OUCH!

SANS SECURITY AWARENESS

Det månedlige nyhedsbrev om IT-sikkerhed

Stop Malware

Oversigt

Du har sikkert hørt om begreber som virus, trojanske heste, ransomware eller rootkit, når folk taler om IT-sikkerhed. Dette er forskellige typer af ondsindede programmer som kaldes malware, og som IT-kriminelle bruger til at inficere computere og andre enheder. Når de er installeret, kan de gøre hvad de vil. Lær hvad malware er, hvilken fare de udgør, og vigtigst af alt hvad du kan gøre for at beskytte dig selv mod det.

Hvad er malware?

Enkelt sagt er malware et stykke software - et computerprogram - der bruges til at udføre ondsindede handlinger. Udtrykket er en kombination af de engelske ord for ondsindede (malicious) og software. IT-kriminelle installerer malware på dine computere eller enheder for at få kontrol over dem. Når malwaren er installeret, kan den gøre det muligt for kriminelle at spionere på dine onlineaktiviteter, stjæle dine adgangskoder eller filer eller bruge dit system til at angribe andre. Malware kan endda tage kontrol over dine egne filer og kræve, at du betaler en løsesum for at få dem tilbage. Mange mennesker mener, at malware kun er et problem for Windows-computere. Desværre kan malware inficere enhver enhed, fra Mac-computere og smartphones til sikkerhedskameraer. Jo flere computere og enheder IT-kriminelle inficerer, desto flere penge kan de få. Derfor er alle et mål, herunder dig.

Beskyt dig selv - Stop malware

Du tror måske, at alt du skal gøre er at installere et sikkerhedsprogram som antivirusprogrammer, og så er du sikker på ikke at blive smittet. Desværre kan anti-virus ikke stoppe alt malware. IT-kriminelle udvikler konstant nye og mere sofistikerede malware, som kan undgå at blive opdaget. Til gengæld opdaterer antivirus leverandører løbende deres produkter med nye muligheder for at opdage malware. På mange måder er det blevet et våbenkapløb, og de onde er normalt et skridt foran. Da du ikke kan stole på antivirusprogrammer alene, er her yderligere trin, du bør tage for at beskytte dig:

IT-kriminelle inficerer ofte computere eller enheder ved at udnytte sårbarheder i din software. Jo mere opdateret din software er, jo færre sårbarheder har dine systemer, og jo sværere er det for IT-kriminelle at inficere dem. Sørg for, at dine operativsystemer, applikationer, browser og browser plugins og enheder altid er opdateret. Den nemmeste måde at sikre dette på er at slå automatisk opdatering til, hvis det er muligt.

En fælles måde, IT-kriminelle inficerer computere eller mobile enheder, er ved at oprette falske computerprogrammer eller mobil apps, sende dem på internettet og derefter narre dig til at downloade og installere en. Download og installer kun programmer eller apps fra betroede kilder. Hold dig også væk fra mobile apps, der er helt nye, har få positive anmeldelser, opdateres sjældent eller er blevet downloadet af et lille antal mennesker. Hvis der er et computerprogram eller en mobil app du ikke længere bruger bør du slette det.

IT-kriminelle lokker ofte folk til at installere malware for dem. For eksempel kan de sende dig en e-mail, der ser legitim ud, og indeholder en vedhæftet fil eller et link. Måske ligner den en e-mail fra din bank eller en ven. Men hvis du åbner den vedhæftede fil eller klikke på linket, ville du aktivere skadelig kode, der installerer malware på dit system. Hvis en besked skaber en stærk følelse af at det haster, eller synes for godt til at være sandt, kan det være et angreb. Vær mistænksom, sund fornuft er ofte dit bedste forsvar.

Sikkerhedskopier dit system og dine filer regelmæssigt til skybaserede tjenester eller gem dine sikkerhedskopier offline, f.eks. på eksterne drev. Dette beskytter dine sikkerhedskopier, hvis malware forsøger at kryptere eller slette dem. Backups er kritiske, de er ofte den eneste måde, du kan genskabe dine data, hvis du er så uheldig at blive ramt af malware.

I sidste ende er den bedste måde at forsvare sig mod skadelig software på, er at holde al din software og enheder opdateret, installere antivirusprogrammer, når det er muligt, og være opmærksom på alle, der forsøger at narre dig til at inficere dit eget system. Når alt andet fejler, er regelmæssige sikkerhedskopier ofte den eneste måde, du kan gendanne dine data.

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Gæsteredaktør

Lenny Zeltser *bekæmper malware ved at oprette endpoint-sikkerhedsprodukter ved Minerva Labs og undervise ved SANS Institute. Lenny er aktiv på Twitter som* @lennyzeltser og skriver en sikkerhedsblog på zeltser.com.

Hvis du vil vide mere

Ransomware:	https://www.sans.org/u/EdI
Backup og gendannelse:	https://www.sans.org/u/EdN
Stop den "Phish":	https://www.sans.org/u/EdS