Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

Stopp skadevaren

Oversikt

Du har sikkert hørt utrykk som virus, trojaner, løsepengevirus/ransomware, eller rootkit når folk omtaler cybersikkerhet. Alle disse er forskjellige varianter av skadelige programmer, kalt skadevare, som kriminelle bruker for å infisere datamaskiner og mobile enheter. Når skadevaren er installert, kan de kriminelle gjøre hva de vil. Lær deg hva skadevare er, hvilke farer det utgjør, og ikke minst: Hva du kan gjøre for å sikre deg selv mot det.

Hva er skadevare?

Skadevare (kalt malware på engelsk), er programvare – et dataprogram – brukt for å utføre skadelige eller uønskede handlinger. Begrepet er en kombinasjon av ordene skadelig og programvare. Cyberkriminelle installerer skadevare på datamaskiner og enheter for å få kontroll over dem. Når skadevaren er på plass, kan de kriminelle bruke den for å spionere på deg og det du gjør, stjele passord og filer, eller bruke enheten din for å angripe noen andre. Skadevare kan til og med ta kontroll over filene dine, og kreve løsepenger for at du skal få dem tilbake. Mange tror at skadevare kun er et problem for Windows-maskiner. Dessverre er det slik at skadevare kan infisere alle typer enheter, fra Mac-maskiner til smarttelefoner, og til og med hjemmerutere og overvåkingskameraer. Jo flere datamaskiner og enheter de kriminelle får infisert, jo mer penger tjener de. Derfor er alle, inkludert deg, et mål for dem.

Vær sikker – stopp skadevaren

Du tenker kanskje at det eneste du må gjøre for å være sikker er å installere et antivirus-program. Dessverre kan ikke antivirus stoppe all skadevare. Cyberkriminelle utvikler hele tiden ny og mer sofistikert skadevare som kan skjule seg for antivirus-programmer. På sin side oppdaterer antivirus-leverandørene konstant sine produkter med nye muligheter for å oppdage skadevare. På mange måter har det blitt som et våpenkappløp, og skurkene er som regel et steg lenger frem. Fordi antivirus i seg selv ikke er nok, bør du også ta følgende grep for å sikre deg:

Cyberkriminelle infiserer ofte datamaskiner og enheter ved å utnytte sårbarheter i programvare. Jo mer oppdatert programvaren din er, jo færre sårbarheter vil det finnes, og da blir det også vanskeligere for cyberkriminelle å infisere deg. Sørg for at operativsystem, apper, programmer, nettleser og alle utvidelser til nettlesere er oppdatert til nyeste tilgjengelige versjon. Aktiver derfor automatisk oppdatering der det er en mulighet, det er den enkleste metoden.

En annen vanlig metode brukt av cyberkriminelle, er å lage falske programmer for datamaskiner, og falske apper for mobile enheter. Disse legger de ut på nettet, der de prøver å lure deg til å laste ned og installere dem. Last kun ned programmer og apper fra pålitelige kilder og app-butikker. Hold deg også unna apper som her helt nye, har få positive anmeldelser, sjelden oppdateres, eller er lastet ned få ganger. Om du ikke lenger bruker en app eller et program bør du avinstallere det.

Cyberkriminelle lurer ofte folk til å installere skadevaren for dem. For eksempel kan de sende deg en e-post som ser legitim ut, og inneholder et vedlegg eller en link. E-posten ser kanskje ut som den kom fra banken din, eller fra en venn. Men dersom du skulle komme til å åpne vedlegget eller klikke på linken, vil skadelig kode bli aktivert, som installerer skadevare på systemet ditt. Hvis en e-post eller melding skaper en sterk følelse av hastverk, eller hvis det virker for godt til å være sant, så kan det være et angrep. Vær på vakt, sunn fornuft er ditt beste forsvar.

Sørg for at du jevnlig sikkerhetskopierer system og filer til skybaserte tjenester, eller lagrer sikkerhetskopiene på frakoblede eksterne harddisker. På denne måten er sikkerhetskopiene beskyttet dersom skadevare forsøker å kryptere eller slette dem. Sikkerhetskopier er kritiske, ofte er de den eneste løsningen du har for å gjenopprette etter en infeksjon med skadevare. Test også at du kan gjenopprette fra sikkerhetskopien.

Til syvende og sist er det å sørge for å oppdatere, installere pålitelig antivirus, og være på vakt mot forsøk på lureri og svindel, det beste forsvaret mot skadevare. Når alt annet svikter, vil du kunne gjenopprette dersom du har sørget for å sikkerhetskopiere jevnlig.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Gjesteredaktør

Lenny Zeltser *bekjemper skadevare ved å lage sikkerhetsprodukter for endepunkter hos Minerva Labs, og gjennom opplæring ved SANS instituttet. Lenny er aktiv på Twitter som @lennyzeltser, og skriver sikkerhetsblogg på zeltser.com.*

Ressurser

Løsepengevirus:	https://www.sans.org/u/EdI
Sikkerhetskopiering:	https://www.sans.org/u/EdN
Stop fiskingen:	https://www.sans.org/u/EdS