Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

- Преглед
- Обновявания
- Архивиране
- „Фишинг“

Уроците от WannaCry

Преглед

Най-вероятно неотдавна сте наблюдавали огромното медийно покритие на нова кибер атака, наречена “WannaCry”. “WannaCry” зарази над 200 000 компютъра, като блокира данните на различни организации, включително болници в Обединеното кралство. Има няколко причини тази атака да получи толкова голямо внимание. Първо, тя се разпространява бързо от компютър на компютър, като използва известна слабост в компютрите с Windows. На второ място, атаката беше вид злонамерен софтуер, наречен “Ransomware” („софтуер за откуп“), което означава, че след като зарази компютъра ви, той криптира всичките ви файлове и блокира достъпа ви до вашите данни. Единственият начин да възстановите данните си е от резервни копия или като заплатите на атакуващия 300 долара откуп за декриптиране на всичките ви данни. Третото, и най-важно е, че тази атака не трябваше да е възможна. Слабостта “WannaCry”, която атакува компютрите с Windows, беше добре известна на Microsoft, които пуснаха корекция няколко месеца по-рано. Но много организации не бяха успели да инсталират коригиращото обновяване или все още използват операционни системи като Windows XP, които са толкова стари, че вече не се правят коригиращи обновявания за тях. Ето три прости стъпки, които можете да предприемете, за да сте сигурни, че атаки като “WannaCry” никога няма да ви заразят.

Гост-редактор

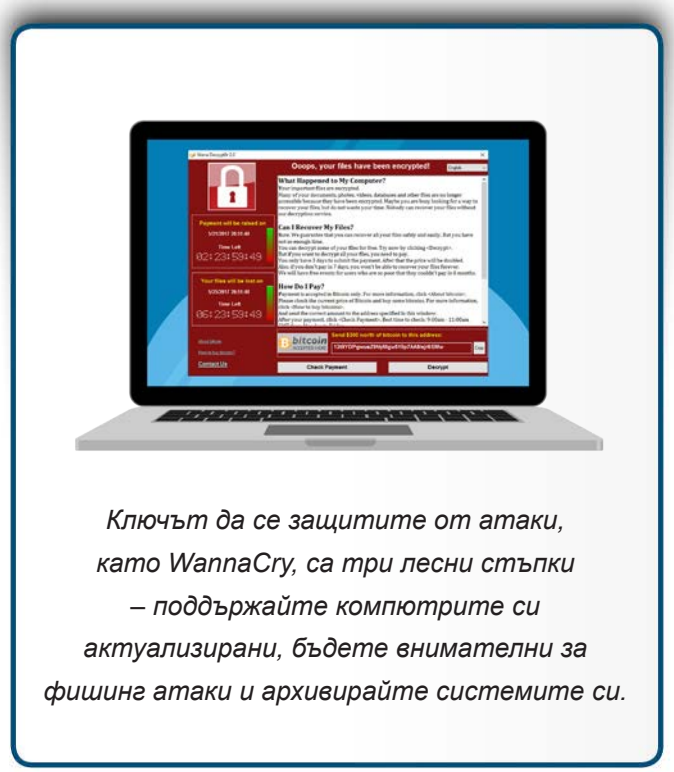
Д-р Йоханес Улрих е декан на отдела по проучвания на Технологическия институт SANS и основател на DShield.org. Той отговаря за **SANS Internet Storm Center**, който наблюдава настоящите заплахи за кибернетичната сигурност. Той преподава Сигурност на уеб приложенията (**DEV522**), Откриване на пробивите (**SEC503**) и IPv6 (**SEC546**).

Обновявания

Първо и преди всичко се уверете, че вашите компютри, мобилни устройства, приложения и всичко останало, свързано с Интернет, са актуализирани. Киберпрестъпниците постоянно търсят нови уязвимости в софтуера, който устройствата използват. Когато открият уязвимости, те използват специални програми, за да проникнат в устройствата, които използвате. Междувременно компаниите, създали софтуера за вашите устройства, работят усилено за премахване на тези уязвимости, като публикуват актуализации. Като инсталирате тези актуализации на своите компютри и мобилни устройства, ще направите много по-трудно някой да ви хакне. Точно това е толкова разочароващото относно разпространението на WannaCry. Актуализациите за коригиране и спиране на тази атака бяха пуснати почти два месеца по-рано от Microsoft. Ако организациите поддържаха компютрите си актуализирани, тази атака никога нямаше да проработи. За да сте сигурни, че устройствата са винаги актуални, активирайте автоматичното им обновяване винаги, когато е възможно. Това правило важи за почти всяка технология, свързана

Уроците от WannaCry

към мрежа, а не само за компютри и мобилни устройства - за телевизори, свързани с Интернет, за домашни рутери, за конзоли за игри или може би един ден дори за вашата кола. Ако вашите операционни системи или устройства са толкова стари, че вече не се поддържат с актуализации за защита, като например Windows XP, заменете ги с нови, които се поддържат.



Ключът да се защитите от атаки, като WannaCry, са три лесни стъпки – поддържайте компютрите си актуализирани, бъдете внимателни за фишинг атаки и архивирайте системите си.

Архивиране

В някои случаи кибер атаките като “Ransomware” дори могат да заразят съвременните системи. Вторият начин да се защитите е да архивирате данните си. Архивите са копия на вашата информация, съхранени някъде другаде, вместо на вашия компютър или мобилно устройство. Когато загубите ценни данни, можете да ги възстановите от архивите си. За съжаление, твърде много хора не успяват да правят редовни архивни копия, въпреки че са прости и евтини. Има два начина да направите резервно копие на данните си: физически носител или хранилище в облак. Всеки подход има предимства и недостатъци. Можете да използвате и двата подхода едновременно, ако не сте сигурни кой метод да използвате.

Физическите носители са устройства, които контролирате, като външни USB устройства или мрежови устройства, разположени във вашия дом или офис. Предимството да използвате собствените си физически носители е, че ви позволяват да архивирате и възстановявате големи количества данни много бързо. Недостатъкът на такъв подход е, че ако се заразите със злонамерен софтуер, като “Ransomware”, е възможно инфекцията да се разпространи в архивите ви. Ако използвате физически носители за архивиране, трябва да съхранявате допълнителни копия на архива извън обекта на сигурно място. Уверете се, че всички резервни копия, които съхранявате, са правилно етикетирани. Решенията, базирани на облак, са онлайн услуги, които архивират и съхраняват вашите файлове в Интернет. Обикновено инсталирате програма на компютъра си, която се грижи за всичко. Предимствата на облачните решения е тяхната простота. Освен това, ако се заразите с “Ransomware”, обикновено инфекцията няма достъп до архивите ви, базирани на облак. Недостатъците са, че може да отнеме много време, за да архивирате или да възстановите много големи количества данни. Не забравяйте да изследвате поверителността и сигурността на облачните архиви. Дали услугата за архивиране предоставя силна защита, като например криптиране на данните ви и добро ниво на удостоверяване?

Уроците от WannaCry

„Фишинг“

И накрая, злосторниците винаги актуализират и променят методите си на атака. Кибер престъпниците често използват друг метод за нападение, наречен “Фишинг”, за да атакуват и заразяват жертвите. Фишингът е, когато кибер престъпниците ви изпратят имейл, опитвайки се да ви подмамят да отворите заразен прикачен файл или да посетите злонамерен уебсайт. Ако го направите, компютърът ви може да се зарази.

Въпреки че WannaCry не го използва, този метод обикновено е избора за много други видове атаки, включително повечето видове “Ransomware”. Освен това кибер престъпниците, които са направили WannaCry, без съмнение ще актуализират методите си на атака през следващите месеци и ще използват нови техники, като например фишинг, за да заразят още повече компютри. Ключът да се предпазите от такива атаки по имейл е здравия разум. Ако имейл или съобщение изглежда странно, подозрително или прекалено хубаво, за да е истина, най-вероятно е атака.

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 securingthehuman.sans.org/ouch/archives.

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

Какво е „злонамерен софтуер“:	https://securingthehuman.sans.org/ouch/2016#march2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
Архивиране:	https://securingthehuman.sans.org/ouch/2015#august2015
Фишинг:	https://securingthehuman.sans.org/ouch/2015#december2015
Използване на облака безопасно:	https://securingthehuman.sans.org/ouch/2016#november2016

Редакторски колектив: Бил Уайман, Уолт Scrivens, Фил Хофман, Кати Кликнете, Черил Конли
Превод: Николай Дачев и Радослава Несторова

