Zavod za sigurnost informacijskih sustava intenzivno prati razvoj nove vrste računalne ugroze koja se tijekom petka, 12. svibnja proširila diljem svijeta, a poznata je pod nazivom Wanna Decryptor, Wannacry ili Wcry. Radi se o samoreplicirajućem računalnom virusu čija je osnovna zadaća kriptiranje podataka koji se nalaze na zaraženom računalu.

Zavod za sigurnost informacijskih sustava intenzivno prati razvoj nove vrste računalne ugroze koja se tijekom petka, 12. svibnja proširila diljem svijeta, a poznata je pod nazivom Wanna Decryptor, Wannacry ili Wcry. Radi se o samoreplicirajućem računalnom virusu čija je osnovna zadaća kriptiranje podataka koji se nalaze na zaraženom računalu.

Kao način širenja Wcry iskorištava ranjivost MS17-010 te korištenjem EternalBlue/DoublePulsar alata ostvaruje pristup na ciljana računala. Također, postoji mogućnost da se u svrhu zaraze ciljanih računala odnosno informacijskih sustava koristi i phishing metoda na način da se ciljanom korisniku isporuči poruka elektroničke pošte sa zaraženim privitkom čijim se otvaranjem pokreće izvršavanje zlonamjernog koda.

Popis sustava koji su podložni ovoj vrsti napada je sljedeći:

• Microsoft Windows Vista SP2

• Windows Server 2008 SP2 i R2 SP1

• Windows 7

• Windows 8.1

• Windows RT 8.1

• Windows Server 2012 i R2

• Windows 10

• Windows Server 2016.

Preporuke za sve korisnike ranjivih sustava su sljedeće:

Provesti hitnu nadogradnju svih ranjivih sustava primjenom zakrpe za operacijski sustav s oznakom MS17-010 (KB4013389). Zbog visoke kritičnosti ranjivosti, Microsoft je izdao zakrpe i za nepodržane operacijske sustave (Windows XP SP2 i Windows Server 2003). Više informacija o zakrpi i ranjivosti prisutno je na stranicama proizvođača:

1. https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

2.https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Ako primjena zakrpe nije moguća, onemogućiti SMBv1 protokol prateći sljedeću proceduru (ovisno o inačici operacijskog sustava):

Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8 i Windows Server 2012:

1. sc.exe config lanmanworkstation depend=bowser/mrxsmb20/nsi

2. sc.exe config mrxsmb10 start=disabled

Windows 8.1, Windows Server 2012 R2 i noviji:

1. Radne stanice: Odabir opcije *Control Panel -> Programs ->Turn Windows features on or off*

Poslužitelji: Odabir opcije *Server Manager -> Manage -> Remove Roles and Features*

2. Onemogućavanje opcije *SMB1.0/CIFS File Sharing Support*

3. Ponovno pokrenuti računalo

Sustave koji nemaju administrativnu podršku, mogućnost nadogradnje ili postoji eksplicitna potreba za SMB protokolom verzije 1 potrebno je ukloniti iz računalne mreže

Onemogućiti komunikaciju prema TCP mrežnim portovima 139 i 445 TCP u računalnoj mreži organizacije. Blokiranje mrežnog prometa prema spomenutim mrežnim portovima može imati štetan utjecaj na uobičajeni rad ostalih sustava u informacijskom sustavu!

Ažurirati antivirusne definicije na najnoviju inačicu.

S iznimnim oprezom pregledavati primljene poruke elektroničke pošte. Prema dostupnim informacijama, jedan od vektora zaraze je poruka elektroničke pošte koja u privitku sadržava PDF datoteku s poveznicom na kompromitiranu web stranicu ili se poveznica na kompromitiranu stranicu nalazi u samom tijelu poruke elektroničke pošte. U oba slučaja, poveznica dohvaća zlonamjernu HTA datoteku kojom počinje zaraza sustava i daljnje širenje zlonamjernog programa po računalnoj mreži.U slučaju primitka sumnjive poruke elektroničke pošte koja sadržava gornja obilježja, potrebno je obavijestiti odgovorne osobe unutar organizacije.

Osigurati postojanje sigurnosne kopije sustava (backup) koja je pohranjena na siguran način, izvan računalne mreže (offline).