**Шта је 'WannaCry'?**

'WannaCry' је тип малициозног софтвера познат као '*Ransomware',* који систем на вашем рачунару чини неупотребљивим, а податке недоступним, (наводно) све до момента док жртва не плати откуп.

**Шта можете учинити да заштитите свој рачунар?**

У циљу заштите својих података и система на рачунару, постоје три ствари које би требало да урадите:

1. **Update Windows – ажурирање оперативног система**

'*WannaCry'* врши напад искључиво на рачунаре који користе Microsoft Windows оперативне системе, који немају инсталиране последње препоручене 'Закрпе', односно '*Patch'*-еве, од стране Microsoft-а. Корисници који имају инсталиране верзије оперативног система: Windows 7, Windows 8, Windows 8.1 и Windows 10, а на својим рачунарима имају укључену опцију аутоматског ажурирања, би требало да су већ заштићени од '*WannaCry'* типа малициозног софтвера.
Уколико опција аутоматског ажурирања није укључена на вашем рачунару, покрените: Windows Update примените све препоручене кораке ажурирања.
Уколико сте корисник Windows XP, Windows Vista, или неке старије верзије Windows оперативног система, предлажемо вам да посетите званичну страницу Microsoft-а, за одговарајућа ажурирања: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

2. **Покрените Антивирус**

Проверите да ли је ваш Антивирус укључен и да ли је ажуриран. Windows је креирао алат за заштиту од *malware*-а (Microsoft Defender), која је одговарајућа за ову намену.
Потребно је да скенирате целокупни саджај вашег рачунара, како би утврдили да се у њему не налазе познате верзије малициозног софтвера.

**3. Креирајте '*Backup*', односно копију свих важних фајлова (JPG,PDF, Word и сл.) који су од великог значаја**

Креирајте '*Backup'*, односно копију свих важних фајлова, који су од великог значаја као нпр. слике, документа, односно копију оних фајлова, који не могу бити поново креирани.
Копију ваших битних података чувајте одвојено од вашег рачунара, односно немојте носаче тих података држати укључене у ваш рачунар (уколико је у питању USB, или посебан Hard Disk – Handy Drive). У супротном, ако је носач података прикључен на ваш рачунар и он ће бити подложан нападу малициозног софтвера.

Сугестија је коришћење *'Cloud'* сервиса за 'Backup' података (креирање резервне копије). Многи провајдери *'Cloud'* сервиса нуде потпуно бесплатно одређену количину простора на својим *'Cloud'* сервисима.

**Шта треба учинити ако је ваш рачунар заражен оваквим малициозним софтвером?**

Препорука је да се обратите Националном ЦЕРТ-у, који се налази на Интернет страници www.cert.rs, и пријавите инцидент.
Уколико је у питању мања компанија, поред пријаве Националном ЦЕРТ-у, неопходно је урадити следеће:

1. Одмах искључите свој рачунар, или мобилни уређај из постојеће мреже и искључите свој Wi-Fi,
2. Пажљиво форматирајте, или замените своје драјвере на диску,
3. Док сте искључени из мреже своје компаније, директно се прикључите на интернет са свог рачунара, или мобилног уређаја,
4. Инсталирајте и ажурирајте свој оперативни систем и остале софтвере које сте користили,
5. Инсталирајте, ажурирајте и покрените ваш антивирусни софтвер који користите,
6. Поново се прикључите на мрежу ваше компаније,
7. Испратите мрежни саобраћај на вашем рачунару и/или покрените свој антивирусни софтвер, у циљу евентуалног детектовања преосталог зараженог дела вашег рачунарског система.

Напомена: Енкриптоване фајлове на вашем рачунару, или мобилном уређају, могу оспособити искључиво они који су извршили напад на ваш рачунар.

**Да ли платити суму новца којом сте уцењени од стране нападача?**

Национални ЦЕРТ не препоручује исплату суме, којом вас уцењују нападачи.
Уколико се ипак одлучите да платите износ уцене, требало би да обратите пажњу на следеће:

1. Нема гаранција да ће вам нападачи вратити податке, које су напали овим малициозним софтвером,
2. У вашем рачунару ће и даље постојати малициозни софтвер, све док не поступите по наведеним препорукама (7 наведених корака за оспособљавање рачунара за даљи рад на мрежи),
3. Новац уплаћујете криминалним групама.

Извор: The National Cyber Security Centre (https://www.ncsc.gov.uk/)