Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

- Какво е „зловреден софтуер”?
- Кой създава зловреден софтуер?
- Как да се предпазите?

Какво е зловреден софтуер

Преглед

Може би сте чували за термини като вируси, троянски коне, ransomware (софтуер искащ откуп) или rootkit (комплект за пълен достъп), когато се дискутира кибер сигурността. Всички тези думи описват едно и също нещо – видове програми, които се използват от престъпници за заразяване на компютри и устройства. Един общ термин, който се използва, за да опише всички тези различни програми е фразата: „зловреден софтуер”. В този бюлетин ще обясним какво е зловреден софтуер, кой го създава и защо, както и най-важното – какво можете да направите, за да защитите себе си от него.

Гост-редактор

Лени Зелцер се концентрира основно върху предпазването на ИТ дейността на клиентите в NCR Corp и преподава борба със зловреден софтуер в института SANS Institute. Лени използва Twitter с името **@lennyzeltser** и списва блог за сигурност на **zeltser.com**.

Какво е „зловреден софтуер”?

Казано просто, зловредният софтуер е софтуер (или компютърна програма), която се използва за извършване на зловредни действия, както говори и името му. Кибер престъпниците инсталират зловреден софтуер на компютрите или устройствата ви, за да получат контрол над тях или да получат достъп до съдържанието им. Веднъж инсталирали го, тези престъпници могат да използват зловредния софтуер, за да шпионират онлайн активността ви, да откраднат паролите и файловете ви или да използват системата ви, за да атакуват други. Зловредният софтуер може дори да ви откаже достъп до собствените ви файлове, освен ако не платите на хакера откуп, за да си възстановите контрола върху тях.

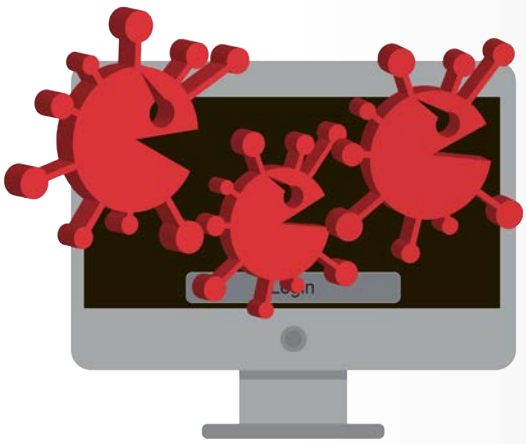
Много хора имат погрешното схващане, че зловредният софтуер е проблем само за компютри с Windows. Въпреки че Windows е широко използвана операционна система и така е сериозна цел, зловредният софтуер може да зарази всяко устройство, включително Mac компютри, смартфони или таблети. Колкото повече компютри и устройства заразяват кибер престъпниците, толкова повече пари могат да спечелят. Затова всички сме мишени, включително и вие.

Кой създава зловреден софтуер?

Зловредният софтуер вече не се създава само от любопитни любители или от хакери аматьори, а от изпечени кибер престъпници. Тяхната цел е да спечелят пари от вашия заразен компютър или устройство, като може би продадат данните, които са откраднали от вас или може би ви изпращат имейли, започнат атака за отказ на услуга или започнат да ви изнудват. Хората, които създават, разпространяват и извличат полза от зловреден

Какво е зловреден софтуер

софтуер могат да варират от хора, които работят сами, до добре организирани престъпни групи или дори правителствени организации. Хората, които създават днешния интелигентен зловреден софтуер често са посветени на тази цел, като създаването на зловреден софтуер за тях е работа на пълен работен ден. В допълнение, веднъж създали своя зловреден софтуер, те го продават на други личности или организации, като дори предлагат на своите „клиенти" редовна поддръжка и актуализации.



Защитете се от зловреден софтуер като гледате скептично на подозрителни съобщения, поддържате устройствата си актуализирани и имате инсталирана модерна антивирусна програма, когато е възможно.

Как да се предпазите?

Широко разпространена стъпка е инсталирането на антивирусен софтуер от доверени източници. Подобни инструменти, наричани понякога „анти-зловреден софтуер", са създадени, за да засичат и спират зловредния софтуер. Въпреки това, тези антивирусни програми не могат да блокират или да премахнат всичкия зловреден софтуер. Кибер престъпниците постоянно измислят и развиват нови и по-интелигентни вируси, които могат да избегнат засичането. Анти-вирусните предприемачи, от своя страна, постоянно актуализират своите продукти с нови способности за засичане на зловреден софтуер. До голяма степен това вече е състезание в което всеки отбор се опитва да надхитри другия. За съжаление, отборът на лошите обикновено е с една стъпка напред. Тъй като не можете да разчитате само на антивирусни програми, ето допълнителни стъпки, които трябва да направите, за да защитите себе си:

- Кибер престъпниците често заразяват компютри и устройства като използват слабости в софтуера им. Колкото по-обновен е софтуерът, толкова по-малко уязвима е системата и толкова по-трудно е за престъпниците да я заразят. Затова, проверявайте дали операционната ви система, приложенията и устройствата ви са настроени да инсталират актуализации автоматично.
- Често срещан начин по които кибер престъпниците заразяват мобилни устройства е да направят фалшиво приложение за мобилен телефон, да го пуснат в Интернет и след това да подмамят хората да го изтеглят и да го инсталират. Заради това препоръчваме да теглите и инсталирате приложения само от надеждни онлайн магазини. В допълнение, използвайте само мобилни приложения, които са били публикувани онлайн преди дълго време, вече са били изтеглени от голям брой хора и имат много положителни коментари.
- При компютрите – използвайте стандартен акаунт, който има ограничени правомощия, вместо акаунти с пълни правомощия, като „Администратор" или „root" (с пълен достъп). Това ви дава допълнителна защита, като не позволява на много видове зловреден софтуер да се инсталират.
- Кибер престъпниците често подлъгват хората да си инсталират сами зловреден софтуер. Например, може да ви изпратят имейл, който изглежда достоверен и съдържа прикачен файл или връзка. Може

Какво е зловреден софтуер

да изглежда, че имейлът идва от банка или от ваш приятел. Ако отворите прикачения файл обаче, или кликнете върху връзката, ще активирате зловреден код, който инсталира зловреден софтуер на вашата система. Ако съобщението съдържа много силно усещане за спешност, ако звучи объркващо или твърде хубаво, за да е истина, може да е атака. Бъдете подозрителни, здравият разум често е най-добрата защита.

- Редовно архивирайте системата и файловете си чрез облачни услуги или съхранявайте архивите си офлайн, като например на външни дискове, които не са свързани с Интернет. Това предпазва вашите архиви в случай, че зловреден софтуер се опита да ги криптира или изтрие. Архивите са критично важни, те често са единственият начин да възстановите всичко след заразяване с вирус.

Като цяло, най-добрият начин да се предпазвате от зловреден софтуер е да поддържате софтуера си актуализиран, да инсталирате надежден антивирусен софтуер от добре познати източници и да бъдете нащрек за всеки, който се опита да ви измами или излъже да заразите сами системата си.

НАУЧЕТЕ ПОВЕЧЕ

Абонирайте се за месечния бюлетин за информационна сигурност OUCH!, разгледайте архивните броеве на OUCH! и научете повече за решенията за информационна сигурност на SANS като ни посетите на http://www.securingthehuman.org.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:
https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962
https://www.linkedin.com/pub/nikolay-dachev/7b/5bb/96b

Ресурси

Фишинг:	https://securingthehuman.sans.org/ouch/2015#december2015
Социално инженерство:	https://securingthehuman.sans.org/ouch/2014#november2014
Сигурни мобилни приложения:	https://securingthehuman.sans.org/ouch/2015#january2015
Защитете новия си таблет:	https://securingthehuman.sans.org/ouch/2016#january2016
Архивиране:	https://securingthehuman.sans.org/ouch/2015#august2015

Редакторски колектив: Бил Уайман, Уолт Скривенс, Фил Хофман, Боб Рудис
Превод: Николай Дачев и Радослава Несторова