



## De wedloop tussen criminelen en beveiligers

# Cybercrime steeds grotere plaag

**De bedreigingen in de IT-wereld zijn nogal veranderlijk. Aanvallers en verdedigers zijn continu bezig de ander een stap voor te zijn. Hoe is de werkwijze van internetcriminelen in de loop der jaren veranderd, waarom dat is gebeurd en wat kunnen we in de nabije toekomst op dit gebied nog verwachten?**

**J**ongeren onder ons nog zijn wel eens verbaasd als ze horen dat internet zijn wortels heeft in de zeventiger jaren van de vorige eeuw. Toch is dat zo. Nadat het internetprotocol werd uitgevonden om verschillende soorten systemen met elkaar te verbinden, zoals UNIX en VMS, groeide internet in de tachtiger jaren heel snel in de academische wereld. Aan beveiliging werd in deze open omgeving weinig gedaan. Firewalls bestonden niet en wachtwoorden waren eenvoudig te raden. De criminaliteit bestond toen vooral uit pestertijtjes met virussen. Deze waren wel vervelend, maar vaak niet destructief (hoewel er ook waren die je harde schijf wisten). Naast puur vandalisme was het motief voor inbraak op systemen vaak het verkrijgen van aanzien in een sociale groep en hackte men om te leren. In die tijd waren aanvallers eigenlijk altijd begaafde computeraars en meestal niet écht crimineel. Geld verdienen was er ook niet bij, men brak in voor status, uit ideologie of om mensen te pesten. Hoe anders is dat nu!

### Een andere wereld

We leven tegenwoordig in een wereld waarin afstanden zijn verdwenen dankzij het internet. Systemen en services over de hele wereld zijn te bereiken vanuit de luie stoel thuis, zowel voor legitieme gebruikers als voor criminelen. De

computernerds die het leuk vonden om de website van het Witte Huis aan te passen hebben plaatsgemaakt voor een hele nieuwe lichter internetcriminelen: mensen die het internet als hulpmiddel gebruiken en geen technische kennis hebben. Internet is voor de crimineel een zegen. Hij kan zijn activiteiten vanaf vrijwel elke locatie doen en vaak zelfs grotendeels automatiseren. Er is een schier oneindige voorraad aan doelwitten. De pakkans is miniem, voornamelijk doordat landsgrenzen er op internet niet toe doen, maar voor opsporing en berechting een bijzonder groot obstakel vormen. Dit laatste heeft ervoor gezorgd dat internetcriminaliteit, gemeten naar de hoeveelheid geld die erin omgaat, de drugscriminaliteit inmiddels heeft ingehaald. U leest het goed: er wordt veel geld verdiend met drugs, maar nog meer met internetcriminaliteit. Dat is een groot verschil met de vorige eeuw, toen er voor internetcriminelen nauwelijks geld te verdienen was. Nu e-commerce echter

## Er is een schier oneindige voorraad aan doelwitten

zo'n opmars heeft gemaakt, zijn op veel plekken creditcardnummers te vinden. Dat is de handelswaar van de internetonderwereld. Afhankelijk van de beschikbaarheid van bijbehorende gegevens zoals naam en card verification code (CVC) kan een enkel creditcardnummer een paar cent tot enkele tientjes opbrengen. De nummers fungeren als ruilmiddel of worden ingezet om bij webshops goederen te kopen. Behalve creditcardnummers zijn ook inloggegevens bij banken en andere financiële instellingen (denk aan PayPal) een geliefd object.

### Twee opties

Om geld te verdienen zijn er eigenlijk twee opties: het stelen van creditcardnummers en inloggegevens of het aanbieden van diensten aan andere criminelen. Het stelen van creditcardnummers gebeurt meestal met behulp van gerichte aanvallen op webshops, waar klantgegevens opgeslagen zijn. De reglementen van de creditcardmaatschappijen schrijven voor dat CVC's niet online mogen worden opgeslagen, maar ook zonder CVC zijn creditcardnummers geld waard. De criminelen worden hierbij geholpen door het feit dat er maar weinig verschillende besturingssystemen en webshopapplicaties zijn. Vrijwel alles werkt tegenwoordig met een webinterface. Dat maakt bepaalde soorten aanvallen herbruikbaar op vrijwel alle applicaties. Als er een fout wordt gevonden in een stuk commerciële webshopsoftware, dan kan die eenvoudig wereldwijd uitgebuit worden.

De crimineel van nu heeft zelf vaak de kennis niet om een bug te vinden en die te misbruiken, dat werk wordt uitbesteed aan slimme criminelen. Die spenderen hun tijd aan het vinden van nog onbekende lekken in systemen en applicaties, die ze verkopen voor bedragen van 4 of 5 cijfers. Na aankoop hoeft je alleen nog maar op de knop te drukken om het lek te misbruiken. Criminelen houden van



dit soort makkelijke aanvallen met een lage pakkans. Naast het gericht inbreken in bepaalde systemen, zoals webshops, is het ook lucratief om gewoon willekeurige systemen van eindgebruikers aan te vallen. Een aanvaller die de controle krijgt over zo'n systeem, kan een aantal dingen doen. Allereerst kan de pc nagepluisd worden om te zien of er creditcardnummers of inloggegevens op staan of dat zulke gegevens live worden gebruikt. Maar ook al is er weinig informatie te vinden, dan nog kan zo'n systeem interessant zijn. Als de crimineel veel systemen heeft gekraakt, kan hij deze namelijk inzetten om bepaalde opdrachten uit te voeren. We spreken dan over botnets. De opdrachten zijn via een eenvoudige webinterface in te geven, dus ook hier is geen intelligentie vereist. Toegang tot op deze wijze gekraakte systemen wordt voor een paar cent per systeem verkocht. Diensten die kunnen worden geboden zijn bijvoorbeeld spamming, waarbij alle gekraakte systemen in hoog tempo berichten de wereld insturen. Een botnet kan ook voor afpersing gebruikt worden. De aanvaller neemt daarbij contact op met een partij en vraagt geld in ruil voor het niet plat leggen van de infrastructuur. Om het slachtoffer te laten zien dat het ernst is, laat hij zijn duizenden gekraakte systemen herhaaldelijk voor een aantal minuten allemaal tegelijk de website van het slachtoffer bezoeken.

### Steeds complexer

Dit soort criminaliteit is erg moeilijk aan te pakken. Het is redelijk makkelijk om anoniem te blijven. Niet omdat internetverkeer niet traceerbaar is, maar omdat de criminelen van het ene naar het andere systeem hoppen. Heb je de vermoedelijke bron gevonden, dan blijkt de verbinding eigenlijk ergens anders vandaan te komen. Omdat al deze systemen in verschillende landen kunnen liggen en bij elk systeem medewerking van de autoriteiten nodig is, is het vinden van de uiteindelijke dader een hopeloze zaak. Indien de aanvaller zich in een land bevindt waar internetcriminaliteit niet berecht kan worden, dan is al het werk nog voor niets geweest ook. Het voorkomen van beveiligingslekken die misbruikt kunnen worden, zou een betere manier zijn om het internet veilig te krijgen dan het achteraf opsporen

## Een botnet kan ook voor afpersing gebruikt worden

van de criminelen. Helaas is beveiligen moeilijker dan menigeeen denkt. Als je je fiets niet op slot zet, ziet iedereen onmiddellijk het beveiligingslek. Bij computers hebben we echter te maken met software, waar je niet zomaar aan afziet of het veilig is. Daar zijn uitgebreide tests voor nodig. Het feit dat een stuk software werkt, is nog geen garantie dat het veilig is – net zoals een goed rijdende fiets onveilig geparkeerd kan worden. Daar komt nog bij dat systemen steeds complexer worden en daarmee ook onveiliger. De geschiedenis leert ons dat bij het herschrijven van de code om die ene bug te verwijderen, er altijd wel weer een nieuwe bug wordt toegevoegd. Per duizend regels programmacode hou je zo altijd vijftien tot vijftig bugs over. Gelukkig worden softwarepakketten wel verbeterd en besteden veel bedrijven aandacht aan de beveiliging van hun systemen en software, ook al is dat vaak vanwege wet- en regelgeving waaraan ze moeten voldoen. Als het gaat om het inbreken in specifieke systemen met interessante informatie, dan gaat de wedloop tussen criminelen en beveiligers op het technische vlak redelijk gelijk op. Het internet is inmiddels echter getransformeerd van hulpmiddel voor mensen met veel IT-kennis tot een basisbehoefte voor iedereen, ook niet-technenuten. Mensen met weinig kennis van computers maken er veel gebruik van, ondanks het feit dat computers erg complexe apparaten zijn. We kunnen apparaten met beperkte functionaliteit redelijk veilig maken (denk aan auto's), maar voor een systeem zo complex als een computer is dat onmogelijk. Criminelen weten dit ook, daarom valt men nu vakerr de eindgebruiker aan dan het systeem zelf.

### Achterdeurtjes

Naast phishing wordt gebruikgemaakt van trojan horses, bijvoorbeeld verstopt in illegale versies van veelgebruikte softwarepakketten, die de pc infecteren. Veel eindgebruikers denken dat een virusscanner ze immuun maakt voor aan-

vallen, maar veel virussen worden niet gedetecteerd, met alle gevolgen van dien, zeker als er een eindgebruiker met beheerrechten (administrator) aan het werk is. Helaas kennen eindgebruikers zonder gedegen IT-achtergrond deze risico's niet en handelen ze er niet naar.

Instellingen als banken proberen de eindgebruiker met technische middelen (calculators, codes via sms) beter te beveiligen, maar uiteindelijk blijft de eindgebruiker altijd de zwakste schakel. Als die ingaat op slinkse verzoeken om de uitvoer van de calculator ergens op te geven, dan helpt geen enkel systeem. Hun inspanningen richten zich niet alleen op het aanvallen van de mens, criminelen verfijnen ook hun aanvallen op systemen. De aandacht verschuift naar het kraken van systemen vóór ze in gebruik genomen worden. Als je pinautomaten voorziet van een achterdeurtje vanaf de fabriek, dan heb je naderhand overal toegang. Dit is ook daadwerkelijk gebeurd. Je kunt zo'n achterdeurtje natuurlijk ook inbouwen in de software, de hardware (van CPU tot harddisk), een stemcomputers enzovoort. Als het basisstelsel veilig wordt veronderstelt, zal dit niet aan het licht komen. Alle logging en auditing die zo'n systeem uitspuwt, is dan namelijk niet te vertrouwen, hoewel we daar nog wel steeds van uitgaan (denk aan de stemcomputers).

De wedloop tussen criminelen en beveiligers duurt dus voort. Als u als eindgebruiker uw verstand gebruikt en niet zomaar overal op klikt, geen schimmige sites bezoekt, niet als beheerder werkt en altijd updates uitvoert, dan kunt u het risico in ieder geval beperkt houden. Het testen van systemen en software op lekken is echter een specialisme dat een eindgebruiker niet heeft, dit zal altijd werk blijven voor specialisten.

**WALTER BELGERS**

*is securityconsultant bij Madison Gurkha.*