يمكنك إرساله مدمج مع صوره أو ملف تنصيب عن طريق بعض البرامج، و من الممكن تغير امتداد الباتش عن طريق الدوس حتى لا يشك الضحية .. وسنذكر الطريقة ان شاء الله.

الكي لوجر Key Logger

الكي لوجر هو برنامج صغير يتم تشغيله داخل جهاز الحاسب ودائما ما يكون مع ملف السيرفر "حصان طروادة" لكي يقوم بأغراض التجسس على أعمالك التي تقوم بها على حاسبك الشخصي .. فهو في أبسط صورة يقوم بتسجيل كل طريقة قمت بها على لوحة المفاتيح منذ أول لحظة للتشغيل ... وتشمل هذه كل بياناتك السرية أو حساباتك المالية أو محادثتك الخاصة على الانترنت أو رقم بطاقة الائتمان الخاصة بك أو حتى كلمات المرور التي تستخدمها لدخولك على الانترنت والتي قد يتم استخدامها بعد ذلك من قبل الجاسوس الذي قام بوضع البرنامج على حاسبك الشخصي

لماذا صممت البرامج التي تستخدم أحصنة طروادة ؟

تصميم هذه البرامج في البداية كان لأهداف نبيلة مثل معرفة ما يقوم به الأبناء أو الموظفون على جهاز الحاسب في غيابك من خلال ما يكتبونه على لوحة المفاتيح . ويوجد العديد من البرامج المنتشرة على الانترنت والتي تستطيع من خلالها التنصت وتسجيل وحفظ كل ما نكتبه على لوحة المفاتيح . من هذه البرامج برنامج يدعى Invisible KeyLloger، والذي يستطيع ان يحتفظ في ملف مخفي بكل ما قمت بكتابته على لوحة المفاتيح مصحوبة بالتاريخ والوقت الذي قمت فيه بعمليات الكتابة هذه ، حيث سيمكنك الإطلاع على الملف المسجل به كل ما تم كتابته على لوحة مفاتيح الحاسب (والتي لن يستطيع أحد معرفة مكانه

الا واضعه) والتأكد من عدم وجود جمل دخيلة أو محاولات اقتحام لم تقم أنت بكتابتها .. أو التأكد مما إذا كان أحد يقوم باستخدام حاسبك والإطلاع على بياناتك في غيابك والتأكد من عدم استخدامهم للانترنت في الولوج على شبكات غير أخلاقية أو التحدث بأسلوب غير لائق من خلال مواقع الدردشة على الانترنت، أيضا يزعم هؤلاء المصممين ان فوائد البرنامج الذي قاموا بتصميمه تظهر حينما تكتشف ان نظام الويندوز أو البرنامج الذي تستخدمه قد توقف فجأة عن العمل دون ان تكون قد قمت بحفظ التقرير الطويل الذي كنت تقوم بكتابته .. حيث ان التقرير بالكامل سيكون موجود منه نسخة إضافية بالملف المخفي ، أيضا من فوائد البرنامج مراقبة سير العمل والعاملين تحت إدارتك للتأكد من عدم قيامهم باستخدام الحاسب الشخصي لأغراض شخصية والتأكد من عدم إضاعتهم لوقت العمل واستغلاله بالكامل لتحقيق أهداف الشركة

خطورة برامج حصان طروادة

تعد برامج حصان طروادة واحدة من أخطر البرامج المستخدمة من قبل الهاكرز والدخلاء .. وسبب ذلك يرجع إلى انه يتيح للدخيل الحصول على كلمات المرور passwords والتي تسمح له ان يقوم بالهيمنة على الحاسب بالكامل .. كذلك تظهر هذه البرامج للدخيل الطريقة (المعلومات) التي يمكنه من خلالها الدخول على الجهاز بل والتوقيتات الملائمة التي يمكن خلالها الدخول على الجهاز... الخ، المشكلة أيضا تكمن في ان هذا الاقتحام المنتظر لن يتم معرفته أو ملاحظته حيث انه سيتم من خلال نفس الطرق المشروعة التي تقوم فيها بالولوج على برامجك وبياناتك فلقد تم تسجيل كل ما كتبته على لوحة المفاتيح في الملف الخاص بحصان طروادة .. معظم المستخدمين يعتقدون انه طالما لديهم برنامج مضاد للفيروسات فإنهم ليسوا معرضين للأخطار ، ولكن المشكلة تكمن في ان معظم برامج حصان طروادة لا يمكن ملاحظتها بواسطة مضادات الفيروسات . أما أهم العوامل التي تجعل حصان طروادة أخطر في بعض الأحيان من الفيروسات نفسها هي ان برامج حصان طروادة بطبيعتها خطر ساكن وصامت فهي لا تقوم بتقديم نفسها للضحية مثلما يقوم الفيروس الذي دائما ما يمكن ملاحظته من خلال الإزعاج أو الأضرار التي يقوم بها للمستخدم و بالتالي فإنها لا يمكن الشعور بها أثناء أدائها لمهمتها وبالتالي فان فرص اكتشافها والقبض عليها تكاد تكون معدومة

و يعتمد الاختراق على ما يسمى بالريموت (remote) أي السيطرة عن بعد ، ولكي تتم العملية لا بد من وجود شيئين مهمين الأول البرنامج المسيطر وهو العميل والآخر الخادم الذي يقوم بتسهيل العملية بعبارة أخرى للاتصال بين جهازين لا بد من توفر برنامج على كل من الجهازين لذلك يوجد نوعان من البرامج ، ففي جهاز الضحية يوجد برنامج الخادم (server) وفي الجهاز الأخر يوجد برنامج المستفيد أو ما يسمى (client) . وتندرج البرامج التي سبق ذكرها سواء كانت العميل أو الخادم تحت نوع من الملفات يسمى حصان طروادة ومن خلالهما يتم تبادل المعلومات حسب قوة البرنامج المستخدم
في التجسس. ، وتختلف برامج التجسس في المميزات وطريقة الاستخدام .. لكنهما جميعا تعتمد على نفس الفكرة التي ذكرناها وذلك بإرسال ما نسميه الملف اللاصق Patch file أو برنامج الخادم والذي

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com