OUCH! | Mars 2016

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- **Hva er skadevare?**
- **Hvem lager skadevare?**
- **Å beskytte seg selv**

Hva er skadevare?

Oversikt

Du har kanskje hørt begreper som virus, trojaner, løsepengevirus eller rootkit når folk diskuterer cybersikkerhet. Alle disse begrepene beskriver det samme, forskjellige typer programvare brukt av kriminelle for å infisere datamaskiner og andre enheter. Et vanlig begrep for å beskrive alle disse forskjellige programmene er ordet skadevare, eller malware på engelsk. I dette nyhetsbrevet skal vi forklare hva skadevare er, hvem som lager det og hvorfor, og viktigst av alt, hva du selv kan gjøre for å beskytte deg mot det.

Gjesteredaktør

Lenny Zeltser fokuserer på å beskytte kunders IT-systemer ved NCR Corp, og underviser i bekjemping av skadevare ved SANS Instituttet. Lenny er aktiv på twitter som **@lennyzeltser**, og blogger om sikkerhet på **zeltser.com**.

Hva er skadevare?

Kort fortalt, skadevare er programvare – et dataprogram – som brukes for å utføre skadelige handlinger. Faktisk er begrepet skadevare en kombinasjon av begrepene skadelig og programvare. Cyberkriminelle installerer skadevare på datamaskiner og andre enheter for å få kontroll over dem, og for å få tilgang til innholdet lagret på dem. Når skadevaren er installert, kan angriperne bruke den til å spionere på nettaktiviteten din, stjele passordene og filene dine, eller bruke systemet ditt til å angripe andre. Skadevare kan til og med nekte deg tilgang til dine egne filer, de blir holdt som gissel til du betaler angriperne en løsepengesum for å få tilbake kontrollen over dem.

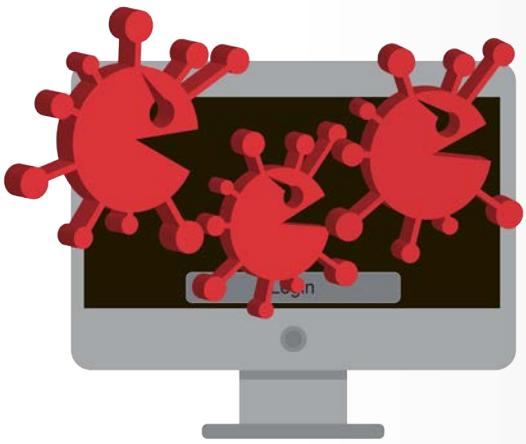
Mange folk tror, feilaktig, at skadevare bare er et problem for brukere av datamaskiner med Windows. Windows er veldig mye brukt og derfor et stort mål, men skadevare kan likevel infisere alle typer enheter, fra Mac-datamaskiner, til smarttelefoner og nettbrett. Jo flere datamaskiner og enheter cyberkriminelle infiserer, jo mer penger kan de tjene. Derfor er alle, inkludert deg, et mål.

Hvem lager skadevare?

Skadevare lages ikke lenger bare av nysgjerrige hobbyprogrammerere og amatørhackere, men også av sofistikerte cyberkriminelle. Målet deres er å tjene penger på din infiserte datamaskin eller enhet, kanskje ved å selge informasjon de har stjålet fra deg, sende spam-eposter, gjennomføre tjenestenektangrep, eller drive utpressing. De som lager, distribuerer og

Hva er skadevare?

tjener på skadevare kan være alt fra individer som handler på egenhånd, til godt organiserte kriminelle grupper, og til og med statlige aktører. Folk som lager nåtidens sofistikerte skadevare er ofte dedikert til akkurat det formålet, de har utvikling av skadevare som en fulltidsjobb. Når de har utviklet skadevaren sin, selger de den ofte videre til andre individer eller organisasjoner, og gir ofte disse «kundene» jevnlige oppdateringer og kundeservice.



Beskytt deg selv mot skadevare ved å være skeptisk ovenfor mistenkelige meldinger, holde enhetene dine oppdatert, og ved å ha oppdatert antivirus installert når det lar seg gjøre.

Å beskytte seg selv

Et vanlig grep for å beskytte seg selv mot skadevare, er å installere antivirus-programvare fra pålitelige utgivere. Slike verktøy er designet for å oppdage og stoppe skadevare. Men antivirus kan ikke blokkere og fjerne alle skadelige programmer. Cyberkriminelle innoverer hele tiden, og utvikler stadig mer sofistikert skadevare som unngår å bli oppdaget. Samtidig jobber antivirus-utgivere konstant for å holde produktene sine oppdatert, slik at de kan oppdage skadevare på stadig nye måter. På mange måter har det blitt som et våpenkappløp der begge sider forsøker å overliste den andre. Dessverre er de kriminelle som oftest et steg foran. Siden antivirus alene ikke er nok, kan du følge disse stegene for å beskytte deg selv:

- Cyberkriminelle utnytter ofte sårbarheter i programvaren på datamaskiner og andre enheter for å få infisert dem med skadevare. Jo mer oppdatert programvaren din er, jo færre sårbarheter vil det være i systemet, og da blir det også vanskeligere for cyberkriminelle å infisere det. Derfor bør du sørge for at operativsystemet ditt, applikasjonene dine og enhetene dine er konfigurert til å oppdatere seg selv automatisk.
- En vanlig metode brukt av cyberkriminelle for å infisere mobile enheter, er å lage en falsk app, legge den ut på internett, og så lure folk til å laste den ned og installere den. Derfor burde du kun laste ned og installere apper fra pålitelige appbutikker. Du burde også kun installere apper som har vært tilgjengelig over lengre tid, har blitt tatt i bruk av mange brukere, og har flere gode anmeldelser.
- På datamaskiner burde du bruke en standard-brukerkonto med begrensede rettigheter istedenfor administrative brukerkontoer som «Administrator» og «root». Dette gir ekstra beskyttelse fordi det hindrer mange typer skadevare i å installere seg selv.
- Cyberkriminelle lurer ofte folk til å installere skadevare selv. For eksempel kan de komme til å sende deg en e-post som ser legitim ut, og inneholder et vedlegg eller en link. Kanskje ser e-posten ut til å ha kommet fra banken din, eller fra en venn. Men hvis du skulle komme til å åpne vedlegget eller klikke på linken, ville du ha aktivert skadelig

Hva er skadevare?

kode som installerer skadevare på systemet ditt. Hvis en henvendelse gir inntrykk av dårlig tid, er forvirrende, eller virker for god til å være sann, kan det være et angrep. Vær skeptisk, sunn fornuft er ofte det beste forsvar.

- Sikkerhetskopier systemet ditt og filene dine jevnlig til skybaserte tjenester, eller lagre dem offline, som på en ekstern harddisk som ikke vanligvis er tilkoblet. Dette vil holde sikkerhetskopiene dine beskyttet i tilfelle skadevare forsøker å kryptere eller slette dem. Sikkerhetskopiering er kritisk, da det ofte er den eneste måten for å komme seg etter et skadevareangrep.

Til syvende og sist er den beste måten for å forsvare seg mot skadevare å holde programvaren sin oppdatert, installere pålitelig antivirus-programvare fra velkjente leverandører, og være på vakt mot ethvert forsøk på å lure deg til å infisere ditt eget system.

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 http://www.securingthehuman.org.

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
Sosial manipulering:	https://securingthehuman.sans.org/ouch/2014#november2014
Sikker bruk av mobilapplikasjoner:	https://securingthehuman.sans.org/ouch/2015#january2015
Slik sikrer du ditt nye nettbrett:	https://securingthehuman.sans.org/ouch/2016#january2016
Sikkerhetskopiering & gjenoppretning:	https://securingthehuman.sans.org/ouch/2015#august2015

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