Avhjälpt hackarattack, så här gjorde jag!

“Jag som inte drabbats av attacker mot hemsidan på länge är nu “under attack”. Värre för svenska myndigheter än för mig. Först krashade sidan. Jag gick in på servern och i filsystemet lägger jag till _ efter pluginmappen/extensionmappen. Nu gick hemsidan upp igen. Krashen var knuten till en äldre opublicerad kommentar och en specifik plugin.

När jag raderat kommentaren kunde jag aktivera pluginen igen, som nu visade att den var hackad. Jag raderade pluginen men hackarscriptet ligger kvar (möjligtvis som cookie i filsytemet) och vill att jag ska arbeta med ftp och ber om uppgifter för att uppdatera plugins. Det är ett virus, skriv inte in uppgifterna.

Att få upp den krashade sidan och hitta orsaken tog mig ca 1 minut. Nu ska jag lokalisera cookien och får troligtvis besöka phpmyadmin. Jag ska även göra en virusskanning på hela servern. Det är 5 ip-adresser som attackerat, som är proxy för en riktig attackerare”.

Jag hittade den ansvariga

Efter att ha blockerat ett antal IP-adresser med hackarförsök hittade jag en “grafikers hemsida” som möjligtvis inte är en grafiker eller hackad själv. På adressens sökresultat genom Google <- observera att jag inte skrev in webbadressen direkt i sökfönstret utan Googlade adressen, fann jag åtskilliga meta-texter.

En metatext ligger i headern (den övre delen av webbsidan) och normalt sett går det endast att ha 1 metatext och en sektion med metataggar (som sökord). Den här designsidan hade ett 30-tal meta-texter. De var placerade i Sydney, i Colombia, hade

huvudkontor i Los Angeles mm och står med företagsinformation på Crunchbase, LinkedIn osv.

Enligt företagsinformationen är huvudkontoret i USA men de jobbar från Filippinerna och deras huvudsyssla förutom hemsidor i olika format, är databasprogrammering! -Se där?

Jag är van vid hackare i olika format och jag kan tycka det är ett måste att kunna lite om säkerhetsåtgärder om man ska uppehålla sig på internet. Sen kan jag också tycka att det finns olika typer av hackare. En hackare som i det här fallet utger sig för att komma från specifika länder, för att orsaka problem för landet de låtsas vara, de hackarna gillar jag väldigt lite.

Under har jag kopierat och översatt en text om DDos-attacker. Hjälper det någon så blir den glad!

“DDoS-attacker finns i ett stort antal. Här är några av dem:

Reflektionsattacker

Attackerna missbrukar en funktion i ett UDP-baserat protokoll där en liten begäran utlöser ett stort svar. DNS och NTP har vissa funktioner som tillåter denna typ av missbruk.

Upptäcka reflektionsattacker

Leta upp DNS/NTP-svar som ditt system aldrig skickar en begäran om. udp.srcport == 53 eller udp.srcport == 123 skulle vara de rätta visningsfiltren

Svaret kan lätt överskrida den maximala storleken på en Ethernet-ram. Håll utkik efter IP-fragmentering. Ett antal visningsfilter hjälper. ip.frag_offset > 0 är en av dem.

Observera att IP-fortsättningspaketen inte kommer att innehålla UDP-portnumren. Wireshark stöder återmontering av IP-fragment, så att hela meddelandet kommer att dissekeras.

TCP SYN översvämningar

Dessa attacker försöker fylla tillståndstabellen i en brandvägg eller försöker överväldiga en servers buffert. Det finns ett antal tekniker för att försvara sig mot denna typ av attack. TCP SYN cookies är en av dem.

Upptäcker SYN-översvämningar

Håll utkik efter ett enormt antal TCP-anslutningsförfrågningar. Det korrekta visningsfiltret är tcp.flags.syn == 1 och tcp.flags.ack == 0

Servern, som är under attack, kommer att svara med ett mindre antal SYN/ACK. Dessa kan ses med visningsfiltret tcp.flags.syn == 1 och tcp.flags.ack == 1

Försök att jämföra antalet SYN med antalet SYN/ACK. Så länge siffrorna är identiska håller din brandvägg eller server.

Mycket ofta är källadresserna förfalskade. En bra indikator på en falsk källadress är ett paket med RST-biten inställd som svar på SYN/ACK från din server. Det normala svaret skulle vara ett paket med bara ACK-flaggan inställd.

Attacker mot lager 7 på dina webbservrar.

De flesta webbservrar har en sökfunktion, användarregistreringsdialog eller liknande funktion, som utlöser ett långt svar i backend. En angripare kan identifiera lämpliga mål genom att undersöka HTTP-svarstiden. Vissa webbplatser kan slås ner av ett förvånansvärt litet antal parallella HTTP-förfrågningar som utlöser sökningar, processinloggningsdata eller utcheckningsprocessen i en webbutik.

Upptäcka attacker från lager 7

Det bästa är webbserverns loggfil, speciellt om du använder HTTPS. (Du använder förhoppningsvis SSL, eller hur?) Försök

att hitta ofta kallade URI:er i loggfilen.

Håll utkik efter användaragenter som indikerar automatisk åtkomst. Bland kandidaterna finns wget eller curl.

Om du har tillgång till okrypterad trafik, försök skapa en separat profil och lägg till kolumner för användaragenten http.user_agent och för URI:n http.request.uri

Kontrollera om HTTP-förfrågningar kommer med en referens, där det är rimligt att förvänta sig dem. Tillgång till utcheckningsfunktionen i en webbutik utan hänvisning skulle vara udda. Lägg till http.referer som en annan kolumn.

Geografisk fördelning av IP-adresser

De flesta webbplatser har ett distinkt mönster när användare från en viss geografisk region besöker webbplatsen. En webbplats för en skola eller högskola skulle oftast dra trafik från lokala eller regionala IP-adresser. Förvänta dig också några sökmotorer och sökrobotar. En plötslig ökning av förfrågningar från ganska avlägsna platser skulle vara en indikator på en attack.

Denna wireshark-webbplats besöks av ett internationellt samfund. Jag har aldrig sett loggfilerna för den här servern. Ändå skulle jag förvänta mig över ett 24-timmars tidsfönster besökare från hela världen. Bara jag tittar på loggfilerna klockan 10 på morgonen europeisk tid skulle jag förvänta mig mestadels europeiska besökare, plus några nattugglor från Asien-Stillahavsområdet och några morgonpigga från Amerika.

En bra baslinje hjälper till att upptäcka attackerna. Wireshark kan lokalisera platsen för en IP-adress. Kolla in Wireshark Wiki för detaljer

DDoS efter popularitet

Även om ovannämnda skolwebbserver för det mesta är inaktiv, kan den locka till sig en enorm ökning av legitim trafik.

Räkna med en allvarlig översvämning av trafik, om stora nyhetsnätverk rapporterar om skolan och lägger en länk på deras webbplats. Något liknande kan hända om en användare av sociala medier med miljontals vänner eller följare nämner din webbplats.

Allmänna tips

Vissa verktyg som används för nätverksöversvämning definierar konstanter i vissa fält i IP- eller TCP-huvudet, där en viss mängd slumpmässighet kan förväntas. Exempel är IP-ID, DNS-transaktions-ID, ett TCP-källportnummer eller sekvensnummer. Ett överdrivet värde av paket med ett konstant IP-ID är en indikator för en mycket konstig IP-stack eller för "handgjorda" paket."

Intressanta verktyg:

https://bgp.tools/

https://ask.wireshark.org/questions/