CENTER FOR CYBERSIKKERHED

Dato: 13. maj 2017

Trusselsvurdering: Sårbarhed i Microsoft Windows SMB software udnyttes i ransomware-kampagne, som også har ramt Danmark.

Formålet med denne trusselsvurdering er, at varsle om en global kampagne, hvor ondsindede cyberaktører lige nu forsøger at installere ransomware på Microsoft Windows operativsystemer via en sårbarhed i disse. Tusindevis af computere og servere i Danmark anvender disse operativsystemer.

Hovedvurdering

- Computere med et Microsoft Windows styresystem er lige nu mål for en alvorlig og global ransomware kampagne.
- CFCS har observeret en markant stigning i datatrafik som viser, at danske it-systemer lige nu scannes for sårbare computere, som kan angribes med denne ransomware. CFCS vurderer derfor, at truslen er **MEGET HØJ.**
- CFCS har på nuværende tidspunkt ikke information om, at det er lykkedes at inficere danske virksomheder eller myndigheder.
- Alle Windows-baserede computere, som ikke er opdateret med sikkerhedsopdateringen MS17-010, som Microsoft udsendte den 14. marts 2017, indeholder sårbarheden, som forsøges udnyttet i ransomware-kampagnen.
- Helt usædvanligt har Microsoft også udsendt sikkerhedsopdateringer til de ellers usupporterede Windows XP og Windows Server 2003 operativsystemer, hvilket understreger sårbarhedens alvorlighed.
- CFCS anbefaler alle ejere og administratorer af Windows-baserede computere, at sikre, at disse er opdateret med de seneste sikkerhedsopdateringer fra Microsoft, samt til at være ekstra opmærksomme på e-mails som kan indeholde ransomware.
- CFCS anbefaler ligeledes alle virksomheder og myndigheder til at orientere sig i CFCS's publikation "Reducér risikoen for ransomware".

Analyse

Flere leverandører af anti-virus systemer har siden den 12. maj meldt om en kraftig stigning i forsøg på kompromittering af Windows baserede computere med den såkaldte WanneCry ransomware. Eksempelvis rapporterede Avast på deres blog, at deres anti-virus software alene den 12. maj 2017 havde registreret 57.000 forsøg på inficering. Udover at understrege truslen, så viser dette også vigtigheden af at benytte sig af opdateret anti-virus software, som ofte vil være i stand til at afværge udnyttelsen af kendte sårbarheder i anvendt software.

De cyberkriminelle udnytter en sårbarhed i Windows Server Message Block (SMB), til at installere WannaCry ransomwaren. SMB er en protokol til fildeling, og sårbarheden kan udnyttes ved, at en aktør via internettet sender særligt udformede beskeder til en SMB-server i Windows operativsystemet, hvorved aktøren vil være i stand til at eksekvere kode på den angrebne computer. Når en computer på et netværk først er inficeret, vil den ondsindede kode forsøge at sprede sig til andre computere på netværket, og kryptere de data den finder.

Sårbarheden omfatter alle versioner af Microsoft Windows, og udnyttelse af sårbarheden kan ske uden involvering af brugeren.

WannaCry ransomware, eller andre typer ransomware, kan også inficere en computer eller et netværk, ved at en person trykker på et link, eller åbner et dokument i en e-mail, hvorved malwaren downloades på computeren. Det er uklart, hvorvidt denne metode også anvendes i den igangværende ransomware-kampagne.

Microsoft udsendte den 14. marts 2017, en sikkerhedsopdatering med navnet MS17-010, som fjerner sårbarheden. De fleste private brugere modtager automatisk disse opdateringer via internettet, men virksomheder og myndigheder kan vælge selv at administrere hvornår sådanne opdateringer skal distribueres i deres netværk, hvilket kan medføre, at denne sårbarhed i visse tilfælde endnu ikke er fjernet.

Helt usædvanligt, har Microsoft den 12. maj 2017 valgt at udsende sikkerhedsopdateringer til Windows XP samt Windows Server 2003, som fjerner SMB-sårbarheden fra disse produkter, som ellers ikke er blevet supporteret siden den 14. juli 2015. Mere information om disse sikkerhedsopdateringer kan findes via dette link:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Anbefaling
CFCS anbefaler, alle ejere og administratorer af computere og servere til at sikre, at alle software sikkerhedsopdateringer implementeres løbende, samt at der anvendes anerkendt anti-virus software.

Specifikt for denne trussel skal det sikres, at sikkerhedsopdateringen MS17-010 er implementeret, samt at ældre systemer baseret på Windows XP eller Windows Server 2003, bliver opdateret med de netop udsendte sikkerhedsopdateringer fra Microsoft.

CFCS anbefaler alle myndigheder og virksomheder til at være ekstra opmærksomme på, om der er modtaget e-mails med ransomware i løbet af bededagsferien, og fjerne disse fra mailservere inden medarbejderne møder mandag morgen.

CFCS anbefaler ligeledes, at virksomheder og myndigheder orienterer sig i publikationen "Reducér risikoen for ransomware", som indeholder en række anbefalinger til forebyggelse af ransomware-angreb, og som beskriver hvorledes man skal forholde sig hvis skaden er sket. Publikationen kan findes på centrets hjemmeside: https://fe-ddis.dk/cfcs/Pages/cfcs.aspx

FE bruger denne skala for sandsynlighed i analyser: