بناء منظومة دفاعية وهجومية للتصدي للفيروسات القادمة والفيروسات الساكنة باستخدام أسلوب فلترة الملفات

م.م انتصار ياسين الخزرجي كلية التربية الاساسية / جامعة ديالى
م. عبد الإله إسماعيل كلية التربية الاساسية / جامعة ديالى

المقدمة

في الماضي كانت وسيلة انتقال الفيروسات من حاسب لآخر عن طريق تبادل الاسطوانات المرنة، فالفيروس الذي يصيب الحاسب يضع نفسه في الذاكرة الالكترونية، وإذا أحس الجهاز أن الحاسوب يقوم بنقل ملف إلى وحدة الاسطوانات المرنة، فانه يقوم بالالتصاق بهذا الملف حتى يتيح لنفسه فرصة إصابة حاسبة جديدة إذا ما قام هذا الحاسب بتشغيل الاسطوانة المصابة.

وجاء الانترنت لتقدم لمستخدميها خدمة البريد الالكتروني التي أصبحنا جميعا لا نستطيع الاستغناء عنها، فوجدت الفيروسات وسيلة أكثر كفاءة للانتشار وإصابة اكبر عدد من الحاسبات، ففيروسات البريد الالكتروني والتي يطلق عليها نو الدودة تصل إلى حاسباتنا في صورة ملف ملحق بالرسالة الالكترونية، فإذا قمنا بتشغيل هذا الملف أو محاولة فتحه ينشط الفيروس لكي يصيب الحاسب .

إن أول ما يقوم فيه الفيروس المصاب عن طريق الانترنت في الحاسب المصاب هو البحث عن عناوين البريد الالكتروني التي توجد على هذا الحاسب، ثم يقوم بإرسال نسخة منه إلى هذه العناوين.

ويمكن أن نتخيل إنفيروسا من هذا النو أصاب حاسبا يوجد فيه ٣٠٠ عنوان بريد الكتروني يستخدمها صاحب هذا الحاسب في مراسلة أصدقائه ، في التعامل مع العملاء في مجال العمل في هذه الحالة فان الفيروس ينتقل في ثوان لكي يصيب ٣٠٠ حاسب، وقد احدث هذا النو من الفيروسات خسائر تقدر بمليارات الدولارات.

فالفيروسات الجديدة تتشابه مع الجيل السابق لها في أنها تستخدم البريد الالكتروني، لكي تنتشر وتصيب الحاسبات التي تستهدفها ، كما تتشابه معها أيضا في أنها تأتي ألينا في صورة ملف ملحق Attachment بالرسالة الالكترونية التي تحملها لحاسباتنا، ولكن مكمن الخطورة في الوجه الذي تتشابه فيه مع حاسبات الجيل السابق وهو أن الفيروسات تنشط وتصيب الحاسب الذي يستقبلها بمجرد أن يقوم المستخدم بفتح الرسالة الالكترونية ودون أن تحتاج لقيام المستخدم بتشغيل الملف الملحق.. معنى ذلك انك بمجرد أن تضغط بمؤشر الفارة على الرسالة لكي تتمكن من قراءاتها أو حتى إلغائها ينشط الفيروس ليصيب الحاسب، وهذا النو من الفيروسات يستغل بعض الثغرات الأمنية التي توجد في برامج التعامل مع البريد الالكتروني ومن خلال هذا المنطلق تعمل الفيروسات الهجومية على تحقيق أهدافها التي تم تصميمها من اجله ألا وهو تدمير برامج الحاسوب وقد تصل في بعض الأحيان إلى تعطيل و تعطيب مكونات الحاسوب، بينما في الجانب الأخر يتم استعمال الفيروسات الدفاعية من اجل حماية الحاسوب من المتطفلين (الهكر) الذين يعملون على الدخول إلى منظومة الملفات الخاصة بك وخاصة نظم الشركات العالمية لذا تعمد هذه الشركات على صنع فيروسات تتسبب بتعطيل أجهزة الحاسوب الخاصة بذلك المتطفل وتعطيلها وهي لا تنتشر مثل النو

الأول بل تكون محدودة على فئة محددة من الحاسبات وتستخدم نفس الطريقة التي تستخدمها الفيروسات الهجومية.

خلاصة البحث

إن الحديث عن بناء منظومات مضادة للفيروسات بالطرق التقليدية والمتعارف عليها أصبحت غير مجدية في الوقت الحاضر وذلك يرجع كوننا أصبحنا نتعامل مع محطات طرفية ضمن شبكات محلية وشبكات دولية مما يجعلنا عرضة للعديد من الفيروسات القادمة عبر تلك الشبكات والتي لا تستطيع البرامج المضادة للفيروسات من التصدي لها كون هذه البرامج تعتمد على أسماء الفيروسات الشائعة والتي يتم تسجليها ضمن ملف المحذورات أو البرامج الغير مسموح بها المرور إلى الحاسبة.

وعليه فان الحاسبات التي لا تشترك ضمن شبكة معينة يمكن السيطرة عليها وحمايتها من الفيروسات باستثناء الفيروسات الحديثة والغير مسجلة لد البرامج المضادة والتي تأتي عبر بعض الوسائط الخزنية المتعارف عليهاأما موضو بحثنا هذا فهو يتناول كيفية بناء منظومات فاعلة بعيدة عن الأسلوب التقليدي المتعارف عليه حيث تتضمن هذه المنظومة تعريف أنظمة التشغيل على الملفات الغير قياسية لحجز تلك الملفات باستخدام برمجيات تعد لهذا الغرض ضمن موسعة أنظمة التشغيل وفي نفس الوقت إعداد ذاكرة خاصة مستقلة تتعامل معها تلك البرمجيات وتوكل عمليات المعالجة لمعالج الإدخال والإخراج. كما تتطلب العملية إن هنالك برمجيات عاملة عبر الشبكة . إن المعمول به عبر شبكة الانترنت هو عمليات المراقبة التي تقوم بها شركة سيمانتك (Symantce) حيث تمتلك هذه الشركة العديد من المواقع ولها قسم خاص يطلق عليه قسم عمليات الأمن MSS حيث ينصب عمل هذه الشركة مراقبة العديد من مواقعها والتصدي لكل الخروقات الحاصلة من خلال الجدران النارية حيث قامت الشركة بإعداد برمجيات تمتلك خرائط جغرافية يتم من خلالها تحديد الموقع الذي تمت مهاجمته وعليه لا يمكن القول بان الشركة المذكورة وعبر كل فروعها تستطيع أن تحكم سيطرتها لكل العمليات الهجومية وان كانت كذلك فمن أين تأتي هذه الفيروسات المدمرة . وعليه لابد من القول إن عمل شركة سيمانتك هو عمل مركزي لرصد مواقع الخطر التي تظهر عبر الشبكة حيثتشر مواقع الرصد بالتصدي لمئات الآلاف من الاختراقات يوميا بعد أن تقوم البرامج التدميريه بإلحاق الضرر في العديد من المواقع وعليه تم التركيز في بحثنا هذا كيف يتم وضع آلية بين أنظمة تشغيل الحاسبات وبرامج الشبكة الدولية كي يكون التصدي لبرامج الفيروس محلي عبر منظومة أو برنامج يتضمنه نظام التشغيل قبل أن تقوم تلك البرمجيات المدمرة بإلحاق الضرر يتم التصدي لها وتدميرها .

هدف البحث

بناء منظومة دفاعية وهجومية من خلال بناء منظومة مشتركة بين الشبكة العالمية للانترنت وبين شركات بناء نظم التشغيل حيث يتضمن البحث بناء منظومة تشفير ومنظومة ترميز الملفات ومنظومة تدقيق وفحص شفرات الملفات الغريبة القادة عبر الشبكة بتحييدها أولا عبر ذاكرة الاستقبال ومن ثم التصدي لها وتدميرها عبر الجدار الناري المعد لهذا

الغرض حيث يتطلب توفير ذاكرة احتياطية يطلق عليها ذاكرة الاستقبال (buffer) وبادرة معالج الإدخال والإخراج بعد تضمين نظام التشغيل الخوارزمية الخاصة لهذا الغرض.

الفيروسات وخاصيتها

جميع الفيروسات المتداولة خاصيتها هجوميه وهي تنقسم إلى فئتان:-

الفئة الأولى الهجومية (الحميدة):-

فقط تقوم بتبطئة جهاز الكومبيوتر عندما يتم تشغيل البرنامج الذي يحملها، ومنها تقوم بتعطيل الملف التشغيلي للبرنامج الذي يحملها، كما هناك نو يقوم بإظهار شكل معين على شاشه الكومبيوتر لإرباك المستخدم فقط، وتلكالأنوا من الفيروسات ممكن بأن نسميها الحميدة حيث يمكن التعامل معها باستخدام برامج الحماية المتداولة في الأسواق لمعرفة موقعها وثم مسح الملف الذي تحمله ومن ثم أعاده نسخ ذلك الملف من نسخة نظيفة.

الفئة الثانية الهجومية (الخطرة أو المدمرة):-

تقوم بتدمير جهاز الكمبيوتر حيث أنها تقوم بتدمير جميع المعلومات والبرامج وتدمير الاسطوانة الصلبة (Hard Disk) وهذه هي الخطيرة وهي ثلاثأنوا :-

النو الأول: مجرد دخوله في جهاز الكمبيوتر يقوم بالتدمير المفاجئ السريع.

النو الثاني: يسكن في ذاكرة الكومبيوتر ينتظر تاريخ معين ليقوم بتدمير مفاجئ وسريع للكمبيوتر.

النو الثالث: لا يسكن في الذاكرة بل يسكن في الـ Bios-CPU أو في مواقع عدة داخل Motherboardأو داخل الأسطوانة ألصلبه Hard Disk وعندما تشغل الكمبيوتر يقوم أما بالتأكد من تاريخ اليوم فان لم يكن هو التاريخ المنتظر يخرج من الذاكرة حيث لن تشعر بوجود وان كان هو التاريخ المنتظر يقوم بتدمير سريع ومفاجئ وهذه أسميها الذكية الخطرة.

أنظمة الحماية من الفيروسات المتداولة في الأسواق ومد فعاليتها:-

هناك أنظمة حماية من الفيروسات المتداولة في الأسواق ولكن جدارها غير مرضي وذلك لأنها جميعها تحتوي على قائمة تحمل فيها جميع أسماء الفيروسات أو حجم الفيروسات (القديمة) المتداولة التي سبق وأن دمرت أنظمة وأجهزة الكمبيوتر ولا يمكن لها أن تعرف إن كان هناك صدور لفيروس جديد إلا بعدما يظهر ذلك الفيروس ويقوم بتدمير أجهزة الكمبيوتر ومن ثم تقوم الشركة المنتجة بتزويد المستخدم بقائمة جديدة تحمل فيها اسم أو حجم الفيروس الجديد وهذه العملية تسمى Update وهنا يلزم المستخدم بمتابعة مستمرة لعملية ال Update، وهذا الأمر لن يحل المشكلة وذلك لأن تلك الشركات لن تعرف الفيروس الجديد إلا بعدما يدمر أجهزة الكمبيوتر وهذه الطريقة تعتبر طريقة غير مجزية وعلى سبيل المثال إن جميع مستخدمي الكمبيوتر يتذكرون فيروس تشرنوبل عندما دمر أجهزة الكمبيوتر، فقد فوجئ العالم بوجوده دون سابق إنذاروهو من نو المدمر المفاجئ السريع.

إن أنظمة الحماية المتداولة في الأسواق لن تستطيع منع أو حل مشكلة تدمير الفيروسات الذكية الخطيرة ولذلك وسائل الإعلام تعلن بين الحين والآخر بضرورة إيقاف أجهزة الكمبيوتر لهجوم فيروس مدمر سوف يدمر في تاريخ معين. ولكن إن وسائل الإعلام لا يمكنها التنبؤ بالفيروسات الذكية الخطيرة التي تعمل بعد تشغيل أجهزة الكمبيوتر.

لذا يمكننا القول إن جميع أنظمة الحماية من الفيروسات المتداولة في الأسواق غير مجزية لن تفي بحماية أنظمة وأجهزة الكمبيوتر.

بناء المنظومة الدفاعية وطريقة التصدي للفيروسات الساكنة

الفكرة الأساسية في بناء هذه المنظومة تبدأ أولا من حاسبة المستخدم حيث يتطلب بناء خوارزمية تشفير وظيفة هذه الخوارزمية تشفير كافة بيانات الحاسبة عند إغلاق الحاسبة حيث تنشط هذه الخوارزمية عند إعطاء أمر الإغلاق حيث تقوم بتشفير كافة الملفات المفتوحة (باعتبار أن الملفات الغير مفتوحة هي أصلا مشفرة عند تطبيق هذا النظام) وعند تشغيل الحاسبة تنشط هذه الخوارزمية في الجزء الثاني منها وهو فك شفرة الملف المطلوب استدعاءه إثناء عملية إقلا الحاسبة حيث يتم عنونة هاتين الخوارزميتين (خوارزمية التشفير وخوارزمية فك الشفرة ضمن المسار الذي تعمل علية الحاسبة path). ففي عملية الإغلاق يكون موقع هذه الخوارزمية في آخر المسار أما في عملية التشغيل فيكون موقعها في أول المسار.

خوارزمية التشفير

يفضل استخدام أسلوب التشفير الخيطي (Stream cipher) لعناوين الملفات والملفات نفسها ويفضل أن يضفي الطابع الصوري عند عمليات التشفير أي أن نحصر الرموز المتولدة ضمن شفرات الرموز الخاصة بالاسم آو أي رمز ضوئي آخر كي يسهل التصدي للملفات التقليدية القادمة عبر الشبكة.

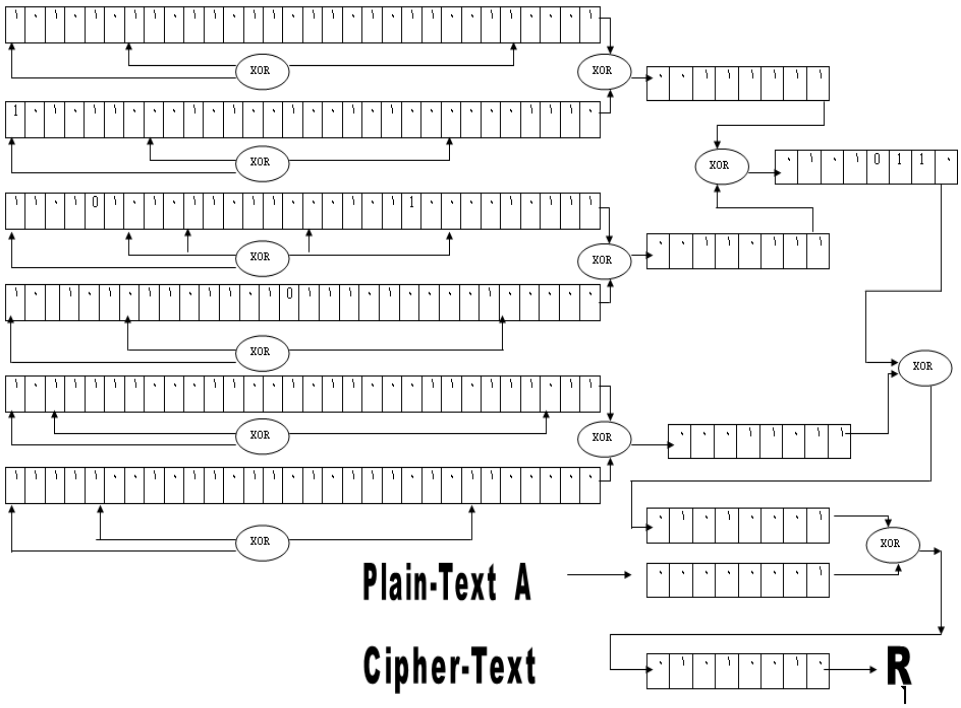
طريقة معالجة الفيروسات المتواجدة ضمن وسائط الخزن

إن الهدف الأساس من عملية تشفير كافة ملفات الأنظمة في بحثنا هذا هو التحكم في الملفات العاملة والملفات الغير عاملة وكما هو معلوم ان كافة ملفات النظام تصبح عاملة عند تحميل نظام التشغيل في الذاكرة أما الملفاتالأخر تبقى مشفرة باستثناء الملفات التي يتم استدعائها من قبل الجهات المستفيدة حيث يتم فك شفرة تلك الملفات وحسب الاتفاق او البروتوكول المتفق عليه بين شركات نظم التشغيل وبين الشركات العاملة على الشبكة العالمية مثل Yaho على سبيل المثال حيث يتم تدقيق كل عنوان لكل ملف مفتوح حيث ان العنوان هو عبارة عن شريحة من المعلومات مكون من شفرة الملف القياسية المتفق عليها واسم الملف وتاريخ الملف وحجم بياناته حيث تلحق هذه الشريحة من البيانات بالملف على غرار عمل الفيروسات عند إرسال ملف ما عبر الشبكة حيث يقوم الفيروس بنسخ نفسه يلحق ملحق مع الملف الأصلي وعليه وبنفس الأسلوب عند فتح أي ملف يسبقه عملية فتح ملف الشريحة الخاصة بالملف المفتوح فإذا كانت شفرة الملف الموجودة في الشريحة قياسية فهذا يعني أن الملف مسموح به للتداول وإذا دون ذلك تقوم برامج الجدران النارية بتدميره قبل فك شفرته ولابد من الإشارة هنا أن كافة الملفات المشفرة لا يمكن استدعائها أو تنفيذها ما لم يتم فك شفرتها وعليه إذا ما كان هنالك ملفات هي بالأصل فيروسات فإنها لا تستطيع العمل كونها مشفرة وبذلك نكون قد وضعنا إلية سيطرة لتلك الفيروسات والتي هي في حالة سبات تنتظر تاريخ ما أو أي إشارة تمت برمجتها كي تنشطها وبهذه الطريقة تكون قد تخلصنا من تلك الفيروسات قبل أن تقوم بأي فعل أو أي تأثير على الملفات الموجودة ضمن وسائط الخزن المتواجدة بها الفيروسات.

الأسلوب المتبع في عملية التشفير

إن الأسلوب الذي تم إتباعه في عملية التشفير هو التشفير الخيطي (Stream cipher) حيث أن الفكرة الأساسية في عملية التشفير بناء شبكة من المسجلات الزاحفة يتم تغذيتها بالبت والتي يطلق عليها بالمفتاح الأساسي (Basic Key) ولغرض توليد Bit يمتلك

درجة تعقيد عالية حيث تم جمع كل مسجلين زاحفين معا لإنتاج البت وان كل مسجل زاحف يتم ربط موقعين معا وجمعهما لتوليد تغذية مرتدة حيث يؤخذ ناتج الجمع من المسجلين الأوليين ويجمعان مع ناتج المسجل الثالث والربع وذلك نحصل عل بت جديد تقوم بجمعهما (XOR) مع ناتج المسجل الخامس والسادس وبالتالي نحصل على بت نقوم بجمعه مع أول بت من أول حرف أو رقم أورمز من محتو الملف حيث تتكرر هذه العملية كل ثمانية مرات لتوليد رمز جديد يتم خزنه وهكذا تتكرر هذه العمليات على كافة محتويات الملف و المخطط التالي يوضح عملية التشفير .



مخطط لتوضيح عملية التشفير

طريقة معالجة الفيروسات القادمة عبر الشبكة والتصدي لها

كما اشرنا سابقا إن بناء هذه المنظومة تتطلب ذاكرة مستقبلة للملفات القادمة عبر شبكة الانترنت فعند وصول هذا الملف أثناء دخولنا إلى الشبكة إلى الذاكرة المستقبلة تقوم خوارزمية أعدت لهذا الغرض بفحص شفرة الملف القادم فإذا ما تبين أن هذه الشفرة غير قياسية يتم مهاجمة هذا الملف أو الفيروس القادم عن طريق الجدار الناري الذي يتم تزويد نظام التشغيل به وبذلك نكون قد تصدينا لتلك الفيروسات قبل وصولها لحاسبة المستخدم دون أن يقوم المستخدم بتجهيز حاسبته ببرامج مضادة للفيروسات وكما اشرنا أن الملف القادم يرافقه ملف صغير يحتوي على شريحة الملف المكونة من شفرة الملف واسم الملف وتاريخ إنشاءه وحجم الملف حيث تقوم خوارزميات عاملة عبر الشبكة بتوليد مثل هذه الملفات عند استدعاء أي ملف من قبل أي مستخدم. ولابد من الإشارة هنا أن عملية التصدي للفيروسات في بحثنا هذا هو محلي عند ذاكرة الاستقبال ولكنه في نفس الوقت محكم لن يسمح لأي

فيروس من النفوذ كما لابد من الإشارة انه قد وردت عبارة ملف قياسي ويقصد به أن أي ملف يتم تداوله عبر الشبكة لابد من توليد له ملف مرفق أطلقنا عليه اسم الشريحة يحتوي على شفرة الملف حيث أن هذه الشفرة هي عبارة عن كلمة السر للملف حيث يتم تحديث هذه الشفرة في كل عملية استدعاء من قبل الخوارزميات التي تسمح بتحرير هذه الملفات والسماح بفتحها ويفضل أن تقوم الشبكة بتزويد شرائح الملفات برموز يمكن ان تفهمها خوارزميات المراقبة وبالتالي تسمح لتلك الملفات بالتعامل معها وفي نفس الوقت يصعب على مصممي برامج الفيروسات من الوصول إلى هذه الشرائح ومعرفة الشفرة والرمز وحتى وان تمكنوا من ذلك فان هذه الشرائح قابلة للتشفير .

الاستنتاجات والتوصيات

١- إن بناء مثل هذه المنظومة يصعب بل يستحيل على مصممي برامج الفيروسات من الوصول إلى موقع المستخدم.
٢- لقد تمت معالجة الفيروسات الساكنة على وسائط الخزن وكذلك التصدي للفيروسات القادمة بدون خسائر .
٣- إذا ما قورن عمل هذا النظام مع النظام المتبع من قبل شركة سيمانتك نجد أن هذا النظام يتصد قبل أي عملية تدمير حين ان عمل شركة سيمانتك تبدأ عملية التصدي بعد ظهور عمليات تدمير الملفات.
٤- بإمكان الشبكة العالمية للانترنت زيادة كفاءة المواقع الداخلة إليها من خلال بناء منظومة برمجيات تجبيك لمعرفة نيات وخفايا تلك المواقع لغرض عمل استباقي وقائي قبل زج تلك الفيروسات عبر الشبكة والتأثير على المواقعالأخر .
٥- بإمكان الشبكة الدولية نشر برمجيات هجومية في كافة محركاتها ومواقعها لغرض التدقيق في الملفات التي يتم فتحها لتدقيقها وإذا ما تبين بأنها فيروسات يتم تدميرها.
٦- كما نوصي أن تقوم محركات الشبكات الدولية عند فتح أي ملف بإرسال شفرة الموقع قبل وصول الملف لمعرفة هل هذا الموقع معتمد أم لا لغرض انسيابية وصول الملفات إلى المستخدم.

المصادر

١. أنظمة التشفير Cipher system ، د. وسيم الحمداني ، سنة ١٩٩٨.
٢. مقدمة في أمنية البيانات Introduction of Data security ، د. بروس يوزوورت، سنة ٢٠٠٣.
٣. مقدمة في التشفير باستخدام تطبيقات جافا ، David bishop ، سنة ٢٠٠١.
٤. الشبكات العالمية للاتصالات، شركة سيمانتك Symantce ،سنة ٢٠٠٦.
٥. مفاهيم نظم التشغيل ، Ibraham Silperchantz ، Fifth edition سنة ٢٠٠٤.