‘WannaCry’ (Ransomware) vodič za kućne računare i korisnike u manjim kompanijama

Šta je ‘*WannaCry*’?

‘*WannaCry’* je tip malicioznog softvera poznat kao ‘*Ransomware’,* koji sistem na vašem računaru čini neupotrebljivim, a podatke nedostupnim, (navodno) sve do momenta dok žrtva ne plati otkup.

Šta možete učiniti da zaštitite svoj računar?

U cilju zaštite svojih podataka i sistema na računaru, postoje tri stvari koje bi trebalo da uradite:

1. Update Windows – ažuriranje operativnog sistema

‘*WannaCry’* vrši napad isključivo na računare koji koriste Microsoft Windows operativne sisteme, koji nemaju instalirane poslednje preporučene ‘Zakrpe’ odnosno ‘*Patch’*-eve, od strane Microsoft-a. Korisnici koji imaju instalirane verzije operativnog sistema: Windows 7, Windows 8, Windows 8.1 i Windows 10, a na svojim računarima imaju uključenu opciju automatskog ažuriranja, bi trebalo da su već zaštićeni od ‘*WannaCry’* tipa malicioznog softvera.
Ukoliko opcija automatskog ažuriranja nije uključena na vašem računaru, pokrenite: Windows Update i primenite sve preporučene korake ažuriranja.
Ukoliko ste korisnik Windows XP, Windows Vista, ili neke starije verzije Windows operativnog sistema, predlažemo vam da posetite zvaničnu stranicu Microsoft-a za odgovarajuća ažuriranja: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

2. Pokrenite Antivirus

Proverite da li je vaš antivirus softver uključen i da li je ažuriran. Windows je kreirao alat za zaštitu od *malware*-a (Microsoft Defender) koja je odgovarajuća za ovu namenu.
Potrebno je da skenirate celokupni sadržaj vašeg računara, kako bi utvrdili da se u njemu ne nalaze poznate verzije malicioznih softvera.

3. Kreirajte *‘Backup’,* odnosno rezervnu kopiju, svih fajlova (JPG,PDF I sl.) koji su od velikog značaja

Kreirajte *‘Backup’,* odnosno rezervnu kopiju,svih fajlova, koji su od velikog značaja, kao npr. Slike, Dokumenta, odnosno kopiju onih fajlova, koji ne mogu biti ponovo kreirani.
Rezervnu kopiju vaših bitnih podataka čuvajte odvojeno od vašeg računara, odnosno nemojte nosače tih podataka držati uključene u vaš računar (ukoliko je u pitanju USB, ili poseban Hard Disk – Handy Drive). U suprotnom, ako je nosač podataka priključen za računar i on će biti podložan napadu malicioznog softvera.

Sugestija je korišćenje ‘*Cloud’* servisa za ‘*Backup’* podataka (rezervnu kopiju). Mnogi provajderi ‘Cloud’ servisa nude potpuno besplatno određenu količinu prostora na svojim ‘*Cloud’* servisima.

Šta treba učiniti ako je vaš računar zaražen ovakvim malicioznim softverom?

Preporuka je da se obratite Nacionalnom CERT-u, koji se nalazi na Internet stranici www.cert.rs i prijavite incident.

Ukoliko je u pitanju manja kompanija, pored prijave incidenta Nacionalnom CERT-u, neophodno je uraditi i sledeće:

1. Odmah isključite svoj računar, ili mobilni uređaj iz postojeće mreže I isključite svoj Wi-Fi,
2. Pažljivo formatirajte, ili zamenite svoje drajvere na disku,
3. Dok ste isključeni iz mreže svoje kompanije, direktno se priključite na Internet sa svog računara,
4. Instalirajte i ažurirajte svoj operativni sistem i ostale softvere koje ste koristili,
5. Instalirajte, ažurirajte i pokrenite vaš antivirusni softver koji koristite,
6. Ponovo se priključite na mrežu vaše kompanije,
7. Ispratite mrežni saobraćaj na vašem računaru i/ili pokrenite svoj antivirusni softver, u cilju eventualnog detektovanja preostalog zaraženog dela vašeg računarskog sistema.

Napomena: Enkriptovane fajlove na vašem računaru, mogu osposobiti isključivo oni koji su izvršili napad na vaš računar.

Da li platiti sumu novca kojom ste ucenjeni od strane napadača?

Nacionalni CERT ne preporučuje isplatu sume kojom vas ucenjuju napadači.
Ukoliko se ipak odlučite da platite iznos ucene, trebalo bi da obratite pažnju na sledeće:

1. Nema garancija da će vam napadači vratiti podatke, koje su napali ovim malicioznim softevrom,
2. U vašem računaru će i dalje postojati maliciozni softver, sve dok ne postupite po navedenim preporukama (7 navedenih koraka za osposobljavanje računara za dalji rad na mreži),
3. Novac uplaćujete kriminalnim grupama.

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