

Курсова Работа:

**ИТ Сигурност**

**Изготвил: мАРИЯ сТАНЧЕВА**

**Ф.Номер: 163011014**

**Съдържание**

1. **Понятие . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3стр**
2. **Spyware . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4стр**
3. **ADWARE . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6стр**
4. **TROJAN . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8стр**
5. **ИЗТОЧНИЦИ . . . . . . . . . . . . . . . . . . . . . . . . . . . 13стр**

Типове вредни програми

A picture containing device

Description automatically generated

Понятие  
Понятието идва от английското словосъчетание "malicious software", което се превежда точно "злонамерен софтуер". Алтернативни наименования са "зловреден софтуер", "злонамерен код" и "зловреден код". На английски има и съкратено наименование - "malware", което е образувано от пълното такова "**mal**icious soft**ware**".   
Злонамерен софтуер е всеки софтуер, който е проектиран да се инсталира на дадена компютърна система без знанието на потребителя и след това да извършва дейности, които са в ущърб на потребителя. Има доста голямо разнообразие от зловреден софтуер и в този проект биват разглеждани най разпространениете от тях.

A picture containing drawing

Description automatically generated

1. Spyware

Spyware е нежелан софтуер, който прониква във вашето изчислително устройство, открадва вашите данни за използване на интернет и чувствителна информация. Шпионският софтуер е класифициран като вид злонамерен софтуер - злонамерен софтуер, предназначен да получи достъп или да повреди вашия компютър, често без ваше знание. Шпионският софтуер събира вашата лична информация и я предава на рекламодатели, фирми за данни или външни потребители.

Spyware се използва за много цели. Обикновено той цели да проследява и продава вашите данни за използване на интернет, да улавя данните на кредитната ви карта или банковата си сметка или да открадне вашата лична самоличност. Шпионският софтуер следи вашата интернет активност, проследявайки данните ви за вход и парола и шпионирайки вашата чувствителна информация.

A close up of a sign

Description automatically generated

Някои видове шпионски софтуер могат да инсталират допълнителен софтуер и да променят настройките на вашето устройство, така че е важно да използвате защитени пароли и да поддържате актуализирани устройствата си.

Ако някога сте ставали жертва на кражба на самоличност или измама с кредитна карта, не сте сами. Статистиката за киберпрестъпленията разказва историята:

*Общо 978 милиона души в 20 държави са били засегнати от киберпрестъпност през 2017 г., според доклада на глобалните резултати на Norton Cyber Security Insights.*

*Жертвите на киберпрестъпността в световен мащаб загубиха 172 милиарда долара.*

Spyware е една от най-често срещаните заплахи в интернет. Той лесно може да зарази вашето устройство и може да бъде трудно да се идентифицира. Той е заплаха за бизнеса и отделните потребители, тъй като може да открадне чувствителна информация и да навреди на вашата мрежа.

A screenshot of a computer

Description automatically generated

1. Adware

Adware е името, което се дава на програми, които са предназначени за показване на реклами на вашия компютър, пренасочване на заявките ви за търсене към рекламни уебсайтове и събиране на маркетингови данни за вас - например типовете уебсайтове, които посещавате - за да могат да бъдат персонализирани реклами.

Adware - който събира данни с вашето съгласие - не трябва да се бърка с програми за шпионски софтуер Trojan, които събират информация, без вашето разрешение. Ако Adware не ви уведоми, че събира информация, той се счита за злонамерен - например злонамерен софтуер, който използва поведение Trojan-Spy.

Освен показването на реклами и събирането на данни, Adware обикновено не показва присъствието си. Обикновено в системната област на компютъра няма да има признаци на програмата - и в менюто на програмата няма индикация, че файловете са инсталирани на вашето устройство.

A close up of a sign

Description automatically generated

Има два основни начина, по които Adware може да влезе в компютъра ви:

* Чрез **freeware или shareware**

Рекламният софтуер може да бъде включен в някои безплатни или Shareware програми - като легитимен начин за генериране на рекламни приходи, които помагат да се финансира разработването и разпространението на freeware или shareware програма.

* Заразени уебсайтове

Посещението на заразен уебсайт може да доведе до нерегламентирано инсталиране на Adware на вашата машина. Често се използват хакерски технологии. Например, вашият компютър може да бъде проникнат чрез уязвимост на браузъра и могат да се използват троянски коне, които са предназначени за стабилна инсталация. Рекламните програми, които работят по този начин, често се наричат ​​браузър похитители.

A circuit board

Description automatically generated

1. Trojan

Троянски кон или троян е вид злонамерен софтуер, който често се прикрива като легитимен софтуер. Троянците могат да бъдат наети от кибер-крадци и хакери, които се опитват да получат достъп до системите на потребителите. Потребителите обикновено са подмамени от някаква форма на социално инженерство да зареждат и изпълняват троянски коне на своите системи. След като се активират, троянците могат да дадат възможност на киберпрестъпниците да ви шпионират, да откраднат вашите чувствителни данни и да получат достъп на заден план до вашата система. Тези действия могат да включват:

* Изтриване на данни
* Блокиране на данни
* Промяна на данни
* Копиране на данни
* Прекъсване на работата на компютри или компютърни мрежи

За разлика от компютърните вируси и червеи, троянците не са в състояние да се самовъзпроизвеждат.

A picture containing shirt, holding, pair, young

Description automatically generated

Tрояните се класифицират според вида на действията, които могат да извършват на вашия компютър:

* Back door.

Дава на злонамерени потребители дистанционно управление на заразения компютър. Те дават възможност на автора да прави всичко, което пожелае на заразения компютър - включително изпращане, получаване, стартиране и изтриване на файлове, показване на данни и рестартиране на компютъра. Задните троянци често се използват за обединяване на група жертви компютри за формиране на зомби мрежа, които могат да бъдат използвани за престъпни цели.

* Exploits

Exploits са програми, които съдържат данни или код, които се възползват от уязвимост в приложния софтуер, който работи на вашия компютър.

* Rootkit

Rootkits са предназначени да скрият определени обекти или дейности във вашата система. Често основната им цел е да предотвратят откриването на злонамерени програми - за да се удължи периодът, в който програмите могат да се изпълняват на заразен компютър.

* Trojan-Banker

Програмите на Trojan-Banker са предназначени да откраднат данните на вашия акаунт за онлайн банкови системи, системи за електронно плащане и кредитни или дебитни карти.

* Trojan-DDoS

Тези програми провеждат DoS (Denial of Service) атаки срещу целеви уеб адрес. Чрез изпращане на множество заявки - от вашия компютър и няколко други заразени компютри - атаката може да надвие целевия адрес ... което води до отказ на услуга.

* Trojan-Downloader

Trojan-Downloaders могат да изтеглят и инсталират нови версии на злонамерени програми на вашия компютър - включително троянски коне и рекламен софтуер.

* Trojan- Dropper

Тези програми се използват от хакери с цел инсталиране на троянски коне и / или вируси - или за предотвратяване на откриването на злонамерени програми. Не всички антивирусни програми са в състояние да сканират всички компоненти вътре в този тип троянски програми.

* Trojan-FakeAV

Програмите Trojan-FakeAV симулират активността на антивирусен софтуер. Те са създадени да изнудват пари от вас - в замяна на откриването и отстраняването на заплахи ... въпреки че заплахите, за които съобщават, всъщност не съществуват.

* Trojan-GameThief

Този тип програма открадва информация за потребителски акаунт от онлайн геймърите.

* Trojan-IM

Програмите Trojan-IM крадат вашите данни за вход и пароли за програми за незабавни съобщения - като ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype и много други.

* Trojan-Ransom

Този тип троянски програми могат да променят данни на вашия компютър - така че компютърът ви да не работи правилно или вече да не можете да използвате конкретни данни. Престъпникът ще възстанови работата на компютъра ви или ще деблокира вашите данни, след като им платите парите за откуп, които изискват.

* Trojan-SMS

Тези програми могат да ви струват пари - като изпращате текстови съобщения от мобилното си устройство до телефонни номера с първокласни цени.

* Trojan-Spy

Програмите Trojan-Spy могат да шпионират как използвате компютъра си - например чрез проследяване на данните, които въвеждате чрез клавиатурата си, правене на снимки на екрана или получаване на списък с изпълнявани приложения.

* Trojan-Mailfinder

Тези програми могат да събират имейл адреси от вашия компютър.

* Други видове троянци включват:
* Trojan-ArcBomb
* Trojan-Clicker
* Trojan-Notifier
* Trojan-Proxy
* Trojan-PSW

4. Източници:

<https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html>

<https://www.kaspersky.com/resource-center/threats/adware>

<https://www.malwarebytes.com/adware/>

<https://www.kaspersky.com/resource-center/threats/trojans>

<https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html>