Ontwormer verovert de wereld

11 september 2012

DeWorm was een van de eerste en een van de meest succesvolle Sentinels-projecten. ‘Georgios Portokalidis, de aio op het project, werkt inmiddels als postdoc bij de prestigieuze Columbia University. Het beveiligingssysteem Argos waaraan hij heeft gewerkt, is binnen verschillende projecten doorontwikkeld en is inmiddels al bijna negenduizend keer gedownload voor gebruik door security-experts,’ vertelt projectleider prof. dr. ir. Herbert Bos.

De naam van zijn onderzoeksproject had Bos zo bedacht. ‘DeWorm, een woordgrapje,’ zegt hij vanuit de Vrije Universiteit in Amsterdam, ‘want het Engelse deworm (ontwormen) is precies wat we voor ogen hadden met Argos toen we eraan begonnen.’ In het begin was Argos gericht op aanvallen van wormen op servers, zoals webservers en mailservers. ‘Want in de tijd dat we het projectvoorstel schreven, richtten aanvallers zich met name daarop. Ze probeerden bijvoorbeeld om webservers uit te schakelen. Maar toen we een jaartje bezig waren, zag je daar duidelijk een kentering in komen. De aanvallen werden nu op de machines van de eindgebruikers zelf gericht. Op browsers in plaats van op webservers, op emailaccounts in plaats van op emailservers. We hebben Argos dan ook wat aangepast, zodat het ook deze aanvallen kan herkennen en afweren.’

Prof. dr. ir. Herbert Bos, projectleider van DeWorm

Argos is een technologie om internetaanvallen te detecteren. Het is gebaseerd op zogeheten dynamische smetanalyse. Argos kijkt welke data wanneer interactie aangaan met het systeem, en beoordeelt of deze interacties al dan niet afwijkend zijn. Als data van buiten ingrijpen op de uitvoering van een programma, is dat bijna altijd foute boel. Binnen Sentinels werd Argos zo gebruikt dat bij verdachte bewegingen een systeem onmiddellijk werd afgesloten. ‘Later hebben we dat wat aangepast, en gebruikten we het systeem om te observeren wat de aanvallers precies van plan waren,’ zegt Bos.

Als bijen op honing

Argos wordt ook gebruikt om aanvallen uit te lokken. De computer waar het op draait wordt een soort honingpot waar de agressieve bijen op af moeten komen. Vervolgens observeert Argos welke acties aanvallers ondernemen nadat ze binnen zijn gekomen.

Argos is geen huis-tuin-en keuken programma dat iedereen thuis op zij pc kan installeren, benadrukt Bos. ‘In het begin is dat in de media weleens zo geportretteerd. Werden wij platgebeld door mensen met vragen waarom het niet draaide op hun Windows pc.’ Het is bedoeld voor systeembeheerders, met aparte machines voor beveiliging bijvoorbeeld. En bij die experts vindt het gretig aftrek. ‘Zo groot is die groep mensen niet, bijna negenduizend downloads is dan ook heel veel.’ Bos verklaart het succes. ‘Er was nog weinig beschikbaar op dit terrein. Het is een compleet en stabiel systeem, en het doet zijn werk goed.’

Toch had de technologie in eerste instantie nog wel een nadeel: je machine wordt er veel trager van. ‘Als je pech hebt wel 16 tot 20 keer.’ Dat was in de oorspronkelijke opzet van het project nog niet zo’n probleem. ‘Het systeem is ontwikkeld voor aparte machines die bijvoorbeeld netwerken en servers moeten beveiligen. Maar langzaam is de focus steeds meer op aparte pc’s en productiemachines komen te liggen, en we kijken nu zelfs naar toepassingen ervan voor handhelds.’ Met die nieuwe focus kwamen er ook nieuwe vragen.

‘We proberen nu dezelfde bescherming te geven zonder de enorme overhead die het platform genereert, want dat trekken bijvoorbeeld smartphones niet qua rekenkracht en batterij.’ Een eerste stap in de richting was al eerder gemaakt. ‘We proberen niet meer altijd alles te beschermen. Alleen als er iets gebeurt wat een aanval zou kunnen uitlokken, zoals een mailtje openen of in een webbrowser een link aanklikken die je nog niet eerder hebt aangeklikt, moet de beveiliging alert zijn.’

Replica onder de loep

Daarnaast bedachten de onderzoekers dat Argos niet fysiek op het mobiele apparaat hoeft te draaien om indringers te kunnen betrappen. ‘We hebben een inmiddels een Argosvariant voor Android telefoons gemaakt, die niet op de telefoon zelf draait, maar op een security server. We maken een exacte replica van de telefoon op die server, en laten daar Argos op los. Feitelijk maken we opnames van je telefoon, en sturen die door. Dat betekent wel een kleine vertraging in de detectie, maar het is beter om een halve minuut later te detecteren dat je smartphone gehackt is, dan dat je helemaal van niks weet.’

En die vertraging heeft ook een onverwacht voordeel. ‘Als aanvaller kun je je niet verbergen. Want we hebben opnames van het exacte moment van binnendringen. Door de executie nogmaals af te spelen, zien we precies wat er gebeurt tussen de schone en de geïnfecteerde toestand. Dat levert waardevolle informatie op om volgende aanvallen af te kunnen slaan.’ Daarnaast zou je met de opnames het systeem kunnen herstellen tot de situatie net voor de aanval. Daar ligt wat Bos betreft nog een grote uitdaging.

‘We hebben net een paper gepubliceerd over hoe Argos kijkt wat malware doet, en of we daar een automatische recoveryprocedure omheen kunnen maken. Autorecovery betekent nu dat alles wat eventueel geïnfecteerd zou kunnen zijn, wordt weggegooid. Dan ben je vaak veel data kwijt. Wij willen alleen wat aangeraakt is door de aanvaller repareren, en alles wat ongewijzigd is gebleven laten staan.’ Helemaal ben je er dan nog niet, zegt hij: ‘Alles wat niet zeker schoon en niet zeker aangeraakt is, moet je nog handmatig checken. Het is dus zaak om die groep zo klein mogelijk te maken.’

Voortdenderende trein

Alhoewel het Sentinelsproject alweer drie jaar geleden is afgelopen, staat Argos sindsdien allesbehalve stil. ‘Binnen andere projecten is Argos verder ontwikkeld. Met name binnen Europese Zevende Kaderproject Noah vormde Argos het hart van de infrastructuur. En binnen het Europese project Wombat wordt Argos gebruikt voor de detectie van internetaanvallen.’ Maar ook buiten het onderzoek wordt er nog volop aan Argos gesleuteld, zegt Bos. ‘Argos zit nu als enige open source software in het hart van het SGNet detectiesysteem van Symantec, de grote virusscannerproducent. En SURFnet, dat lid was van de gebruikerscommissie van het Sentinels-project, was zo geïnteresseerd dat het Argos heeft geïmplementeerd in zijn eigen systemen.’ Binnenkort komt zelfs een nieuwe versie op de markt. Bos zegt niet zonder enige trots: ‘Argos is een van de eerste smetanalyse systemen die geschikt is gemaakt voor de nieuwste besturingssystemen, zoals Windows 7.’

Foto: Sjoerd van der Hucht Fotografie
Tekst: Sonja Knols, IngenieuSe