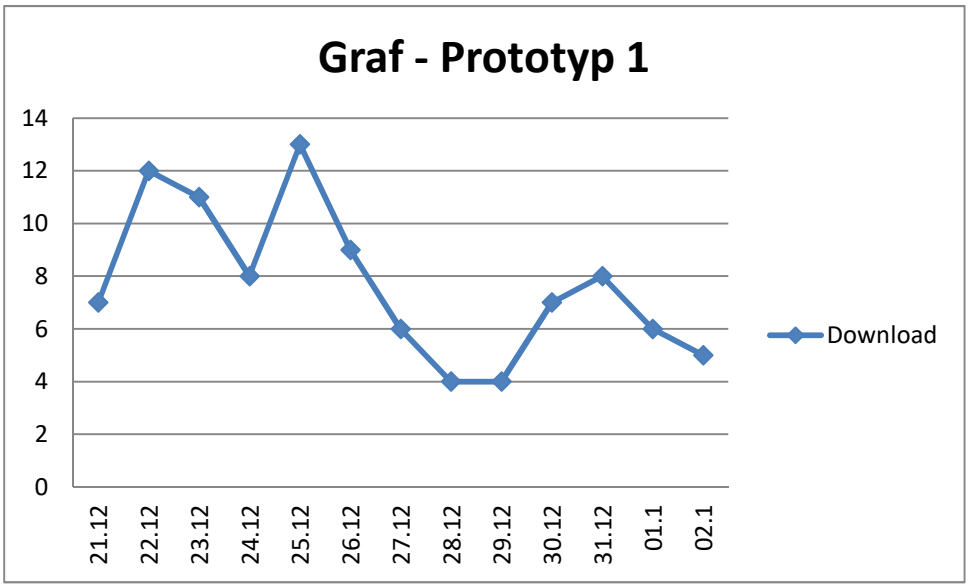
4. **Prototyp 4 → Clickbaitové reklamy**

   K šíření reklamy jsme využili fóra, která se přímo či nepřímo zabývají danou tématikou a v sekci komentářů sdíleli link s odkazem na stažení programu zdarma, který obsahoval rady a triky, masáže a stravovací plán. Téma bylo 1. zvětšení penisu, 2. zkvalitnění vzhledu a tvaru poprsí, 3. zkvalitnění erekce a prodloužení výdrže v posteli. Každý den jsme evidovali počet stažení s různou tématikou.

2 Experiment

2.1 Parametry experimentu

2.1.1 Prototyp 1

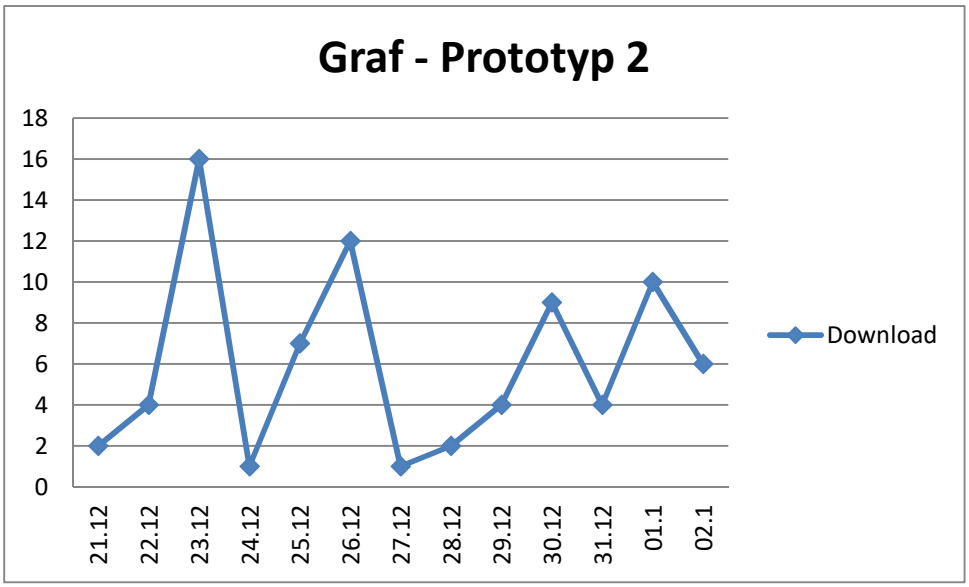


Datum	Download
21.12	7
22.12	12
23.12	11
24.12	8
25.12	13
26.12	9
27.12	6
28.12	4
29.12	4
30.12	7
31.12	8
01.1	6
02.1	5

U tohoto prototypu můžeme na datech sledovat trend, kdy download zprvu poměrně narůstá, načež nejspíše díky svátkům (25.12.) dochází k razantnímu poklesu, přičemž tento trend nadále pokračuje s anomálií okolo oslav Nového roku, jemuž ji nejspíš můžeme i přisuzovat. Samotný pokles přitom je nejspíše způsoben řadičem komentářů, kdy komentář odkazující na náš web postupně „zapadá“ a ztrácí na viditelnosti

Celkový počet stažení: 100

2.1.2 Prototyp 2

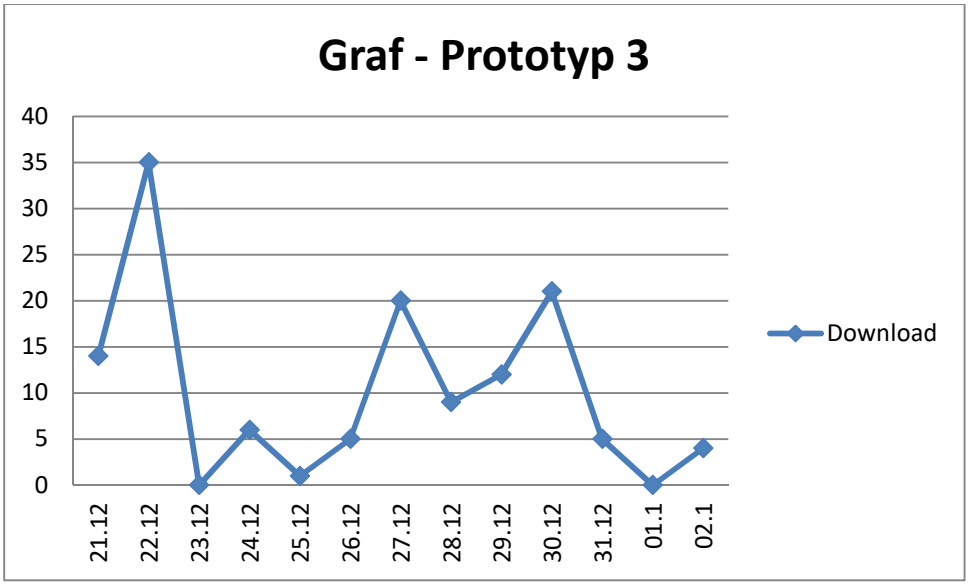


Datum	Download
21.12	2
22.12	4
23.12	16
24.12	1
25.12	7
26.12	12
27.12	1
28.12	2
29.12	4
30.12	9
31.12	4
01.1	10
02.1	6

Jelikož jsme experiment dělali přes Vánoce, čísla nebyla až tak vysoká. Ale i přes to si myslíme, že i tahle důvěra v neplatný facebookový profil, který jen sdílí jakýsi .exe soubor je až příliš velká. Samozřejmě je to způsobeno nesouhlasem a obavy ze zmiňovaného očkování.

Celkový počet stažení: 78

2.1.3 Prototyp 3

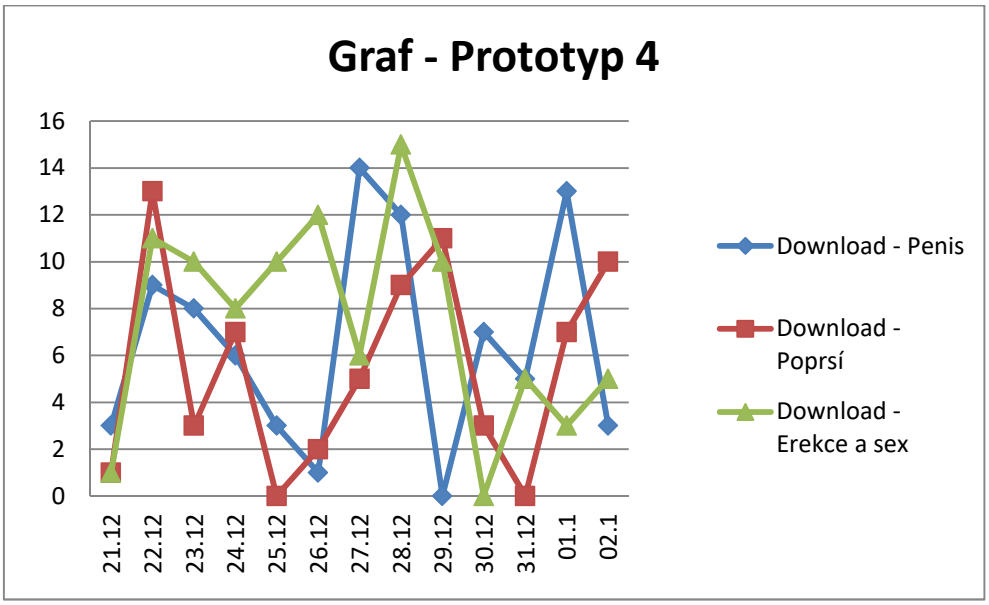


Datum	Download
21.12	14
22.12	35
23.12	0
24.12	6
25.12	1
26.12	5
27.12	20
28.12	9
29.12	12
30.12	21
31.12	5
01.1	0
02.1	4

U třetího prototypu můžeme vidět, že si uživatelé v dnešní době dávají větší pozor na falešné stránky, neboť počet stahování nebyl kromě předvánočního dne moc vysoký, jen zřídka přesáhl počtu desíti stáhnutí za den. Důvodů může být více, my se však domníváme, že v dnešní době jsou uživatelé internetu bystřejší a už se nenechají tak lehce nachytat. Různé antiviry, či pomocné addony v prohlížeči mohly taktéž zamezit vyššímu počtu stáhnutí, jelikož hodnotily náš soubor jako nedůvěryhodný.

Celkový počet stažení: 132

2.1.4 Prototyp 4



Datum	Download - Penis	Download - Poprsí	Download - Erekce a sex
21.12	3	1	1
22.12	9	13	11
23.12	8	3	10
24.12	6	7	8
25.12	3	0	10
26.12	1	2	12
27.12	14	5	6
28.12	12	9	15
29.12	0	11	10
30.12	7	3	0
31.12	5	0	5
01.1	13	7	3
02.1	3	10	5

Z grafu vyplývá, že největší aktivita na stránkách zabývajících se mužským či ženským tělem je v období 27.12. - 29.12., což naznačuje povánoční nekomfortnost se svým tělem (popř. výkonem v posteli) a snaha uživatelů ji zlepšit buďto s výhledem na oslavy nového roku, nebo i dále do budoucna. V celkovém počtu stáhnutí vede reklama zabývající se výdrží v posteli a zkvalitnění erekce s 96 stáhnutími. Dále reklama na zvětšení mužského údu 84 a nakonec zlepšení tvaru a vzhledu poprsí u žen 71 stáhnutí.

Celkový počet stažení: 251 (96 jedna reklama)

Z těchto čísel může plynout hned několik závěrů:

1. Muži častěji vyhledávají pomoc v této oblasti na internetu. Také sledování erotického obsahu, kde se reklamy tohoto typu často vyskytují, jsou navštěvovány především mužskou částí populace.
2. Většina mužů si je vědoma, že zvětšení penisu pomocí masáží, je z dlouhodobého hlediska nemožné, nicméně vidina kvalitnější erekce a delší výdrže za pomoci určitého životního stylu, je mnohem reálnější.

2.2 Zhodnocení prototypů

Nejlepší výsledek byl dosažen na prototypu č. 4, avšak musíme brát v potaz kombinování 3 reklam, tudíž jde-li pouze o čistě jednu cílovou skupinu, tak je nejúspěšnější volbou prototyp č. 3.

2.3 Vyhodnocení hypotéz

2.3.1 Hypotéza č. 1

Jak nám může prototyp č. 4 ukázat na při více cíleném zaměření i na fragmentace na více částí je možno docílit lepších výsledků než u ostatních řešení, čímž by se tato hypotéza dala potvrdit.

2.3.2 Hypotéza č. 3

Tato hypotéza se ukázala jako mylná, přičemž výsledek můžeme přisuzovat lepší technologické gramotnosti mladší populace, což ji také odděluje od ostatních cílových skupin.

3 Závěr

Z 3 hypotéz byly testovány 2. Jedna z nich byla potvrzena, druhá vyvrácena. Z výsledku práce vyplynulo, že nejlepší cestou k šíření botnetu při minimálním námaze je buďto cílená reklama nebo přizpůsobení se momentálním trendům na které však musíme být schopni reagovat.

Pro navazující experimenty tudíž bude nejefektivnější se dále zaměřit již jen na 2 zmíněné prototypy, které přinesly největší úspěch, avšak jak bylo zmíněno je potřeba aktualizovat trend pro prototyp č. 3. Pro navazující výzkum tak bude možné vyselektovat konkrétnější metodu, popřípadě zefektivnit metodiku. Pro závěr by bylo taktéž přínosné prodloužit testovací období pro přesnější výsledky.

4 Zdroje obrázků

[1] Number of botnet C&Cs observed in 2019. In: *The Spamhaus Project* [online]. Ženeva: Spamhaus, c1998-2021 [cit. 2021-01-02]. Dostupné z: https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

[2] Top 20 Countries by Traffic. In: *Pornhub* [online]. Montréal: MindGeek, c2021 [cit. 2021-01-02]. Dostupné z: https://cs.phncdn.com/insights-static/wp-content/uploads/2019/12/1-pornhub-insights-2019-year-review-top-20-countries-traffic.png