CENTER FOR CYBERSIKKERHED

Vejledning

Ransomware-angrebet WannaCry – fjernelse af malware

Indledning

Center for Cybersikkerhed udgav i maj 2016 publikationen "Reducer risikoen for ransomware", hvor centeret giver en række anbefalinger til, hvorledes en organisation kan beskytte sig i mod disse angreb, og hvorledes man forholder sig, hvis organisationen er blevet ramt. På baggrund af det aktuelle ransomware-angreb baseret på WannaCry, vil Center for Cybersikkerhed fremhæve en række vigtige detaljer vedrørende dette angreb samt genopfriske væsentlige aspekter i forsvaret mod netop denne type angreb.

WannaCry fakta:

WannaCry er ransomware, som er i stand til automatisk at kryptere udvalgte filtyper på ofrets computer, slette originalerne og opkræve en løsesum for at dekryptere filerne igen. WannaCry er i stand til både at sprede sig på lokalnetværket og via internettet ved at udnytte en sårbarhed i SMBv1-protokollen. Denne sårbarhed er også kendt som EternalBlue.

Udover at udnytte EternalBlue-sårbarheden installeres der en bagdør på ofrets computer kaldet DoublePulsar. Bagdøren, som blandt andet kan installeres ved at udnytte EternalBlue, gør det muligt for en angriber at installere yderligere malware på ofrets computer. Bagdøren forbliver på ofrets system, uanset om WannaCry har krypteret filer på computeren eller ej.

Den første version af WannaCry indeholdt en såkaldt "kill switch", som får malwaren til at undlade at kryptere filer, hvis malwaren kan skabe forbindelse til et specifikt domæne. Initielt var dette domæne uregistreret. Kort efter kampagnens udbrud blev det registreret af en sikkerhedskonsulent, hvorfor den første version af WannaCry i visse tilfælde ikke længere krypterer filer. Dog er det fortsat muligt at blive inficeret med bagdøren fra den første WannaCry-version, ligesom ovenstående ikke beskytter mod nye versioner af WannaCry.

Er du blevet ramt?

Umiddelbart kan dette opfattes som et irrelevant spørgsmål, hvis alle ens filer er blevet krypteret, men som nævnt i faktaboksen, så kan den uønskede malware godt ligge på ens systemer, uden at krypteringen er blevet aktiveret.
Kontrol af, om den uønskede malware er installeret på egne systemer kræver en vis viden om operativsystemet, men med en sådan viden kan man lede efter følgende indikatorer på kompromittering (Indicator of Compromise, IOC):

1) Systemet er sandsynligvis kompromitteret, hvis en eller flere filer på systemet har følgende hashværdi (SHA1):
   - 51e4307093f8ca8854359c0ac882ddca427a813c
   - e889544aff85ffaf8b0d0da705105dee7c97fe26

2) Man kan ligeledes kontrollere, om følgende filer er oprettet på systemet:
   - %SystemRoot%\mssecsvc.exe
   - %SystemRoot%\tasksche.exe
   - %SystemRoot%\qeriuwjhrf
   - b.wnry
   - c.wnry
   - f.wnry
   - r.wnry
   - s.wnry
   - t.wnry
   - u.wnry
   - taskdl.exe
   - taskse.exe
   - 00000000.eky
   - 00000000.res
   - 00000000.pky
   - @WanaDecryptor@.exe
   - @Please_Read_Me@.txt
   - m.vbs
   - @WanaDecryptor@.exe.lnk
   - @WanaDecryptor@.bmp
   - 274901494632976.bat
   - Files with ".wnry" extension
   - Files with ".WNCRY" extension

3) En sidste indikation kan søges i operativsystemets "Registry", hvor man skal lede efter følgende nøgle (Key):
   - HKLM\SOFTWARE\WanaCrypt0r\wd……

Anbefalinger hvis man er blevet ramt

Hvis filerne på et eller flere systemer er blevet krypteret som følge af en inficering med WannaCry, anbefaler Center for Cybersikkerhed, at man kontrollerer, om øvrige systemer ligeledes er inficeret, også selvom filerne på disse systemer ikke er blevet krypteret.

Er et system inficeret, uafhængig af om filer er blevet krypteret eller ej, anbefaler Center for Cybersikkerhed, at der foretages en komplet reinstallation af de specifikke systemer (operativsystemer og applikationer). Et forsøg på rensning af systemerne bør absolut ikke overvejes. Årsagen til dette er, at en oprensning efter en inficering med en specifik malware ikke giver nogen garanti for, at systemet er fri for andre former for malware. Mange typer af malware, herunder WannaCry , udgør en risiko for yderligere inficering med andre typer af malware. Dette har Center for Cybersikkerhed har set utallige eksempler på.

Ved indlæsning af konfigurationer og data fra sikkerhedskopier er det afgørende, at disse kopier kontrolleres, således at der ikke sker en geninficering af systemerne. I tilfælde af at systemerne forsat er inficeret, bør man anvende en ældre backupkopi.

Betalingsmodulet i WannaCry-ransomwaren er dårligt implementeret, og betaling af løsesum for at fjerne krypteringen giver på ingen måde sikkerhed for at få adgang til data.

Anbefalinger til fremadrettet tiltag

Baseret på erfaringer i forbindelse med tidligere ransomware-angreb vil Center for Cybersikkerhed fremhæve en række af de anbefalinger, som blev nævnt i publikationen ”Reducer risikoen for ransomware”:

- Det er altafgørende, at der systematisk tages sikkerhedskopier af alle kritiske informationer med en frekvens, der er tilpasset de enkelte informationers kritikalitet.
- Det er endvidere vigtigt, at der regelmæssigt foretages en verifikation af, at sikkerhedskopieringen fungerer efter hensigten.
- Hold samtlige operativsystemer og applikationer opdateret med seneste rettelser, således at systemerne ikke er sårbare over for gamle og kendte problemer. I relation til WannaCry er det specifikt Microsofts patch MS17-010, der er vigtig.
- Gennemfør regelmæssige øvelser og informationskampanger, der sikrer, at alle medarbejdere har en opdateret viden og indarbejdet rutine om sikkerhedsmæssige forhold og risici.
- Hvis organisationen er ramt anbefaler Center for Cybersikkerhed, at man indberetter hændelsen via Center for Cybersikkerheds underretningsordning eller anmelder det til politiet.

Referencer til yderligere informationer

1. **WannaCrypt ransomware worm targets out-of-date systems.** https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
2. **Microsoft Security Bulletin MS17-010 – Critical**. https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

3. **GitHub projekt til at detektere om Double Pulsar er installeret:**
   https://github.com/countercept/doublepulsar-detection-script
4. **Symantec om Double Pulsar:**
   https://www.symantec.com/security_response/writeup.jsp?docid=2017-042122-0603-99&tabid=2
5. **CFCS specifikke trusselvurdering om WannaCry**
   Trusselsvurdering: WannaCry ransomeware kampagne
6. **CFCS vejledning Reducer risikoen for ransomware**
   https://fe-ddis.dk/cfcs/publikationer/Documents/Ransomware_maj2016.pdf