

Firewall rond DNS tegen criminele misleiding

www.niet-de-site-die-je-denkt-dat-het-is.nl

Een surfer merkt het nauwelijks, maar het internet bestaat helemaal niet uit *www*'s en *.nl*'s. Eigenlijk wijzen alleen getallen, IP-adressen, de browser de juiste koers. De koppeling tussen de domeinnamen en de getallen wordt gelegd door DNS-servers. Zij vormen een vitale, maar kwetsbare schakel. Eentje die de misdaad uit kan buiten.

DOOR HANS STEEMAN

Ze duiken regelmatig weer op, nep-e-mails die zijn bedoeld om gebruikers naar webpagina's van criminelen te lokken. Met een website die er nageoeg hetzelfde uitziet als de oorspronkelijke pagina, worden bankgegevens van gebruikers afgetrosgeld. Tijdens zo'n zogenaamde man-in-the-middleattack krijgen gebruikers het gevoel dat zij zakendoen met hun eigen bank. Ze weten niet dat tussen hen en de bank een criminele organisatie zit, die stilletjes gegevens aanpast zodat een flinke som geld ongewild van eigenaar wisselt. De transactie lijkt normaal te verlopen.

Pas als het bankafschrift in de brievenbus valt, blijkt wat deze aanval heeft aangericht. De meest voor de hand liggende manier om een man-in-the-middleattack uit te voeren, was tot nu toe het sturen van een e-mail met een gemodificeerde URL naar de website van een financiële instelling. Inmiddels is tegen de zogenaamde phishing-e-mails en de virussen die dit gedrag vertonen een adequaat medicijn ontwikkeld. De criminelen hebben niet stilgezeten. De volgende generatie bedreigingen dient zich al weer aan: aanvallen op de domainnameservers (DNS). Daarbij

passen ze de vertaaltabellen van een DNS aan, zonder dat de gebruiker erg in heeft. Het probleem kan zich zelfs voordoen in bedrijfs-DNS'en, een plaats waar vaak te weinig controle is. Deze verandering van strategie heeft grote gevolgen voor het computergebruik. Applicaties, zoals browsing, e-mail, internettelefonie, e-commerce et cetera, zoeken allemaal via de DNS-toegang naar servers op het netwerk of internet. Deze nieuwe soort aanvallen zet dus de bijl aan de wortels van de moderne internetsamenleving. Geen enkele DNS is compleet immuun te maken voor dit probleem, kant en klare fixes zijn dan ook niet snel beschikbaar. Netwerkbeveiligingsexperts en -leveranciers hebben de handen ineengeslagen om te werken aan een eerste pleister. Het is geen definitieve oplossing, maar het begin van de zoektocht naar een remedie. Langetermijnoplossingen zijn nog onderwerp van discussie. Een reeks van patches zal het levenslicht zien, totdat er een permanente oplossing is. Ondertussen zijn er al weer heel wat aanvallen geweest, zelfs op de DNS'en die met een eerste patch waren opgelapt. Netwerkbeheerders kunnen

Zonder DNS-propagatie geen world wide web



zich opmaken voor een langdurig gevecht met de cybercriminelen.

Vergiftigde servers

De domainnameserver is een intern telefoonboek voor een netwerk. Het vertaalt een naam die de gebruiker begrijpt, bijvoorbeeld de URL *www.telecommagazine.nl*, in een IP-adres dat de computer begrijpt, bijvoorbeeld 213.193.237.180. Deze vertaalslag is de kern van het proces op basis waarvan webbrowsers en andere internetprogramma's werken.

Door de DNS is een dienst ook te benaderen, zonder dat het fysieke netwerkadres bekend is. Verandert het IP-adres van een server, bijvoorbeeld bij een migratie, dan is slechts een aanpassing in de DNS-tabel nodig om de configuratie weer te laten werken. Op het internet zijn mechanismen aan het werk, die de veranderingen in deze tabellen op een betrouwbare manier uitwisselen tussen DNS'en. Zonder die mechanismen kan internet niet bestaan.

Beveiligende laag tussen DNS en internet

Op 6 augustus van dit jaar doken de eerste signalen van DNS-attacks op. Toen beschreef Dan Kaminsky, een bekende internetbeveiligingsexpert, hoe criminelen zwakke plekken in de DNS-architectuur kunnen misbruiken voor hun activiteiten. Het nieuwe beveiligingsprobleem is DNS-poisoning, het vervuilen van de informatie in de DNS-cache van serviceproviders of in die van grotere bedrijven, die hun eigen DNS-service hosten. Als de DNS een domeinnaam naar een IP-adres vertaalt, krijgt hij niet meer het juiste resultaat, maar geeft hij het IP-adres van een crimineel domein op. Is het verkeer eenmaal naar dat domein omgeleid, dan is er gelegenheid voor tal van misdadige activiteiten. Het ontfoetselen van persoonlijke, privacygevoelige informatie is het eenvoudigst. Andere praktijken zijn het

onderscheppen van e-mail, het ontregelen van een spamfilter, het redirecten naar fake sites van banken of andere officiële instellingen en het afvangen van een wachtwoord, met de 'forgot password'-optie die veel websites ondersteunen. Uiteraard is het ook mogelijk al het webverkeer te sniffen en er bedrijfskritische informatie uit te filteren. Sommige van deze cyberaanvallen hoeven de gebruiker niet eens op te vallen, al zorgen ze ondertussen vaak wel voor gigantische schadeposten. De totale impact van dit risico is nog niet goed vastgesteld, maar het is wel duidelijk dat de gevolgen heel erg groot kunnen zijn.

Verdedigingslinie

De eerste pogingen om het probleem onder controle te krijgen dateren van juli dit jaar. Toen verstuurde het

advertentie

TELECATS

Flexibele klantcontactoplossingen met IVR, Taal- en Spraaktechnologie en VoIP

Krachtig, betrouwbaar en flexibel Multi-channel VoIP contact center

**IVR
Taal- en Spraaktechnologie
Voice over IP**

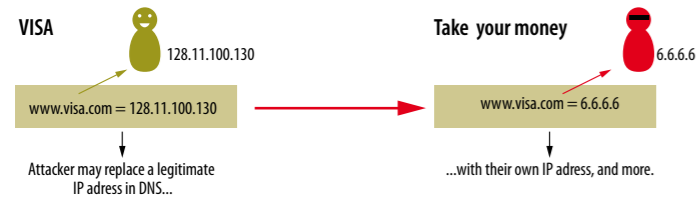
**Multi-channel
VoIP contact center**

**Innovatieve
Klantcontactoplossingen**

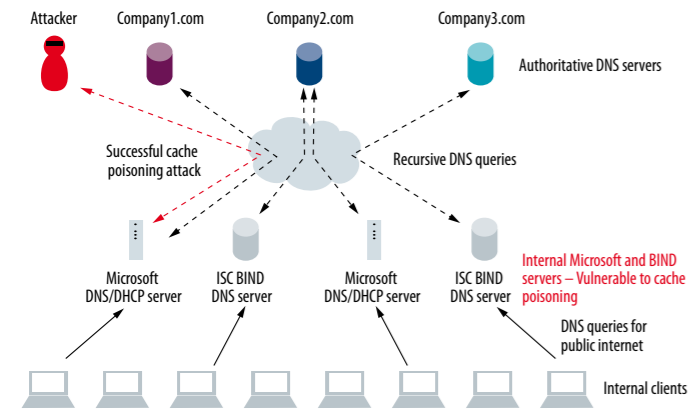
VoIP systemen en diensten

Telecats BV - Colosseum 42 - 7521 PT Enschede - 053 488 99 00 - www.telecats.nl

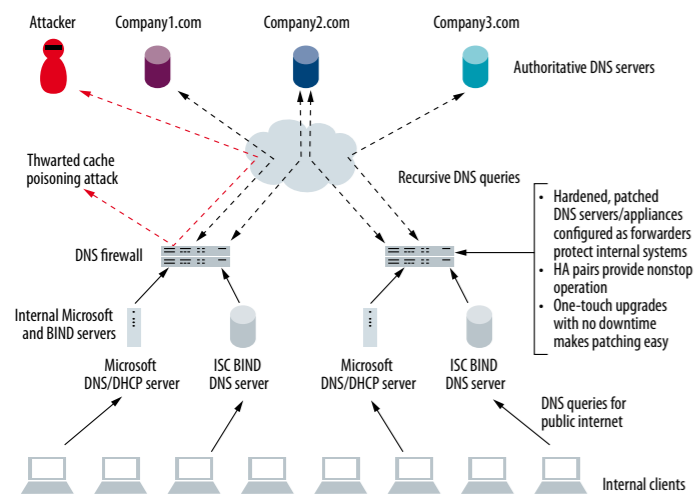
Figuur 1. Zo werkt een DNS-aanval.



Figuur 2. DNS zonder firewall.



Figuur 3. DNS met firewall.



Figuur 4. Ingebouwde beveiliging van de firewall.

DNS protocol monitoring

- Real-time reporting

Attack alerts

- E-mail/trap when attack profile thresholds exceeded

Attack mitigation

- Limit DNS query rate by source address and other parameters

De eerste patch maakte hacken hooguit moeilijker

Computer Emergency Response Team (CERT) een brandbrief over deze nieuwe attack en de noodzaak van DNS-patches. De reactie daarop viel tegen, want slechts de helft van de organisaties voerde de update daadwerkelijk uit. Deze eerste patch was niet de laatste, hij maakte het hacken van de DNS hooguit moeilijker. Omdat de DNS vaak de identificatie van certificaten en andere identificatiemiddelen regelt, lopen ook SSL en OpenID behoorlijke veiligheidsrisico's. Het is niet verwonderlijk dat zelfs de gepatchte DNS'en nog steeds onder vuur liggen.

Infoblox heeft DNS QuickSecure Solution ontwikkeld, een beveiligende laag tussen de DNS'en van een organisatie en het internet. Deze DNS-firewall is eenvoudig te onderhouden en te updaten als dat noodzakelijk is. De oplossing werkt op een aantal principes. DNS'en zijn vooral gevoelig voor cachepoisoning, wanneer zij via het internet een recursieve DNS-request naar een niet-vertrouwde DNS afhandelen. Dit gebeurt als een DNS de vraag van een gebruiker niet kan beantwoorden en de hulp inroept van een andere DNS. Juist omdat de DNS-informatie in de cache vluchtig is, is hij gevoelig voor aanvallen.

De DNS-firewall schermt de fysieke DNS af van het internet, maar staat de systemen wel toe om recursieve vragen te beantwoorden. Dit maakt ze immuun voor cachevervuiling. Daarnaast is er een rapportagehulpmiddel, dat direct opmerkt wanneer een specifiek DNS-request vaker voorkomt dan verwacht. Zo bespeurt het mogelijke aanvallen. Snel en tijdig waarschuwt het systeem de administrators dat er iets gaande is op hun DNS-farm en ze mogelijk moeten ingrijpen. Anycast stuurt DNS-verzoeken bovendien automatisch door naar servers die niet tijdelijk onbereikbaar zijn of aangevallen worden.

De firewallhardware bestaat uit dedicated en robuuste systemen, die inherent veiliger zijn dan de standaard serverhardware en besturingssystemen. Door ze in een grid te gebruiken, wordt de downtime geminimaliseerd en ontstaat er een solide netwerk. Het besturingssysteem NOIS van Infoblox staat op alle hardware, inclusief autorisatieservers, secondary servers, cachingservers en een combinatie daarvan. Het OS kan verschillende configuraties aannemen, zodat het elke DNS-functie uit kan voeren. Naast DNS ondersteunt de hardware ook DHCP, IPAM, Radius, ftp/tftp/http, NTP en andere protocollen. Daardoor vormen ze een stabiel, veilig en centraal te managen systeem voor de corenetwerkdiensten.



Razendsnel e-mailen en internetten waar en wanneer u wilt. Met de Dongel van KPN.

- Net zo snel als op de zaak (7,2 Mbit/s)
- Gemakkelijk te installeren en met twee muisklikken online
- Probeer het de eerste maand vrijblijvend

19,95/mnd excl. btw



Mobiel werken. Makkelijk toch?

