CYBERSCHERMUTSELINGEN

"Mensen hebben de afgelopen millennia oorlog gevoerd met alle denkbare middelen", vertelt Aiko Pras, onderzoeker aan de UT. "Pas sinds de atoombom zijn we terughoudender geworden met de inzet van alles wat mogelijk is. Via internet krijgen we instrumenten in handen waarmee we elkaar op een heel ander niveau dwars kunnen zitten. Er zijn absoluut landen die hierin investeren. Nederland is op dit vlak naïef." DOOR **Christian Jongeneel** ILLUSTRATIE **Rhonald Blommestijn**

Pras noemt het voorbeeld van het Stuxnet-virus, dat vorig jaar een aantal nucleaire installaties in Iran lamlegde. Analyse van experts wees uit dat het zeer geavanceerde software betrof, die specifieke apparatuur zo ontregelde dat het niet meteen opviel, maar die de installatie wel onklaar maakte. Alom wordt aangenomen dat de Israëlische overheid (eventueel met Amerikaanse hulp) de auteur van het virus was. Pras: "In het verleden heeft Israël een nucleaire installatie in Syrië gebombardeerd. Als ze dat in Iran hadden gedaan, zou dat grote politieke en militaire consequenties hebben gehad. Met het virus hebben ze hetzelfde bereikt, een terugslag van twee jaar in het Iranese atoomprogramma. Maar nu denkt iedereen: die Iraniërs hebben zich in de luren laten leggen. Cyberwar heeft serieuze gevolgen. Maar de perceptie ervan is anders."

Botnets

Dat overheden zich zichtbaar op het verschijnsel cyberoorlog storten is een recente trend. Tot een decennium geleden waren hackers vooral hobbyisten, die een technische uitdaging zagen in het kraken van systemen. Vijf jaar geleden begon de georganiseerde misdaad zich ermee te bemoeien, met name vanuit Rusland en Nigeria. Criminelen zetten zogeheten 'botnets' op, netwerken van pc's waarvan de gebruikers niet weten dat ze misbruikt worden. Botnets misbruiken pc's voor het 'oogsten' van informatie, zoals creditcardnummers, en het verspreiden van spam en DDoS-aanvallen – het platleggen van een systeem door een bombardement van informatieverzoeken.

DDoS

Pras deed in detail onderzoek naar DDoS-aanvallen op de websites van creditcard-maatschappijen, toen deze weigerden nog financiële diensten te leveren aan de klokkenluiders-website WikiLeaks. Een groep die zich Anonymous noemde, verspreidde een programmaatje waarmee iedereen kon hacken. "Dat was ook nieuw", aldus Pras. "Geen hobbyisten, criminelen of geheimagenten, maar het grote publiek werd ingezet als soldaten in een cyberoorlog. Als dat een trend wordt, zal de impact steeds groter worden."
Vanuit technisch oogpunt was de software van Anonymous primitief. Maar nu de potentie van hacken door het grote publiek aangetoond is, is het wachten op een programma dat wel 'state of the art' is.

Achterbuurten

Het onderzoek binnen Pras' groep richt zich vooral op het bestuderen van informatiestromen, niet door naar de inhoud van over internet verzonden informatiepakketjes te kijken, maar naar timing en adressen. Als een DDoS-aanval gelanceerd wordt, is te zien vanaf welke computers de eerste aanzet kwam. Verder terug in de tijd zijn die computers met bijvoorbeeld een chatkanaal in verband te brengen. Door te bepalen wie er met dat kanaal verbonden waren, kan de organisatiestructuur van de daders worden blootgelegd.
Pras en de zijnen proberen op deze manier de 'achterbuurten' van internet in kaart te brengen. Dat veel sporen naar Rusland en China leiden, is bekend, maar gerichte maatregelen zijn alleen te nemen als op het niveau van providers de rotte appels aan te wijzen zijn. Sommigen zijn daar overigens zeer open over. Een Chinese provider gaf onlangs openlijk toe enkele honderden criminele hackers onderdak te bieden op zijn systemen. Dat was geen probleem, vond hij, want ze betaalden goed en de overheid deed niks.

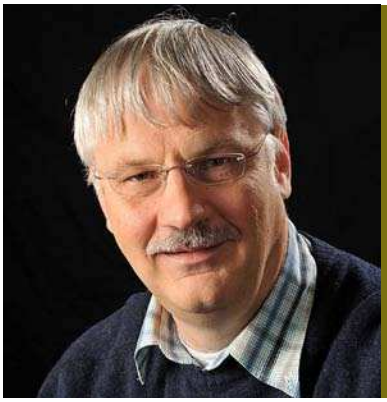
Ernstiger

Tot voor kort was Pras geneigd DDoS-aanvallen af te doen als minder relevant. Daar is hij op teruggekomen. Het platleggen van websites is hinderlijk, maar overkomelijk. Maar nu steeds meer infrastructuur op de een of andere manier op internet is aangesloten, zijn de potentiële gevolgen ernstiger. Een DDoS-aanval op het elektriciteits- of waternet kan de maatschappij werkelijk lam leggen.
"Daar komt bij dat we steeds meer kastjes in huis hebben die we niet meer als computer herkennen, zoals de netwerk-router en het voip-kastje dat telefonie via internet mogelijk maakt", zegt Pras. "Stel je voor dat iemand erin slaagt het voip-kastje van een provider te kraken. Dan kan hij in een enkele dag al die kastjes in zijn macht krijgen. Alleen door bij alle gebruikers langs te gaan kan de aanbieder de macht over zijn aansluitingen herwinnen. Die schade zal de aanbieder waarschijnlijk niet overleven."

"Cyberwar heeft serieuze gevolgen. Maar de perceptie ervan is anders"

Monter

Sterker nog, wie garandeert dat de kastjes niet met opzet achterdeurtjes bevatten? Onlangs werd een kastje van Chinese makelij aangetroffen dat bij verzending van een bepaalde code de microfoon aanzette en zo de telefoon effectief veranderde in een afluisterapparaat. Het zou een programmeerfout zijn, maar Pras waagt dat te betwijfelen. "Het is een geweldig interessant vakgebied", constateert hij monter.



**Dr. ir. A. (Aiko) PRAS is als universitair hoofddocent verbonden aan de faculteit Elektrotechniek, Wiskunde en Informatica van de Universiteit Twente.
Hij geeft leiding aan het onderzoek in Dynamische Systemen en Processen (DACS).**