ملاحق الخليج, ملحق الخليج الرقمي

3 فبراير 2008 01:15 صباحا

علوم وتكنولوجيا ... "فيستا" والمواقع الاجتماعية في خطر خلال 2008

حذر التقرير الأخير الصادر عن الشركة العالمية سي أيه، عن رؤيتها لأمن الإنترنت من جدية وشراسة هجمات الإنترنت في عام ،2008 مشيراً إلى أن عشاق ألعاب الإنترنت ومواقع الشبكات الاجتماعية والشركات ذات المعلومات والبيانات الحساسة هم الأكثر عرضة لأخطار ومخاطر مثل هذه الهجمات. وتضمّ الدراسة المبنية على بيانات جمعها باحثون متخصصون من الخدمة الاستشارية العالمية لأمن الإنترنت المنبثقة عن شركة سي أيه أهم تنبؤات الشركة العالمية للسنة الحالية فضلاً رؤية موجزة لأهم التوجهات التي سادت في عام 2007. ويقول جانيسان لاكشمانان، رئيس فريق العمل في شعبة حلول إدارة الأمن في سي أيه: لا يألو مجرمو الإنترنت جهداً في اقتناص الفرص مستفيدين من أية ثغرة برمجية أو أمنية. ورغم أن الحلول الأمنية باتت أكثر فاعلية في رصد وصد البرمجيات الخبيثة، غير أن مجرمي الإنترنت باتوا أشدّ حيلة في مهاجمة حواسيبنا وشبكاتنا.وتابع قائلاً: يشهدُ قطاع التقنية في منطقة الشرق الأوسط نمواً يفوق ما تشهده مناطق عديدة في العالم، غير أنه من المؤسف حقاً أن العديد من الشركات والمؤسسات مازالت تنظر إلى الحلول الأمنية بوصفها شيئاً ثانوياً أو تابعاً يمكن تأجيله إلى ما بعد، فيما تكتفي شركات عديدة بنشر حلول أحادية بسيطة وغير منيعة. وأنا شخصياً أعتقد أن هناك حاجة حقيقية وماسة لمعايير أمنية صارمة فيما يتصل بتقنية المعلومات في العديد من الشركات العاملة في المنطقة. ولابد أن تتحقق مثل هذه الشركات من أن مزودي خدمة

الإنترنت يوفرون لهم معلومات مُحدثة ومتواصلة بشأن المخاطر الأمنية التي تحيق بحواسيبهم.ويقول جانيسان لاكشمانان، رئيس فريق العمل في شعبة حلول إدارة الأمن في سي أيه: البصمة الرقمية التي يتم رصدها وجمعها وتخزينها كلما استخدمنا الإنترنت من الأهداف السهلة وغير المنيعة بالنسبة إلى المسوقين ومجرمي الإنترنت. وقد رأينا في الأعوام القليلة الماضية كيف أن صناعة البرمجيات الخبيثة تنطلق من صناعة بدائية خفية إلى صناعة احترافية متكاملة للاحتيال والتحايل وانتحال الشخصية. الحقيقة الصادمة حقاً أن صناعة البرمجيات الخبيثة باتت تعتمد ممارسات واستراتيجيات تشبه تلك المعتمدة من قبل صناعة البرمجيات الشرعية. وأودّ أن أؤكد هنا أن حماية خصوصية الإنترنت والإجراءات اللاحقة التي نتخذها إنما تدعم سلامتنا وأمننا على الإنترنت إلى أبعد الحدود.يشار هنا إلى أن تقرير رؤية سي أيه لأمن الإنترنت 2008 تم إعداده بغية تعريف المستخدمين والشركات عامة بأحدث تهديدات الإنترنت الخطرة والمدمرة، وتزويدهم برؤية عامة للتوجهات الحالية والمستقبلية، وكذلك تزويدهم بالنصيحة العملية حول أفضل السبل لتوفير الحماية المنيعة. التحليلات المتضمنة في التقرير مبنية على بيانات جمعها باحثون متخصصون من الخدمة الاستشارية العالمية لأمن الإنترنت المنبثقة عن شركة سي أيه العالمية، وهي مدعومة ببيانات قدمها عملاء سي أيه في الفترة بين يناير/كانون الثاني وأكتوبر/تشرين الأول 2007 وكذلك بالبيانات المتاحة للعامة. أما فريق الخدمة الاستشارية العالمية لأمن الإنترنت المنبثقة عن شركة سي أيه العالمية فيوفر منذ أكثر من 16 عاماً خبرته الموثوقة والمجرّبة على مدار الساعة للعملاء حول العالم. ويوفر فريق العمل الذي يضمّ نخبة من الخبراء والباحثين وطواقم الدعم مواردَ إدارة التهديدات المتكاملة. أهمّ توقعات 2008 1 هيمنة البوتنيت:سيشهد هذا العام هيمنة البوتنيت وهي الآلية المستخدمة للتحكم بشكل كامل في حواسيب الآخرين وسلبها إرادتها كلياً، حيث سنشهد زيادة مطردة في عدد الحواسيب المصابة بها. وفي محاولة منهم للإفلات من برمجيات رصد الهجمات الحاسوبية، فإن من يشنون مثل هذه الهجمات الشبكية يغيرون أساليبهم واستراتيجيتهم ويتجنبون المركزية عبر الهيكليات النظيرية. وهم يستخدمون آلية المراسلة الفورية كوسيلة رئيسية لنشر البوتنيت.2 برمجيات خبيثة أشد فتكاً: البرمجيات الخبيثة والضارة تزداد تعقيداً يوماً بعد آخر. وقد تهاجم البرمجيات الخبيثة والضارة الحواسيب الافتراضية، كما قد تعتمد أساليب تعتيمية من أجل الاختفاء والاختباء، بما في ذلك اللغة الاختزالية أو التشفيرية، ومن ثم مهاجمة الحواسيب والشبكات بشراسة.3 عشاق الألعاب من أكثر ضحايا الهجمات: عشاق ألعاب الإنترنت من أسهل الضحايا في هذا السياق؛ إذ من السهل على مجرمي الإنترنت أن يسرقوا بياناتهم ومعلومات حساباتهم المصرفية وغيرها من المعلومات الحساسة التي تمكنهم من انتحال شخصياتهم.4 مواقع الشبكات الاجتماعية في خطر: من المتوقع أن يزدادَ انتشار الشبكات الاجتماعية على الإنترنت، وهذا يجعلها أكثر عرضة لهجمات الإنترنت الخبيثة والشرسة. ومع تزايد أعداد المتصفحين وقلة الاهتمام بحلول أمن الحواسيب المنيعة، فإن هذا يجعل مثل هذه المواقع جهة مفضلة لمجرمي الإنترنت ممن سيوقعون عدداً هائلاً من الضحايا.5 اقتناص الفرص في الأحداث التاريخية: يتصيد مجرمو الإنترنت فرصة الأحداث التاريخية المهمة مثل حملات الانتخابات الرئاسية الأمريكية أو دورة الألعاب الأولمبية في بكين 2008 وغيرها، حيث تعد مثل هذه المناسبات فرصة مواتية لشن هجمات شرسة من أجل سرقة المعلومات الحساسة التي يمكن استغلالها لاحقاً.6 خدمات الويب 0.2 هدف دائم: في حين أنه من السهل نسبياً تثبيت خدمات الويب 0.،2 فإنه ليس من السهل تهيئة هذه الخدمات لتكون آمنة ومنيعة كلياً. لذا، فإن العديد من مواقع الإنترنت التي تستخدم هذه الخدمات تعد فريسة سهلة لهجمات الإنترنت الخبيثة والشرسة.7 فيستا في خطر: رغم أن مايكروسوفت أعلنت أن ويندوز فيستا هو أكثر نظم التشغيل أمناً حتى يومنا هذا، غير أن المعهد الوطني للمعايير والتقنية أعلن عن 20 نقطة غير حصينة أو غير منيعة يسهل اختراقها في عام ،2007 وكلما زادَ عدد مستخدميه، فإن نظام التشغيل ويندوز فيستا سيكون أكثر استهدافاً من أولئك الذين يشنون هجمات الإنترنت الشرسة.8 الأجهزة النقالة آمنة: الأجهزة النقالة مازالت آمنة رغم الإشاعات التي تنطلق من حين لآخر حول انتشار برمجيات خبيثة وضارة تستهدف الأجهزة النقالة. ولن تكون الهواتف الذكية وغيرها

من الأجهزة النقالة هدفاً سلساً للمجرمين في عام ،2008 ولم تسفر البرمجيات الخبيثة التي تستهدف الأجهزة النقالة عن أي هجمات حقيقية واسعة النطاق. وفي عام 2007 لم يتم الإعلان عن أية ثغرات أمنية حقيقية يمكن من خلالها شن هجمات خبيثة إلا في أجهزة أبل آي فون. ماذا حصل في 2007 * تضاعفت كمية البرمجيات الخبيثة بنسبة 16 مرة في أكتوبر/تشرين الثاني 2007 مقارنة مع يناير/كانون الثاني من السنة نفسها.* للمرة الأولى، تفوقت البرمجيات التجسسية الخبيثة في عددها على فيروسات حصان طروادة لتكون أكثر البرمجيات الخبيثة ضرراً وانتشاراً. وفي عام ،2007 شكلت البرمجيات التجسسية الخبيثة ما نسبته 56 في المائة من مجمل البرمجيات الخبيثة، فيما شكلت فيروسات حصان طروادة ما نسبته 32 في المائة، والديدان 9 في المائة، والفيروسات 2 في المائة. * كانت البرمجيات الدعائية وحصان طروادة وبرمجيات التنزيل التلقائية أكثر أصناف البرمجيات التجسسية شيوعاً.* أكثر أنواع الديدان انتشاراً هذا العام كانت الديدان الشبكية والقابلة للإزالة. بعض الديدان تعطل وتشلّ الحواسيب أثناء انتشارها، فيما تعمد بعض الديدان إلى إسقاط المزيد من البرمجيات الخبيثة أو إلى استباحة الحواسيب المصابة أمام الهجمات الخلفية الخبيثة.* الحلول البرمجية المارقة، أو الزائفة، بقيت مشكلة مزمنة، وهي دليل على انتشار ظاهرة التطبيقات المضللة. وقد شكلت البرمجيات الأمنية المارقة ما نسبته 6 في المائة من مُجمل البرمجيات التجسسية في عام 2007 وفي العادة، فإن الحلول البرمجية الأمنية المارقة يتم توزيعها عبر إعلانات الإنترنت المروجة للحلول البرمجية المجانية المكافحة للبرمجيات التجسسية.* الهجمات المُدمجة والتهديدات المركبة التي تتألف من أجزاء متعددة هي الأكثر شيوعاً.* أكثر من 90 في المائة من الرسائل الإلكترونية هي رسائل متطفلة، و80 في المائة من الرسائل المتطفلة تضم وصلات إلى مواقع خبيثة أو برمجيات خبيثة.* الرسائل المتطفلة لم تعد رسائل بسيطة ومتخلفة ومملوءة بالأخطاء الطباعية، بل أضحت أكثر احترافاً ومدعومة بمرفقات مختلفة مثل الصور وملفات بي دي إف والمستندات والجداول الإلكترونية والمقاطع الفيديوية التي تضم جميعاً برمجيات خبيثة أو وصلات إلى مواقع خبيثة.* البرمجيات الخبيثة قضية عالمية. إذ تشير الدراسات إلى أن معظم الأنشطة الإجرامية تنطلق من أوروبا الشرقية وآسيا وتستهدف في معظمها الدول التي يكثر فيها عدد مستخدمي الإنترنت. كما تشير الدراسات إلى أن نحو 40 في المائة من الرسائل المتطفلة استهدفت الولايات المتحدة الأمريكية وأستراليا والمملكة المتحدة وفرنسا وألمانيا. كما تعد البرمجيات الخبيثة قضية ناشئة في أمريكا اللاتينية وكوريا الجنوبية والصين.