Connection reset by Peer! Vem är Peer?!

Tänk dig in i ett scenario där du sitter och chattar och surfar på hemsidor och helt plötsligt så kommer du inte åt en hemsida. På hemsidan står det: ”Connection reset by Peer!”… Jag har länge undrat vem den där Peer egentligen är… Något som är sant är i alla fall att han inte verkar vara någon trevlig kille! Eller… är det kanske en tjej?

apr_socket_recv: Connection reset by peer

Skämt å sido… Vad vet vi egentligen om Denial of Service-attacker? Det känns som att hela begreppet om DoS-attacker idag handlar om överbelastningsattacker. Vi tar för givet att en Denial of Service-attack är en överbelastningsattack, men faktum är att det handlar om helt olika attacker. Men vad är då en Denial of Service-attack?

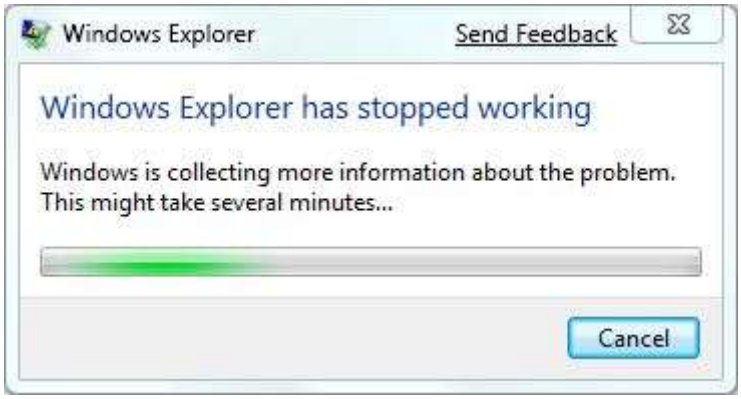
Jo, själva attacken handlar om att förhindra åtkomst till en tjänst. Det handlar alltså inte om att krascha eller sänka en hel server, utan att förhindra att personer får åtkomst till en tjänst. Då är kanske frågan; hur går angriparna tillväga för att göra detta? Det hade såklart fungerat att krascha hela servern, men det finns givetvis andra tillvägagångssätt.

Innan vi kommer dit vill jag berätta lite om DDoS-attacker då jag tidigare i texten bara pratat om DoS-attacker. Vad är då skillnaden mellan en DDoS- och en DoS-attack. Förkortningen står för Distributed Denial of Service attack och betyder kort och gott att attacken kommer från flera källor. Det är alltså inte bara en dator som utför attacken utan det är jättemånga. Nätverken bakom dessa attacker brukar oftast vara hackade datorer som ingår i ett större botnät där en av funktionerna för botnätet kan vara att utföra en DDoS-attack. En av de absolut vanligaste attackerna för att utföra en DDoS-attack är just överbelastningsattack.

Ett botnät kan bestå av flera hundra tusen kapade datorer och om varje dator finns på en vanligt snabb Internetuppkoppling så blir den totala bandbredden från alla de kapade datorerna enorm. När alla datorerna samtidigt försöker att kommunicera med måldatorn så har måldatorn inte resurser eller bandbredd att svara på alla förfrågningar. Det är då den datorn inte går att nå. Det är en klassisk överbelastningsattack; den med mest bandbredd vinner helt enkelt.

Men det behöver inte vara så att man konsumerar all bandbredd, det går även att konsumera alla sessioner för en tjänst. Om man har en hemsida klarar servern bara av att svara X antal besökare samtidigt. Det är ofta därför en hemsida blir slö när den får många besökare, det har alltså inte bara med bandbredden att göra. När man sedan lägger in stora bilder eller om hemsidan kanske har en databas eller mer kod än bara statisk text och bilder så börjar det bli ännu svårare att skydda sig.
Tänk dig själv att du har en hemsida med en sökfunktion; i databasen finns flera tusen tabeller som man skall sökas igenom. Om man lyckas att få hemsidan att söka genom hela databasen så tar det ganska långt tid innan man får svaret tillbaka. Då kan angriparen helt enkelt starta flera sökningar på samma sida, vilket binder upp tjänsten till en och samma användare.

För att göra en tjänst otillgänglig behövs inte massvis med bandbredd, om man har otur räcker det med ett enda litet paket för att tjänsten ska krascha. Vi pratar väldigt ofta om att man måste ha alla säkerhetspatchar installerade på sin dator, det gäller såklart även på servrar. I programkoden kan det finnas buggar som gör att hela programmet kraschar. Ni har väl själva varit med om det? Att er webbläsare eller något annat program helt enkelt hänger sig och man måste starta om. Det räcker med att man ställer en konstig fråga, en fråga som programmet/tjänsten inte klarar av att hantera för att den ska balla ur.



Förr i tiden, när folk var uppkopplade med modem, fanns det en bugg i vissa US Robotics-modem som gjorde att du kunde skicka AT-kommandon. Det var kommandon som modem använde för att exempelvis ringa upp ett telefonnummer eller lägga på luren osv. Ett av dom var +++ATH0 som just var kommandot för att lägga på luren. Om man omvandlade ”+++ATH0” till hexadecimala värden och skickade de som ”meddelande” i ett vanligt ping-paket kunde man få modemet att helt enkelt lägga på. Vilket var en form av DoS-attack. Man kunde utföra denna attack genom att enkelt i en kommandopromp köra följande kommando:

ping -p 2b2b2b415448300d -c 5 <IP>

Vissa tjänster var så pass sårbara att om man enbart skickade ”+++ATH0” till dator, i ett inputfält för användarnamn, lösenord eller vad som helst, så lade modemet på… Så frågan är om det verkligen var bättre förr? :D

Jag får ofta frågan om hur man som användare kan skydda sig? Självklart är det bra om all mjukvara man kör är uppdaterad med de senaste säkerhetspatcharna, men det är absolut inte allt. Som jag beskrev tidigare så är det extremt svårt att skydda sig eftersom det kan handla om allt från en dåligt skriven hemsida till att någon med mer bandbredd helt enkelt slår ut kommunikationen. Det finns massvis av tekniska lösningar som skall förhindra DoS-attacker men de fungerar väldigt dåligt om man inte betalar otroliga summor.

En bransch som är speciellt utsatt för dessa typer av attacker är hostingföretag, vilket gör detta inlägget kanske än mer betydelsefullt. Hos nästan alla hostingföretag så finns flera kunder installerade på samma fysiska server, vilket medför att om en av kunderna blir mål för en DoS-attack är sannolikheten stor att de andra kunderna på samma server också blir drabbade.

Detta kan vara lite svårt att förstå ibland, men när man tänker på det så är det ganska logiskt. Om ett hostingföretag har 500 stycken kunder så kan de såklart inte ha 500 fysiska servrar, det hade varit tokigt och riktigt dåligt för miljön också.

Jag tror inte vi kommer att se ett slut på dessa attacker i den närmsta framtiden men det betyder inte att vi ska sluta agera! Försök att hålla er uppdaterade med de senaste säkerhetspatcharna och ha lite förståelse för att det nästan inte finns något hostingföretag som kan skydda sig mot detta.

Tack för mig!

MVH David Jacoby, säkerhetsforskare på Kaspersky Lab