التحيين التلقائي .. جيد أو سيء

Brian Wilson الكاتب
CCNA, CCSE, CCAI, MCP, Network+, Security+, JNCIA
Slimjim100@gmail.com
anti-hacker.info
www.ethicalhacker.net
Translated by medfox2010@hotmail.com ترجمت
medfox2010@gmail.com

أرغب في تسليط الضوء في هذه المقالة على مجال من مجالات الامن التي يهملها العديد منا ربما لثقتنا العمياء فيها . أنا هنا أتحدث عن البرمجيات التي تحتوي على خاصية التحيين التلقائي ، فمعظمنا عندما يسمع مصطلح "التحيين التلقائي auto-update" يفكر ب نظام النوافذ ، لكن هناك أنواع عديدة من البرامج بهذه الخاصية وفي احيان كثيرة مفعلة دون معرفتك .
تعتبر خاصية التحيين التلقائي مفيدة للغاية بالنسبة للمستخدمين الغير مؤهلين تقنيا ، و من الأهمية بما كان تفعيل هذه الخاصية لنظام النوافذ أو أنظمة التشغيل الأخرى . تبدأ المشاكل عندما يقوم المبرمجون بإستخدام هذه الخاصية وتفعيلها بطريقة غير آمنة ، لقد إطلعت على تقارير من مصادر متعددة (أحدها www.sploitcast.com) تتحدث على أن بعض الألعاب من أجل التحيين تستخدم شبكات الآخرين ، مثل " تورينت " و ملفات التحيين يتم جلبها من حواسيب العملاء الآخرين ، الخطورة تكمن هنا عندما يقرر أحد الأشخاص دوي النوايا الخبيثة زرع بعض سطور البرمجة في ملف التحيين ، يستطيع بهذا أن يسيطر على مجموعة كبيرة من الحواسيب .
فلنلقي نظرة الآن على كيفية حدوث هذا الهجوم ، فلنقل أني قمت بتنزيل نسخة من لعبة ما وتوجهت للعب مع آخرين على الشبكة ، سوف أحتاج للتحيين من سيرفر اللعبة كي أتمكن من اللعب وهنا تبدأ مشاكل التحيين التلقائي ، فالعديد من منتجي اللعب الآن يقومون بتفعيل التحيين دون معرفتك والعديد منها يستعمل لهذا الغرض شبكات الآخرين ، فبعض هذه الشركات تستخدم سيرفرات تابعة لطرف ثالث ولا يسيطرون عليها بشكل كامل . المشكلة التي تطرح نفسها هنا هي من يراقب ما يرسل إلى الزبائن وهل عملية التحيين آمنة ، إذا كان بمقدور أحد ما معرفة كيفية إشتغال عملية التحيين في بيئة الند للند peer to peer وأراد ان يسيء للمستخدمين الآخرين بإستخدام برمجيات خبيثة ، هل هناك طريقة لمعرفة ذلك وكيف يمكنك إيقافه . الطريقة المثلى لوقف هذا النوع من الهجمات هو أن يكون هناك رمز للباعة موقع رقميا بحيث ان أي رمز آخر لا يكون مقبولا (بهذه الطريقة تقوم بعض شركات الألعاب بعملية التحيين) .
ربما تقول الآن " عندي جدار ناري ولذلك لن اتأثر " إسمحلي أقول لك أنه إذا قام حاسوبك بالإتصال مباشرة بسرفر يقوم بتوجيه الإتصالات إلى الزبناء الآخرين يكون لديك إتصال مفتوح بذلك الحاسوب والجدار الناري يثق بهذا الإتصال حتى نهاينه ، عندما يكون الحساب مفتوحا فهذا يعني أنكما مرتبطان دون تدخل يدكرللجدار الناري (ينطبق هذا على الجدران النارية NAT و أي نوع آخر يسمح بالإرتباط المفتوح) . إحدى الطرق لمعرفة ما يجري في حاسوبك هي أن تشغل Netstat من سطر الأوامر لويندوز ، هذا سيريك الروابط المفتوحة لحاسوبك وكذلك المنافذ والبروتوكولات المستخدمة لذلك ، هناك طريقة أخرى بتشغيل بروتوكول التنصت مثل Ethereal/WireShark وراقب حزمة البيانات لتعرف مايقوم به حاسوبك ، سوف تفاجيء بماترسله البرامج المختلفة في حاسوبك إلى سيرفرالبائعين ، وفي معظم الأحيان تكون موافقا على مايتم إرساله من بياناتك الشخصية بضغطك على أيقونة موافق عندما تقوم بتنصيب هذه البرامج . إن أسلم ما يمكن ان تقوم به هو أن لا تستخدم البرامج التي لا تكون في حاجة إليها وإذا كنت راغبا في إستخدام بعض الألعاب أو التطبيقات تأكد أنها برامج قانونية لأن العديد من البرامج التي تتداول بشكل غير قانوني بها ملفات تجسس (وهي بالتأكيد مسروقة) .
أعتقد أنها مسألة وقت فقط قبل أن يقوم مستخدموا الألعاب بإيجاد حل لهذه المسألة ، وحتى ذلك الحين نحن تحت رحمة البائعين وشركات مكافحة الفيروسات . آمل مع النسخ الجديدة لويندوز (فيستا) أن نكون في مأمن ، ولكن في حقيقة الأمر المسؤولية الحقيقية لأمن الحاسوب تقع على عاتق صاحب الحاسوب ، لذلك يجب علينا جميعا أن نقوم بتعليم دوي الخبرة الفنية المحدودة من أصدقائنا وعائلتنا والمستخدمين الآخرين . كي تعرف المزيد عن ما تحدثت عنه هنا وكان هوسبب إلهامي لكتابة هذه المقالة المتواضعة، قم بزيارة هذا الموقع Sploitcast http://www.sploitcast.com Episode #17 .