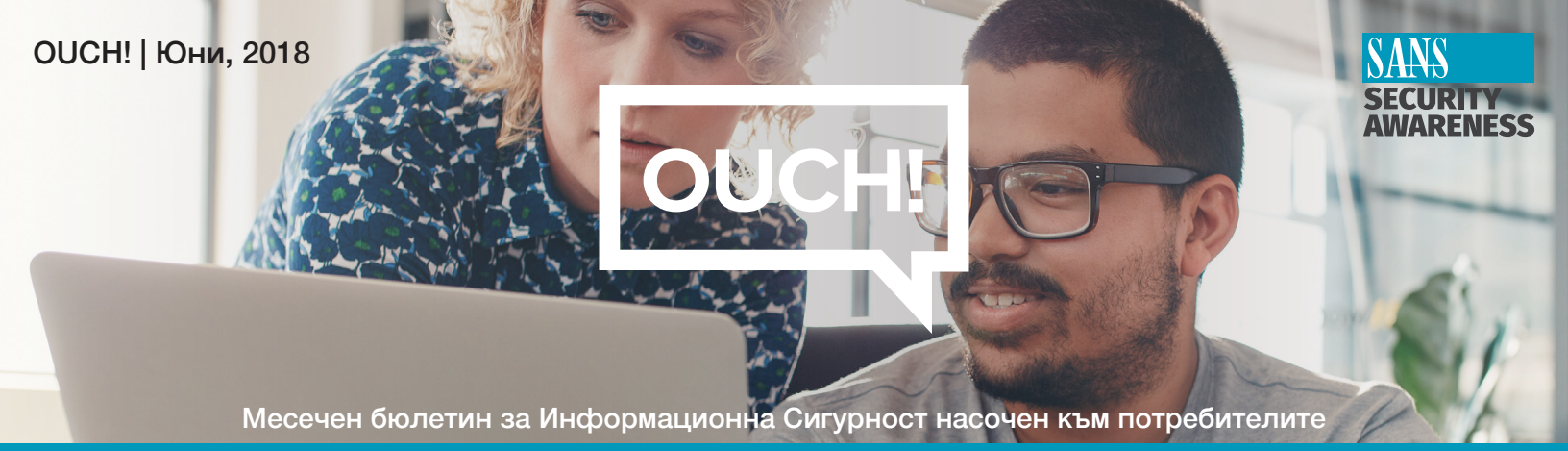

Месечен бюлетин за Информационна Сигурност насочен към потребителите

Спрете тези вируси

Преглед

Може би сте чували за термини като вирус, троянски кон или рууткит в разговори на тема киберсигурност. Това с различни видове зловредни програми, или malware, които кибер престъпниците използват за да заразят компютри и устройства. Веднъж инсталирани, те могат да правят практически всичко. Научете какво е зловреден софтуер, какви са опасностите свързани с него, и най-важното – какво можете да направите, за да се предпазите от тях.

Какво е зловредна програма?

Най-просто казано, зловредната програма е софтуер – компютърна програма, използвана за престъпни дейности. Този термин е комбинация от 2 думи - malicious (зловреден) и software (софтуер). Кибер престъпниците ги инсталират на компютрите и устройствата, за да могат да ги контролират. Веднъж инсталиран, типичната зловредна програма позволява да се наблюдават действията ви докато сте онлайн, да се откраднат пароли или файлове, или да се използва системата, за да се атакуват други устройства. Такава програма може дори да поеме контрол над файловете ви, изисквайки откуп, за да си ги получите обратно. Много хора смятат, че това е проблем само при Windows-базирани компютри. За съжаление всяко устройство може да бъде инфектирано, от Мак компютри и смартфони до устройства за видеозаписи и охранителни камери. До колкото повече компютри и устройства престъпниците получат достъп, толкова повече пари могат да спечелят. Следователно всеки е мишена, включително вие самите.

Защитете се – спрете зловредния софтуер

Може би си мислите, че всичко, което трябва да направите е да инсталирате програма за сигурност - например антивирусен софтуер – и това ви предпазва от инфектиране. За съжаление, антивирусните програми не могат да предпазят от всичко. Кибер престъпниците постоянно изработват нови и по-съвършени зловредни програми. В отговор, разработчиците на антивирусен софтуер постоянно обновяват продуктите си с нови възможности да откриват такива програми. Това се е превърнало в състезание, в което лошите обикновено са винаги една крачка напред. Тъй като не може да разчитате само на антивирусната си програма, ето няколко стъпки, които можете да предприемете, за да се предпазите:

Кибер престъпниците често заразяват компютри или устройства, като се възползват от уязвимост в софтуера ви. Колкото по-нов е софтуера ви, толкова по-малко уязвимости имат системите ви и толкова по-трудно е за кибер престъпниците да ги инфектират. Уверете се, че операционната система, приложенията, уеб браузърите и добавките към тях, както и устройствата, са винаги обновени. Най-лесният начин за това е да се включи автоматичното обновяване, където е възможно.

Популярен начин за инфектиране на компютри и устройства е създаването на фалшиви програми или мобилни приложения, публикуването им в Интернет, и после да ви убедят да ги изтеглите и инсталирате. Ползвайте програми и приложения само от доверени онлайн източници. Също така избягвайте мобилни приложения, които са скоро публикувани, имат малко положителни отзиви, рядко биват обновявани, или са изтеглени от малък брой хора. Вече не ползвате някоя програма или приложение? Изтрийте ги.

Кибер престъпниците често подмамват хората да инсталират зловреден софтуер вместо тях. Например, те могат да ви изпратят имейл, който изглежда убедително и съдържа връзка или прикачен файл. Възможно е имейла да изглежда така, сякаш е изпратен от банката ви или от приятел. Ако обаче отворите файла или щракнете на връзката, вероятно бихте активирали процес, който инсталира зловреден софтуер на системата ви. Ако едно съобщение се опитва да създаде усещане за спешност, или изглежда твърде добре, за да е истина, твърде вероятно е да е атака. Бъдете подозрителни, здравият разум е често най-добрата ви защита.

Архивирайте често системата и файловете си в облачна услуга за съхранение, или ги съхранявайте на външно устройство, което не е постоянно включено в компютъра, като например външен твърд диск. Това предпазва архивните ви копия в случай на опит те да бъдат криптирани или изтрити. Архивите са изключително важни, те са често единственият начин да възстановите всичко след инфектиране.

В обобщение, най-добрият начин да се защитите от зловредни програми е да поддържате софтуера и устройствата си обновени, инсталирате доверен антивирусен софтуер където е възможно, и да сте нащрек за опити да ви подмамят да инфектирате собствената си система. Когато всичко друго се провали, архивните копия са често единственият начин да се възстановите от инфектиране.

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

Гост-редактор

Лени Зелцер се бори с вирусите чрез създадени от него продукти в Minerva Labs и преподавайки в SANS Institute. Лени е активен в Туитър като @lennyzeltser и пише блог за сигурността на zeltser.com.

Ресурси

Софтуерно изнудване:	https://www.sans.org/u/EdI
Архивиране:	https://www.sans.org/u/EdN
Спрете този фишинг:	https://www.sans.org/u/EdS

OUCH! се публикува от SANS Security Awareness и се разпространява под лиценза на Creative Commons BY-NC-ND 4.0. *Имате право да разпространявате този бюлетин или да го използвате във вашата информационна кампания, при условие че не го модифицирате. За преводи или повече информация моля пишете на* www.sans.org/security-awareness/ouch-newsletter. *Редакторски колектив: Уолт Scrivens, Фил Хофман, Кати Кликнете, Черил Конли | Превод: Николай Дачев и Радослава Несторова*