CENTER FOR CYBERSIKKERHED

Dato: 1. juni 2017

Trusselsvurdering: Truslen fra hackerværktøjer mod Windows styresystemer

Formålet med denne trusselsvurdering er at varsle om, at brugen af computere med operativsystemerne Windows XP og Windows Server 2003 fortsat medfører en risiko for, at en virksomhed eller myndighed bliver inficeret med malware.

Hovedvurdering

- Det er sandsynligt, at WannaCry ransomware-kampagnen fra maj 2017, vil blive fulgt op af nye kampagner, som vil anvende andre offentliggjorte hackerværktøjer til at inficere gamle og usupporterede Microsoft Windows XP og Server 2003 styresystemer såvel som nyere og fortsat supporterede Microsoft styresystemer op til Windows 10. Kampagnerne vil ikke nødvendigvis være begrænset til cyberkriminalitet i form af ransomware men vil også kunne gennemføres med henblik på cyberspionage eller andre former for cyberangreb
- CFCS anbefaler alle ejere og administratorer af Windows-baserede computere at sikre, at der benytters softwareversioner, som supporteres af Microsoft, samt at softwaren er opdateret med de seneste sikkerhedsopdateringer.
- CFCS anbefaler ligeledes it-sikkerhedsansvarlige i alle virksomheder og myndigheder at holde sig orientere hos softwareleverandører – især Microsoft, i offentlige medier samt fagmedier om eventuelt nye malware-kampagner, således at eventuelle mitigerende foranstaltninger kan iværksættes hurtigst muligt i henhold til deres kritikalitet.
- Hvis en virksomhed er nødsaget til at benytte computere med usupporterede styresystemer, så anbefaler CFCS, at disse computere isoleres fra internettet og det øvrige lokalnet, samt at datatrafik til og fra disse computere kun tillades i forhold til specifikke IP-adresser og porte, ligesom computerne bør være omfattet af en effektiv virusbeskyttelse.

Analyse

Den meget omtalte WannaCry ransomware-kampagnen, som startede omkring den 12. maj i år, har haft begrænset effekt i Danmark.

WannaCry ransomware-kampagnen var blandt andet mulig, fordi en hackergruppe, kendt som Shadow Brokers, den 14. april 2017 offentliggjorde en række hackerværktøjer rettet mod Microsoft Windows styresystemer. I den forbindelse udsendte Center for Cybersikkerhed (CFCS) et varsel om værktøjerne til Netsikkerhedstjenestens kunder og andre samarbejdspartnere.

Et af værktøjerne fra Shadow Brokers, som udnytter en sårbarhed i SMB-protokollen i Microsoft Windows operativsystemer, blev netop benyttet i WannaCry kampagnen. CFCS offentliggjorde under WannaCry kampagnen en trusselsvurdering, som kan ses her: https://fe-ddis.dk/cfcs/nyheder/arkiv/2017/Pages/WannaCryransomewarekampagne.aspx

Selvom WannaCry ransomware-kampagnen ser ud til at være overstået, så vurderer CFCS, at fremtidige malware-kampagner vil kunne benytte hackerværktøjer, som udnytter andre sårbarheder i Microsoft Windows styresystemer, og som endnu ikke er offentliggjorte. Shadow Brokers vil ifølge åbne medier udbyde andre sårbarheder til salg, som potentielt kan udnyttes mod både ældre usupporterede og nyere supporterede Microsoft styresystemer, herunder Windows 10.

Microsoft udsendte den 14. marts 2017 en række sikkerhedsopdateringer til supporterede Windows systemer, som fjerner sårbarhederne, der udnyttes af de nævnte hackerværktøjer. Imidlertid er der stadig virksomheder og myndigheder, som anvender Windows XP og Server 2003 systemer, der ikke længere supporteres. Disse systemer er derfor stadig særligt sårbare overfor fremtidige malware-kampagner.

Anbefaling
CFCS anbefaler alle ejere og administratorer af computere og servere at opdatere deres systemer til supporterede versioner og sikre, at alle software sikkerhedsopdateringer implementeres inden for to dage, samt at der anvendes anerkendt og opdateret anti-virus software.

Bemærk at sårbare computere kan inficeres, selvom de ikke er direkte forbundet til internettet. Dette kan ske når malware, som f.eks. ransomware, spreder sig internt i et lokalt netværk, eller via USB-sticks og andre flytbare datamedier, som anvendes på de sårbare computere.

CFCS opfordrer it-sikkerhedsansvarlige i virksomheder og myndigheder at holde sig orienteret hos softwareleverandøren, i offentlige medier samt i fagmedier om eventuelt nye malware-kampagner, så mitigerende foranstaltninger kan iværksættes hurtigst muligt i henhold til deres kritikalitet.

Hvis en virksomhed eller myndighed er nødsaget til at benytte computere, som indeholder sårbar og usupporteret software, er det muligt at mindske risikoen for inficering. Dette kan blandt andet gøres ved at anvende et eller flere af følgende sikkerhedstiltag:

- Isoler de pågældende computere fra internettet og det øvrige lokalnet.
- Tillad kun datatrafik til og fra specifikke IP-adresser og domæner.
- Bloker for datatrafik til computerporte som ikke specifikt anvendes, herunder de computerporte som kendt malware kommunikerer med.
- Undlad at give medarbejdere mulighed for selv at installere software på computeren, og tillad kun brug af såkaldt whitelistet software, så der er kontrol med hvilken software, som kan aktiveres på computeren.
- Deaktiver funktioner og services, som ikke benyttes, eller som kendt malware udnytter.
- Anvend opdateret virusbeskyttelse
- Undgå brugen af flytbare datamedier, eller scan disse for malware inden de anvendes på de pågældende computere.

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: