OUCH! | Februar 2014

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Hva er virus
- Hvem og hvorfor
- Beskytte deg selv

Hva er virus

Oversikt

Du har kanskje hørt om begreper som virus, ormer, trojanere eller rootkit når folk snakker om datasikkerhet. Disse begrepene beskriver programmer brukt av kriminelle for å infisere og ta over datamaskiner og mobile enheter. En samlebetegnelse for alle disse begrepene er malware, eller virus som vi kaller det. I dette nyhetsbrevet vil vi beskrive hva virus er, hvem som utvikler det, hvorfor det utvikles og hva du kan gjøre for å beskytte deg selv.

Gjesteredaktør

Lenny Zeltser fokuserer på å sikre kunders IT operasjoner hos NCR Corp og underviser hvordan man kan bekjempe virus på SANS instituttet. Lenny er aktiv på Twitter som **@lennyzeltser** og har en sikkerhetsblogg på **blog.zeltser.com**.

Hva er virus

Kort fortalt er virus et program, et program som utfører ondsinnete handlinger. Ordet malware er en kombinasjon av ordene malicious(ondsinnet) og software(programvare). En norsk oversettelse er derfor ofte skadevare. Målet til angripere er ofte å installere virus på datamaskinen eller den mobile enheten din. Etter at viruset har blitt installert kan angriperen ta full kontroll over enhetene dine. Mange er av den oppfatningen at virus bare er et problem for maskiner som kjører Windows. Windows er mye brukt og derfor et attraktivt mål, men virus kan infisere hvilken som helst plattform, inkludert mobile enheter, virus mot smarttelefoner og nettbrett øker stadig. Husk også at alle er et mål, også deg, desto flere datamaskiner og enheter kriminelle greier å infisere, desto mer penger kan de tjene. Disse angriperne bryr seg som regel ikke om hvem de infiserer, de vil bare infisere så mange som mulig.

Hvem og hvorfor

Virus blir ikke lenger lagd av amatører eller folk som har dette som en hobby, nå er det sofistikerte kriminelle som vil oppnå et spesifikt mål. Noen vanlige mål er: stjele konfidensiell data, samle inn brukernavn og passord, sende ut søppelpost, utføre tjenestenektangrep, utpressing eller ID-tyveri. Et eksempel er viruset kjent som Cryptolocker, dette viruset ble brukt av kriminelle til å kryptere filene på datamaskinen. Den eneste måten du kunne få tilbake filene, var ved å betale penger til angriperne.

Hva er virus

Menneskene som lager, distribuerer og tjener penger på virus kan variere fra individuelle personer til godt organiserte kriminelle grupper eller statlige organisasjoner. I tillegg, personene som lager dagens sofistikerte virus er ofte veldig dedikerte til det formålet, utvikle virus er deres fulltidsjobb. Etter de har utviklet viruset er det ikke uvanlig at de selger det til andre, inkludert med oppdateringer som kommer underveis og støtte til "kundene" deres. De som kjøper virus tjener penger ved å infisere intetanende offer med dette viruset. Ofte infiserer de mange millioner brukere og skaffer seg stort nettverk av infiserte systemer (dette blir kalt et botnet). Dette nettverket av infiserte maskiner blir som en fjernstyrt hær som bakmennene kan bruke for deres eget formål, eller selge det videre til andre kriminelle.

Den beste måten å beskytte seg mot virus er å sørge for at enhetene er oppdatert, du har oppdatert antivirus, hvis mulig og du er på vakt mot angrep.

Beskytte deg selv

Et vanlig steg for å beskytte din datamaskin og mobile enheter fra virus er å installere antivirus fra en leverandør du stoler på. Antivirus er sikkerhetsprogramvare lagd for å oppdage og stoppe ondsinnet programvare, men antivirus greier ikke å stoppe alle virus. Kriminelle kommer hele tiden opp med nye og mer sofistikerte metoder for å unngå å bli fanget av antivirus, antivirus på sin side oppdaterer hele tiden produktene sine med nye muligheter til å oppdage virus. Dette har på mange måter blitt et kappløp der begge sider prøver å overliste hverandre. Dessverre har kriminelle nesten alltid overtaket, så husk at antivirus kan detektere og blokkere mange virus, men angripere lager hele tiden nye versjoner som ikke vil bli fanget opp av antivirus. Derfor kan du ikke stole på at antiviruset alene vil beskytte deg, du må ta ekstra steg selv.

Steg 1 er å sørge for at operativsystemet og applikasjoner er satt til å automatisk installere oppdateringer. Hvis programvaren din er oppdatert, er det vanskeligere for angripere å infisere datamaskinen eller den mobile enheten.

Steg 2 er å huske at du er det beste forsvar mot virus. Infeksjon av virus involverer ofte sosial manipulering, som innebærer at angriperen lurer deg til å installere viruset for dem. Et vanlig eksempel på sosial manipulering er epost som ser legitimt ut, men er blitt lagd for å lure deg til å infisere maskinen. En angriper kan for eksempel sende deg en epost der de utgir seg for å være banken din og ber deg om

Hva er virus

å klikke på en lenke. Hvis du klikker på lenken blir du tatt til en side som automatisk prøver å infisere maskinen din. Eller kanskje de sender en epost om at pakken ikke kunne bli levert og spør deg om å åpne det vedlagte dokumentet, som vil prøve å infisere maskinen når det blir åpnet.

Sosial manipulering kan også skje over andre teknologier, som telefonen. Et eksempel er angripere som ringer deg og utgir seg for å være teknisk support fra Microsoft og informerer deg om at din datamaskin er infisert. Historien er en løgn og datamaskinen din er sannsynligvis trygg. Målet til angriperen er å lure deg til å tro at du er infisert så du vil gi dem fjerntilgang til systemet ditt, eller kjøpe deres sikkerhetsprodukt som ofte er et virus. Bruk sunn fornuft, hvis en telefonsamtale eller beskjed virker merkelig, mistenkelig eller for god til å være sann, er det som regel det.

Den beste måten å beskytte seg mot virus er å holde programvare oppdatert, installere antivirus du stoler på fra en kjent leverandør og vær på vakt for angripere som prøver å lure deg til å infisere din egen maskin.

Les Mer

Abonner på månedlig OUCH! nyhetsbrev om sikkerhetsbevissthet, se gjennom OUCH! arkivene og lær mer om SANS sine programmer for sikkerhetsbevissthet hos http://www.securingthehuman.org.

Norsk Versjon

NorSIS er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge. NorSIS jobber for at informasjonssikkerhet skal bli en naturlig del av hverdagen. Les mer på www.norsis.no.

Ressurser

OUCH Phishing:
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_no.pdf
OUCH Sikre datamaskinen:
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201212_no.pdf
Du er et mål plakat:
http://www.securingthehuman.org/resources/posters
NorSIS veiledning om virus på PC:
https://norsis.no/2012/06/virus-pa-pc/

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis