المقالات العلمية

ديدان الكمبيوتر

الكاتبة : سكينة بنت مبارك أحمد آل مبارك

تنبيه:
تعتبر هذه المقالة مشاركة من كاتبها في زيادة التوعية والمحتوى الخاص بأمن المعلومات، وقد راجعها مراجع واحد على الأقل، ولا يتحمل مركز التميز لأمن المعلومات أي تبعات لهذه المقالة، ولا أي معلومات تطرح في هذه المقالة ولا يضمن دقة المعلومة وصحتها.

الملخص

وفقاً للتخصصات الكثيرة التي يهتم بها مجال أمن المعلومات والتطور السريع لمجالات التقنية وما يوافقها من أخطار وتحديات كثيرة، تتناول هذه المقالة نوع من أنواع التحديات الذي يدخل ضمن سلك البرمجيات الخبيثة وهي الديدان، الديدان التي أرعبت مستخدمو الشبكات فترة من الزمن ومازالت تنتشر و تتطور حتى وقتنا الحاضر وتشكل خطر كبيراً على الشبكات خصوصا على أجهزة الشركات الكبيرة ذات التخصصات الحساسة ، حيث أنها تسعى إلى تدمير عميق و يصعب التخلص منها بصورة سريعة، ستتناول المقالة أيضاً نشأتها وامتدادها وكذلك أنواعها وسبل الوقاية منها.

المقدمة

في ظل التقدم الكبير لوسائل التقنية الحديثة التي استحالت إلى هاجس في حلقة العلم العظيمة، التي يدور حولها الكثير من المخترعين والعلماء والمطورين لا سيما في مجال الحاسوب وتقنيات المعلومات و التي بسببها تحولت الحياة الواقعية إلى حياة افتراضية باتت تشكل الأنموذج المثالي السريع لمواكبة تطورات وحاجيات الحياة سواء على المجال الشخصي أو المجال الاقتصادي العام أو حتى على المجال السياسي،وقد لازم هذا التطور ظهور أخطار كثيرة متعمدة في أحيان كثيرة تُصيب الأجهزة كنوع من أنواع الإرهاب الشخصي أو حتى الاقتصادي الذي يعاني منه أغلب مستخدمي أجهزة الحاسوب لاسيما عند اتصالهم بالشبكة العنكبوتية.

ضريبة هذا التطور وخصوصا في مجال الحاسوب ظهرت البرمجيات الخبيثة وهي اختصار كلمة malicious software وتعني البرمجية الماكرة أو الخبيثة،وهي برامج حاسوبية تدخل داخل النظام وتدمر محتوياته بدون علم المستخدم وقد ظهرت منها أنواع كثيرة منها الديدان والفيروسات وأحصنة طروادة و الجواسيس وغيرها من البرمجيات التي تسبب أضرار بالغة يصل مداها إلى تدمير اللبنة الأساسية لمجتمع أو دولة .[1]

وحيث أن الخبراء والمتخصصين في عالم الحاسوب ينصحون بشكل كبير وبالغ على أن يكون المستخدم لأجهزة الحاسوب محيط بجميع تطورات التقنية فهم أيضاً أشد حرصا على أن يكون المستخدم محيط بجميع الأخطار التي يمكن أن تواجهه عند دخوله في الشبكة الإلكترونية أو حتى عند استخدامه للجهاز الإلكتروني على الأقل بدون اتصال في أي شبكة تُذكر.

سوف نتطرق في هذا المقال عن ديدان الكمبيوتر من التاريخ والنشأة إلى طرق الوقاية.

الكلمات المفتاحية

دودة الكمبيوتر،أسماء ديدان الكمبيوتر،ديدان البريد الإلكتروني،خطورة الديدان.

ديدان الكمبيوتر

هي عبارة عن برامج حاسوب ذاتية الاستنساخ ،تكتفي الدودة بنفسها للانتشار دون الحاجة إلى ربط نفسها ببرامج أو أدوات أو مضيفات تساعدها على ذلك كما يفعل الفايروس وربما هذا سبب تسميتها بالدودة[2].تستخدم الدودة الشبكات لإرسال نسخ منها من كمبيوتر إلى آخر وذلك باستخدام تقنيات تساعدها على ذلك بطريقة سريعة [3]

النشأة والامتداد

أول دودة كمبيوتر ظهرت في Xerox الأسطوري في مركز بحوث ألتو وذلك عن طريق الدكتور جون شوج حيث كان يعمل على دكتوراه ستانفورد ، وعند ظهورها أخ ذ برنامجه اسم "الدودة الوحيدة".والطريف في الأمر أن الدكتور جون استنتج فكرة الدودة من رواية(راكب موجة الاهتزاز) التي تُصنف ضمن مجال الخيال العلمي على يد الكاتب جون برونير .تقوم فكرة هذه الرواية منذ البداية على كيفية الارتقاء بأفكار البرامج المتكررة أكثر من الكتابة في ذات المواضيع الجادة.وعلى العكس من الدودة الموجودة في رواية "راكب موجة الاهتزاز" التي تقوم الدودة فيها بالقضاء على شبكة الحاسوب الشريرة،بينما كان جون شوج كان يحلل أنماط المرور المختلفة على شبكة PARS إلى شبكات من ذات النوع المربوطة بأكثر من مئة ج هاز شخصي داخل المختبر وتدور فكرته حول ترتيب مئة من الأجهزة لقذف وحدات المعلومات إلى الإيثرنت بشكل آني،ثم بعد ذلك قياس مدى الاختناق الإلكتروني بشكل متتابع بدلا من تحميل نفس البرنامج إلى كل ماكينة، ولهذا السبب أبتكر الدودة لتقوم بعملية التحميل ذاتيا وذلك عن طريق البحث عن أجهزة مركز البحوث العاطلة وإرسال برنامج الاختبار للسلك للأجهزة التي تمت الإشارة بأنها متوفرة على الشبكة، هذا الاختبار لاقى نجاحا عظيما مما جعل الدكتور يفكر جديا بتحويل عملية الاتصال من عملية مباشرة من جهاز إلى آخر إلى عملية إرسال أوامر التحدث فيما بين الأجهزة مع بعضها البعض وذلك عن طريق إدخال طريقة لعمل نسخ عن طريق الآلة ذاتها وإرسالها إلى أخرى بطريقة متتالية.[2]

في إحدى الليالي فشل شيء ما غير متوقع،مما دفع شوج واثنان من زملائه إلى وضع دودة صغيرة وأطلقوها في الإيثرنت لعمل سيطرة على الفشل الحاصل ،وبعد ذهابه إلى منزله تنبه إلى ظهور خطأ في برنامج الدودة بسبب فقد جزء منه مما أفضى إلى ذهاب (دودة السيطرة) إلى أجهزة الألتو المعطلة وقد سبب ذلك إلى تعطيل الكمبيوتر الأساسي وبالتالي انتشار الدودة إلى كل أجهزة مبنى البحوث جميعها بدون أي سبب واضح أو حتى إشارات إنذار من الأجهزة نفسها. وللأسف لم يكن بإمكان شوج وزملائه إيقاف الدودة وضررها .[2]

الدودة الثانية ظهرت كنكته أو كمزحة بريئة ،الدودة أُطلقت من ألمانيا في ديسمبر /كانون الأول 9، 1987،قبل ظهور الإنترنت بشكل رسمي. نشأت في الشبكة الألمانية EARN وتطورت خلال مواقع البتنت. تم اعطائها اسم Christma Exec وسبب تسميها بهذا الاسم حاجتها إلى تنفيذ المستخدم لسكريبت معين في البريد الإلكتروني ينفذ بعض الأوامر والأدوات التي تتكاثر بها الدودة . على الرغم من أن هذه الطريقة أصبحت مألوفة ومعروفة في العالم الإلكتروني إلا أن فكرة الـ Christma Exec مختلفة قليلة ومُبتكرة بالنسبة لسنة نشأتها حيث ُ أنها ما أن ينفذ المستخدم السكريبت الموجود في البريد فأنه ينشأ بما يشبه شجرة الميلاد ذو محطات طرفية ينتشر بواسطته البريد بذاته عن طريق ملف الأسماء الموجود في البريد الإلكتروني،وبعد إرسال نفسها إلى جميع الأسماء فأنها تقوم بمسح نفسها من الضحية الأصلية لتتجدد في الضحايا الجدد وتتكرر العملية بصورة سريعة جدا بهذه الطريقة. أدى انتشار هذه الدودة على القضاء على شبكة IBM في ذلك الوقت لكن الوضع أصبح تحت السيطرة في وقتٍ ما . [2]

على الرغم من الاكتشاف المبكر للديدانومعرفة البنية الأساسية لها إلا أنها لم تُصبح معروفة ومنتشرة تحت الاختبارات إلا متأخرا وذلك عن طريق طلبة العلوم وبعض المتخصصين بواسطة إطلاق دودة خطيرةٍ جدا وسيئة السمعة في وقت انتشارها سُميت بدودة موريس أو(الدودة العظيمة). تكمن خطورتها على أنها دودة متعددة الأنماط حيث ُ أنها قامت في ديسمبر كانون الأول على مهاجمة أنظمة التشغيل لشركة SUN العالمية وكذلك BSD ،حيث ُ تم استغلال كلمات السر الضعيفة بالإضافة إلى استغلال نقاط الضعف الموجودة في البريد الإلكتروني لنظام التشغيل يونيكس وذلك لأن كل هجوم على سيرفر معين في منطقة ما يستبب في هجوم للأجهزة المتصلة على ذلك السيرفر،وعن طريق هذه العملية حدث أول هجوم Denial of service (DOS) وقد تسبب في إصابة أكثر من 6000 خادم في ذات اللحظة بمعدل 10 مليون إلى 100 مليون من قيمة الأضرار. [2]

إما في الوقت الحاضر فبسبب تطور الحاسوب خمدت أخطار الديدان قليلا حتى ظهور دودة م يليسا التي بدلت الخمود إلى انفجار في عالم الديدان فقد تبعتها بعد ذلك أنواع كثيرا من الديدان كما هو موضح في الجدول رقم(1).[2]

جدول رقم(1):توضيح لبعض أسماء الديدان المنتشرة في الوقت الحاضر.

اسم الدودة	سنة الظهور	عملها	الضرر المُخمن
Melissa	1999	تستخدم الفجوات الموجودة في برنامج Microsoft outlook .	1.1 بليون.
I Love you	2000	يستخدم أي عنوان فردي موجود على استضافة الشبكة في دفتر عناوين الـ Outlook.	8.75 بليون.
Anna konnikova virus worm	2001	ظهرت بواسطة "scrip kiddie" وهي معروفة في تحميل ملفات الهندسة الاجتماعية المجهزة بواسطة صورة فوتوغرافية للاعبة التنس الروسية آنا كونيكوفا وذلك بمجرد فتح الملف تنتشر الدودة.	166.827 بليون.
Code Red	2001	تستغل نقاط الضعف الموجودة في Microsoft internet information server(IIS) بواسطة خادم الويب ونسخ ملف الأوامر وتغيير اسمه الأساسي.	2.6 بليون.
Sircam	2001	تستغل نقاط الضعف الموجودة في برنامج Microsoft windows Outlook و Windows Network share.	1.03 بليون.
SQL slammer	2003	تستغل نقاط الضعف الموجودة في Microsoft's SQL Server Database product	1.2 بليون.
Mydoom	2004	تستغل نقاط الضعف في البريد الإلكتروني وقد انتشرت بصورة كبيرة وسريعة.	38.5 بليون.
Sasser	2004	تستغل نقاط الضعف الموجودة في LSASS (Local Security Authority subsystem service)	14.8 بليون.

إما في المستقبل فمن المتوقع أن تكون الديدان أكبر و أعظم ضرراً ولهذا تم تُسميتها بـ "الديدان الخارقة" حيثُ أنها تستخدم تقنيات وطرق متطورة ومبتكرة، مثل دودة الـ Mytob والتي سوف تستغل نقاط الضعف الموجودة في المواقع الإلكترونية لإرسال الديدان واستضافة الكود الخاص بها على ذات الموقع. [2]

أنواعها

1) ديدان البريد الإلكتروني

تنتشر بواسطة رسائل البريد ،بأي شكل من أشكال الملفات المرفقة أو روابط لمواقع خطيرة ، ويكمن الخطر في حالة تم تحميل الملف المرفق أو عن طريق الضغط على الرابط الغير موثوق،ثم ترسل نسخ منها إلى جميع قوائم البريد وذلك باستعمال عدة طرق منها MAPI functions.

2) ديدان المراسلة الفورية

وذلك عن طريق إرسال رابط لموقع مُبطن بالدودة باستخدام أحد برامج المراسلة الفورية .[4]

3) ديدان الانترنت

وذلك عن طريق استغلال نقاط الضعف في النظام والمنافذ المفتوحة ليتم اختراقها ونشر الديدان عن طريقها .[4]

4) ديدان آي آر إس (IRS)

تنتشر بواسطة قنوات الدردشة وذلك بإرسال الروابط و الملفات المبطنة فيها الديدان عن طريق بروتوكول (IRS)، وتعتبر من الطرق المؤثرة جدا لانتشار الديدان.[4]

5) ديدان شبكات مشاركة الملفات

تنتشر عن طريق نسخ نفسها في أحد ملفات المشاركة ويتم انتشارها بين المستخدمين الموجودين في نفس الشبكة عن طريق برنامج البيتلورد.[4]

خطورتها

تكمن خطورة الديدان في أنها تستطيع أن تنتشر بذاتها دون الحاجة إلى حدث من قِبل المستخدم، فيعتقد المستخدم بأنه في أمان في حالة لم يضغط على أي ملف أو على أي ملف مرفق في البريد إلكتروني وهذا الاعتقاد خاطئ ج داً ، حيث أنها تنتقل بمجرد فتح البريد الإلكتروني لا أكثر، أنها تنتشر عن طريق خداع المستخدم في الصيغة النهائية للملف المرفق فيعتقد المستخدم بأن الملف لبرنامج معروف وهو في الواقع مُبطن بالديدان الخطيرة.[5] .

سُبل الوقاية والتخلص منها

ينصح مهندسو التقنية في مج الات الحماية من أخطار الديدان على التأكد من وجود عدة أمور للوقاية من الديدان تتلخص في عدة خطوات أهمها :

1) شغل جدار الحماية الموجود على الجهاز.
2) اجعل نظام التشغيل مواكب لجميع تحديثات الحماية.
3) جدد استخدام برامج مكافحة الفيروسات من مصادر موثقة.
4) استخدم كلمات سر قوية وخصوصا على شبكتك الخاصة. [6]

الخاتمة

على الرغم من الأبحاث الكثيرة التي تسعى إلى الحد من انتشار ديدان الكمبيوتر إلا إن التقدم التقني والسرعات الكبيرة التي تم تُدشينها في أجهزة الحاسوب ساعدت كثيرا في انتشارها وكذلك من تطورها إلى ديدان أكثر خطورة من ذي قبل، وهذا في الواقع ضريبة من ضرائب التطور التقني.

المراجع

[1] Wikipedia, Malware http://en.wikipedia.org/wiki/Malware

[2] Computer Worms: Past, Present, and Future
Craig Fosnock
CISSP, MCSE, CNE
East Carolina University
http://www.infosecwriters.com/text_resources/pdf/Computer_Worms_Past_Present_and_Future.pdf

[3] Wikipedia ,computer worm http://en.wikipedia.org/wiki/Computer_worm

[4] Computer worm information, types of worm
http://www.virusall.com/computer%20worms/worms.php

[5] Security Guide to Network security fundamentals, Second Edition ,Mark Ciampa,WORMS,Text book.

[6] Hot to prevent computer worms, Microsoft security,
http://www.microsoft.com/security/worms/prevent.aspx