# تصميم نموذج لتوليد تواقيع الفيروسات (البرامج الضارة) بطريقة أتوماتيكية

**محمد ع. الأمين[1] ، أسامة ع. موسى[1] ، براءة ب. علي[1] ، المدينة م حسن[1] ، نبيلة م. يوسف[1]**

[1]كلية العلوم الرياضية والحاسوب، جامعة الجزيرة.

## الملخص

تواجه بيئة تقنية المعلومات ( Information Technology Infrastructure) العديد من المهددات التقنية اليومية مثل الفيروسات (Viruses) والديدان (Worms) والأحصنة الطروادة (Trojans) التي توثر سلبا على أدائها وتشغيلها، الشيء الذي يلزم توفير الحماية منها. في هذه الورقه البحثية تم تصميم نموذج (Model) يقوم باكتشاف وملاحظة البرامج الضارة (Male-Wares) مثل الفيروسات ( Virus) والديدان (Worms) والأحصنة الطرو ادة (Trojans)ومن ثم توليد (Virus Signature) لها بطريقة أتوماتيكية حيث توفر هذه الآلية الحماية من هذه البرامج الضارة. بدأت الدراسة بدراسة الطرق الحالية الشائعة المتبعة في عملية اكتشاف والحماية من البرامج الضارة

(Male-Wares) مثل مضاد الفيروسات (Antivirus) ونظام كشف ومنع الدخلاء على نظام التشغيل (HIDS/HIPS) ، وتبعها مجموعة من البحوث السابقة ذات الصلة حيث تم تحديد نقاط الضعف وأوجه القصور فيها حيث لاحظنا أنها جميعا لا تدعم الية توليد التوقيع للبرامج الضارة (Signature Virus) بطريقة أتوماتيكية. أخيرا تم تصميم النموذج (Model) وذلك بدراسة جميع احتياجاته حيث تم تحديد الأدوات اللازمة لبناء هذا النموذج.

## المقدمة(INTRODUCTION )

يمكن الاستفادة من تقنيات الحاسب الآلي بكل امكانياته ومعداته لانجاز وتسهيل المهام المطلوب انجازها من قبل الانسان في مختلف مجالات الحياة اليومية. إلا ان هذه الانظمة تواجه بعض المهددات التي تعيق عملها مثل الفيروسات ( Viruses) وهي برامج خبيثة تدخل الي نظام التشغيل بهدف التخريب ، والديدان (Worms) نفسه داخل نظام التشغيل عدة مرات وهو مصمم لإبطاء هي عبارة عن برنامج ينسخ الشبكات ، والأحصنة الطروادة (Hours Trojans) وهي احدى البرامج الخبيثة التي يتم تشغيلها داخل نظام التشغيل ويبدو كانه يقوم بأداء وظائف مرغوب فيها ولكنه في الواقع يؤدي وظائف خبيثة والتي تنتشر وتوجد إما في الشبكة أو نظام التشغيل.

في الوقت الحالي توجد مجموعة من الانظمة التي تستخدم في الحماية من الفيروسات والديدان والاحصنة الطروادة سواء كانت هذه المهددات في نظام التشغيل او في الشبكة وهذه الانظمة تشمل مضاد الفيروسات (Anti–virus ) ونظام كشف ومنع الدخلاء على الخادم ( HIDS/HIPS) ونظام كشف ومنع الدخلاء على الشبكة (NIDS/NIPS).

مضاد الفيروسات (Anti–Virus) و هو برنامج يستخدم لمنع واكتشاف وإزالة البرمجيات الخبيثة، بما فيها فيروسات الحاسب، والديدان واحصنة طراودة. قاعدة بيانات، مضاد الفيروسات تستخدم تقنية القوائم السوداء (List Black) حيث تقوم بمقارنة كل البيانات مع البيانات الموجودة داخل قاعدة البيانات واذا وجدت تعتبر هذه البيانات هي فيروسات أو غيرها من المهددات ولا تسمح لها بالدخول اما اذا كانت، غير موجودة داخل قاعدة البيانات تعتبر غير ضارة .(Dan Liu, et al, 2008).

أما بالنسبة للأنظمة المستخدمة في الحماية من هذه المهددات للشبكات نظام كشف ومنع الدخلاء على الشبكة Network Intrusion Detection System/Network Intrusion Prevention System (NIDS/NIPS) وهي تكنولوجيا مهمه في حماية الشبكات التي تراقب حركه المرور علي الشبكة وتبحث عن نشاط مشبوه و الذي يمكن أن يكون هجوم أو نشاط غير مصرح به وهي تقوم

بعمل مشابه لمضاد الفيروسات من ناحية طريقة التقنية حيث تستخدم تقنية Black List ( Tran thinh,et al,. 2007) .

نظام كشف ومنع الدخلاء على نظام التشغيل (Host Intrusion Prevention / System /Host Intrusion Detection System ) (HIDS/HIPS) وهو نظام يقوم بكشف الاحداث علي الخادم او محطة العمل فرعية ويمكن ان يولد انذارات مشابهة ل NIDS وتكون قادرة علي تفتيش الاتصالات الكاملة. قاعدة بيانات هذا النظام تستخدم تقنية List White حيث تقوم هذه التقنية بمقارنة كل البيانات مع البيانات الموجودة داخل الجهاز واذا لم تكن ضمن تلك البيانات الموجودة داخل الجهاز فتعتبر ضارة وعندئذ يجب منعها (.ZHANG Yan et al,.2010 ).

## الدراسات السابقة(RELATED WORKS)

تتلخص عيوب الدراسة الاولي في ان Honeypot يصنف كنوع – Low interaction Honey pot ولا يدعم الية توليد Virus Signature بطريقة اتوماتيكية كما انه يعطي المهاجم فرصة للوصول إلي نظام التشغيل الحقيقي. أيضا نجد انه لا يستطيع أن يحل محل التكنولوجيا الحالية لكنه يعمل معها و البيانات التي يتم جمعها ب Honey pot ليست بيانات حقيقية كما ان نسخه محدودة ويحتوي علي المخاطر ( Smah, et al.,2010) .

تتلخص عيوب الدراسة الثانية في انها لاتدعم الية توليد توقيع البرامج الضارة (Virus Signature) بطريقة اتوماتيكية وعدم مجانية التطبيقات المستخدمة في إنشاء تطبيق Anti – Virus مثل بيئة تطوير التطبيقات Visual Basic وقاعدة البيانات المرتبطة بها وهي MS SQL Server 2000 ، كما نجد انه عدم توفر معلومات الدعم الكافية يؤدي هذا إلي نقص في الأداء والكفاءة وذلك لان معظم المعلومات تكون حكرا عند شركات معينة وبعضها تجاري لا يفي بالغرض المطلوب . (Asmaa, et al.,2008)

تتلخص عيوب الدراسة الثالثة في انه لا توجد عملية فحص لبورت معين، كما نجد إن الآلية نفسها التي تم استخدامها بالرغم من مميزاتها وقدراتها الا أنها ليست لديها إمكانية توليد ,Virus Signature بطريقة اتوماتيكية. أيضا عدم مجانية البرامج المستخدمة في تطوير الأداة أي انك تحتاج غالبا للدفع للحصول عليه ( Abdalla .(, al et.,2009)

من خلال دراستنا لهذه الانظمة الحالية المتبعة في الحماية وجدنا انها لا تدعم الية توليد Virus Signature بطريقة اتوماتيكية ومن هنا جاءت اهمية الورقة البحثية حيث المشكلة تتمثل في تصميم نموذج يقوم بتوليد Virus Signature بطريقة اتوماتيكية كما هو موضح في جدول1 .

**أ/ خطوات تصميم النموذج (Model):**

النموذج (Model) الذي قمنا بتصميمه يتكون من، نظام تشغيل مثبت على جهاز حاسب ألي موضوع في شبكة داخلية وهي بدورها متصلة بشبكة أخرى (الشبكة تكون من Router , Firewal و NIDS/NIPS و Switch وجهاز كمبيوتر (PC) ومن المعروف ان البرامج الخبيثة (Male– Wares) بجميع انواعها سواء كانت فيروسات او ديدان او احصنة طرواده تنتشر اما في الشبكة او جهاز الحاسوب كما موضح في الشكل .1 .Fig. وسائل الحماية المتبعة الى هذا اليوم للكشف والتعرف على البرامج الخبيثة في الجهاز عن طريق مضاد الفيروسات (Anti – virus) و HIPS/HIDS اما في الشبكة تكون الحماية عن طريق .NIDS/NIPS .

**الجدول 1: يوضح عيوب الانظمة الحالية المتبعة في الحماية من البرامج الخبيثة**

| الانظمة الحالية المتبعة في عملية الحماية من البرامج الخبيثة | النواقص او القصور |
|---|---|
| مضاد الفيروسات ( Anti–Virus) | • قد يواجه المبتدئين مشكلة في فهم الرسائل الفيروسات والتعليمات الخاصة بمنتجات مضاد الفيروسات مثل تحديث قاعدة البيانات لمضاد الفيروسات.<br>• لاتدعم الية توليد Virus Signature |
| نظام كشف ومنع الدخلاء على المخدم (HIPS/HIDS ) | • لاتدعم الية توليد Virus Signature<br>• تعاني من False Positive |
| ذظام كشف ومنع الدخلاء علي الشبكة (NIPS/NIDS ) | • لاتدعم الية توليد Virus Signature<br>• تعاني من False Positive |

## مواد وطرق البحث(MATERIALS AND RESEARCH (METHODOLEGY

بعد تطبيق النموذج (Model) على بيئة العمل، في حالة دخول برنامج خبيث أو ضار جديد للشبكة فان نظام NIDS/NIPS يقوم بمقارنة المحتوي الفعلي للرسالة (Payload) لمرور الشبكة مع قاعدة بياناته. فاذا تطابق المحتوى مع قاعدة البيانات تقوم بمنعه وأما غير ذلك تسمح له بالدخول . حيث نجد أن هذه الخاصية المميزة غير موجودة في أنظمة Anti – Viruses و أنظمة .HIDS/HIPS فعند دخول البرنامج الخبيث الى جهاز الحاسب الآلي فان أنظمة Anti – Virus و HIPS/HIDS ليست لهما القدرة على اكتشاف هذا البرنامج الخبيث وذلك لانهما يعملان بتقنية Black List و White List ، بمعنى ليست لديهما تقنية الاكتشاف الا ان تقوم الشركة المصممة لهذه البرامج بتحديث قاعدة البيانات. ولحل هذه المشكلة قمنا بتصميم هذا النموذج حيث يقوم بتوليد (Virus Signature) بطريقة أتوماتيكية .

لتصميم هذا النموذج بحثنا عن مجموعة من التطبيقات والادوات التي توفر لنا الية توليد Virus Signature بطريقة اتوماتيكية حيث أننا احتجنا إلى مجموعة من العمليات المتسلسلة والتي بتكاملها جميعا توفر الآلية المطلوبة للنموذج. ومن هذه العمليات المتسلسلة خطوة تحليل التصرفات أو العمليات الشاذة، خطوة كتابة التقرير

المفصل عن العملية السابقة، وأخيرا عملية الإستفادة من التقرير في كتابة الأوامر للحماية من البرنامج الضار (Male – Wares) موضع الدراسة. وبعد بحث معمق توصلنا إلى مجموعة من الأدوات المتفرقة والتي بدمجها تؤدي العمل المنوط بالنموذج المصصم، وهي كما يلي:

**تطبيق (أداة) Argos :**

هو أداة تقوم بتحليل وتتبع عمل البرامج الخبيئة (Male – Vares) داخل نظام التشغيل (Operating System) ومن ثم انشاء التقارير للتصرفات الغريبة لهذه البرامج. غير أن أداة و Argos لا تدعم آلية ارسال هذه التقارير مباشرة إلى أنظمة NIDS/NIPS او HIDS/HIPS ، لذا قمنا بالبحث عن تطبيق مكمل وبديل يدعم هذه الآلية وهو أداة Nebula.( Herbert Boss, et al2006 ).

**تطبيق (أداة Nebula :**

هو تطبيق يقوم بتوليد Signature خاصة بالبرامج الضارة (Male – Wares) التي تم تحليلها بواسطة أداة و Argo السابقة حيث يمكن أن يساعد علي تأمين الشبكة وذلك عن طريق عملية الاستنتاج ومن ثم التوليد بطريقة اتوماتيكية .أيضا يعمل تطبيق Nebula على استقبال تقارير التحليل للهجمات من Honey Trap أو Argos ومن

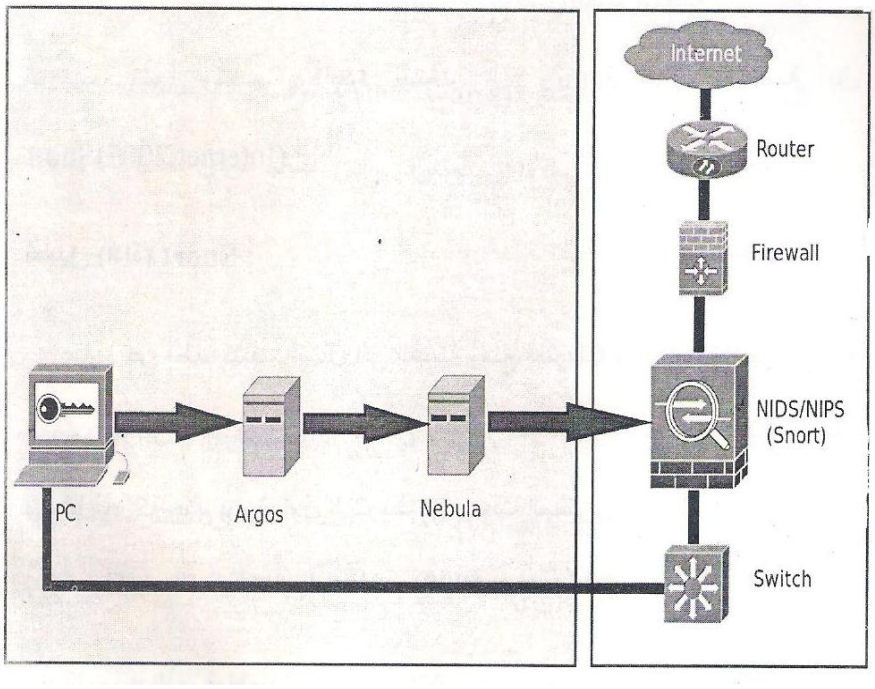
ثم يتم نشر وتحديث قاعدة بيانات إلـ Signature الخاصة بإل Snort (Internet ,2007).

**تطبيق (أداة) Snort:**

عبارة عن نظام كشف التسلل إلي الشبكة ومنع اختراقها وهو برنامج حر ومفتوح المصدر. وتبرز اهمية Snort في ان لديه القدرة على التنفيذ في الوقت الحقيقي وتحليل حركة حزم بروتوكول الإنترنت IP وبحث المحتوي ومطابقة المحتوي وايضا يستخدم لكشف التحقيقات أو الهجمات (Martin 1999,) .

**ب/ النموذج الذي قمنا بتصميمه يعمل كالاتي :**

حيث تم تثبيت تطبيق Argos في نظام التشغيل والذي يقوم بتحليل ومراقبة البرامج الخبيثة وعند اكتشافها يقوم Argos بتوليد تقارير ويقوم بإرسالها الى تطبيق Nebula الذي يعمل كوسيط بين Argos و Snort يقوم Nebula بدوره بنشر Signature للفايروس بعد ذلك يقوم بإرسالها الى Snort والذي بدوره يقوم بتحديث قاعدة البيانات وتخزين Signature للفايروس وعند دخول الفايروس مرة اخرى الى Snort يقوم بمنعه .




**الشكل.1: يوضح الشكل العام للنموذج المصمم ومكونات الداخلية.**

## النتائج والمناقشة(RESULTS AND DISCUSSION)

من خلال تحليلنا ومناقشتنا لمجموعة من الدراسات السابقة من منظور توليد توقيع البرامج الضارة (Virus Signature) بطريقة اتوماتيكية استخلصنا مجموعة من النتائج لهذه الدراسات حيث تتلخص نتائج الدراسة الاولي التي بعنوان lntrusion Deception ln Defense Of Web Server Using Honeypot Technique ، في ان Honeypot يصنف كنوع

Low - interaction Honey pot و يدعم الية توليد Virus Signature بطريقة اتوماتيكية، كما انه يعطي المهاجم فرصة للوصول إلي نظام التشغيل الحقيقي .

تتلخص نتائج الدراسة الثانية التي بعنوان lntrusion Deception ln Server Using Honey pot technique Defense Of Web في ان، تدعم الية توليد Virus Signature بطريقة اتوماتيكية، بالإضافة إلى عدم مجانية التطبيقات المستخدمة في إنشاء تطبيق Anti – Virus مثل بيئة تطوير التطبيقات Visual Basic وقاعدة البيانات المرتبطة بها وهي MS SQL Server 2000. أيضا نجد انه عدم توفر معلومات الدعم الكافية يؤدي هذا إلي نقص في الأداء والكفاءة وذلك لان معظم المعلومات تكون حكرا عند شركات معينة وبعضها تجاري لا يفي بالغرض المطلوب .

تتلخص نتائج الدراسة الثالثة والتي بعنوان Design Tool to Combat Hackers and Virus انه لا توجد ألية لفحص لمنفذ (Port) معين، كما نجد إن الآلية نفسها التي تم استخدامها بالرغم من مميزاتها وقدراتها الا أنها ليست لديها إمكانية توليد Virus Signature بطريقة اتوماتيكية. أيضا عدم مجانية البرامج المستخدمة في تطوير الأداة أي انك تحتاج غالبا للدفع للحصول عليها .

أيضا تفحصنا آليات الانظمة الحالية المتبعة في الحماية من البرامج الخبيثة (Male wares ) حيث وجدنا انها تحتوي على مجموعة من الاشكاليات والتي من اهمها انها

لا تدعم الية توليد Virus Signature بطريقة اتوماتيكية كما تم الاشارة اليها في الجدول 1 السابق .

بعد ذلك قمنا بتصميم نموذج لسد النقص في الدراسات السابقة، والنقص في النماذج او الانظمة المستخدمة حاليا في الحماية من البرامج الخبيثة حيث تكمن مهمته الاساسية هي توليد توقيع للبرامج الضارة (Virus Signature) بطريقة اتوماتيكية . تتلخص ألية عمل النموذج المصمم لإنجاز مهمة كشف البرامج الضارة ومن ثم توليد التوقيع لها بطريقة أوتوماتيكية في ثلاث مراحل متكاملة ومتناسقة مع بعضها البعض كما يلي:في المرحلة الأولى يقوم تطبيق أو برنامج Argos المثبت على نظام التشغيل حيث يقوم بالكشف والتنبيه على النشاطات المشبوهة أو الغريبة التي تحدث داخل نظام التشغيل حيث يرسل تقرير متكامل عن الحالة إلى تطبيق او برنامج Nebula . في المرحلة الثانية يستخدم تطبيق Nebula بإنتاج وتوليد التوقيع حسب التقرير المرسل من المرحلة الأولى عن طريق تطبيق Argos في المرحلة الثالثة والأخيرة، تتم تغذية قوانين وقواعد تطبيق Snort لإستخدامها في اكتشاف هذه البرامج الضارة في المرات القادمة. هذا بدوره وفر لنا آلية جديدة في التعامل مع البرامج الضارة حيث أصبح بإمكاننا توليد توقيع لها – الشيء الذي غير موجود أو مدعوم في أنظمة الحماية من البرامج الضارة الأخرى .

## دراسات مستقبلية(FUTURE WORKS )

نوصي بتطبيق هذا النموذج وتطويره وتعميم هذا النموذج على مستوى جهاز الحاسوب والشبكة لما له من فوائد عديدة في الحماية حيث يوفر تقنية جديدة وهي توليد (Digital Signature) بطريقة اتوماتيكية تساعد على اكتشاف البر امج الضارة (Male – Wares) الجديدة، الشيء الذي لم يتوفر بعد للائظمة المستخدمة في الحماية مثل Anti-Virus و أنظمة .HIDS/HIPS .

## شكر و عرفان(ACKNOWLEDGEMNT)

تتقدم بأسمى آيات الشكر والتقدير إلى عميد كلية العلوم الرياضية والحاسوب الأستاذ / محمد البراء عبدالجبار حسن لمساعدته القيمة التي قدمها لإنجاح هذا البحث. كذلك نتقدم بالشكر لكل من ساعد على إتمام هذا البحث وقدم لنا العون وزودنا بالمعلومات اللازمة لإتمام هذا البحث ونخص بالذكر مشرف البحث الذي زرع التفاؤل في دربنا وقدم لنا المساعدات والتسهيلات والأفكار والمعلومات فله منا جزيل الشكر .

## المراجع (REFERENCES)

**Abdalla, M. F., M H. And Ahmed (2009)**. Design Tool to Combat Hackers and Virus. Bachelor Degree College of Mathematical and Computer Sciences, University of Gazira.

**Asmaa, R . A, Arid Bahauddin (2008)** .lntrusion Deception InDefense Of Web Server Using Honey pot technique-Search forobtainhonor Bachelor degree College of Mathematical Sciences and Computer, University of the Gazira.

**Dan Liu, x. w. Y. ,And Yi-chao Li(2008).**Review on the application of Artificial Intelligence In Anti- virus Detection System. School of Computer Science and Engineering ,University of Electronic Science Technology of China Chengdu, China.

**Herbert Bos,G, B.,And Asia Slowinska (2006).**Argos: an Emulator for Fingerprinting ZeroDay Attacks. Department of Computer Science Faculteit der Exacte Wetenschappen Vrije Universiteit Amsterdam De Boelelaan 1081,1081 HV Amsterdam Netherlands Internet (2007) Nebula. **http://nebula.carnivore.it/**

**Martin (1999).**Snort — Lightweight Intrusion Detection for Networks ,Stanford Telecommunications.

**Smah , Wesal (2010).**Intrusion Deception In Defense Of Web Server Using Honey pot technique. Bachelor Degree, Faculty of Mathematical Sciences and Computer, University of khartoum.

**Tran thinh , S. K. .And Shigenori.Tomiyama (2007)**. Applying Cuckoo Hashing for FPGA - based Pattern Matching in NIDS/NIPS . Department of Computer Engineering, Faculty of engineering, King Mongkut's Instituteof Technology Ladkrabang, Bangkok, 10520 Thailand, Department of Embedded Technology School of lnformation Technology and Electronics, Tokai University, Japan

**ZHANG Yan Y. ,AndOU Yang-Jia (2010)** . The Design and Implementation of Host-based Intrusion Detection System School of Software Yunnan University Kunming, Yunnan Province, China, Computer Science Department Southwest Forestry University Kunming.