

Uppsala den 14 April 2004

## Utpressning på Internet

En mängd företag i Sverige och utomlands har under den senaste tiden drabbats av utpressning. Utpressarna har hotat med att stänga ner företagets affärskritiska Internettjänster så som spel- och banktjänster.

Företagen har mottagit utpressningsbrev innehållandes dessa hot och med en anmodan att betala ett visst belopp till utpressaren. En kort tid efter att brevet anlänt (oftast i email form) startar attacken och företagets Internettjänster blockeras för kunderna genom så kallade överbelastningsattacker (DDOS attacker).

Mycket tyder på att detta är ett omfattande och samtidigt växande problem. I ett stort antal fall ligger organiserad brottslighet bakom dessa hot.

### Trendbrott

Fram tills i höstas har utpressning av kriminella på Internet varit mest en hypotetisk fråga och i de fall det förekommit har det varit ytterst sporadiskt. Från hösten 2003 har det dock skett en vändning till det sämre och ett mycket stort antal företag är drabbade. Attackerna har inte visat några tecken på att avta och det som talar för att det kommer fortsätta är att vissa företag har betalat utpressarna.

Hittills har det mest varit online betting företag som varit drabbade men steget för utpressarna att gå över till andra branscher är mycket litet. De företag som främst är i riskzonen är företag som är omsätter mycket pengar online, exempelvis webbshopar, nätmäklare, online banker, resebyråer etc.

### Skydd

Det finns många olika sätt att skydda sig mot DDOS attacker, men inget sätt som garanterat fungerar i alla lägen. Däremot borde det vara självklart att för alla företag som bedriver affärskritisk verksamhet på Internet att tänka efter i förväg och upprätta en plan för denna och andra typer av incidenter.

Planen skall hantera bland annat hur man detekterar angrepp, hur man handlar vid ett angrepp, hur man eskalerar en incident (identifierade kontakt personer hos större ISP:er och polisväsendet etc.), hur man sköter information till kunder och media, om man skall försöka spåra etc.

Planen bör vara en del av en större incidenthanteringsplan för hela företaget och hållas aktivt uppdaterad. Först efter att man upprättat en incidenthanteringsplan och gjort en grundlig genomgång av infrastrukturen bör man titta på tekniska lösningar.

### Spårning

Att spåra DDOS attacker är relativt komplicerat och varierar beroende på hur attacken går till. Även i de svårare fallen kan man dock med rätt utrustning och kunskap ofta skapa sig en relativt god bild av vem som ligger bakom. Det faktum att denna typ av attacker oftast spänner över ett stort antal länder försvårar dock arbetet avsevärt

## För ytterligare information

Martin Zetterlund  
Sentor MSS AB  
Tel: 018-65 30 00  
Mobil: 070 – 757 30 02  
Web: [www.sentor.se](http://www.sentor.se)  
Email: [martin.zetterlund@sentor.se](mailto:martin.zetterlund@sentor.se)

### Fakta ruta

#### Dos attacker

Dos står för "Denial Of Service" och går ut på att som namnet antyder slå ut en tjänst, till exempel en Internettjänst. Det finns i princip tre olika kategorier av DOS attacker;

- *den första kategorin går ut på att man utnyttjar en svaghet i den attackerade datorns mjukvara för att få den att krascha*
- *den andra går ut på att man överlastar servrar eller brandväggar med speciell trafik så att Internettjänsten blir otillgänglig*
- *och den tredje går ut på att man fyller internet förbindelsen med så mycket skräptrafik att ingen av de legala besökarna kan komma fram*

Generellt dock för alla typer av dos attacker är att de inte går ut på att stjäla eller modifiera data utan endast att göra Internettjänsten otillgänglig.

#### Distribuerade DOS attacker

Med en Distribuerad DOS attack menas att man har ett stort antal klienter som attackerar den tjänst man vill slå ut. Klienterna kontrolleras från en server av angriparen, detta brukar populärt kallas ett DDOS nätverk.

Klienterna till DDOS nätverken samlas in på många olika sätt, vissa med hjälp av virus, andra med hjälp av trojaner och ytterligare andra genom att utnyttja kända säkerhetshål eller "back doors" upplagda av andra virus. De maskiner som oftast hamnar som klienter i DDOS nätverken är bredbandsanslutna hemanvändare med dålig säkerhet eller företag med bristande skydd och rutiner.

DDOS attacker är i princip uteslutande av den andra och tredje kategorin DOS attacker nämnda ovan.

### Om Sentor

*Sentor kombinerar människor med teknologi för att skydda våra kunders digitala tillgångar. Interaktion mellan övervakning och respons, samt leverantörs-oberoendekonsulttjänster, ger högre informationssäkerhet till en lägre kostnad.*

*Vår metodik stött av egenutvecklade verktyg samt en systematiserad omvärldsbevakning över hot och risker stödjer allt vi gör. Sentor grundades 1998 och är sedan dess självfinansierat. Bolaget ägs till 100% av ledning och personal samt var ett av de första företagen i Sverige att implementera SS-ISO 627799 (Standard för informations-säkerhet) i hela sin verksamhet.*