Зловреден софтуер

За повече информация: SEC.EFF.ORG
Проект на Фондация за електронни граници

MALWARE или на кратко зловреден софтуер, е инструмент, създаден да извършва нежелани действия на вашето устройство

Примерите за зловреден софтуер включват:

- компютърни вируси
- приложения, които „крадат“ пароли
- приложения, които ви записват без вашето знание
- приложения, които изтриват ваши данни без разрешение

ЗЛОВРЕДЕН СОФТУЕР ЧРЕЗ ФИШИНГ

Фишинг е действие, при което нападател изпраща съобщение, имейл или връзка, който изглежда безобидно, но всъщност е злонамерено. Фишингът най-често се извършва чрез познат профил или платформа, на която вярвате.

Забележка: Не всеки фишинг съдържа зловреден софтуер. Понякога нападателят иска да открадне пароли, използвайки сайт, без да инсталира нежелан софтуер на потребителското устройство.

Често срещани начини, чрез които се инсталира зловреден софтуер

чрез отваряне на прикачен зловреден документ или файл	Зловредни прикачени документи най-често се получават чрез измамни съобщения.
чрез отваряне на съмнителни връзки	Зловредни връзки най-често са споделяни чрез измамни съобщения.
чрез изтегляне на нелицензиран софтуер	Софтуер, който не получава обновявания на сигурността, е рисков (не от Apple App store или от Google Play store.)

чрез влизане в компрометирани уебсайтове	Понякога „откраднати“ уебсайтове служат като платформа за зловредно съдържание.

ВИДОВЕ ЗЛОВРЕДЕН СОФТУЕР

НЕЖЕЛАН РЕКЛАМЕН СОФТУЕР	появяващи се навсякъде реклами Този вид зловреден софтуер показва на потребителя реклами, чрез постоянно появяващи се изскачащи прозорци, претоварващи системата. Някои подобни софтуери могат да проследяват данни на потребителя и да извличат лична информация. Този софтуер може да бъде пакетиран с други приложения и най-често да бъде изтеглен от ненадеждни източници, неофициални магазини за приложения или директно от софтуерен разработчик.
СОФТУЕР ЗА ТАЙНО НАБЛЮДЕНИЕ И ПРОСЛЕДЯВАНЕ	когато вашето устройство всъщност помага на нападателя Този софтуер работи незабележимо и дава пълен достъп до устройството. Подобен софтуер може да бъде инсталиран, ако някой има физически достъп до вашето устройство (например член на семейството или партньор, “ще използвам телефона ти за момент”) и инсталира зловредно приложение. По същия начин, потребител може да бъде подлъган да изтегли зловредно приложение.
ТРОЯНСКИ КОН	изглежда като подарък, но атакува под прикритие Когато бъде изтеглен, Троянският кон, може да работи като нормално

	приложение, но всъщност да извършва зловредни действия на заден план. Най-често се среща в пиратски, “разбит“ или фалшив антивирусен софтуер.
Софтуер за искане на откуп за откраднати данни	такъв софтуер ви държи като заложник Когато бъде изтеглен, такъв софтуер съхранява данни на фирми, организации и хора, за да бъдат използвани като разменна монета. Този вид зловреден софтуер набира популярност през последното десетилетие и се превръща в многомилионен бизнес за недоброжелатели по целия свят.
Заплаха от вида A.P.T.	Разширена постоянна заплаха A.P.T. атаката е зловреден софтуер от противник със значителни възможности и повече ресурси, посветени на постигането на техните цели - да компрометират вашата система. A.P.T. атаките се извършват най-често от платени от чужди правителства лица, които поддържат дългосрочен достъп до системите, които „пробиват”.

5 СЪВЕТА ЗА ЗАЩИТА ОТ ЗЛОВРЕДЕН СОФТУЕР

СЪВЕТ №1: ОБНОВЯВАЙТЕ СОФТУЕРА

(И СЕ УВЕРЕТЕ, ЧЕ ИЗПОЛЗВАТЕ ЛИЦЕНЗИРАН* СОФТУЕР)

Основната част от зловредните приложения използват известни уязвимости. Софтуерните компании често поправят тези уязвимости и ги разпространяват към потребителите си под формата на обновявания.

Затова обновяването на софтуера е от решаващо значение за сигурността на потребителите, тъй като това е най-сигурният начин да се предпазите от известните слабости, които атакуващите биха могли да използват.

*Ако не сте сигурни как да се сдобиете с лицензиран софтуер, попитайте координатора по цифрова сигурност за съвети и ресурси.

СЪВЕТ №2: РЕЗЕРВНИ КОПИЯ ЗА БЪДЕЩЕТО

Създайте резервно копие на данните си днес и в бъдеще - ще бъдете благодарни. Ако изгубите устройството си (поради зловреден софтуер, кражба или ако просто спре да работи), не всичко е загубено: информацията от него се пази в резервните копия. Защитете ги с добра парола и шифроване.

СЪВЕТ №3: СПРЕТЕ ЗА МОМЕНТ ПРЕДИ ДА ОТВАРЯТЕ ВРЪЗКИ

Споделянето на връзки и файлове е често срещана практика, но бъдете бдителни, когато взаимодействате с тях или ги споделяте. Преди да ги отворите се запитайте: не изглеждат ли необичайно?

ВНИМАВАЙТЕ ЗА…СКЪСЕНИ И ОТРЯЗАНИ ВРЪЗКИ

На мобилно устройство връзките и електронните писма могат да изглеждат по-къси, от колкото когато се преглеждат на компютър. Услугите за скъсяване на връзки като bit.ly и други могат да пренасочват към злонамерени страници в интернет.

Съвет: използвайте услуги като https://unshorten.it, за да видите целия адрес!

ИМИТАЦИЯТА - НАЙ-ВЕЛИКАТА ФОРМА НА ИЗМАМА

Правописните грешки, сходните и повтарящите се знаци и фалшивите или наподобяващи на истински търговски марки са предназначени да ви измамят. Уверете се, че това е истинската услуга.

Съвет: когато използвате автентична услуга, използвайте отметките на браузъра: така компютърът ще ви помогне да запомните истинския адрес на услугата.

Съвет: Запазете правилната връзка в приложението за управление на пароли

Пазете се от манипулации от вида „социално инженерство“, като получаване на съобщение от някой, който се представя за ваш приятел.

Съвет: Свържете се с приятеля си по друг начин и проверете дали наистина това е той.

СЛУЧАЙНИ ДОКОСВАНИЯ НА ЕКРАНА И ЩРАКВАНЕ С МИШКАТА

Докато проверявате връзки на устройството си, едно случайно докосване на екрана или щракване с мишката може да отвори връзката!

Съвет: ако използвате мишка, можете да поставите курсора върху адреса, за да го видите целия.

СЪВЕТ №4: ВНИМАВАЙТЕ ЗА ФИЗИЧЕСКИ ДОСТЪП

Понякога нашите противници са хора, които познаваме или имат достъп до устройствата ни докато не им обръщаме внимание. Използването на шифроване на целия твърд диск и добра парола могат да ви помогнат при защитата на устройството ви от нежелан физически достъп. Бъдете внимателни, когато давате отключеното си устройство на някого. Прочетете повече на ssd.eff.org.

СЪВЕТ №5: ИЗПОЛЗВАЙТЕ АНТИВИРУСЕН СОФТУЕР

Не всички антивирусни програми са еднакви: някои приложения се предлагат като антивирусни, но могат да бъдат прикрит зловреден софтуер. Препоръчително е да използвате антивирусната програма от производител. Ако предпочитате антивирусен софтуер от друг източник, проверете:

- отзивите за софтуера от независими източници
- дали страницата на производителя поддържа и обновява списък със зловреден софтуер* за вида на зловредния софтуер и противника, от когото се притеснявате.

*Публикувано изследване на заплахите може да покаже, че разработчикът разполага с активен екип, който работи по защитата от този вид зловреден софтуер.

МИСЛЯ, ЧЕ ИМАМ ЗЛОВРЕДЕН СОФТУЕР. КАКВО ТРЯБВА ДА НАПРАВЯ?

Случва ли се нещо странно с вашето устройство? Конкретен профил (например в социална мрежа) ли е засегнат или цялото устройство? Ако изглежда като зловреден софтуер, внимавайте как използвате заразеното устройство в бъдеще - след това използвайте друго устройство*, от което да се свържете със специалист за помощ.

*Отделното устройство не трябва да бъде свързано със засегнатото. Това може да бъде например компютър в библиотеката или телефон на доверен приятел.

СВЪРЖЕТЕ СЕ С ДОВЕРЕН ТЕХНИК

Направете дневник със странните съобщения, които сте получили, в оригиналния им вид (например, ако се касае за електронно писмо, препратете оригиналното с всички описателни данни и заглавки, а не екранна снимка). Включете подробности като дата, час и описание. Изпратете ги на доверен технически специалист.

ОЦЕНЕТЕ ЩЕТИТЕ

Каква чувствителна информация може да е компрометирана? Трябва ли да промените паролите или профилите си? Планирайте следващите стъпки за безопасност, като направите оценка на риска (известна още като „моделиране на заплахи“).

Защо са от значение метаданните

Последна промяна: 11 март 2019

Като описателни данни или още метаданни, често се означава всичко друго, освен съдържанието на вашите съобщения. Можете да мислите за тях като за цифровия еквивалент на плик за писмо. Точно като него те съдържат информация за подателя, получателя и крайната цел на съобщението. Метаданните са информация за цифровите съобщения, които изпращате и получавате. Ето няколко примера:

- темата на имейлите
- продължителността на разговорите
- времето от деня, в което е проведен даден разговор
- местоположението ви по време на разговор (както и с кого)

В исторически план, в някои държави, включително САЩ, описателните данни се ползват с по-слаба защита от закона за лични данни, от колкото съдържанието на съобщенията. Полицията в много държави може да получи, например, по-лесно записи за това на кого сте се обадили миналия месец, отколкото да организира подслушване на телефонната линия, за да чуе какво всъщност казвате.

Тези, които събират или изискват достъп до метаданни, като правителствата или телекомите, твърдят, че разкриването (и събирането) на метаданни не е от голямо значение. За съжаление тези твърдения просто не са верни. Дори малка извадка от описателните данни може да предостави интимни подробности от живота на дадено лице. Нека разгледаме колко разкриващи могат да бъдат метаданните в действителност за правителствата и компаниите, които ги събират:

- Знаят, че сте звъннали на секс-линия в 02:24 ч. и разговорът е продължил 18 минути. Но не знаят за какво сте говорили.
- Знаят, че сте се обадили на телефона за предотвратяване на самоубийства от моста Голдън Гейт. Но темата на обаждането остава тайна.
- Знаят, че в един и същи час сте получили имейл от лаборатория за изследване на серопозитивни, след това сте се обадили на личния си лекар и сте посетили интернет страницата на група за подкрепа на болни от ХИВ. Но те не знаят какво е било в имейла или за какво сте говорили по телефона.
- Знаят, че сте получили имейл от група активисти за цифрови права с тема „Да кажем на Конгреса: Спрете SESTA/FOSTA“ и веднага след това сте се обадили на избрания от вас депутат. Но съдържанието на тези съобщения остава защитено от правителствена намеса.
- Знаят, че сте се обадили на гинеколога си, говорили сте половин час и по-късно през деня сте се обадили на номера на местната клиника за аборти.

Може да е трудно да защитите метаданните си от събиране, тъй като трети страни често се нуждаят от метаданни, за да бъде доставена успешно вашето съобщение. Точно както пощальонът трябва да може да прочете външната страна на плика, за да достави писмото,

цифровите комуникации често трябва да бъдат маркирани с източник и цел. Компаниите за мобилни телефони трябва да знаят приблизително къде се намира телефонът ви, за да насочват повикванията към него.

Услуги като Tor се използват с надеждата да ограничат количеството описателни данни, които се създават чрез обичайните методи за разговори през интернет. Докато законите не бъдат променени така, че да се справят по-добре с метаданните, а инструментите, които ги намаляват, не станат по-разпространени, най-доброто, което можете да направите, е да сте наясно какви метаданни предавате докато общувате, кой има достъп до тази информация и как тя може да бъде използвана.

План за сигурност

Последна промяна: 01 февруари 2021

Да се опитвате да предпазите всички свои данни през цялото време и от всички е непрактично и изтощително. Няма страшно! Сигурността е процес и чрез внимателна подготовка можете да съставите подходящ план. Сигурността не се отнася само до използваните инструменти или до изтегляния софтуер. Тя започва с разбирането на уникалните заплахи, пред които сте изправени и как можете да им противодействате.

В областта на компютърната сигурност заплахата е потенциално събитие, което може да подкопае усилията ви да защитите информацията. Можете да противодействате на заплахите, пред които сте изправени, като определите кое и от кого трябва да защитите. Това е процес на планиране на сигурността наричан анализ на риска или „моделиране на заплахите“.

В това ръководство ще научите как да съставите план за сигурността на вашата цифрова информация и как да определите най-подходящите за вас решения.

Какво представлява планът за сигурност? Да кажем, че искате да защитите дома и имуществото си. Ето няколко от въпросите, които можете да си зададете:

Кое от нещата в дома ми си струва да бъде защитено?

Активите могат да включват: бижута, електроника, финансови документи, лични документи или снимки.

От кого искам да го защитя?

Противниците могат да бъдат: крадци, съседи или гости.

Колко вероятно е да трябва да се защитя?

Има ли случаи на кражби с взлом в квартала? Колко надеждни са моите съквартиранти/гости? Какви са възможностите на моите противници? Какви са рисковете, които трябва да взема предвид?

Какви ще са последствията в случай на неуспех?

Имам ли нещо в къщата си, което не мога да заменя? Разполагам ли с време и средства да заменя тези неща? Имам ли застраховка, която покрива откраднатите вещи?

Колко усилия съм готов да положа, за да предотвратя тези последствия?

Готов ли съм да купя сейф за поверителните документи? Мога ли да си позволя да купя висококачествена брава? Имам ли време да отворя депозитна кутия в местната банка, където да съхранявам ценностите си?

След като сте си задали всички тези въпроси, можете да прецените какви мерки да предприемете. Ако имуществото ви е ценно, но вероятността за проникване с взлом е малка, може да не искате да инвестирате много средства в браза. Но ако вероятността за проникване е голяма, ще искате да си осигурите най-добрата брава на пазара и да помислите за система за сигурност.

Изготвянето на такъв план ще ви помогне да разберете уникалните за вас заплахи и да оцените активите си, противниците си, а също и вероятността от рискове, пред които сте изправени.

Как да направя собствен план за защита? От къде да започна?

Планирането на сигурността ви помага да определите какво би могло да застраши нещата, на които държите и от кого трябва да ги предпазите. Когато изграждате план за сигурност, си отговорете на тези пет въпроса:

- Какво искам да защитя?
- От кого искам да го защитя?
- Какви ще са последствията в случай на неуспех?
- Колко вероятно е да трябва да се защитя?
- През какви неприятности съм готов да премина, за да избегна потенциални усложнения?

Нека разгледаме отблизо всеки от тези въпроси

Какво искам да защитя?

„Актив“ е нещо, което цените и искате да предпазите. В контекста на цифровата сигурност, актив обикновено е някакъв вид информация. Например, вашите имейли, контакти, съобщения, местоположение и файлове се разглеждат като възможни активи. Вашите устройства също биха могли да бъдат активи.

Направете списък на активите: данни, които искате да запазите, къде се съхраняват, който има достъп до тях и какво би спряло останалите да достигнат до тях.

От кого искам да го защитя?

За да си отговорите на този въпрос е важно да разберете, кой може да иска да достигне до вас или вашата информация. Човек или обект, който представлява заплаха за вашите активи е „противник“. Примери за ваши противници могат да бъдат вашият шеф, партньор, бизнес конкуренция, правителството или хакер в публичната мрежа.

Направете списък с вашите противници или тези, които биха искали да се сдобият с активите ви. В списъка си можете да включите отделни личности, правителствени служби или корпорации.

В зависимост от това, кои са вашите противници, при някои обстоятелства, този списък може да бъде унищожен, след като сте готови с планирането на сигурността си.

Какви ще са последствията в случай на неуспех?

Има много начини, чрез които противник може да получи достъп до вашите данни. Например, противник може да прочете ваша лична комуникация, ако влезе в мрежата, но може и да изтрие или повреди данните ви.

Мотивите на противниците могат да бъдат различни, както и тактиките им. Правителство, опитващо се да спре публичното разпространение на видео, показващо полицейско насилие, може просто да го изтрие или да ограничи достъпа до него. И обратно, политически опонент би могъл да осигури достъп до тайно съдържание и да го публикува, без вашето знание.

Планирането на сигурността изисква разбиране на това, колко лоши могат да бъдат последствията, ако противник получи достъп до някой от вашите активи. За да установите това, трябва да сте наясно с възможностите на вашите противници. Например, вашият доставчик на мобилни услуги има достъп до всички ваши телефонни обаждания. Хакер в свободна Wi-Fi мрежа може да достигне до вашата нешифрована комуникация. Правителството обаче може да има много по-големи възможности.

Напишете, за какво вашите противници биха искали да използват личните ви данни.

Колко вероятно е да трябва да се защитя?

Риск представлява вероятността, определена заплаха срещу определен актив, действително да възникне. Тя върви ръка за ръка с възможностите, способностите. Все пак, ако вашият доставчик на мобилни услуги има достъпа до цялата ви лична информация, рискът той да я публикува онлайн, за да компрометира репутацията ви е малък.

Важно е да се направи разлика между това, какво може да се случи и вероятността то да се случи. Например, има опасност вашата сграда да се срути, но рискът това да се случи е много по-голям в Сан Франциско (където земетресенията са често явление), отколкото в Стокхолм (където не са).

Оценката на риска е както личен, така и субективен процес. Много хора смятат, че определени заплахи са неприемливи, независимо от вероятността те да се случат, защото самото наличие на заплаха без значение на вероятността не си струва цената. В други случаи, хората пренебрегват сериозни рискове, защото не виждат в заплахата нещо сериозно.

Запишете кои заплахи ще приемете сериозно и кои са твърде редки или безобидни (или твърде трудни за преодоляване), за да се тревожите за тях.

Колко усилия съм готов да положа, за да предотвратя тези последствия?

Няма идеален вариант за сигурност. Всеки човек има различни приоритети, притеснения или достъп до ресурси. Оценката на риска ще ви даде възможност да планирате подходящата за вас стратегия, като балансирате между удобство, разходи и поверителност.

Например адвокат, който представлява клиент по дело, свързано с националната сигурност, може да е готов да положи по-големи усилия за да защити комуникацията си по делото, като например използва шифрована електронна поща, от колкото член на семейството, който редовно изпраща забавни видеоклипове с котета.

Запишете с какви възможности разполагате, за да намалите уникалните за вас заплахи. Отбележете дали имате някакви финансови, технически или социални ограничения.

Планиране на сигурността като редовна практика

Имайте предвид, че вашият план за сигурност може да се променя с промяна на ситуацията. Затова честото му преразглеждане е добра практика.

Създайте свой собствен план за сигурност въз основа на собствената си уникална ситуация. След това отбележете в календара си дата в бъдещето. Това ще ви подтикне да прегледате плана си и да определите дали той все още е адекватен за вашата ситуация.

Credit for translation and localization goes to Journalist Security Fellowship fellows in partnership with Localization Lab.

In partnership with

LOCALIZATION LAB