**PRESSMEDDELANDE 7 mars 2018**

**Akamai: En DDos-attack av den här storleken kan slå ut viktiga samhällsfunktioner i Sverige**

**DDoS-ttacken mot en av Akamais kunder i torsdags var den största Akamai hittills upplevt och var på hela 1,3 Tbps – dubbelt så stor som den i september 2016. Erik Henriksson på Akamai menar att attacker av den här storleken kan slå ut viktiga samhällsfunktioner i Sveriges och att vårt skydd på området har försämrats de senaste åren.**

Det var den 27 februari som Akamai och andra företag informerade om en Memcache-driven DDoS-attack på hela 1,3 Tbps. Akamais Prolexic-plattform kunde dock mildra attacken genom att filtrera all trafik som kommer från UDP-porten 11211, standardporten som används av Memcached.

– Vi har aldrig bekrämpat en sådan här stor attack av den här typen tidigare. Hade den varit riktad mot till exempel Sverige, hade den kunnat slå ut många viktiga samhällsfunktioner, ungefär som att hela Essingeleden alla filer i båda riktningar, samt andra vitala delar av det svenska vägnätet skulle slås ut. Det sätter det onekligen i perspektiv. Många andra organisationer har haft liknande reflektionsattacker som startade förra måndagen, bland annat i Tyskland som har varit enormt drabbat. Vi räknar med många fler potentiellt större attacker inom kort, säger Erik Henriksson, kundansvarig på Akamai.   
  
Erik Henriksson menar att Svenska myndigheter är en riskgrupp för den här typen av attacker och Sverige fortsätter att falla på FN:s cyber security-lista.   
  
– I Sverige är banker och de stora varumärkena inom detaljhandel bättre skyddade, alltså de branscher som verkar inom e-handel eller i någon form har sin affär online. Det sprids rykten i media angående vem eller vilka som ligger bakom de senaste attackerna. Rent tekniskt kan Cyberattacker och attackmönster spåras, men att bekräfta på vems kommando är en helt annan sak och här vill jag inte spekulera, säger Erik Henriksson.

Akamai samarbetar med andra branschpartner för att hjälpa företag, myndigheter och organisationer att använda Best Common Practices (BCP) och praktisk memcached-sanering för att minska hoten mot Internet. Den nu aktuella attacken har inte drabbat Sverige.

Akamai släppte nyligen den senaste säkerhetsrapporten ”Akamai State of the Internet” och konstaterade där att det totala antalet DDoS-attacker ökade med 14 procent det sista kvartalet (Q4) 2017 jämfört med samma tid förra året (Q4 2016). Rapporten varnade också för att ökad scanning från just Mirai Botnet kan komma att växa explosivt liksom en kraftig ökning av stöld av användaruppgifter.

**Frågor och svar från Erik Henriksson:**  
**Hur mycket är 1,3TBps?**   
För att sätta den siffran i perspektiv kan vi börja med att omvandla 1,3 terabit/sekund till megabit/sekund vilket då blir 1 300 000 och ställa det i jämförelse med ett genomsnittligt hem i Sverige som har cirka 22,5 Mbps enligt State Of the Internet 2017. Många har idag 100 Mbps men även med 100 Mbps mot 1,3 miljoner är man ganska liten.

Man skulle kunna dividera 1,3 Tbps med uppkopplingshastigheten ett genomsnittligt hushåll har och på så vis få ett antal hushåll det skulle motsvara. Internets uppbygnad är mer komplex än så vilket gör den jämförelsen ointressant. Internet är som många vet ett globalt nätverk som består av många sammankopplade nätverk och då har man flera anslutningspunkter. Om vi tittar på en anslutningspunkt exempelvis Netnod, en av de största kopplingspunkterna i Norden, så kan man läsa på deras webbsida att Stockholm har under 1,3 Tbps aggregerad trafik. Då skulle man kunna dra slutsatsen att en attack i den storleksordningen skulle få stor påverkan.

**Hur står företagen rustade mot den här typen av attacker?**  
Många företag har ganska bra förbindelse mot internet, men då pratar vi om kanske 1 Gbps (1000 Mbps) eller i vissa fall 10 Gbps (10 000 Mbps) så att försöka skydda sitt datacenter att stå mot en attack om 1 300 000 Mbps är lönlöst. Den här typen av attacker måste stoppas längre ut på internet, det är som hävstångseffekten, mitigerar man attacker nära varje avsändare är varje individuell attack relativt liten och hinner stoppas innan den likt snöbollseffekten bygger upp till en mega attack.

Vanligtvis behöver inte attacker vara så stora, vid riktade attacker skjuter man ofta strax över den förväntade kapaciteten, det räcker trots allt med strax över 10 Gbps för att totalt slå ut en 10 Gbps förbindelse, så varför ”slösa” mer kraft än nödvändigt när det räcker med en mindre attack för att slå omkull det mesta.

**Hur gör man då för att skydda sig om man har en webbplats som ska vara tillgänglig och stå mot den här typen av förhållandevis ”enkla” attacker, men kraftfulla?**Att bygga ut sitt datacenter är meningslöst. Trafiken kommer hindras långt innan så brandväggar och annan utrustning ska man givetvis ha, men mot den här typen av attacker som blir mer och mer vanlig är det inte ens värt tanken. Vad är då nästa nivå? Se till att din internetleverantör har kapacitet det är en bra start för i händelse av en attack kan de dels ta emot större attacker samt även har såväl teknik som kunskap om hur man hanterar stora attack volymer. Glöm inte att kontrollera ditt avtal, vanligtvis garanterar internetleverantörer att skicka vidare så kallad ”clean traffic” till ditt datacenter över en viss nivå, många skydd har ett tak om t.ex. 10 Gbps så det som händer när du blir utsatt för en attack som går över den gränsen tar man ut ditt företag, s. k. ” Blackholing” och det får samma effekt som själva DDoS-attacken, du är borta från internet. Men internetleverantören måste ta ut dig som är under attack för att såväl skydda sina andra kunder som sitt eget nätverk.

**Vad ska man då göra?**  
En allmän rekommendation är att ha en webbplats som levereras av någon med kraft att stå emot attacker och identifiera densamma. Det gör man genom att flytta ut det primära säkerhetslagret på internet där Terabit inte är så stora siffror och det gäller helt oavsett om man har ett privat datacenter eller om man har sina servrar i molnet på olika sätt. Dessutom bör man skydda på såväl applikationsnivå med en Web Application Firewall (WAF) samt på nätnivå alltså från applikationslagret och neråt.

Vi har också tagit fram ett antal punkter som stöd:<https://www.akamai.com/uk/en/multimedia/documents/brochure/8-steps-to-a-ddos-mitigation-plan.pdf>

Här kan du läsa hela rapporten Q4 2017 Akamai State of the Internet på engelska: <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf>

Här kan du läsa mer om den senaste attacken: <https://blogs.akamai.com/2018/03/memcached-fueled-13-tbps-attacks.html>

**För mer information, kontakta**  
Erik Henriksson, kundansvarig på Akamai  
[ehenriks@akamai.com](mailto:ehenriks@akamai.com)   
0708-35 46 35  
Bild på Erik Henriksson, <https://www.linkedin.com/in/erikhenriksson/>  **Om Akamai**Akamai erbjuder världens största och mest pålitliga plattform för leveranser av molntjänster. Kunderna får de bästa och säkraste digitala upplevelserna på vilken enhet som helst, när som helst och var som helst. Dessutom ger plattformen som används i över 200 000 servrar i 130 länder en överlägsen prestanda och skydd mot hot. Akamais portfölj innehåller webb- och mobilprestanda, molnsäkerhet, företagsåtkomst och videoleveranslösningar som levereras tillsammans med en exceptionell kundservice och övervakning dygnet runt alla dagar. Bland kunderna finns många av de bästa finansinstituten, e-handelsledarna, media- och underhållningsleverantörerna och de statliga organisationerna. Läs mer på [www.akamai.com](http://www.akamai.com), [blogs.akamai.com](http://blogs.akamai.com/) eller @Akamai på Twitter.