

JOOP BAUTZ INFORMATION SECURITY AWARD JURY RAPPORT 2014

De Jury van de Joop Bautz Information Security Award 2014 is na ampel beraad tot de eenstemmige conclusie gekomen dat zij voor de Joop Bautz Information Security Award 2014 nomineert:

Riccardo Bortolameotti

voor zijn werkstuk getiteld:

"C&C Botnet Detection over SSL" ¹

De Jury overweegt hierbij het volgende:

In 2014 werd het voor de dertiende maal mogelijk om kandidaten voor te dragen voor de Joop Bautz Information Security Award, een prijs ingesteld door 3 instituten, actief op het gebied van informatiebeveiliging in Nederland (PvIB, ISACA en NOREA).

De toetsingscriteria hiervoor luiden:

- **Theoretische diepgang:** bronnengebruik, diepgang, aanpak, presentatie, nauwkeurigheid
- **Praktische Relevantie:** originaliteit, effectiviteit & efficiency, "zitten we er op te wachten"
- **Vernieuwing:** originaliteit, gemak, vernieuwend
- **Toepasbaarheid:** maatschappelijk draagvlak, kostenfactoren, werkingsfeer, acceptatie

Na bestudering van de in totaal 10 voordrachten heeft de jury er 3 genomineerd, waaronder de voordracht van Riccardo Bortolameotti. De Jury overweegt daarbij het volgende.

Iedere regelmatige internet gebruiker zal bekend zijn met het slotje in de adresregel van de browser, het icoon voor het Secure Socket Layer (SSL) protocol. We kennen en vertrouwen dit slotje, vooral omdat we er telkens, bij aankopen en betalingen via internet op moeten letten. Riccardo Bortolameotti heeft zich de vraag gesteld of het mogelijk zou zijn via dit protocol (de de-facto standaard voor de beveiliging van internet) te weten te komen of een aanval via zgn. "botnets" gaande is. Botnets, netwerken van gemanipuleerde computers, zijn, aldus Riccardo, te beschouwen als bedreiging nummer één van een veilig internet. De eis die hij zich daarbij stelde hield onder andere in dat zijn benadering niet mocht inhouden een inhoudelijke toetsing van het SSL beveiligde verkeer (geen "deep packet inspection" maar "light weight"). Zijn onderzoek heeft uitgewezen dat het inderdaad mogelijk is om via bepaalde SSL eigenschappen kwaadaardig verkeer, afkomstig van botnets te onderkennen. Riccardo verrichte zijn afstudeer onderzoek op diepgaande wijze en bracht daar een zeer inzichtelijk verslag van uit. De uitkomst van een experiment op basis van zijn hypothese bleek direct praktisch toepasbaar, de betreffende partijen heeft hij van het resultaat op de hoogte gebracht.

De Jury beoordeelde het werkstuk als potentieel prijswinnend op de criteria van de Award. De Jury overwoog daarbij dat hij zeer relevant en doorwrocht onderzoek heeft verricht dat direct bij kan dragen aan verdere verbetering van de algemene internetveiligheid.

Kortom, het betreft een goed onderbouwd werkstuk over een actueel thema met hoge maatschappelijke relevantie, met een aantal vernieuwende inzichten, te nomineren als winnaar van de Award.

De Jury van de Joop Bautz Information Security Award 2014,

Mr. P. van Dijken (voorzitter)

ing. K.F. Rorive MSc CISSP CISA CISM (secretaris)

¹) Afstudeeronderzoek University of Twente, EIT ICT Labs Masterschool, begeleiding onbekend
Juryrapport 2014 Bortolameotti