Maandenlang hield de geheimzinnige computerworm Conficker de IT-wereld in zijn greep. Miljoenen pc's raakten besmet, maar wat waren de Conficker-makers nu eigenlijk van plan? Een reconstructie van de digitale krachtmeting tussen internetcriminelen en webbeveiligers.

WORSTELEN
met een worm

EEN GROEPJE EXPERTS op het gebied van computerbeveiliging staat aan een hotelbar in Arlington, Virginia. Het is 23 oktober 2008, en ze hebben zojuist de hele dag hun jaarlijkse topoverleg gevoerd over cybercriminaliteit. Die avond draait de kletspraat al snel om een ongebruikelijke beveiligingsupdate van Microsoft – ook wel een patch genoemd. Normaal gesproken komen die updates elke maand uit, maar deze diende zich twee weken te vroeg aan. "Ik dacht nog, dit is verdacht" zegt Paul Ferguson, onderzoeker bij Trend Micro, een beveiligingsbedrijf in Californië.

Dat vond ook de rest van de beveiligingsindustrie. De maanden erop stond hun werk grotendeels in het teken van de Conficker-worm, een uiterst doordacht stukje criminele software. In een paar maanden tijd besmette de worm ruim 9 miljoen computers in huizen, universiteiten, ziekenhuizen, overheden en legers. Zelfs Britse onderzeeers en oorlogsschepen raakten besmet, en ook de Bundeswehr in Duitsland en de Franse marine ontsprongen de dans niet. Daarmee ontstond een lucratief netwerk van zombiecomputers, wachtend op nadere instructies van de Conficker-makers. Maar Microsoft en enkele grote internetbeveiligingsbedrijven besloten niet lijdzaam toe te kijken. Ze pakten de handschoen op, en begonnen onder de naam *Conficker Working Group* een spannend kat-en-muisspel met de Conficker-makers.

De oktober-update van Microsoft deed aanvankelijk weinig stof opwaaien. Het verhaalde in droge technische taal over een beveiligingsprobleem in Windows 2000, XP en Vista waardoor computerwormen toegang kunnen krijgen tot het besturingssysteem. Wormen zijn stukjes code die zich ongezien voortplanten over het internet. Dit doen ze actief, in tegenstelling tot computervirussen die zich enkel hechten aan bestanden en afhankelijk zijn van mensen om zich te verspreiden. Geïnfecteerde computers vormen vaak *botnets*, netwerken van zombiecomputers die doen wat de virus- of wormmaker wil, vaak zonder dat de gebruiker het doorheeft.

Als alle Windowsgebruikers netjes hun updates hadden gedownload, was er niets gebeurd. Maar niet elke gebruiker volgt het update-advies even trouw, en bedrijven wachten soms weken met het installeren van een update. Grote bedrijven testen de patch vaak eerst voordat ze het installeren op al hun computers. Zelfs in januari 2009 – twee maanden na de uitbraak van Conficker – was nog 30 procent van de computers kwetsbaar, aldus veiligheidsfirma *Qualys*. Dit achterstallig onderhoud geeft criminelen genoeg gelegenheid om misbruik te ▶

maken van de situatie. Het is zelfs een beproefd middel onder criminelen: wachten tot Microsoft een beveiligingslek in Windows bekendmaakt, en dan snel een nieuwe worm uitbrengen die in het gat springt.

Lokaas Welke computer als eerste geïnfecteerd raakte met de Conficker-worm, is nog onbekend. Waarschijnlijk was het een computer die de hackers al in hun macht hadden. Vanaf het eerste moment struinde de worm het internet af, op zoek naar andere kwetsbare computers. Al snel vond het een zogeheten netwerktelescoop van het *San Diego Supercomputing Center*. Een dergelijke 'telescoop' is een soort lokaas voor wormen en virussen. Het bestaat uit miljoenen nep-internetadressen die allemaal uitkomen op een enkele computer. Alleen verdacht internetverkeer is er te vinden, want 'echte' internetgebruikers hebben er niets te zoeken – er is immers geen website op te vinden. Wormen zijn daar echter blind voor. De wormen proberen vanaf geïnfecteerde computers in te breken bij de telescoop, met als doel het te infecteren. De telescoop weert de aanval vervolgens af en registreert die als een inbraakpoging.

Het logboek van de telescoop toont de snelle uitbraak van Conficker. Op 22 november ontving de telescoop 3000 inbraakpogingen – niet veel meer dan achtergrondruis voor de telescoop, die wel vaker wormen ontvangt. De volgende dag stond de teller al op 115.000 aanvallen per uur. Conficker was duidelijk op dreef. Dezelfde dag dook de worm ook op in 'honingpotten'; opzettelijk onbeschermde computers die het digitale ongedierte op internet in de val lokken voor analyse. Al snel werd duidelijk dat het ging om een uiterst vernuftige worm. Na infectie zorgde het ervoor dat andere wormen en virussen geen toegang meer kregen tot de besmette computer. "Slimme dieren doen het raam dicht waardoor ze zijn binnengekomen", aldus Brandon Enright, netwerk-beveiligingsspecialist aan de universiteit van Californië.

Vernuftig was ook de communicatie met de makers. Elke dag genereerde Conficker 250 pseudo-willekeurige internetadressen waarvan het instructies verwachtte. De makers, die vooraf wisten welke internetadressen dat zouden zijn – hoefden alleen maar een van de internetadressen te registreren en daar een bericht voor de worm achter te laten. De beveiligingsalliantie had dit truc je snel door, maar liep telkens achter de feiten aan. Pas op het moment dat de worm zijn update downloadde – en een nieuwe variant

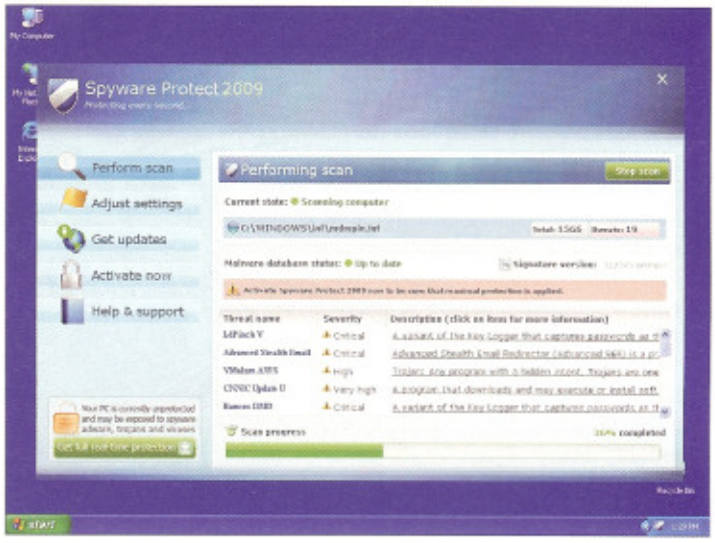
• Geïnfecteerde computers zijn niet meteen rijp voor de sloop. Internetcriminelen houden de schade liever beperkt. Hoe langer computers geïnfecteerd blijven, des te langer ze gebruikt kunnen worden voor criminele activiteiten.

van de worm geboren was – kwam het nieuwe internetadres aan het licht. De beveiligers konden een nieuw internetadres snel blokkeren, maar de volgende dag stonden er alweer 250 nieuwe adressen klaar. Met geen mogelijkheid was dit tempo bij te houden.

Zuurstof Het tij keerde toen Phillip Porras zich in de strijd mengde. Porras en zijn beveiligingsteam van SRI International ontcijferden de broncode van Conficker. De ontrafeling was een moeilijk en langzaam proces, want de worm had zich versleuteld in twee lagen van encryptie die het gebruikelijke beveilingsgereedschap van Porras te boven ging. Een week voor kerstmis lukte het toch, in samenwerking met het Russische beveiligingsbedrijf Kaspersky Labs. De werkwijze van de worm was eindelijk bekend, net als de internetadressen die het zou raadplegen.
Nu was het zaak die internetadressen onmiddellijk te blokkeren. "De worm gebruikt ze als zuurstof", zegt Rick Wesson van Support Intelligence, een netwerkbeveiligingsbedrijf in San Francisco. "Als je de adressen blokkeert, zou het vuur uitgaan". Wesson besloot de internetadressen met geld uit eigen zak op te kopen en zodoende Conficker tot stoppen te dwingen. Dat lukte, maar het bleek een tijdelijke overwinning. Op 29 december dook alweer een nieuwe variant van de worm op, met nog meer trucjes in huis – door de internetbeveiligers Conficker.B gedoopt. In tegenstelling tot de eerste variant, die zich enkel via internet verspreidde, kon Conficker.B zich ook voortplanten via bedrijfsnetwerken en USB-sticks. Eén geïnfecteerde computer was genoeg om een heel netwerk te infecteren. Ook blokkeerde Conficker de toegang tot websites van Microsoft en bekende antivirus-bedrijven. Wanneer een geïnfecteerde computer de Microsoft-patch tegen de worm probeerde te downloaden, stuitte het op een foutmelding. Om te voorkomen dat Porras opnieuw de code zou kraken, maakten de virusmakers de versleuteling nog wat lastiger. Was de vorige Conficker-variant al moeilijk te kraken, bij deze bleek dat zo goed als onmogelijk. De versleuteling was gebaseerd op een vrijwel onbekende encryptie – nauwelijks bekend buiten een selecte kring van wetenschappers – en was pas drie maanden eerder vrijgegeven door onderzoekers aan het Massachusetts Insitute of Technology (MIT).

> "De hackers zeiden in feite dat we 50.000 internetadressen in de gaten moesten houden."

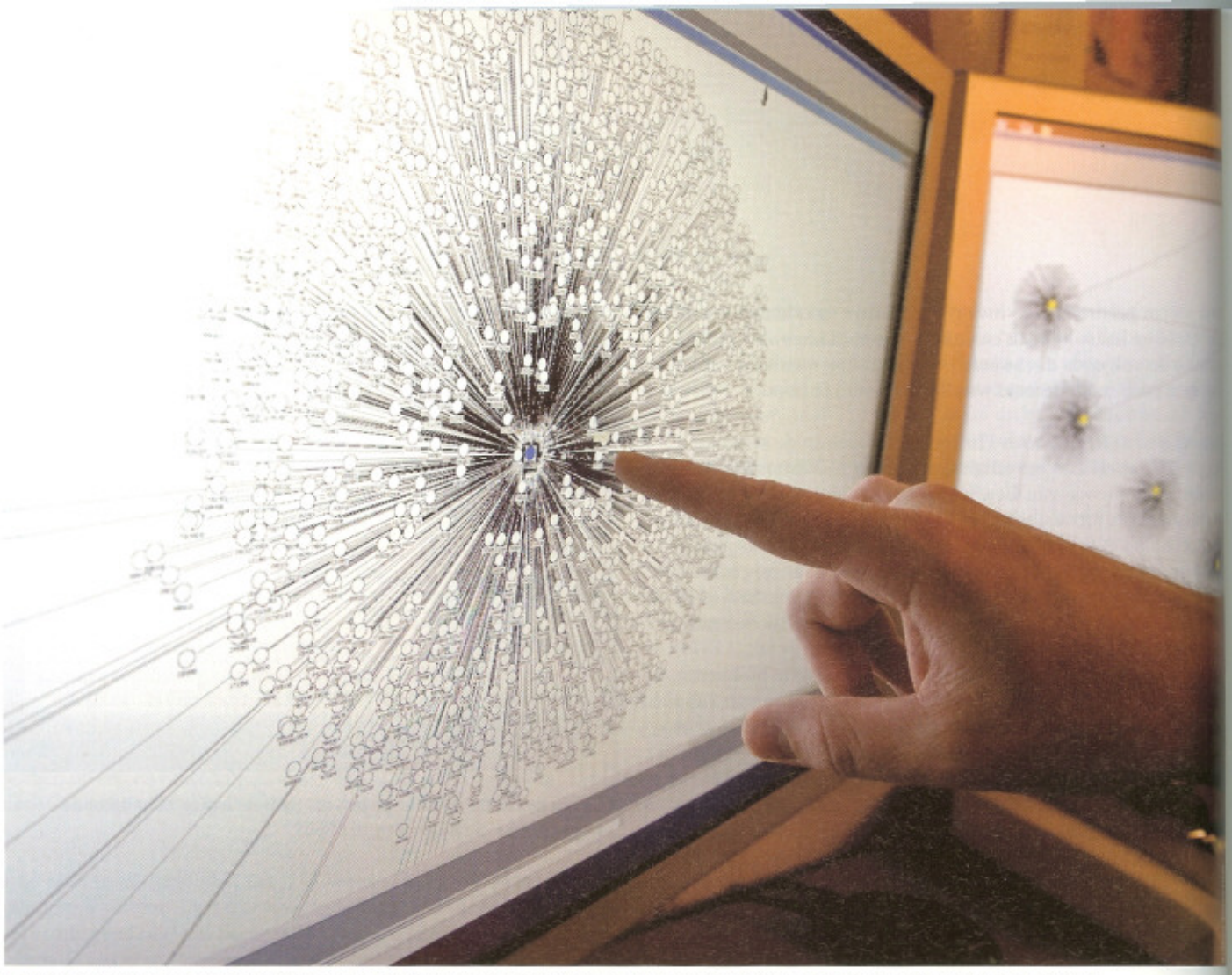
De nieuwe versie van Conficker verspreidde zich vervolgens razendsnel. Hoewel het precieze bereik moeilijk te meten is, raakten waarschijnlijk meer dan 3 miljoen computers besmet. Nederland en België bleven niet gespaard. "In België werden enkele ziekenhuizen en een grote overheidsinstelling getroffen", zegt Eddy Willems, virusanalist bij Kaspersky Labs Benelux. "In Nederland zijn enkele middelgrote bedrijven en een overheidsinstelling besmet, maar bij de overheid betrof het slechts enkele computers. Om welke overheden en bedrijven het gaat, mag ik niet vertellen. Dat houden ze liever geheim." Wel kan hij bevestigen dat Europa er redelijk goed vanaf is gekomen, in tegenstelling tot Azië. "Daar hebben



• Conficker zette de deur open voor de bedrieglijk echt lijkende 'virusscanner' Spyware Protect 2009.

veel computergebruikers een illegale versie van Windows, die niet automatisch updates installeert. Van die zwakke plek kon Conficker gebruik maken." Aangezien de worm alleen Windows-computers infecteerde – Linux en Macintosh zijn immuun voor de worm – zag Microsoft de bui al hangen. Op 12 februari loofde het bedrijf een beloning uit van 250.000 dollar aan degene die de Conficker-makers zou aangeven.

Misleiding De grote vraag bleef: wat bracht de makers van Conficker ertoe om zo'n vernuftige worm te maken? Want hoewel de worm slim was opgebouwd en zich over miljoenen computers had verspreid, deed het verder niets. Conficker had nog geen enkele schade aangericht, afgezien van kosten voor de bestrijding ervan. De computerbeveiligers waren er echter niet gerust op en wisten dat het slechts stilte voor de storm was. Men kon alleen maar wachten tot de worm zich zou vernieuwen tot een schadelijke variant. Deze zou mogelijk uitgroeien tot een botnet bestaande uit miljoenen computers die centraal bestuurd kunnen worden – en daar is een hoop schade mee aan te richten.
Alleen al het platleggen van overheidssites kan vestrekkende gevolgen hebben. Dat kan bijvoorbeeld door de computers massaal contact te laten zoeken met een website, die vervolgens overbelast raakt en stopt met functioneren. Het gevolg is dat de website uren of zelfs dagen uit de lucht is. Zo'n *distributed denial-of-*service-aanval (DDoS) bombardeerde in het verleden bijvoorbeeld de website van de Nationale Bank van Georgië, tijdens de aanloop naar de oorlog in Zuid-Ossetië. Ook waren Estlandse overheidswebsites eens vijf dagen lang overbelast nadat de Estlandse overheid had besloten een Russisch standbeeld te verplaatsen uit de hoofdstad. "Zo'n netwerk kan gebruikt worden om vernietigende dingen uit te voeren", zegt Ferguson. "Het kan de infrastructuur van de halve wereld platleggen." Een manier om dit teweeg te brengen is bijvoorbeeld de grote centrale verbindingspunten van het internet aan te vallen.
Maar voorlopig gebeurde er niets, en veiligheidsexperts volgden ▶



• De infectieroute van een computerworm of -virus is vaak nauwkeurig te volgen, zoals hier met het programma Bot Herder.

nauwlettend elke stap die Conficker zette. Op 15 maart sloeg Conficker plotseling weer toe. De worm reisde naar de website rmpez-rx.org. Deze site stond op de lijst die Porras had gepubliceerd, maar was om onbekende redenen niet geblokkeerd. Deze ene site was alles wat de hackers nodig hadden. Een nieuwe versie stond klaar om gedownload te worden door alle geïnfecteerde computers, compleet met een hoop nieuwe trucjes. Conficker.C was een feit.
De nieuwe Conficker-variant maakte korte metten met de strategie van Porras en Wesson om internetadressen op te kopen en te blokkeren. Vanaf 1 april zou Conficker in staat zijn om dagelijks updates te zoeken op 500 internetdomeinen, willekeurig geselecteerd uit een lijst van 50.000 mogelijke domeinnamen. Op de lijst bevonden zich domeinnamen uit Nederland en België, maar ook uit Kazachstan, Haïti en de Verenigde Arabische Emiraten. Aangezien elk land zijn eigen procedures hanteert voor het vastleggen van domeinnamen, was het vrijwel onmogelijk alle mogelijke domeinen vooraf te blokkeren. Wesson deed niettemin een verwoedde poging. Direct nadat de lijst met cruciale adressen bekend was geworden – Parras had zijn vorige trucje herhaald – nam Wesson contact op met de Internet Corporation for Assigned Names and Numbers (ICANN). Dit is een overkoepelend orgaan dat waakt over de uitgave van landdomeinen, zoals .nl en .be. Wesson kreeg echter weinig gedaan. Door de grote verschillen in nationaal beleid rondom domeinnamen, was er weinig kans om de tijdbom voor 1 april te ontmantelen. De inspanningen van Wesson waren hoe dan ook vergeefs, want uiteindelijk bleek de hele domeintoer van Conficker een afleidingsmanoeuvre te zijn. In plaats daarvan maakte de nieuwe versie van Conficker gebruik van dezelfde techniek die wordt gebruikt voor het verspreiden van illegale software en films: peer-to-peer-communicatie (P2P). Hierbij wisselen computers onderling gegevens uit, in plaats van via een centrale computer. Het laat de worm direct contact maken met kopieën van zichzelf op andere computers, waarna het gegevens kan uitwisselen.
De misleiding via een centraal webadres lijkt niet meer geweest dan een prachtige manier om de internetbeveiligers op het verkeerde been te zetten. "De hackers zeiden in feite dat we 50.000 internetadressen in de gaten moesten houden. Maar ze hebben nooit de bedoeling gehad om deze te gebruiken", zegt Joe Stewart van SecureWorks. "In plaats daarvan gebruikten ze peer-to-peer. Ze hebben ons voor de gek gehouden."

De beveiligingers liepen telkens achter de feiten aan.

Businessmodel Ondertussen hing 1 april als een zwaard van Damocles boven het internet. Niemand wist wie achter Conficker zat of wat het ging doen, en dat zaaide angst. Kranten, radio

en tv kondigden een mogelijke catastrofe aan. Maar 1 april ging geruisloos voorbij, en voor de buitenwereld leek Conficker niets meer dan een 1-aprilgrap. Maar nog geen zeven dagen later dook alweer een nieuwe variant op, genaamd Conficker.E. Deze variant verspreidde zich via peer-to-peer, waardoor autoriteiten geen mogelijkheid hadden het te stoppen. Eindelijk liet Conficker zijn ware aard zien, en werd de worm ook zichtbaar voor de doorsnee computergebruiker. Het was nog geen massale aanval, met krakende harde schijven of rokende computers tot gevolg, maar wel een eerste poging tot oplichtingspraktijken. Conficker.E downloadde de spambot *Waledac* en een pop-up genaamd *Spyware Protect 2009*. De pop-up deed computergebruikers geloven dat een antivirusprogramma op hun pc een scan uitvoerde. De computergebruikers werden bang gemaakt met meldingen van fictieve virussen die zogenaamd waren aangetroffen op de computer. Vervolgens moesten ze 50 dollar betalen om de virussen te verwijderen. "Alles aan het programma is nep, behalve de 50 dollar – dat kwam wel in criminele handen terecht", aldus Ferguson. Waledac is zo mogelijk nog schadelijker. "Het programma is de ergste spambot op aarde", zegt Ferguson. "Het adverteert voor van alles – van replicahorloges tot erectiepillen."

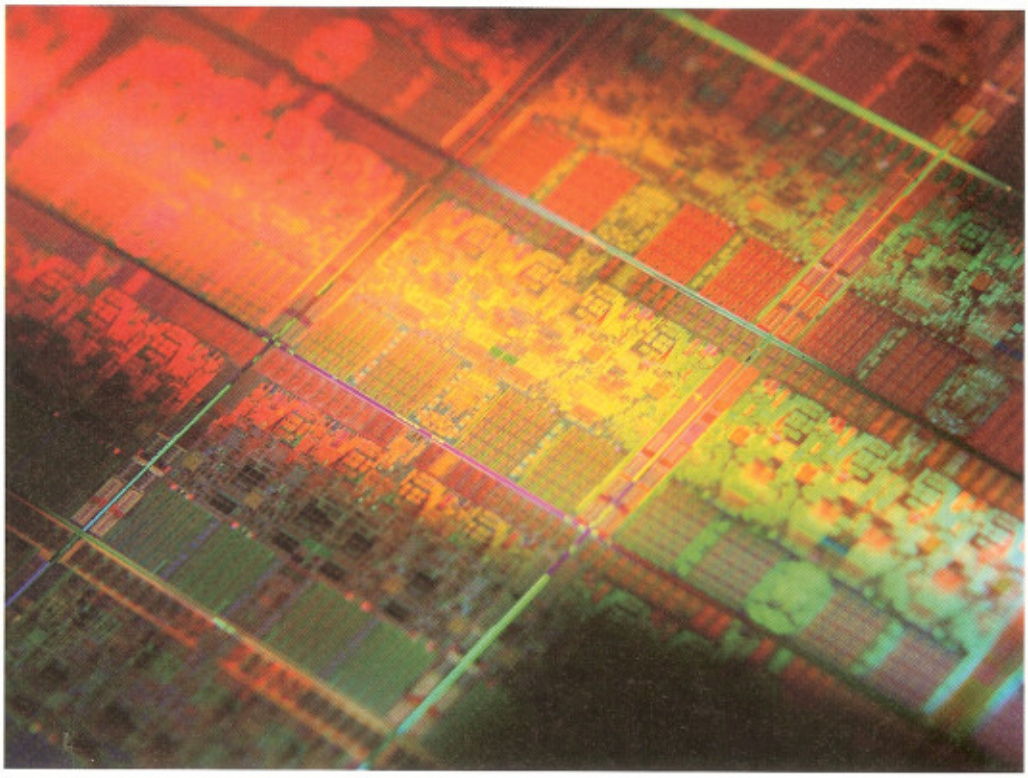
Dergelijke oplichterspraktijken kunnen erg lucratief zijn. In het geval van spam hoeft slechts een fractie van de benaderde computergebruikers op een link te klikken. Storm, voorheen een van de grootste spamverstuurders, verdiende miljoenen dollars per jaar met deze methode. Hetzelfde geldt voor nepsoftware. Toen de rekeningen van de Russische makers van een nep-antivirusprogramma afgelopen jaar boven water kwamen, bleek dat zij binnen tien dagen meer dan 145.000 dollar hadden verdiend. Het is niet onwaarschijnlijk dat de makers van Conficker eveneens bezig waren enorme bedragen binnen te harken.

Waledac en Spyware Protect 2009 zijn echter niet per definitie van dezelfde makers zijn als Conficker. Vaak zorgt een worm voor een botnetwerk van geïnfecteerde computers, dat vervolgens wordt verhuurd aan criminelen die er spam mee willen versturen, DDoS-aanvallen uitvoeren of gebruikers strikken voor het kopen van valse software. Jan Van Haver, contactpersoon bij het Duitse IT-beveiligingsbedrijf G Data: "Het is een professionele industrie geworden. Vroeger werden virussen geschreven door ontslagen werknemers die wraak wilden nemen, of studenten die het voor de grap deden. Tegenwoordig is er veel geld mee te verdienen en zit er een georganiseerde misdaad achter." Van Havers collega Ralf Benzmüller, ook werkzaam bij G Data, beaamt dit. "De sfeer is veranderd. Vroeger ging het om de eer – veel media-aandacht gaf een hacker aanzien. Tegenwoordig gaat het om geld en blijven criminelen liever onder de radar." Geïnfecteerde computers zijn via internet per honderden of zelfs duizenden te huur, vaak voor slechts een paar euro. Het lijkt erop dat de Conficker-makers eenzelfde businessmodel voor ogen hadden.

Onzichtbaar Sinds de updates in april werd het ongemakkelijk stil rond Conficker. In zekere zin was dat een overwinning voor de makers. Het zombienetwerk was gevestigd en werd gebruikt voor het beoogde doel: illegaal geld verdienen. Via het peer-to-peernetwerk kon de worm zich updaten als dat nodig mocht zijn. Alles leek op rolletjes te lopen voor Conficker, totdat bekend werd dat de worm zichzelf op 3 mei zou verwijderen. Dat riep meteen de nodige vragen op. Waarom zouden de mensen achter Conficker er nu ineens mee ophouden? Volgens Ralf Benzmüller zijn de makers geschrokken van alle media-aandacht. "Criminelen houden hun botnetwerk liever onzichtbaar. Hoe langer computers geïnfecteerd blijven, des te langer ze gebruikt kunnen worden voor criminele activiteiten." Volgens Ferguson heeft alleen de laatste variant (Conficker.E) zichzelf verwijderd. Waledac en Spyware Protect 2009 zijn gebleven, alsook vorige versies van de worm. "Het eerste wat Conficker.E deed was checken of de datum 3 mei al verstreken was. Zo niet, dan downloadde het Spyware Protect 2009 en Waledac. Was het al 3 mei geweest, dan verwijderde het zichzelf, waarbij het de malware en vorige versies van de worm liet staan."

Opvallend genoeg echter is Conficker.E nauwelijks gesignaleerd, aldus Ferguson. Volgens zijn observaties heeft maar één

• Nadat Conficker een computer heeft geïnfecteerd, blokkeert het de toegang voor andere wormen en virussen.



• Winkelend publiek in een computerwinkel in Beijing. China wordt al jaren onevenredig hard getroffen door virussen en wormen zoals Conficker, omdat het snel groeiende aantal internetters van het land vaak onvoldoende bewust is van de risico's van internet en door het gebruik van illegale kopieën van Windows en slechte anti-virussoftware.

procent van Conficker.C zichzelf vernieuwd naar versie.E. Dat betekent dat de criminele software (Waledac en Spyware Protect 2009) vreemd genoeg ook nauwelijks werd gedownload. "We denken dat de makers wilden uitvinden welke software meer oplevert, Waledac of Spyware Protect. Ze hebben wel andere geïnfecteerde netwerken om geld mee te verdienen. Conficker is te bekend geworden." Ralf Benzmüller sluit zich daarbij aan: "Conficker is succesvol geworden in zichzelf verspreiden, maar niet in ongedetecteerd blijven. Misschien was de laatste variant een poging ermee te stoppen, of in ieder geval die indruk te wekken."

Maar dat betekent niet dat de dreiging voorbij is. Nog altijd zijn miljoenen computers besmet met de worm, aldus Ferguson. "Miljoenen computers onder controle van onbekende mensen, dat vormt altijd een bedreiging. Hoewel op zichzelf niet schadelijk, kan Conficker op elk moment vernieuwen naar een kwalijke variant. Identiteitsdiefstal, financiële gegevens verduisteren, fraude, het is nog steeds allemaal mogelijk." Waledac vormt op zijn beurt weer een andere bedreiging. Eddy Willems van Kaspersky Labs Benelux: "Behalve het versturen van spam heeft Waledac ook de mogelijkheid nieuwe virussen binnen te halen via een achterdeur. Conficker en Waledac worden al langer tegengehouden door antivirus-software, maar niet iedereen heeft de laatste updates. Sommige mensen en bedrijven zijn daar heel laks mee."

Positief Toch heeft de Conficker-epidemie volgens beveiligingsexperts ook iets positiefs opgeleverd. Met het groeien van de angst bundelden academici, experts en domeinregistratiebureaus hun krachten tot een ongekend opsporingsverbond tegen de worm. Na deze ervaring kan een dergelijke samenwerking alleen nog maar makkelijker worden, denken de experts.

Geïnfecteerde computers zijn via internet per honderden of zelfs duizenden te huur.

Dat maakt alle problemen en onkosten waard, zegt Wesson. Zelf heeft hij bijna 30.000 dollar uit eigen zak in het project gestoken, in een poging de door Porras geïdentificeerde internetadressen te blokkeren. Nog altijd is het onzeker of hij daar ooit een cent van terugziet."Maar we hebben ontzettend veel geleerd. Ik zou zo nog eens 30.000 dollar betalen om de wereld anders naar kwaadaardige software te laten kijken", aldus Wesson.

Wereldwij ligt de schade echter een stuk hoger. Onderzoekers van het Amerikaanse *Cyber Secure Institute* hebben berekend dat Conficker-worm inmiddels voor ruim 7 miljard dollar schade heeft aangericht. De schade zit in verspilde tijd en middelen van de cybergemeenschap, overheden, bedrijven en individuen. Instanties moesten bergen werk verzetten om de worm van hun netwerken te verwijderen. En nog altijd is het gevaar niet geweken. Zo lang computereraars hun beveilingsupdates niet bijhouden, kan Conficker zomaar weer de kop opsteken. ●