Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

Хакнаха ме, а сега какво?

Преглед

Знаем, че ви е грижа за защитата на вашия компютър и мобилни устройства и предприемате стъпки за тяхната сигурност. Въпреки това, без значение колко сигурно използвате технологиите, рано или късно може да бъдете хакнати или "компрометирани". В този бюлетин ще се научите как да определите дали вашият компютър или мобилно устройство са били хакнати и ако е така, какво можете да направите за това. В крайна сметка, колкото по-бързо откриете, че нещо не е наред и колкото по-бързо реагирате, толкова по-вероятно е да намалите вредата, която кибер нападателят може да нанесе.

Гост-редактор

Саманта Дейвисън (@sam_e_davison) е мениджър на програмата Информираност по сигурност и образование в компанията „Юбер" (Uber), като образова нейните служители по целия свят в над 350 града.

Признаци, че сте били хакнати

Може да бъде трудно да се определи дали сте били хакнати, тъй като често няма един единствен начин да го разберете. Вместо това, хакерите обикновено оставят няколко улики, които често се наричат показатели. Колкото по-близо вашата система си съвпада с някоя от тези улики, толкова по-вероятно е да е била хакната.

- Антивирусната ви програма е задействала сигнал, че системата ви е заразена; особено ако казва, че не е в състояние да премахне или постави под карантина засегнатите файлове.
- Началната страница на браузъра ви неочаквано се промени или браузърът ви води до уебсайтове, на които не искате да отидете.
- Има нови акаунти на вашия компютър или устройство, които не сте създали, или вървят нови програми, които не сте инсталирали.
- Компютърът или приложенията ви блокират постоянно, има икони за неизвестни приложения или се появяват странни прозорци.
- Програмата ви иска разрешение да направи промени в системата, въпреки че инсталирате или актуализирате някои от вашите приложения.
- Паролата ви вече не работи, когато се опитате да влезете в системата си или в онлайн акаунт, въпреки че знаете, че паролата ви е вярна.
- Приятели ви питат защо им пращате имейли, които знаете, че не сте изпратили.
- Мобилното ви устройство причинява неупълномощени такси към премийни SMS номера.
- Вашето мобилно устройство изведнъж има необяснимо високо потребление на данни или на батерията.

Хакнаха ме, а сега какво?

Как да отвърнем?

Ако смятате, че вашият компютър или устройство са били хакнати, колкото по-скоро отвърнете, толкова по-добре. Ако компютърът или устройството ви са били предоставени от вашия работодател или се използват за работа, не се опитвайте да отстраните проблема сами. Не само може да причините повече вреда, отколкото полза, но можете и да унищожите ценни доказателства, които могат да се използват за разследване. Вместо това, докладвайте за инцидента на работодателя си веднага, обикновено като се свържете с отдела за помощ, екипа за сигурност или ваш ръководител. Ако по някаква причина не можете да се свържете с вашата организация, или сте загрижени за закъснение, изключете своя компютър или устройство от мрежата и след това го поставете в заспало състояние, самолетен режим или режим за съхраняване на батерията. Дори и да не сте сигурни дали сте бил хакнати, далеч по-добре е да докладвате сега за всеки случай. Ако компютърът или устройството са ваши собствени, за лична употреба, ето няколко стъпки, които можете да предприемете.

Рано или късно компютърът или устройството ви могат да бъдат компрометирани. Колкото по-бързо откриете инцидента и колкото по-бързо реагирате, толкова по-добре.

- **Смяна на паролите**. Това включва не само смяна на паролите за вашите компютри и мобилни устройства, а за всичките ви онлайн сметки. Уверете се, че не използвате хакнат компютър да променяте паролите. Вместо това, използвайте друг компютър или устройство, които знаете, че са сигурни, за да променяте паролите.
- **Анти-вирусен софтуер**. Ако вашият антивирусен софтуер ви информира за заразен файл, можете да следвате действията, които той препоръчва. Това обикновено може да включва поставяне на файла под карантина, почистване на файла или изтриване на файла. Повечето антивирусни софтуери имат връзки, които можете да последвате, за да научите повече за конкретното заразяване. В случай на съмнение, поставете файла под карантина. Ако това не е възможно, изтрийте го.
- **Възстановяване**. Ако не сте в състояние да оправите заразяването или искате да бъдете абсолютно сигурни, че вашата система е оправена, по-сигурен вариант е да възстановите фабричните й настройки. За компютри, следвайте инструкциите на производителя на вашата система. В повечето случаи това ще означава да преинсталирате операционната система, като използвате вградените инструменти. Ако тези инструменти са изчезнали, повредени са или са заразени, свържете се с производителя за насоки или посетете сайта му. Не преинсталирайте операционната система от архиви, те могат да имат същите уязвимости, които са позволили на хакера да получи достъп първоначално. Архивите трябва да се използват само за възстановяване на вашите данни. За мобилни устройства следвайте инструкциите от производителя или доставчика на услуги, които би трябвало да бъдат на техния уебсайт. В много случаи това може да бъде проста операция като възстановяване на фабричните настройки на вашето мобилно устройство. Ако се чувствате неудобно с процеса на възстановяване, помислете за използване

Хакнаха ме, а сега какво?

на професионални услуги, за да ви помогнат. Или, ако вашите компютър или устройство са стари, може да бъде по-лесно и по-евтино да купите нови. Най-накрая, след като сте възстановили своя компютър или устройство, или сте купили нови, уверете се, че те са напълно обновени и актуални и активирайте автоматичното актуализиране, когато е възможно.

- **Архивиране**. Най-важната стъпка, която можете да предприемете, за да защитите себе си е да се подготвите с редовни резервни копия. Колкото по-често архивирате, толкова по-добре. Някои решения автоматично архивират всички нови или променени файлове на всеки час. Независимо кое решение за архивиране използвате, периодично проверявайте дали сте в състояние да възстановите тези файлове. Доста често възстановяването на данни от архив е единственият начин, по който можете да се възстановите от това, че сте били хакнати
- **Отнасяне до властите**: Ако се чувствате по някакъв начин застрашени, докладвайте за инцидента на местната полиция.

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

Архиви:	https://securingthehuman.sans.org/ouch/2015#august2015
Пароли:	https://securingthehuman.sans.org/ouch/2015#april2015
Какво е „зловреден софтуер”:	https://securingthehuman.sans.org/ouch/2016#march2016
Сигурност на новия ви таблет:	https://securingthehuman.sans.org/ouch/2016#january2016

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