OUCH! | Mai 2014

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Oversikt
- Kjennetegn på at du har blitt kompromittert
- Hvordan reagere

# Jeg er blitt hacket, hva nå?

## Oversikt

Vi vet at du tar steg for å beskytte datamaskinen din og informasjonen den inneholder. Likevel, man er aldri 100% sikker, samme som når du kjører bil, uansett hvor forsiktig du er, så er det en mulighet for at du havner i en ulykke. I dette nyhetsbrevet vil vi lære deg hvordan du kan oppdage om du har blitt kompromittert og hva du kan gjøre med det. Desto fortere du greier å oppdage at datamaskinen er kompromittert og reagere på angrepet, desto lettere er å det å hindre skade på deg og din organisasjon.

**Gjesteredaktør**

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) er forskningssjef hos CSRgroup Computer Security Consultants. Han er også medforfatter av SANS-kursene Memory Forensics (FOR526) og Malware Reverse Engineering (FOR610).

## Kjennetegn på at du har blitt kompromittert

Det finnes ikke ett enkelt steg du kan ta for å finne ut om datamaskinen din er blitt infisert. Man må i stedet se på flere indikatorer, hvis du identifiserer flere av disse, så tyder det på at datamaskinen din har blitt kompromittert. Under er noen eksempler:

- Antiviruset har utløst en alarm som sier du er infisert, spesielt hvis du får beskjed om at de ikke greide å fjerne de berørte filene.
- Nettleserens hjemmeside er blitt forandret, eller at nettleseren tar deg til sider som du ikke ville besøke.
- Det er nye kontoer på datamaskinen som du ikke har lagt til.
- Programmer som du ikke har installert starter å kjøre på maskinen.
- Datamaskinen din krasjer gjentatte ganger eller går veldig tregt.
- Et program på datamaskinen spør om tillatelser til å forandre systeminnstillinger når du ikke installerer eller oppdaterer et program.
- Brannmuren sier at et program den ikke kjenner igjen spør om tillatelser til å aksessere Internettet.

# Jeg er blitt hacket, hva nå?

## Hvordan reagere

Hvis du tror du har blitt kompromittert bør du reagere så fort som mulig. Hvis datamaskinen ble gitt til deg av arbeidsgiver, bør du ikke prøve å fikse datamaskinen selv, eller skru den av. Dette kan både skade mer enn det hjelper og ødelegge bevis som kan være nyttig i en etterforskning. Du bør i stedet rapportere hendelsen til arbeidsgiver så fort som mulig, enten ved support, sikkerhetsteam eller overordnet. Hvis dette ikke er en mulighet, eller det vil ta for lang tid, bør du koble datamaskinen fra Internettet og legge datamaskinen i sleep eller hibernate modus. Selv om du ikke er sikker, så er det bedre å rapportere det, da er du på den sikre siden. Organisasjonen din har sannsynligvis rutiner og ansatte for å håndtere hendelser som dette, det er best å la de håndtere det.

*Før eller senere kan din datamaskin bli kompromittert, jo fortere du greier å reagere, desto bedre.*

Hvis det er snakk om din personlige datamaskin kan du følge stegene under:

- **Sikkerhetskopi**. Det viktigste steget du kan ta er å forberede deg før hendelsen skjer. Ta sikkerhetskopi av dataene regelmessig, sjekk også regelmessig at sikkerhetskopiene fungerer som forventet. Hvis en datamaskin har blitt kompromittert, så må du ofte slette alt på harddisken og reinstallere operativsystemet, eller kjøpe en ny datamaskin. Uansett, så må du gjenopprette dataene dine.
- **Bytt passord**. Du må bytte alle passordene dine. Dette gjelder ikke bare passord på datamaskinen og mobile enheter, men også passord på nettkontoer. Sørg for at du bytter passord på en datamaskin som du stoler på og vet er sikker.
- **Antivirus**. Hvis antiviruset informerer deg om en infisert fil bør du følge stegene som antiviruset anbefaler. Mulighetene er ofte å legge filen i karantene, rengjøre filen eller slette filen. De fleste antivirus har også linker der du kan lære mer om infeksjonen. Hvis du er usikker bør du legge filen i karantene, hvis det ikke er mulig bør du slette filen.
- **Reinstallere**. Hvis det ikke er mulig å fikse datamaskinen med antiviruset, så er reinstallering av systemet en av de sikreste måtene å bli kvitt infeksjonen på. Først må du koble datamaskinen fra Internettet, deretter må du følge leverandørens instruksjoner. I de fleste tilfeller vil dette være å bruke den innebygde

## Jeg er blitt hacket, hva nå?

gjenopprettingspartisjonen eller reinstallere operativsystemet. Hvis gjenopprettingspartisjonen er korrupt, infisert eller borte fra systemet, kontakt leverandøren og be de om å sende en DVD. Du bør ikke reinstallere operativsystemet fra sikkerhetskopier, sikkerhetskopien kan ha den samme svakheten som angriperen brukte for å få tilgang. Du bør kun bruke sikkerhetskopien for å gjenopprette dine data. Hvis datamaskinen er gammel eller utdatert, kan det være enklere og kanskje billigere å kjøpe ny datamaskin, i stedet for å bruke flere timer på å gjenopprette datamaskinen til en trygg status.

- **Profesjonell hjelp**: Hvis du er bekymret for at du har blitt kompromittert, men ikke føler at du har de nødvendige kunnskapene til å fikse det, så kan det være best å spørre en profesjonell om hjelp. For eksempel: du finner kanskje ut at sikkerhetskopien din er utdatert, etter at du har blitt infisert. Da kan det være fristende å overføre kritiske filer (som bilder og dokumenter) fra den infiserte maskinen til en ny maskin. Ved å gjøre dette så er det en mulighet for at du også overfører viruset. Dermed blir også den nye maskinen infisert. Et mye sikrere alternativ er å ta med den infiserte datamaskinen til en profesjonell tekniker som kan gjenopprette filene uten å overføre infeksjonen.

## 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! Sikkerhetskopi: | http://www.securingthehuman.org/ouch/2013#september2013 |
| OUCH! Passord: | http://www.securingthehuman.org/ouch/2013#may2013 |
| OUCH! Hva er virus: | http://www.securingthehuman.org/ouch/2014#february2014 |
| Plakat om hva som er ondsinnet: | https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf |



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