OUCH! I maj 2014

Det Månatliga Nyhetsbrevet Om Säkerhetsmedvetenhet för Datoranvändare

OUCH!

I DENNA UTGÅVA…

Jag är Hackad, Vad Gör Jag Nu?

Översikt

Vi vet att du är oroad över att skydda din dator och information och vidtar åtgärder för att säkra dem. Likväl - precis som att köra bil - oavsätt hur säkert du kör, förr eller senare har du kanske en incident. I detta nyhetsbrev kommer vi att lära dig vad du ska vara uppmärksam om ifall din dator blir hackad och vad du kan göra om det. Ju snabbare du upptäcker att din dator har blivit hackad och ju snabbare du reagerar, desto bättre kan du mildra skador till din organisation.

Gästredaktör

Jake Williams (@MalwareJake; malwarejake.blogspot.com) är Vetenskapschef vid CSRgroup Computer Security Consultants. Han är även medförfattare av Memory Forensics (FOR526) och Malware Reverse Engineering (FOR610) kurserna på SANS.

Indikatorer för Kompromiss

Först måste du förstå att i många fall finns det inte bara ett steg som du kan ta för att fastställa att din dator har blivit hackad. Istället är det vanligen flera indikatorer. Om du identifierar en kombination av dessa kan det antyda att din dator är hackad. Här är några exemplar:

- Ditt anti-virus program har triggat ett larm som säger att din dator är infekterad, speciellt om det står att programmet inte kunde avlägsna eller karantäna de påverkade filerna.
- Din webläsares hemsida har ändrats oväntat eller din webläsare tar dig till en sajt som du inte ville gå till.
- Det är ny konton på din dator som du inte skapade.
- Det är nya program som du inte installerade.
- Din dator krashar ofta eller går sakta.
- Ett program på din dator begär tillstånd att göra förändringar till ditt system, även om du inte installerar eller ändrar på dina program.
- Din brandvägg larmar dig att ett program som du inte känner igen begär tillstånd att få tillgång till nätet.

Hur Man Reagerar

Om du tror att din dator har blivit kompromissad, ju snabbare du bemöter problemet, desto bättre. Om den dator du andvänder var försedd av din arbetsgivare eller den andvänds i arbetet, försök inte laga din dator själv och stäng inte av datorn. Inte bara kan du orsaka mera skada än nytta, men du kan också förstöra värdefulla bevis som kan

Jag är Hackad, Vad Gör Jag Nu?

andvändas vid en utredning. Istället ska du rapportera händelsen till din arbetsgivare direkt, vanligtvis genom att ta kontakt med support, säkerhetsgruppen, eller arbetsledare. Om du av någon anledning inte kan kontakta din organisation, eller om du är orolig för en försening, koppla bort din dator från nätverket och sätt den i vänteläge, viloläge, eller stömspararläge. Även om du inte är helt säker på att du blivit hackad, det är bäst att rapportera nu bara i fall att. Din organisation har troligen processer och ett lag som tar hand om situationer som den här, låt dem ta hand om det.

Förr eller senare kan din dator bli kompromissad, ju snabbare du upptäcker en incident och ju snabbare du svarar, desto bättre.

Om datorn är din och för eget bruk, här är steg som du kan ta själv.

- **Säkerhetskopiering**. Det viktigaste steget du kan ta är att vara förberedd med säkerhetskopieringar. Definitivt säkerhetskopiera din data reguljärt och kolla periodiskt att att du kan återställa mappar från din säkerhetskopiering. Ofta när en dator är kompromissad, är det enda alternativet att radera din systemhårddisk och installera om ditt operativsystem, eller köpa en ny dator. I vilket fall som helst behöver du dina säkerhetskopieringar för att återfå din personliga data.

- **Byt Ditt Lösenord**. Var noga med att byta alla dina lösenord.Detta inkluderar inte bara lösenord på dina datorer och mobila enheter, men alla dina lösenord på nätet. Se till att du ändrar alla dina lösenord från en annan dator som du vet är tillförlitlig och säker.

- **Anti-Virus**. Om ditt antivirusprogram informerar dig om en infekterad fil, kan du följa de åtgärder som den rekommenderar. Vanligtvis inkluderar detta karantän av filen, rengöring av filen eller ta bort filen. De flesta antivirusprogram kommer att ha länkar som du kan följa för att lära sig mer om den specifika infektionen. När du är osäker, karantäna filen. Om detta inte är möjligt, ta bort den.

- **Ominstallation**. Om du inte kan rengöra datorn med anti-virus, är ett av de mest säkra sätten att återställa data att bygga om datorn från grunden. Först koppla bort datorn från nätverket. Följ sedan systemtillverkarens instruktioner, i de flesta fall innebär det användning av den inbyggda återställningspartition för att installera om operativsystemet. Om återställningspartitionen saknas, är skadad eller infekterad, kontakta tillverkaren

Jag är Hackad, Vad Gör Jag Nu?

och be att de skickar en återställnings-DVD. Installera inte om operativsystemet från säkerhetskopior. Dina säkerhetskopior kan ha samma sårbarheter som gjorde att hackare från början fick tillträde. Det enda du ska använda dina säkerhetskopior för är återhämtning av dina personuppgifter. Dessutom, om din dator är gammal eller omodern kan det vara enklare (och kanske till och med billigare) att köpa en ny dator än att spendera timmar på att försöka bygga om den.

- **Professionell Hjälp**. Om du är orolig att du har blivit hackad, men känner att du inte har kompetens eller kunskap för att fixa det, kan du lämna in din dator till en datorexpert. Till exempel, efter att ha blivit hackad kanske du inser att dina säkerhetskopior är ofullständiga eller föråldrade. Du kanske frestas att överföra viktiga filer såsom foton, dokument eller videoklipp mellan den infekterade maskinen och en ny maskin. Men genom att göra detta kan du oavsiktligt överföra skadlig kod och infektera din nya dator samtidigt. Ett betydligt säkrare alternativ är att ta den infekterade datorn till en kvalificerad datorexpert som på ett säkert sätt kan återvinna dessa filer utan att riskera att överföra den skadliga koden.

LÄR DIG MER

Prenumerera på det månaltliga OUCH! nyhetsbrevet om säkerhetsmedvetenhet, ha tillgång till OUCH! arkiven, och lär dig mer om SANS lösningar inom säkerhetsmedvetenhet genom att besöka oss på http://www.securingthehuman.org

Swedish Version

OUCH! är översatt av Andreas Bohman och Marcus Andersson. Båda arbetar inom informationssäkerhets-branchen och har många års erfarenhet i etablering av säkerhetsmedvetenhetsprogramm.

Resurser

OUCH! Säkerhetskopior:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! Lösenord:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Vad är Skadlig Kod?:	http://www.securingthehuman.org/ouch/2014#february2014
Upptäcka Ont Affisch:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Översatt Av: Andreas Bohman och Marcus Andersson