Ekonomisk kommentar

Överbelastnings-attacker i den finansiella sektorn

Gabriella Ström

NR 10 2025, 6 november

Sammanfattning

Under de senaste åren har överbelastningsattackerna blivit både fler och mer komplexa. I Sverige har flera allvarliga attacker riktats mot samhällsviktig digital infrastruktur, inklusive finansiella tjänster. Attackerna mot finansiella aktörer har lett till kortvariga problem med att komma åt vissa tjänster. Om hotbilden mot Sverige skulle trappas upp finns emellertid en risk för mer avancerade attacker, som potentiellt skulle kunna få mer långtgående konsekvenser. Detta skulle kunna minska förtroendet för det finansiella systemet eller mer långvarigt försämra möjligheterna att genomföra betalningar. För att förhindra överbelastningsattacker och minska effekterna av sådana krävs åtgärder på flera olika nivåer i samhället. Däribland en effektiv samverkan mellan privat och offentlig sektor.

Författare: Gabriella Ström, verksam vid avdelningen för finansiell stabilitet på enheten infrastruktur och cyber[1]

Överbelastningsattacker kan påverka tillgängligheten till finansiella tjänster

Den finansiella sektorn är i stor utsträckning digitaliserad och tätt sammankopplad, både av finansiellt och digitalt. För att den ska fungera krävs att tjänsterna tillgängliga, och att aktörerna känner tillit till och förtroende för systemet. De finansiella aktörerna riskerar dock att utsättas för cyberangrepp, och överbelastningsattacker (eng. Distributed-Denial-of-Service (DDoS)) är ett exempel på sådana. Vid en överbelastningsattack påverkas tillgängligheten i en tjänst genom att angriparen gör anrop mot den utsatta måltavlan och på så vis tar en påtaglig del av en begränsad resurs i anspråk, till exempel en servers kapacitet att svara på anrop eller ett nätverks förmåga att hantera mycket trafik samtidigt. En konsekvens av detta blir att legitim trafik till servern, tjänsten eller nätverket inte når fram eftersom målet eller dess omgivande infrastruktur överväldigas med en flod av internettrafik vars enda syfte är att blockera annan trafik.

[1] Tack till Olof Sandstedt, Johanna Stenkula von Rosén, Kristian Jönsson, Björn Segendorff, Joacim Häggmark och Emanuel Hedestig.

Bild 1.

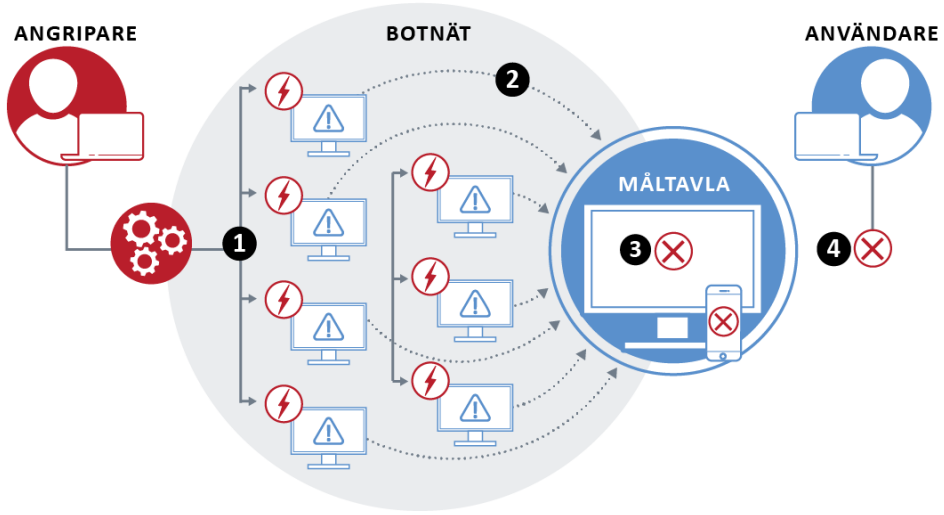

Bild 1. (1) Ett nätverk av datorer infekteras med skadlig kod och kan fjärrstyras av en angripare. (2) Vid en given signal skickar alla enheter samtidigt trafik mot ett mål, t.ex. en webbplats. (3) Den stora trafikmängden överbelastar målets kapacitet. (4) Tjänsten blir otillgänglig för vanliga användare.

Återkommande störningar kan ge intrycket att systemet är instabilt, vilket i sin tur kan leda till en förtroendeförlust. Sådana scenarion kan vara skadligt för det finansiella systemet, eftersom förtroende är en av grundförutsättningarna för att det finansiella systemet ska fungera väl. För att förtroendet ska upprätthållas måste data vara korrekta och tillgängliga för rätt personer vid rätt tidpunkt.

Flera allvarliga attacker mot svenska aktörer

Under hösten 2024 och våren 2025 blev flera svenska banker och finansiella infrastrukturer måltavla för ett antal allvarliga överbelastningsattacker. Attackerna skapade störningar i flera av de drabbade aktörernas tjänster. Det handlade till exempel om att det inte gick att komma åt banktjänster via mobil-appar eller göra Swish-betalningar.

En av de drabbade var Finansiell Id-teknik BID AB:s tjänst BankID. Tjänsten är en central komponent i flera viktiga samhällstjänster, däribland finansiella. Detta eftersom den ger åtkomst till olika tjänster genom att tillhandahålla identifiering och underskrift. I och med att så många tjänster använder BankID medförde attacken att flera olika aktörer drabbades av problem samtidigt. Detta märktes inte minst bland finansiella aktörer där flera olika institut rapporterade in incidenter i samband med att BankID överbelastades. Attackerna påvisade hur angrepp mot systemkritiska komponenter får ett bredare genomslag.

Däremot blev konsekvenserna av de attacker som skedde mot svenska finansiella aktörer under 2024 och 2025 endast kortvariga avbrott under en begränsad period. Detta gjorde att avbrotten inte fick någon direkt betydelse för den finansiella

stabiliteten. Attackerna har inte heller fått effekter på kapitalmarknaden eller gjort betydande avtryck i de drabbade aktörernas balans- och resultaträkningar.

Alltjämt är det viktigt att kunna hantera attacker på ett motståndskraftigt sätt för att de inte ska leda till förtroendeskada. De aktörer som drabbades av överbelastningsattacker har behövt avsätta en del resurser för att lyckas hantera och dämpa effekterna av angreppen. Resursåtgången har varit märkbar både under tiden attackerna pågick och i upprustningen för att kunna hantera eventuella framtida angrepp.

I regel snabb återhämtning efter attack

Förklaringen till att överbelastningsattacker vanligtvis inte får större direkta finansiella effekter ligger delvis i angreppsmetoden. Ett system som utsätts för en överbelastningsattack är otillgängligt under den tid som attacken pågår. Om angriparen pausar eller avbryter attacken så försvinner också effekterna av den. Den som utsätts kan som regel återhämta sig så snart attacken är över utan någon kvarvarande påverkan på systemet.

Utpressningsangrepp (eng. ransomware) fungerar annorlunda. Då krypterar angriparen det data som systemet innehåller och gör det därmed otillgängligt. Därefter krävs offret ofta på en lösensumma för att få en dekrypteringsnyckel, med vilken data kan göras tillgängliga igen. Däremot finns det inga garantier för att data som dekrypteras är tillförlitliga och korrekta. Vid en utpressningsattack är både påverkan och återhämtningstiden betydligt längre. Systemet förblir otillgängligt till dess att det har isolerats, undersökts och de krypterade data, om möjligt, ersatts av data från backuper.

Fler och mer sofistikerade överbelastningsattacker

Överbelastningsattacker är inget nytt fenomen. Däremot är attackerna mer sofistikerade idag än tidigare. Detta eftersom de till större del är precisionsinriktade och planerade för att ge så stor effekt som möjligt. Därtill har attackerna blivit mer omfattande.

Den europeiska cybersäkerhetsmyndigheten ENISA rapporterar att överbelastningsattacker är ett av de primära cyberhoten mot finansiell sektor i Europa. Dessutom framgår det i Nationellt cybersäkerhetscenters (NCSC) rapport *Överbelastningsangrepp mot kritisk infrastruktur i Norden och Baltikum hösten 2024* att knappt 30 procent av de överbelastningsattacker som observerades i den svenska IP-rymden under september och oktober år 2024 riktades mot kritisk infrastruktur. Detta innefattar bland annat statliga myndigheter, akademiska institutioner och sektorerna telekom och finans. Dessutom har överbelastningsattackerna de senaste två åren ökat i intensitet och blivit vanligare.

Bild 2.

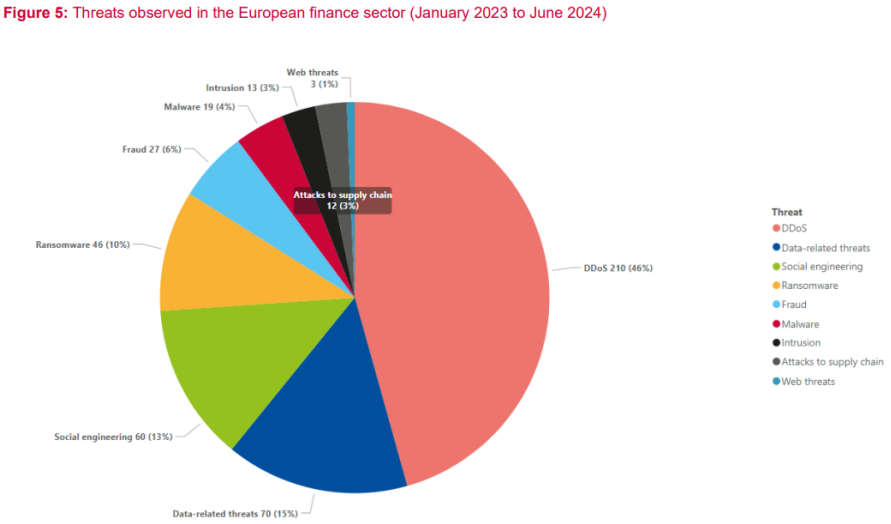

Bild 2. Följande typer av hot riktades mot den europeiska finanssektorn. Analysen baseras på incidenter inrapporterade till ENISA. Eftersom en incident kan tillhöra flera hotkategorier överstiger den totala procentandelen i figuren 100 %. (Källa: ENISA, 2024).

Även om de senaste årens attacker inte har haft någon betydande påverkan på den finansiella sektorn och dess tjänster så går det i dagsläget inte att förutse hur utvecklingen kommer att te sig framöver. Attackerna skulle kunna öka ytterligare i både komplexitet, volym och frekvens, vilket kan medföra fler avbrott och mer omfattande konsekvenser.

Möjligtvis kan även skräddarsydda överbelastningsattacker gentemot vissa aktörer, med målet att blockera samtliga betalningsmöjligheter, ge märkbara effekter. I ett scenario där en eller flera aktörer överbelastas samtidigt är det tänkbart att möjligheten att göra betalningar skulle störas på ett mer genomgripande sätt.

Överbelastningsattacker som tjänsteutbud

Överbelastningsattacker kan genomföras från angriparens egna datorer eller från datorer som angriparen på annat sätt förfogar över. Attackerna kan få större effekt genom att man använder flera hackade datorsystem som källor till attacktrafiken. De utnyttjade enheterna kan vara datorer och andra nätverksanslutna resurser, som IoT-enheter[2]. I sådana enheter är dessutom säkerhetsstandarden oftast lägre än i en konventionell dator.

De enskilda enheterna kallas för botar, och en grupp av sådana botar kallas för ett botnät. När ett botnät har etablerats kan angriparen styra en attack genom att skicka

[2] Internet-of-things (IoT) innebär att vardagsföremål som sensorer, lampor eller kylskåp kopplas upp mot internet för att kunna samla in data eller styras på distans.

fjärrinstruktioner till varje bot och eftersom varje bot är en legitim internetansluten enhet kan det vara svårt att skilja attacktrafiken från vanlig trafik.

Idag tillhandahålls botnät och andra nödvändiga tekniska medel som en del av ett tjänsteutbud från olika cyberbrottsnätverk. Det kan närmast liknas vid en affärsmodell vilken kan se olika ut från fall till fall. Vissa leverantörer erbjuder sig att utföra attacken åt klienten, medan andra ger klienten tillgång till en kontrollpanel med överbelastningsfunktioner. Detta medför att det inte krävs någon djupare teknisk kompetens för att utföra en överbelastningsattack. Det krävs oftast inte heller någon personlig kontakt mellan leverantör och klient, vilket gör att hotaktören bakom en attack kan hålla sig dold och förbli anonym.

Ett exempel på en sådan leverans är botnätverket GorillaBot, se bild 3. Botnätverket har bland annat använts i flera av attackerna riktade mot svenska finansiella aktörer.

Bild 3.

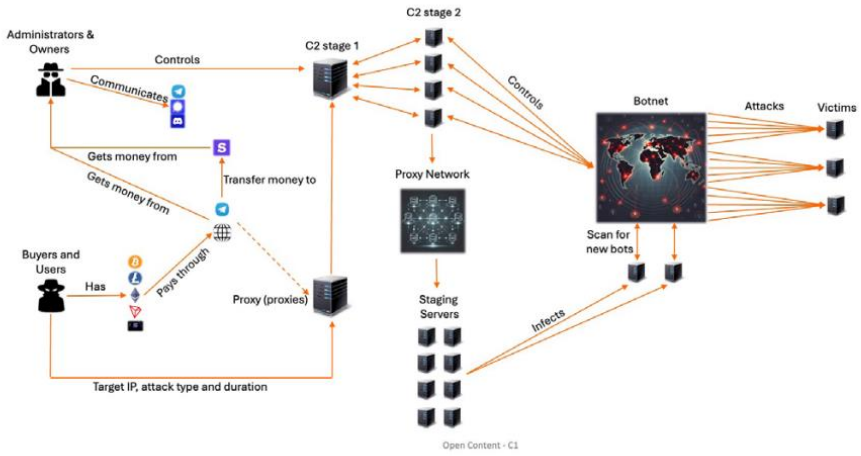

Bild 3. En överblick av infrastrukturen bakom botnätet GorillaBot (Källa: NCSC, 2025).

Stora och störande attacker har alltså blivit vanligare. Det beror bland annat på att det går att köpa överbelastningsattacker som en tjänst och det faktum att det är så enkelt att bygga ett botnät, i och med att vår tillvaro inrymmer uppkopplade enheter med låg säkerhet.

Hotaktörerna bakom attackerna

Hotaktörerna som utför cyberangrepp mot Sverige är främst kriminella, ideologiskt motiverade och statsaktörer. Eftersom alla kan nyttja samma infrastruktur för att utföra en cyberattack är det ofta svårt att avgöra vem som ligger bakom ett angrepp. I vissa fall är det tydligare vem som ligger bakom, som till exempel den pro ryska gruppen NoName 057(16). I andra fall så nyttjar hotaktören möjligheten till anonymitet vilket gör det svårt att utpeka en attack till en specifik aktör.

När det är svårt att identifiera hotaktörerna blir det också svårare att förstå motiven bakom attackerna. Däremot har det observerats mönster som tyder på att det finns geopolitiska motiv bakom de senaste årens överbelastningsattacker. Därtill påpekar NCSC att attackerna under 2024 sannolikt drivits på av geopolitiska konflikter och ideologiska motiv, så kallad hacktivism, samt framväxten av mer avancerade tillvägagångssätt. Likaså rapporterar ENISA att hacktivistledda överbelastningsattacker tydligt dominerar hotbilden gentemot finansiella aktörer i Europa.

Stoppa överbelastningsattacker och överbelastningstjänster

Vågen av överbelastningsattacker som sköljde över Sverige under hösten 2024 och våren 2025 drev fram en ökad medvetenhet och ett skärpt förhållningssätt gentemot angreppsmetoden. Den upptrappade hotbilden ledde till att aktörer i den svenska finansiella sektorn utvecklade ytterligare skydd för att skapa motståndskraft mot dessa attacker. Däremot är det ovisst hur avancerade överbelastningsattacker kommer att utvecklas med tiden. För att upprätthålla motståndskraften gentemot dem krävs ett proaktivt arbete med att justera och utveckla skyddet. Detta för att på ett robust sätt kunna hantera allt fler och alltmer komplexa attacker.

Omfattningen av leverantörer som erbjuder överbelastningstjänster har lett till ett ökat arbete med att försöka begränsa problemet. Brottsutredande myndigheter samarbetar internationellt med insatser för att försöka nedmontera leverantörer av överbelastningstjänster och botnätverk (Europol, u.å).

Därtill väntas förordningen Cyber Resilience Act (EU, 2019) börja tillämpas från och med 2027. Förordningen syftar till att höja säkerheten i uppkopplade enheter, som IoT-enheter, genom att införa säkerhetskrav på hård- och mjukvara. Detta kan medföra att enheterna blir svårare att hacka och därför inte lika lätt kan utnyttjas i botnätverk. Även privatpersoner kan bidra till att enheterna blir svårare att hacka. Detta genom att regelbundet uppdatera programvara, inte använda samma inloggningsuppgifter och lösenord för flera ändamål och genom att ändra fabriksinställda lösenord när en enhet installeras.

Ledning och samverkan behövs

Det behövs dessutom åtgärder på flera olika nivåer. Förutom förbättrade skyddsmekanismer på organisatorisk nivå krävs också samverkan på samhällsnivå, detta för att motverka- och begränsa effekterna av cyberattacker i den finansiella sektorn. Riksbanken deltar i dagsläget i både internationella- och nationella samverkans forum. Ett exempel är NCSC finansforum. Forumet syftar till att stärka cybersäkerheten och därmed den finansiella stabiliteten genom att främja informationsutbyte mellan privat- och offentlig sektor. Sedan 2023 är dessutom Riksbanken medlem i Nordic Financial Computer Emergency Response Team (NFCERT). Organisationen stödjer den nordiska finanssektorn i att försvara sig mot cyberattacker, exempelvis genom att dela hotbildsinformation.

För att upprätthålla en god motståndskraft krävs att befintliga samverkansformer kontinuerligt utvecklas men också att nya initieras. Därav har Riksbanken föreslagits leda en ny krishanteringsfunktion (Riksbanken, 2025). Funktionens uppdrag är att samordna insatser vid allvarliga driftstörningar i finanssektorn. Utöver Riksbanken föreslås Finansinspektionen, Riksgäldskontoret och vissa företag i den finansiella sektorn ingå i funktionen tillsammans med andra aktörer vars kunskaper eller resurser är av betydelse för funktionens arbete. Riksbanken ser positivt på uppdraget att leda en sådan funktion eftersom denna skulle kunna stärka samverkan vid allvarliga störningar.

Referenser

ENISA. (2024). Threat Landscape: Finance Sector. Februari 2024. European Union Agency for Cybersecurity.

NCSC. (2024). Överbelastningsangrepp mot kritisk infrastruktur i Norden och Baltikum hösten 2024. Nationellt cybersäkerhetscenter.

ENISA. (2025). ENISA Threat Landscape 2025. European Union Agency for Cybersecurity.

Europol. (u.å.). *Cyberattacker*. Europol. Hämtad från https://www.europol.europa.eu/crime-areas/cyber-attacks (hämtad 16 oktober 2025).

EU. (2019). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. Official Journal of the European Union, L 151, 7 June 2019, pp. 15–69. Tillgänglig på: https://eurlex.europa.eu/eli/reg/2019/881/oj

Riksbanken. (2025). Riksbanken stödjer förslaget om ny funktion för krishantering i finanssektorn. Hämtad 13 oktober 2025 från https://www.riksbank.se/sv/press-och-publicerat/nyheter-och-pressmeddelanden/nyheter/2025/riksbanken-stodjer-forslaget-om-ny-funktion-for-krishantering-i-finanssektorn/

SVERIGES RIKSBANK
Tel 08 - 787 00 00
registratorn@riksbank.se
www.riksbank.se

PRODUKTION SVERIGES RIKSBANK)