OUCH! | August 2016

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Løsepengevirus

Hva er løsepengevirus?

Løsepengevirus (kjent som ransomware på engelsk), er en type skadevare som for tiden aktivt spres på internett, der den er en farlig trussel mot ofrenes filer. Skadevare er programvare – et dataprogram – som brukes for å begå skadelige handlinger. Selv om løsepengevirus kun er en av mange former for skadevare, har det blitt svært vanlig fordi det er så lønnsomt å bruke for kriminelle. Når datamaskinen din blir infisert med løsepengevirus, blir filene dine, og muligens hele harddisken kryptert. Dermed er du enten fullstendig utestengt, eller hindret i å få tilgang til viktige dokumenter, bilder, og andre filer. Skadevaren informerer deg så om at du er nødt til å betale de kriminelle bakmennene en løsesum (derav navnet løsepengevirus) for å få dekryptert filene dine igjen. Som oftest må løsepengene betales i form av digital valuta, som Bitcoin. Løsepengevirus spres på samme måte som mange andre typer skadevare. Den vanligste metoden er å sende en skadelig e-post til offeret, der de kriminelle forsøker å lure deg til å åpne et infisert vedlegg eller klikke på en link som vil ta deg til angriperens nettside.

Gjesteredaktør

Lenny Zeltser har fokus på beskyttelse av kundenes IT-systemer ved NCR Corp, og lærer bort skadevarebekjempelse ved SANS instituttet. Lenny er aktiv på Twitter som **@lennyzeltser**, og har en blogg på **zeltser.com**.

Burde du betale løsesummen?

Dette er et vanskelig spørsmål. Problemet er at jo oftere folk betaler de kriminelle når de blir infisert, jo mer motivert blir de kriminelle til å infisere enda flere. På den annen side kan det være at dette er eneste utvei for å få tilbake filene dine. Men vær oppmerksom på at selv om du betaler løsepengene, er det ingen garanti for at du får filene dine tilbake. Det er kriminelle det er snakk om, kanskje de ikke dekrypterer filene dine. Og selv om de lar deg dekryptere i bytte mot betaling, kan noe annet gå galt under prosessen, eller datamaskinen din kan bli infisert med andre typer skadevare.

Sikkerhetskopier filene dine

Den beste måten å få tilbake filene dine på uten å betale løsepengene, er å gjenopprette dem fra sikkerhetskopier. Selv om du blir infisert med løsepengevirus, kan du med denne metoden renske datamaskinen og gjenopprette filene dine.

Løsepengevirus

Men vær oppmerksom på at dersom sikkerhetskopiene er direkte tilgjengelige fra den infiserte datamaskinen, kan løsepengeviruset slette eller kryptere dem også. Derfor er det viktig å lagre sikkerhetskopiene av filene dine hos pålitelige skytjenester, eller på eksterne harddisker som ikke alltid er tilkoblet datamaskinen. I tillegg finnes det en feil som mange gjør, og det er å anta at sikkerhetskopieringen virker, uten å teste om de faktisk kan bruke det for å gjenopprette filer. Sørg for å gjøre jevnlige tester av at sikkerhetskopieringen virker, og bekreft at du faktisk kan gjenopprette filer du trenger dersom systemet ditt skulle bli infisert med et løsepengevirus. Sikkerhetskopiering er generelt viktig, fordi det gjør deg i stand til å gjenopprette filer også når du sletter dem ved et uhell, eller dersom harddisken din krasjer.

Løsepengevirus er skadevare som kan infisere datamaskinen din, kryptere alle filene på den, og nekte deg tilgang til dem.

Ytterligere beskyttelsestiltak

Du kan også beskytte deg mot løsepengevirus på samme måte som du beskytter deg mot andre typer skadevare: Ikke bli infisert. Start med å finne ut om du har oppdatert antivirus-programvare fra en pålitelig utgiver. Slike verktøy som også noen ganger kalles anti-malware programmer, er spesiallaget for å oppdage og stoppe skadevare. Men anti-virus kan ikke blokkere og fjerne alle skadelige programmer. Cyberkriminelle utvikler hele tiden ny og mer sofistikert skadevare som kan unngå å bli oppdaget. På samme måte oppdaterer konstant anti-virus utgiverne programvaren deres med nye muligheter for å oppdage ny skadevare. På mange måter har det blitt et våpenkappløp, der begge sider forsøker å ta innersvingen på den andre. Dessverre er skurkene som regel ett steg foran, og derfor må du sørge for at du har fungerende sikkerhetskopi, og følger disse ekstra rådene for å beskytte deg selv:

- Ofte infiserer cyberkriminelle datamaskiner og andre enheter ved å utnytte sårbarheter i programvaren. Jo nyere og mer oppdatert programvaren din er, jo færre kjente sårbarheter vil systemet ha, og da blir det også vanskeligere for de kriminelle å infisere det. Derfor bør du sørge for at operativsystemet, applikasjonene og enhetene dine er innstilt til å automatisk installere oppdateringer.
- På datamaskiner bør du bruke en standard brukerkonto med begrensede rettigheter, heller enn en privilegert brukerkonto som “Administrator” eller “root”. Dette øker sikkerheten ved at mange typer skadevare ikke vil klare å installere seg selv.

Løsepengevirus

- Ofte lurer cyberkriminelle folk til å installere skadevare for dem. For eksempel kan det være de sender deg en e-post som virker legitim, og inneholder et vedlegg eller en link. E-posten ser kanskje ut til å komme fra banken din eller en venn. Men, om du åpner vedlegget eller klikker på linken, aktiverer du skadelig kode som installerer skadevaren på systemet. Om en melding skaper en sterk følelse av hast, er forvirrende, virker for god til å være sann, eller har dårlig grammatikk og rettskrivning, kan det være et angrepsforsøk. Vær mistenksom, sunn fornuft er ofte ditt beste forsvar.

Beskytt deg mot løsepengevirus ved å være på vakt ovenfor e-poster med vedlegg og linker, sørge for at du har oppdatert antivirus, og sørg for at filene dine jevnlig blir sikkerhetskopiert og kan gjenopprettes.

Lær mer

Abonner på det månedlige OUCH!-nyhetsbrevet om sikkerhetsbevissthet, se gjennom OUCH!-arkiver, og lær mer om SANS sine løsninger for sikkerhetsbevissthet ved å gå inn på securingthehuman.sans.org/ouch/archives.

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.

Ressurser

Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
Hva er skadevare:	https://securingthehuman.sans.org/ouch/2016#march2016
Kryptering:	https://securingthehuman.sans.org/ouch/2016#june2016
Sikkerhetskopiering:	https://securingthehuman.sans.org/ouch/2015#august2015
Artikkel fra Microsoft:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
SANS FOR610 Course - Reverse Engineering Malware:	https://sans.org/for610

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversatt av: NorSIS