الفصل الرابع

التعريف بالاختراق والتجسس

Chapter for

Hacking Information

تعريف الاختراق

تسمى باللغة الانجليزية (Hackin) وهي عملية قرصنة الانترنت يقوم بها احد الأشخاص مما لا يملكون الصلاحية وغير مصرح لهم الدخول إلى نظام التشغيل في الأجهزة الشخصية الخاصة بالأفراد والمؤسسات بهدف السرقة والتخريب أو لأغراض التسلية مما يتيح له العبث بمحتويات تلك الأجهزة ونقل ومسح أو إضافة ملفات وبرامج كما يكون بإمكانه التحكم في نظام التشغيل وإصدار أوامر مثل أمر الطباعة أو التصوير أو التخزين، كما يتميز الشخص المخترق بالقدرة على الوصول لمعلومات وبيانات الأفراد والحصول على ملفاتهم الخاصة من خلال الانترنت ويتم ذلك بطرق غير مشروعة كالتحايل على الأنظمة لكي يتمكن من الدخول للمواقع أو الاجهزة.

تاريخ الاختراق

قبل عام 1969 لم يكن للكمبيوتر وجود ولكن كان يوجد شركات الهاتف والتي كانت المكان الأول لظهور ما نسميهم بالمخترقون (الهاكرز) في وقتنا الحالي، لتوضيح طريقة عمل الهاكرز في تلك الفترة الزمنية نعود للعام 1878 في الولايات المتحدة الأمريكية وفي إحدى شركات الهاتف المحلية، كان أغلب العاملين في تلك الفترة من الشباب المتحمس لمعرفة المزيد عن هذه التقنية الجديدة والتي حولت مجرى التاريخ، كان هؤلاء الشباب يستمعون إلى المكالمات التي تجرى في هذه المؤسسة وكانوا يقومون بتبديل الخطوط الهاتفية على سبيل المثال مكالمة موجهة للسيد مارك تصل للسيد جون، كان هذا العمل بغرض التسلية ولأجل ذلك قامت الشركة بتغيير الكوادر العاملة بها إلى كوادر نسائية، في الستينات من القرن الحالي ظهر الكمبيوتر الأول الذي امتاز بكبر حجمه مما لم يمكن الهاكرز من الوصول إليه بالإضافة لوجود حراسة على هذه الاجهزة لأهميتها ووجودها في غرف ذات درجات حرارة ثابتة كل هذه العوامل منعت الهاكرز من الوصول لتلك الاجهزة.

في الستينات كان يعتبر المخترق مبرمج عبقري يقوم بتصميم أسرع برنامج من نوعه ويعتبر دينيس ريتشي وكين تومسون أشهر مخترقين لأنهم قاموا بتصميم برامج اليونكس الأسرع في تلك الفترة وذلك في عام 1969.

تعتبر الفترة ما بين عام 1980 حتى عام 1989 العصر الذهبي للمخترقين، عام 1981 قامت شركة IBM بإنتاج جهاز أسمته بالكمبيوتر الشخصي يتميز بصغر حجمه وسهولة استخدامه لهذا بدأ المخترقون في تلك الفترة بالعمل الحقيقي لمعرفة طريقة عمل هذه الأجهزة وكيفية تخريبها .

في تلك الفترة ظهرت مجموعات من المخترقين كانت تقوم بعمليات التخريب في أجهزة المؤسسات التجارية، أما في عام 1983 ظهر فيلم سينمائي اسمه (حرب الألعاب) تحدث هذا الفيلم عن عمل الهاكرز وكيف أن الهاكرز يشكلون خطورة على الدولة و على اقتصادها كما حذر الفيلم من الهاكرز.

كانت البدايات الأولى لحرب الهاكرز هذه في عام 1984 حيث ظهر شخص اسمه (ليكس لوثر) أنشأ مجموعة أسماها (LOD) وهي عبارة عن مجموعة من الهاكرز الهواة والذي يقومون بالقرصنة على أجهزة

الآخرين وكانوا يعتبرون من أذكى الهاكرز في تلك الفترة، إلى أن ظهرت مجموعة أخرى اسمها (MOD)، كانت بقيادة شخص يدعى (فيبر)، كانت هذه المجموعة منافسة لمجموعة (LOD)، مع بداية العام 1990 بدأت المجموعتان بحرب كبيرة سميت بحرب الهاكرز العظمى، هذه الحرب كانت عبارة عن محاولات كل طرف اختراق أجهزة الطرف الآخر استمرت هذه الحرب ما يقارب الأربعة أعوام، انتهت بإلقاء القبض على (فيبر) رئيس مجموعة (MOD)، مع انتهاء هذه الحرب ظهر الكثير من المجموعات الهاكرز الكبار.

اختراق نظم الهواتف

أطلق هؤلاء الأشخاص على أنفسهم اسم (هاكرز نظم التلفونات) غالباً ما يتمتع الهاكرز بالمهارة أفضل الكلمات التي تم إطلاقها على هذه الأنظمة هي كلمة Warez، تشير هذه الكلمة إلى برامج الكمبيوتر التجارية التي تم اختراقها أي تم التوصل إلى كلمة المرور أو أي نظام حماية آخر لحماية النسخ، يمكن لأي شخص في هذه الحالة أن يقوم بتوزيع برامج Warez واستخدامها بحرية، بالتالي تعتبر هذه النسخ من البرامج التي تتمتع بحقوق طباعة ونشر نسخ غير مشروعة فهي تقلل من حجم الدخل المشروع المكتسب للمبرمجين وغيرهم ممن ينتجون برامج الكمبيوتر المحترفة، يقصد بعمليات تخريب الهواتف محاولة تخريب نظم شبكات الهاتف، والهدف الأساسي من هذا التخريب هو تجنب الدفع مقابل المكالمات الخارجية، في أواخر السبعينات وأوائل الثمانينات استخدم هاكرز نظم التليفونات براعتهم الفنية في محاكاة الأصوات الإلكترونية التي كانت تنشط وتستخدم الدوائر التليفونية، لكن إلكترونيات التخريب التي استخدمتها شركات التليفونات في الدفاع لم تكن بمثل قوة تلك المستخدمة في الهجوم، منذ بداية الثمانينات انحدر هاكرز نظم التليفونات من التحديات العقلية المتفردة إلى مجرد خرق للقوانين مثل سرقة أرقام بطاقات الائتمان التلفونية.

يتخذ بعض الأشخاص من أساليب مهاجمة نظم التليفونات أو البريد الصوتي وسيلة تساعدهم على تعلم كيفية تخريب نظم الكمبيوتر، فنظم التليفونات هي نفسها نظم الكمبيوتر باستثناء أن كونها بدائية، عادة ما تكون أساليب دفاعها ضعيفة كما أن استيعاب نظم الهواتف يعتبر قاعدة أساسية للعثور على الطرق التي يمكن بها اختراق الشبكات المحلية.

كيفية الاختراق

اختراق الأجهزة هو كأي اختراق آخر لشيءٍ ما له طرق وأسس يستطيع من خلالها المخترق التطفل على أجهزة الآخرين عن طريق معرفة الثغرات الموجودة في ذلك النظام، غالباً ما تكون تلك الثغرات في المنافذ (Ports) الخاصة بالجهاز، هذه المنافذ يمكن وصفها بأبسط شكل على أنها بوابات للجهاز على الانترنت، على سبيل المثال: المنفذ 80 غالباً ما يكون مخصصاً لموفر الخدمة كي يتم دخول المستخدم للانترنت، في بعض الأوقات يكون المنفذ رقمه 8080.

لكي تتم عملية الاختراق لابد من وجود برنامج يتم تصميمه ليتيح للمخترق اختراق جهاز حاسب آلي لشخص آخر واختراق موقع الكتروني أو اختراق عنوان أو بريد الكتروني خاص لشخص معين فقد صمم برامج تحقق هذه الغاية بل العديد من البرامج التي تتيح عملية الاختراق.

لم تخلو البرامج التي تم تصميمها للاختراق من نقاط الضعف التي تطلب من أصحابها، من هذه النقاط إمكانية الشعور بتلك البرامج على الجهاز الذي تم اختراقه، عليه يكون من الممكن متابعة تلك البرامج والقضاء عليها باستثناء برنامج واحد تمكن مصممو من التغلب على هذا العيب الموجود في باقي بلدان الاختراق الأخرى وأطلق على هذا البرنامج (حصان طروادة).

طرق الاختراق

أبسط هذه الطرق التي يمكن للمبتدئين استخدامها هي البرامج التي تعتمد نظام (الزبون/الخادم) (client/server) حيث تحتوي على ملفين أحدهما Server يرسل إلى الجهاز المصاب بطريقة ما والآخر Client يتم تشغيله من قبل المخترق للتحكم في الجهاز المصاب، عند تشغيل ملف الـ Server من قبل المخترق، يصبح الكمبيوتر عرضة للاختراق حيث يتم فتح أحد المنافذ (Ports) وغالباً ما يكون البورت 12345 أو 12346، بذلك يستطيع المخترق ببرنامج مخصص لذلك كبرنامج NetBus أو برامج الاختراق الأخرى، كما يستطيع أشخاص آخرون (اضافة إلى من قام بوضع الملف في جهاز الضحية)، أيضا يقوم المخترق بعمل مسح للبورتات (Port Scanning) فيجد البورت لدى جهاز الضحية مفتوح، هذه الطريقة هي أبسط أشكال الاختراق هناك طرق عديدة تمكن المتطفلين من اختراق أجهزة الأفراد الشخصية مباشرة بدون إرسال ملفات لدرجة أن جمعية للمقرصنين في أميركا ابتكرت طريقة للاختراق متطورة للغاية حيث يتم اختراق الأجهزة عن طريق حزم البيانات التي تتدفق مع الاتصالات الهاتفية عبر الانترنت فيتم اعتراض تلك البيانات والتحكم في الأجهزة الشخصية.

برامج الاختراق

NetBus

من أقدم البرامج في ساحة الاختراق بالسيرفرات، الأكثر شيوعا بين مستخدمي المايكرو سوفت شات هو برنامج به العديد من الإمكانيات التي تمكن المخترق من التحكم بجهاز الضحية، توجد نسخ مختلفة من النت باس، كل نسخة منها أكثر تطوراً من الأخرى.

pinger

برنامج لمعرفة إذا كان الشخص صاحب الجهاز المراد اختراقه متصلا بالانترنت أم لا.

Ultrascan

أسرع برنامج يعمل Scan على جهاز الضحية لمعرفة المنافذ المفتوحة التي يمكن لصاحب الجهاز الدخول من خلالها.

Girl Friend

برنامج قام بتصميمه شخص يدعى (الفاشل العام)، مهمته الرئيسية والخطيرة هي سرقة جميع كلمات السر الموجودة في جهاز الضحية بما فيها الكلمة السرية الخاصة بالبريد الالكتروني، كذلك اسم المستخدم والرمز السري الذي يستخدمه لدخول الانترنت.

Hackers Utility

برنامج مفيد للاختراق يمتلك أغلب إمكانيات مختلف برامج الهاكرز، يمكن من خلاله كسر الكلمات السرية للملفات المضغوطة وفك تشفير الملفات السرية المشفرة، كذلك تحويل عناوين المواقع إلى أرقام آي بي (IP).

كيفية دخول الهاكرز إلى أنظمة الكمبيوتر

يستخدم الهاكرز العديد من الأساليب لاقتحام أجهزة الكمبيوتر أو شبكات الاتصال، من الأساليب المستخدمة في دخول نظام كمبيوتر مؤمن هو ترك برنامج من برامج Mockingbird هو برنامج صغير يقوم تلقائياً باعتراض طريق تركيبات الأسماء أو كلمات المرور الخاصة بتسجيل الدخول في الوقت الذي يتم فيه إدخالها ومن ثم إرسالها مرة ثانية إلى الهاكرز، يمكن أن يتم اقتحام آخر يقوم به أحد الهاكرز عن طريق استشارة أحد المبرمجين حيث يقوم هذا المبرمج بإنشاء ثغرة التي تعتبر مدخل إلى أحد الأنظمة التي تخترق نظام الأمان، يمكن للمبرمجين ترك ثغرات في مكانها أحياناً يكون ذلك لأسباب مشروعة مثل منح تكنولوجيا الخدمات فرصة لفحص النظام أو ليتم تطبيقها تشبه الثغرات كلمة سرية للدخول، عادة ما يعرف المبرمج مفتاح الوصول إلى هذه الثغرة، لكن لا يعلم أي شخص آخر بوجود هذه الثغرة.

انتحال الشخصيات

يعتبر استغلال نقاط الضعف الموجودة عند مستخدمي الكمبيوتر كوسيلة لاقتحام أنظمة الأمان حيلة قديمة لا زالت تستخدم على شبكة الانترنت، يستخدم الهاكرز مصطلح **Social engineering** للإشارة إلى الطرق التي يتم استخدامها في خداع مستخدمي الكمبيوتر أو إرباكهم، من المحتمل أن هذه الطريقة من أفضل الطرق المستخدمة في دخول أي نظام مؤمن لكن لا يعتبر أسلوب ذو تقنية عالية إلا إذا تم اعتبار التمثيل الجيد إنجاز تكنولوجي على الرغم من ذلك فهذا الأسلوب غالباً ما يعمل بنجاح، يعتبر انتحال الشخصيات نوع من أنواع Social engineering التي يستخدمها الهاكرز، غالباً يُخدع الكثيرون بهذه الحيلة فالكثير من مستخدمي الكمبيوتر عادة ما يكونون معتادين على التصرف بأدب والاستجابة لمحدثيهم خاصة عندما يكون محدثهم أعلى منهم شأناً.

نماذج من انتحال الشخصيات

1. انتحال شخصية موظف جديد

يعتبر الاتصال بمدير النظام للتقدم كموظف جديد أسلوب من أساليب Social engineering المتعددة، التي يمكنها اختراق نظم الأمان، فعلى سبيل المثال يمكن الاتصال بمدير النظام والإدعاء بأن المخترق موظف جديد أنه يحاول تسجيل الدخول على النظام، يحتاج إلى بعض المساعدة، هكذا يطلب منه أن يزوده بقائمة بالخطوات التي يجب إتباعها لتسجيل الدخول على شبكة الاتصال.

من المحتمل أن تفشل هذه الحيلة للعديد من الأسباب ربما يسأل مدير النظام عن سبب عدم استشارة المشرف المباشر، لكن الهاكرز الماهر سيعثر على حل لكل مشكلة فعلى سبيل المثال يمكنه إرسال الرسالة قبل بداية يوم العمل بساعة أو بعد انتهائه بساعة مدعياً عدم وجود أحد في القسم الذي يعمل به.

2. انتحال شخصية فني في قسم الكمبيوتر

يعتمد هذا النوع من انتحال الشخصيات على عنصر المفاجأة حيث يقوم الهاكرز بالاتصال بالهدف ثم يقوم بإغراقه بالعديد من الأسئلة حتى يتمكن في النهاية من الحصول على كلمة المرور، على سبيل المثال يمكنه الاتصال بأي موظف والإدعاء بأنه موظف في قسم الكمبيوتر، أنه يقوم بالتأكد من تأمين النظام، بذلك يبدأ في إرشاده إلى إتباع بعض الخطوات لكي يتمكن من الحصول على كلمة المرور، فيتم اخباره أن يقوم بتسجيل الخروج من النظام ثم يسأله عما كتب، بعد ذلك يخبره أن يقوم بتسجيل الدخول مرة ثانية، ثم يسأله أيضاً عما كتب، ثم يطلب منه بعد ذلك كتابة كلمة المرور، بذلك يكون قد حصل على كلمة المرور بعد ذلك يقوم بتقديم الشكر للموظف وإنهاء المكالمة.

الأشياء التي تساعد المتجسس على اختراق الأجهزة

1- وجود ملف باتش أو تروجان

لا يستطيع الهاكر الدخول إلى أي جهاز إلا مع وجود ملف يسمى (patch) أو (trojan) في تلك الأجهزة، هذه الملفات هي التي يستطيع الهاكر بواسطتها الدخول إلى جهاز الضحية الشخصي حيث يستخدم الهاكر أحد برامج التجسس التي ترتبط مع ملف الباتش الذي يعمل مثل
(سيرفر) يستطيع أن يضع له الهاكر(إسم مستخدم) و(رمز سري) تخوله أن يكون هو الشخص الوحيد الذي يستطيع الدخول إلى الأجهزة، كذلك يستطيع أن يجعل هذه الأجهزة مفتوحة فيستطيع أي هاكر أن يدخل إليها.

2- الاتصال بشبكة الإنترنت

لا يستطيع الهاكر أن يدخل إلى أي جهاز إلا إذا كان متصلاً بشبكة الإنترنت أما إذا كان الجهاز غير متصل بشبكة الإنترنت أو أي شبكة أخرى فمن المستحيل أن يدخل أحد إلى إليه سوا صاحبه.

3- برنامج التجسس

حتى يتمكن الهاكر العادي من اختراق جهاز الحاسوب لابد أن يتوافر معه برنامج يساعده على الاختراق.

كيف يتمكن المخترقون من الدخول إلى الأجهزة

عندما يتعرض جهاز الكمبيوتر للإصابة بملف التجسس هو (الباتش أو التروجان) فإنه يقوم على الفور بفتح منفذ (port) أو منفذ داخل جهاز الضحية فيستطيع كل من لديه برنامج تجسس أن يقتحم هذا الجهاز من خلال هذا الملف الذي يقوم بفتح منطقة أشبه بالنافذة السرية التي يدخل منها اللصوص هم الهاكرز.

كيف يتمكن المخترقون من الدخول إلى جهاز كمبيوتر بعينه

يستطيع المتجسس أن يخترق جهاز كمبيوتر إذا توافرت الشروط الأساسية الأتية :

1- احتواء جهاز الحاسوب على ملف التجسس (الباتش).

2- معرفة المتجسس لرقم الآي بي أدرس الخاص بالجهاز المراد اختراقه.

لابد من توافر الشروط الأخرى وهي اتصال الضحية بالإنترنت ومعرفة المتجسس (الهاكر) بكيفية استخدام برنامج التجسس والاختراق من خلاله.

بمعنى آخر إذا كان جهاز الكمبيوتر سليماً ولا يحوي أي ملفات باتش فمن المستحيل أن يدخل عليه أي هاكر عادي حتى لو كان يعرف رقم الآي بي أدرس ما عدا المحترفين فقط وهم قادرون على الدخول بأية طريقة وتحت أي مانع، لديهم طرقهم السرية في الولوج إلى مختلف الأنظمة.

إذا كان المتجسس لا يعرف رقم الآي بي أدرس الخاص بالجهاز المستهدف لن يستطيع الدخول له حتى لو كان الجهاز يحوي ملف الباتش.

طرق إصابة جهاز بملفات الباتش و التروجان و الفيروسات

الطريقة الأولى :

وصول ملف التجسس من خلال شخص عبر برامج المحادثة أو (الشات) بأن يرسل أحد المتجسسون (الهاكر) صورة أو ملف يحتوي على الباتش أو التروجان، كما بإمكان الهاكر أن يغرز الباتش في صورة أو ملف فلا يمكن معرفته إلا باستخدام برنامج كشف الباتش أو الفيروسات حيث يمكن مشاهدة الصورة أو الملف بشكل طبيعي دون العلم أنه يحتوي على باتش أو فيروس ربما يترك جهاز الضحية عبارة عن شوارع يدخلها الهاكر والمتطفلون.

الطريقة الثانية :

وصول ملف الباتش من خلال رسالة عبر البريد الإلكتروني دون معرفة مصدر الرسالة ولا ماهية الشخص المرسل، حين تحميل الملف المرفق مع الرسالة، من ثم فتحه سيتسبب ذلك باتاحة المجال لدخول المتجسسون لجهاز الضحية.

الطريقة الثالثة :

تنصيب برامج أو ملفات من مواقع مشبوهة مثل المواقع الإباحية أو المواقع التي تساعد على تعليم التجسس.

الطريقة الرابعة :

الدخول إلى مواقع مشبوهة حيث أنه بمجرد الدخول إلى هذه الموقع فإنه يتم تحميل ملف التجسس الى جهاز المستخدم العادي بواسطة كوكيز لا يعلم عنها.

كيفية اختيار جهاز لاختراقه من قبل المتجسسون

بشكل عام لا يستطيع الهاكر العادي من اختيار كمبيوتر بعينه لاختراقه إلا إذا كان يعرف رقم الآي بي أدرس الخاص به، حيث يقوم بإدخال رقم الآي بي أدرس الخاص بكمبيوتر الضحية في برنامج التجسس ومن ثم إصدار أمر الدخول إلى هذا الجهاز، أغلب المخترقين يقومون باستخدام برنامج مثل (**IP Scan**) أو كاشف رقم الآي بي ، هو برنامج يقوم الهاكر باستخدامه للحصول على أرقام الآي بي التي تتعلق بالأجهزة المضروبة التي تحتوي على ملف التجسس (الباتش).

يتم تشغيل البرنامج ثم يقوم المخترق بوضع أرقام آي بي افتراضيه، أي أنه يقوم بوضع رقمين مختلفين فيطلب من الجهاز البحث بينهما على سبيل المثال يختار هذين الرقمين :

212.224.123.10

212.224.123.100

آخر رقمين وهما 10 و 100

فيطلب منه البحث عن كمبيوتر يحوي منفذ (كمبيوتر مصاب بملفات التجسس) بين أجهزة الكمبيوتر الموجودة بين رقمي الآي بي أدرس التاليين 212.224.123.10 و212.224.123.100، هي الأجهزة التي طلب المتجسس من البرنامج البحث بينها، بعدها يقوم البرنامج بإعطائه رقم الآي بي الخاص بأي كمبيوتر مصاب بملفات الباتش يقع ضمن النطاق الذي تم تحديده مثل :

212.224.123.50

212.224.123.98

212.224.123.33

212.224.123.47

فيخبره أن هذه هي أرقام الآي بي ادرس الخاصة بالأجهزة المصابة التي تحوي منافذ أو ملفات تجسس فيستطيع الهاكر بعدها أخذ رقم الآي بي ووضعه في برنامج التجسس، من ثم الدخول إلى الأجهزة المضروبة.

معرفة اذا كان جهاز الحاسوب مخترق ام لا

في البداية يمكن معرفة إذا كان الجهاز مخترقاً من خلال معرفة التغيرات التي يحدثها الهاكرز في نظام التشغيل مثل فتح و غلق الشاشة تلقائياً أو وجود ملفات جديدة أو مسح ملفات كانت موجودة أو فتح مواقع إنترنت أو إعطاء أمر للطابعة بالإضافة إلى العديد من التغيرات التي يمكن مشاهدتها و عن طريقها يمكن معرفة وجود متطفل يستخدم الجهاز غير صاحبه.

الطريقة التي يستطيع صاحب الجهاز من خلالها أن يعرف اذا كان أحد المتطفلين قد دخل إلى جهازه أم الجهاز سليم

فتح قائمة (Start) و منها اختيار أمر (Run)

كتابة التالي : system.ini

ستظهر صفحة نتوجه للسطر الخامس فيها فإذا وجد أن السطر مكتوب هكذا :

user. exe=user. exe

يعني ذلك أن الجهاز لم يتم اختراقه من قبل الهاكرز.

أما إذا وجد السطر الخامس مكتوب هكذا

*** *** *** user. exe=user. exe

يعني ذلك أن الجهاز قد تم اختراقه من قبل الهاكرز.

أهم الأشياء التي يبحث عنها الهاكرز

بعض الهاكرز يمارسون التجسس كهواية وفرصة لإظهار الإمكانيات وتحدي الذات، البعض الآخر يمارس هذا العمل بدافع تحقيق عدة أهداف تختلف من هاكر لآخر كما ما يلي :

- الحصول على المال من خلال سرقة المعلومات البنكية مثل أرقام الحسابات أو البطاقات الائتمانية.
- الحصول على معلومات أو صور شخصية بدافع الابتزاز لأغراض مالية أو انحرافية كتهديد بعض الفتيات بنشر صورهن على الإنترنت إذا لم يستجبن لمطالب انحرافية أو مالية.
- الحصول على ملفات جميلة مثل ملفات الباوربوينت أو الفلاش و الملفات المرئية (الفيديو) والأصوات أو الصور .
- إثبات القدرة على الاختراق ومواجهة العقبات وفرصة للافتخار بتحقيق نصر في حال دخول الهاكر على أحد الأجهزة أو الأنظمة المعلوماتية.
- الحصول على الرموز السرية للبريد الإلكتروني ليتسنى له التجسس على الرسائل الخاصة أو سرقة إسم البريد الإلكتروني بأكمله.
- الحصول على الرمز السري لأحد المواقع بهدف تدميره أو التغيير في محتوياته.
- الانتقام من أحد الأشخاص وتدمير جهازه بهدف قهره أو إذلاله.

طرق اختراق المواقع

يتبع المخترقون عدة أساليب، في عمليات تشويه صفحات الويب (مواقع الانترنت، تختلف هذه الأساليب من موقع إلى آخر، بناءً على نوع نظام التشغيل ومزود الويب الذي يعتمد عليه الموقع.

أكثر هذه الأساليب انتشاراً

1- الدخول بهوية مخفية (anonymous) عبر منفذ بروتوكول FTP تمكن هذه الطريقة في بعض الحالات المخترق من الحصول على ملف كلمة الدخول المشفرة الخاصة بأحد المشرفين على الشبكة أو من يملكون حق تعديل محتويات الموقع والعمل على فك تشفيرها حيث يتم إرسال كلمة السر مشفرة في مختلف المزودات، لكن هذه الشيفرة تظهر في بعض المزودات ضمن ملف كلمة السر ويظلل البعض الآخر من المزودات هذه الكلمة بعد تشفيرها **(أي يظهر حرف x مكان كل رمز من الكلمة المشفرة)**، يصعب على المخترقين في الحالة الأخيرة عملية كسر الشيفرة.

يلجأ المخترقون بعد الحصول على ملف كلمة السر إلى استخدام برامج خاصة لتخمين كلمات السر، من أكثر هذه البرامج انتشاراً: Cracker Jack، John The Ripper و Jack The Ripper و Cracker Brute Force، تعمل هذه البرامج على تجربة جميع الاحتمالات الممكنة لكلمة السر من حروف وأرقام ورموز لكنها تستغرق وقتاً أطول في التوصل إلى هذه الكلمة إذا احتوت على عدد كبير من الرموز، قد تصل الفترة التي تتطلبها هذه البرامج للتوصل إلى كلمة السر إلى عدة سنوات بناءً على عدد الرموز المستخدمة والنظام المستخدم في عمليات التخمين.

كما ينصح باستخدام كلمة سر طويلة نسبياً وتغييرها خلال فترات متقاربة للتقليل من احتمال توصل أحد المخترقين إليها.

2- استغلال الثغرات الأمنية في مزودات ويب وأنظمة التشغيل حيث لا يخلو أي نظام تشغيل أو مزود ويب من ثغرات أمنية تعرض مستخدميه لخطر الاختراق، يعمل المطورون بشكل مستمر على سد هذه الثغرات كلما اكتشفت، يستغل المخترقين هذه الثغرات الأمنية في عمليات الاختراق إلى أن تجد الشركة المصممة للنظام الحل المناسب لها، تبقى بعض الثغرات متاحة لفترة طويلة حتى يتم اكتشافها، ذلك لأن أغلب هذه الثغرات يكتشفها المتجسسون الذين لا يعلنون عنها بسرعة ليتمكنوا من استغلالها فترة أطول لذا ينصح جميع مدراء ومشرفي الشبكات بمتابعة مواقع الشركات المصممة لنظم التشغيل ومزودات الويب للاطلاع على آخر ما تم التوصل إليه من ثغرات أمنية وجلب برامج الترقيع (patches) لها، حيث تحرص هذه الشركات على تقديم مثل هذه البرامج بأسرع وقت ممكن.

3- استخدام بروتوكول Telnet تسمح كثير من الثغرات الأمنية في الأنظمة المختلفة سواء كانت يونكس أو ويندوز أو غيرها من الأنظمة باستخدام تطبيقات تعتمد على بروتوكول Telnet الذي يسمح بالوصول إلى أجهزة الكمبيوتر عن بعد وتنفيذ الأوامر عليها، يمكن استخدام هذا البروتوكول للدخول إلى مزودات الويب وتغيير الصفحات فيها.

الأهداف و الأسباب التي تدفع جهة معينة او شخصاً معيناً الى القيام بهجمات اختراق الأجهزة و التجسس على الافراد و المؤسسات و قرصنة الانترنت

1- التسلل إلى النظام يمكن أن يتمكن بعض المخترقين من التسلل إلى النظام وقت انهياره وحجبه عن الخدمة أو وقت إعادة إقلاعه، توجد عدة طرق لذلك على مختلف الأنظمة، هي أحد الأسباب الأكثر منطقية لمثل هذه الهجمات.

2-أسباب سياسية قد توجه جهة معينة مثل هذه الهجمات إلى موقع حكومي يتبع دولة تعاديها أو موقع شركة تنتمي إلى هذه الدولة، يتوقع أن تزداد في المستقبل هذه الهجمات ذات الأهداف السياسية مع ازدياد انتشار الإنترنت.

3-أسباب اقتصادية قد توجه شركة صغيرة مثل هذه الهجمات إلى شركة كبيرة تسيطر على السوق في نوع من المنافسة التجارية غير الشريفة.

4-الانتقام يحدث كثيراً أن تفصل شركة أحد الموظفين المسؤولين عن إدارة الشبكة، يلجأ بعض هؤلاء إذا ما شعروا بالظلم، إلى الانتقام من الشركة.

5- الطبيعة التخريبية يلجأ بعض الأشخاص إلى مثل هذه الهجمات لإشباع رغبات تخريبية تتملكهم.

عمليات الاختراق الخاصة بخدمة البريد

تتعدد أشكال العمليات التي يمكن من خلالها التسلل إلى خدمات البريد الالكترونية الموجودة على الشبكات فهناك العملية التي يتم فيها استخدام رسائل خاصة بالبريد الإلكتروني بهدف تدمير خدمة البريد الإلكتروني الخاص بالشخص المستقبل (Mail Bombing)، تعرف الرسائل في هذا النوع باسم Mai Bombs أو التسلل من خلال إرسال بريد غير مرغوب فيه من خلال بوابة الاتصال الخاصة ببرتوكول SMTP المتعلقة بالمصدر (Mail spamming)، تتعدد في الواقع أشكال رسائل البريد المدمرة (Mail Bombs) فمنها ما يكون عبارة عن رسالة بريد إلكتروني واحد مرفق بها الكثير من الملفات الضخمة أو عدة رسائل إلكترونية يتم إرسالها بهدف إحداث نوع من زيادة التدفق في صندوق البريد أو وحدة الخدمة (هي العملية المسماة ب flooding)، توجد على سبيل المثال برامج تقوم بإنشاء آلاف رسائل البريد الإلكتروني، تقوم بإرسالها إلى صندوق البريد الخاص بمستخدم معين مما قد يؤدي إلى إتلاف وحدة الخدمة الخاصة بالبريد أو إعاقة بريد إلكتروني معين حيث سيتجاوز الحد الافتراضي لسعة التخزين الخاصة به.

من الأشكال الأخرى لعمليات الاختراق الخاصة بالبريد ما يمكن أن يتم خلاله إرسال رسالة إلى شخص ما بحيث لا يكون له الخيار في قبولها أو رفضها، تعرف هذه العملية باسم Mail spamming، خير مثال على هذا النوع هو الإعلانات التجارية، تطرح الأدوات الخاصة بهذا النوع من العمليات للبيع عبر الانترنت في كثير من خدمات البريد الإلكتروني.

علاوة على ما سبق لا نستطيع أن نغفل شكلاً آخر من عمليات الاختراق الخاصة بالبريد يتمثل في تزييف البريد الإلكتروني (Mail spoofing) أو (Mail fraud)، فيها يقوم الشخص المهاجم للشبكة بتزييف البريد من خلال كتابة عنوان البريد الإلكتروني الخاص بشخص آخر في حقل From داخل رسالة البريد الإلكتروني، ثم يقوم بتوجيه كم هائل من الرسائل التي تطلب من المستقبلين ضرورة إرسال الرسائل إلى صندوق البريد الخاص بهذا العنوان المزيف للحصول على مزيد من المعلومات، هكذا، بذلك بدأ مزودو خدمات الإنترنت بالانتباه لتلك الأنواع من الهجمات المتعلقة بتزييف البريد الالكتروني، التي انتشرت بشكل يسبب الازعاج، يعمل على إتلاف خدمات الشبكات بأكملها.

يدعي معظم الأشخاص المخترقين لخدمات البريد الإلكتروني أن الأساليب والآليات التي يعملون بها من شأنها تأمين عملية الإرسال بحيث لا يتم التعرف على هوية المستخدم سواء كان الغالبية العظمى من هؤلاء الأشخاص يمتلكون قائمة بوحدات الخدمة التي تعد بروتوكول SMTP، التي لا تشمل حالياً على عناوين IP لإجراء عمليات تسجيل الدخول، هذا هو الأسلوب الذي يتم به تزييف رسائل البريد الإلكتروني من جانب الأشخاص المستخدمين لنظام التشغيل Windows .

عمليات الاختراق المرتبطة بكلمة المرور

في أي نظام كمبيوتر يكون لكل مستخدم كلمة مرور معينة، تظل كلمة المرور هذه ثابتة إلى حين أن يقرر المستخدم تغييرها، عند كتابة كلمة المرور تقوم النواة الخاصة بإمكانية التأكد والتوثيق بتشفيرها من خلال تحويلها إلى رموز ثم تدرجها ضمن قائمة كبيرة من كلمات المرور المشفرة. عندما يجري هذا المستخدم عملية تسجيل دخول في المرة القادمة تقوم الوحدات النمطية بفحص كلمة المرور التي يكتبها ثم تقارنها بتلك الكلمات المشفرة المدرجة في القائمة، في حالة حدوث تطابق بين كلمة المرور التي تم إدخالها وكلمة أخرى من كلمات المرور المخزنة يتمكن المستخدم على الفور من الدخول إلى النظام، بناءً على هذا فإن أي شخص يرغب في اختراق النظام أو التسلل إليه بعد ذلك يوجه اهتمامه الأول إلى ملف كلمات المرور، اعتماداً على إعدادات التوصيف الخاصة بالجهاز، لو استطاع الأشخاص المتسللون الحصول على مستوى وصول معين، سيكون في إمكانهم الحصول على نسخة من هذا الملف وتشغيل أحد البرامج الخاصة بكشف كلمة المرور لتحويل هذه الرموز مرة أخرى إلى حروف فعلية ومعرفة كلمة المرور الأصلية التي تم إدخالها.

تتركز المهام التي يتم تنفيذها من جانب برنامج الكشف عن كلمة المرور في تشفير قائمة طويلة من السلاسل الحرفية كمجموعة الكلمات الموجودة في قاموس ما ثم فحصها ومقارنتها بملف كلمات المرور المشفرة، إن حدث تطابق يتمكن الشخص على الفور من التسلل إلى النظام، لا يحتاج هذا النوع من الهجمات إلى مستوى مهارة عالٍ ولذلك تنتشر الكثير من برامج الكشف عن كلمات المرور على شبكة الانترنت، لكن الفرصة لا تزال متاحة لتأمين بعض النظم ضد هذه البرامج من خلال الاحتفاظ بملف كلمات المرور في مستوى تأميني أعلى، أما المشكلة الفعلية تكمن في برامج الرصد والاستكشاف.

مخاطر الاختراق

في عام 1993م فاز ثلاثة من الهاكرز بسيارتي بورش ورحلة مجانية و20 ألف دولار بعد مشاركتهم في مسابقة هاتفية تم فيها اختراق الخطوط الهاتفية ومنع أي مكالمات من الوصول إلا مكالماتهم هم، تم سجنهم جميعاً، كان من بينهم الأسطورة كيفن بولسن الصحفي المتعاون مع صحف كثيرة حالياً في مجال الكمبيوتر والانترنت، أما في عام 1995 تم اعتقال أشهر مخترق في العالم الأسطورة كيفن ميتنك، بقي متنيك 4 سنوات من دون محاكمة في السجن، في التوقيت نفسه استطاع هاكرز من دولة روسيا سرقة 10 ملايين دولار من اكبر بنك تجاري في الولايات المتحدة تقريباً في العالم أما في عام 1998م تم إطلاق برنامج التجسس الشهير باك أولافيس في مؤتمر ديفكون السنوي.

أنظمة عربية برسم الإختراق

لا يخفى أن كثيراً من الجهات والدوائر الرسمية العربية تفتقر إلى وجود الأنظمة المؤتمتة أو قواعد البيانات الرقمية، ما زالت تعتمد على أنظمة يدوية قديمة في الأرشفة والتشبيك، تختلف درجة انتشار الأنظمة

المؤتمتة من دولة عربية إلى أخرى والحقيقة التي يجب أن تكون معلومة هي أن هذه الأنظمة القديمة التي تفتقر إلى أي نوع من الأتمتة أو الربط الشبكي تعتبر أكثر أماناً من كثير من الأنظمة المعلوماتية المؤتمتة التي تستخدمها الجهات الرسمية العربيّة.

التجسس الإلكتروني

ارتبطت غالبية الدول العربية بالإنترنت، هو أمر طال انتظاره فازدادت الأخطار التي يمكن أن تتعرض لها شبكات البيانات الحكومية في هذه الدول، لا نعني هنا أن مصدر الخطر يكمن في الربط بالإنترنت بل في ضعف الجانب الأمني لهذه الشبكات واعتمادها على أنظمة عالمية واسعة الانتشار يعرف معظم خبراء الشبكات والمعلومات أدق جوانبها الأمنية، تنتشر في الإنترنت مواقع كثيرة تقدم شروحاً وافية لطرق اختراق هذه النظم واستغلال الثغرات الأمنية فيها للحصول على المعلومات المختلفة فتكون بذلك سهلة الاختراق نسبياً إذا لم تتوفر الحلول الأمنية المناسبة.

يعتقد الكثيرون أن مصادر محاولات اختراق الأنظمة والشبكات العربية تقتصر على المخترقين الأفراد أو منظمات عالم الإنترنت السفلي مثل منظمات الهاكر التي تحاول دائماً توجيه محاولات الاختراق نحو أنظمة و شبكات ومواقع المنظمات والجهات الحكومية في العالم أجمع لكن هذه المحاولات لا تؤدي في أغلب الأحيان إلا إلى نتائج تخريبية يمكن إصلاحها إذا وجدت نسخ احتياطية من هذه البيانات، أما الجانب الأخطر في هذه العمليات فيكمن في محاولات التجسس الدولي التي تنقل أسرار دول بأكملها إلى دول معادية.

تقلص دور الجواسيس الدوليين الذي كان منتشراً أيام الحرب الباردة، اقتصر هذا الدور على حالات خاصة، قلت لذلك الحاجة لتجنيد وتدريب أشخاص ذوي كفاءات ذهنية وبدنية عالية لسنوات عديدة، من ثم دسهم في قلب نظام دولة معادية لسرقة أسرارها وتسريبها إلى دولتهم الأصلية، تحولت طرق التجسس في عصر الإنترنت إلى عمليات تجسس إلكترونية واختراق لأنظمة وشبكات الدول بعضها بعضاً فمعظم دول العالم تحتفظ بوثائقها السرية مخزنة بهيئة رقمية في مزودات سرية بعد تشفيرها بمفاتيح تشفير عالية الأمان، تضمن بذلك شبه استحالة كسر هذه الشيفرة والاطلاع على فحوى هذه الوثائق، تفيد تقارير عديدة عن وجود محاولات من وكالات الاستخبارات العالمية للتجسس على مستخدمي الإنترنت في العالم مثل الكشف الذي تم منذ فترة عن مفتاح " وكالة الأمن القومي الأمريكية" (NSA) في أنظمة ويندوز، أشارت الدراسات وقتها إلى ارتباط ذلك المفتاح بهذه الوكالة ليسمح لها بجمع المعلومات عن جميع مستخدمي نظام ويندوز عبر الإنترنت، نفت كل من مايكروسوفت ووكالة الأمن القومي الأمريكية أن يكون لهذا المفتاح أغراض تجسسية، قالت مايكروسوفت أنه يتعلق بمستوى التشفير الذي تقره الوكالة المعنية.

شكك بعض المحللين بهذا التبرير في ذلك الوقت حيث ثبتت على وكالة الأمن القومي الأمريكية عدة حالات من التجسس العالمي نفتها نفياً قاطعاً لعشرات السنوات.

نشرت جامعة جورج واشنطن في موقعها على الإنترنت عشرات الآلاف من الوثائق السرية الخاصة بالوكالة تمثل معظم عملياتها طوال خمسة عقود مضت حتى منتصف التسعينيات، هي معروضة للبيع بآلاف الدولارات برعاية الوكالة ذاتها.

بينت هذه الوثائق مثلاً حقيقة مشروع تجسس إلكتروني عالمي يسمى (Echellon) كانت الوكالة تنفيه لسنوات عديدة تقول أنه من نسج خيال بعض الصحفيين والمحللين، يمكن الاطلاع على فهرس الوثائق في الموقع (http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.htm1)
جدير بالذكر أن هذه الوثائق تشمل سياسات وسلوك الولايات المتحدة خلال أحداث عالمية عديدة مثل السياسة النووية وحرب الخليج وحروب أفغانستان والسياسة ضد إيران وكوبا والصين لكنها لا تأتي على ذكر أي كلمة عن سياسة أو عمليات الولايات المتحدة بالنسبة لإسرائيل أو الصراع العربي الإسرائيلي، ربما لأن إسرائيل منعت وكالة الأمن القومي " الأمريكي" من نشرها.

المصادر المفتوحة هي الحل

تكمن المشكلة الرئيسية في أنظمة التشغيل العالمية المنتشرة في أنها ذات مصادر مغلقة أي أن الشركة المصممة للنظام تخفي الشيفرات المكونة لبرنامج وأجزاء نظام التشغيل المختلفة عن أي جهة أخرى لمنع تطوير أو تعديل هذا النظام بدون أخذ الموافقة من الشركة الأصلية، لا يمكن لذلك أن يعدّل المطورون أو الجهات المستخدمة للنظام أياً من إعداداته الأمنية أو أن يتخطوا الثغرات التي تكتشف فيه إلا بعد أخذ الإذن من الشركة المصممة أو بعد أن تقدم تحديثات لسد هذه الثغرات.
من غير المستبعد أن تعلم جهات كثيرة في العالم بهذه الثغرات وتستغلها لأغراض تجسسية قبل أن يعلم بها مدراء النظم و الشبكات في العالم العربي، على الرغم من خطورة هذه الحالة إلا أن الخطر الحقيقي يكمن في أن يُسمح لجهات معينة أو دول معينة في العالم بالتعرف على المصادر
والشيفرات المكونة لهذه النظم أو أن تُضمّن منظمات معينة أبواباً خلفية فيها لأهداف خاصة كما هو الأمر بالنسبة لمفتاح NSA في نظام ويندوز إذا كان الغرض منه هو ما أشيع فعلاً.

التوجهات الرئيسية التي تضمن استقلالية و سرية نظم المعلوماتية التابعة للحكومات العربية

- يجدر بنا الاعتماد على أنظمة التشغيل ذات المصادر المفتوحة مثل لينكس(Linux) أو يونكس (Unix) مع التشديد على تعديل الجانب الأمني فيها محلياً لإلغاء إمكانيات الدخول عبر الثغرات المعروفة فيه وإعطائه خصوصية أمنية مستقلة، جدير بالذكر أن شركة صن (Sun) أعلنت أخيراً عن نيتها طرح الإصدار الثامن من نظام التشغيل Solaris على أن يكون مصدره مفتوحاً بالإضافة إلى توزيعه مجاناً ليضاف لاعب جديد في عالم أنظمة التشغيل ذات المصادر المفتوحة.
- أن تتمكن مؤسسات علمية أو شركات عربية من تقديم أنظمة تشغيل عالية الأداء للعمل مع الشبكات بدرجة أمان مرتفعة، أن تقدم حلولاً متخصصة للأنظمة الحكومية على أن يتفرد كل حل بمواصفات أمنية خاصة بهذا النظام، نعلم أنه أمر يحتاج إلى زمن طويل وأبحاث كثيرة، إن كثيراً من الناس سيشككون في إمكانية حدوثه، إننا نملك كلاً من الإمكانيات المادية والخامات العلمية اللازمة لتطوير هذه النظم، لكن ينقصنا دمجهما معاً هو أمر يقع على عاتق رجال الأعمال العرب حيث لم يدرك معظمهم حتى الآن أنهم إذا استثمروا أموالهم في مثل هذه المشاريع

التي تسمح بتطوير أنظمة معلوماتية عربية مستقلة وإيصالها إلى العالمية فإن الفائدة ستكون علمية وحضارية بل ومادية بأرباح عظيمة، يمكن لمن لم يقتنع النظر إلى الأرباح الخيالية لشركات الأنظمة المعلوماتية في العالم، منها الشركات التي تقدم أنظمة التشغيل.

- تطوير الحلول الأمنية والتطبيقات المختلفة المعتمدة على المصادر المفتوحة التي يمكن تطويرها ذاتياً وتعديل الجانب الأمني فيها بحيث يصعب اختراقها لأن بنيتها ستكون غامضة على الجهات الخارجية خلافاً للبرامج التي تطورها الشركات العالمية الشهيرة.
- توخي الحذر عند تبني أي حل أمني خارجي في الأنظمة المعلوماتية الحكومية في العالم العربي وعدم الاكتفاء بدراسة إمكانياته الأمنية بل يجب أن يوضع تحت اختيارات صارمة لدراسة كافة عمليات الإدخال والإخراج التي تحدث خلال عمله، أن تدرس جوانب أخرى.

أنظمة معلومات الدول العربية تحت تصرف إسرائيل

يتفق معظم الخبراء أن إسرائيل تصنف في المرتبة الثانية بعد الولايات المتحدة الأمريكية بين الدول المنتجة للتقنيات المعلوماتية خاصة الأمنية منها، لا يخفى كذلك أن ما تقدمه الدول العربية مجتمعة للبشرية في مجال تقنية المعلومات يماثل في ضآلته ما قدمته هذه الدول للبشرية في مجالات الفضاء أو الطب أو غيرها من العلوم في القرن الماضيّ فهي تقف اليوم في موقع المتلقى للتقنيات على الرغم من وجود العديد من المحاولات الجادة والطموحة، لكن ما سبب التفوق الإسرائيلي عالمياً في مجال أمن المعلومات.

التفوق الإسرائيلي بتكنولوجيا المعلومات على الدول العربية

تلقت إسرائيل حوالي 800 ألف مهاجر من الاتحاد السوفييتي السابق، أدت هذه الهجرة إلى ارتفاع نسبة العلماء و المهندسين فيها لتصل أواخر التسعينيات إلى رقم قياسي عالمي هو 135 عالماً أو مهندساً لكل 10 ألآف نسمة، كان لهؤلاء دور بارز في دفع عجلة الصناعة المعلوماتية لكن لم يكن لهم أن يفعلوا ذلك لولا وجود التخطيط السليم الذي يجب أن نعترف به.

العوامل الرئيسية التي جعلت من الصناعة المعلوماتية الإسرائيلية إحدى أكثر الصناعات المعلوماتية تطوراً على مستوى العالم إلى درجة دفعت شركات كبرى في عالم تقنية المعلومات إلى التهافت على إسرائيل والاستثمار فيها بالموارد المادية والبشرية:

- وجود الجامعات و المعاهد التقنية المتخصصة في المعلوماتية: كان لجامعات ومعاهد مثل معهد Technion في مدينة حيفا دور بارز في تقديم العقول المختصة في تقنية المعلومات تشير بعض الإحصائيات إلى أن هذا المعهد قدم عدداً من المهندسين والتقنيين يعادل العدد الذي قدمته كل من جامعة Standford ومعهد MIT في الولايات المتحدة الأمريكية لتغذية صناعة المعلوماتية بالعقول الخبيرة، كانت هذه المعاهد نقطة مركزية لنشوء صناعات معلوماتية مهمة.
- اعتماد خطط تجارية مبتكرة لدعم المشاريع المعلوماتية: إن إنشاء شركة جديدة في عالم تقنية المعلومات أمر محفوف باحتمالات الفشل في هذا الخضم الهائل من الشركات التي تستخدم

الإنترنت للوصول إلى الأسواق العالمية متخطية كافة الحواجز ومطيحة بأي شركة جديدة منافسة أينما كانت، تنبه الخريجون الجدد في المعاهد التقنية الإسرائيلية إلى هذا الأمر فاعتمدا أسلوباً تجارياً مبتكراً لدفع شركاتهم الصغيرة إلى السوق العالمية يعتمد على تكوين تجمعات من كل الشركات الصغيرة التي تمتلك أفكاراً أو مشاريع معلوماتية مبتكرة في مواسم محددة ومشاركة هذه التجمعات في أجنحة مشتركة ضمن أكبر المعارض العالمية المختصة في تقنيات المعلومات لعرض أفكارها على الشركات العالمية وطرح فكرة رعاية المشاريع أو المشاركة في تمويلها، أدى هذا الأسلوب إلى دخول معظم الشركات العالمية العاملة في سوق تقنية المعلومات مثل مايكروسوفت وإنتل وهيوليت باكرد و كومباك Motorolla 3Com, Cisco, Lucent, AOL, IBM, General Electic, Computer Associates, Texa Instruments,Yahoo, Cent وغيرها الكثير إلى سوق تقنية المعلومات الإسرائيلية وتبنيها شركات إسرائيلية صغيرة أو تمويلها بعشرات أو مئات الملايين من الدولارات لكن ما سبب التفوق في مجال أمن المعلومات تحديداً.

- القوات المسلحة الإسرائيلية منبع لخبراء أمن المعلومات: تختلف سنوات الخدمة الإلزامية العسكرية في الجيش الإسرائيلي عنها في الكثير من دول العالم إذ تعتبر فترة تطوير لخبرات المختصين في مجال أمن المعلومات، يعتبر هذا الأمر من أهم العوامل المؤثرة في دفع تطوير الحلول الأمنية والتطبيقات المتعلقة بأمن المعلومات في إسرائيل فيكفي أن نعلم أن شركة CheckPoint الإسرائيلية التي تقدم أكثر حلول أمن المعلومات انتشاراً في العالم التي وصلت حصتها في إحدى السنوات إلى 44 في المائة من سوق الجدران النارية في العالم هي شركة طورها ضابط سابق في الجيش الإسرائيلي يدعى شارون كارمل مع زملائه قضى هؤلاء فترة خدمتهم الإلزامية في تطوير أنظمة كمبيوترية لمحاكاة ساحات القتال وتطوير وسائل ربط شبكات كمبيوترية عالية الأمان، يقول كثير من رؤساء شركات أمن المعلومات في إسرائيل أن سنوات الخدمة الإلزامية الثلاث تُزّف الجندي إلى كثير من التقنيات الحديثة، تتيح له الفرصة للتعامل معها، تشكل أرضاً خصبة لعمليات ابتكار التقنيات الحديثة التي يمكن تطبيقها تجارياً بعد إنهاء الخدمة الإلزامية، من أهم المجالات التي تفوقت فيها الشركات الإسرائيلية مجال برامج أمن الشبكات كالجدران النارية حيث لاحظ الوافدون الجدد إلى سوق المعلوماتية الإسرائيلية أهمية أنظمة الشبكات وتطبيقات الإنترنت و مدى انتشارها فركزوا إنتاجاهم على هذا المجال وظهرت شركات مثل Checkpoint,Aladdin قدمت منتجات عالمية، لاحظوا أيضاً أهمية التشفير في عصر الإنترنت فأجريت دراسات عديدة في هذا المجال أدت إلى ظهور عدد من التقنيات العالمية مثل تقنية RSA الشهيرة للتشفير التي ننتجها شركة RSA، التي تستخدم في كثير من مواقع التجارة الإلكترونية والتبادلات الإلكترونية في الإنترنت.
- الدعم الحكومي: لاحظت الحكومة الإسرائيلية التطور الكبير في ميدان تقنيات المعلومات في الدولة والتدافع العالمي من شركات تقنيات المعلومات للحصول على حصة في الشركات الإسرائيلية العاملة في هذا المجال فرأت أن تزيد من الاستثمارات الحكومية في الشركات الصغيرة الناشئة، قدمت لذلك مليار دولار عام 1998 لعمليات التطوير التقني في هذه الشركات، الجدير بالذكر أن الحكومة الإسرائيلية تخصص 3 في المائة من ميزانيتها السنوية للصرف على البحث

العلمي أي يبلغ مقدار ما يصرف سنوياً في هذا المجال 3 مليارات دولار، فمتى نشهد مثل هذه المبادرات من الحكومات العربية التي لا تنقصها الموارد المادية.

لا يقتصر الامتداد الإسرائيلي في مجال تقنية المعلومات على جانب أمن المعلومات على الرغم من أنه أهم المجالات وأكثرها انتشاراً حيث تتفوق صناعة المعلوماتية الإسرائيلية في الكثير من المجالات الأخرى مثل التشفير والتراسل الفوري وتقنيات الصوت والفيديو، من أشهر البرامج الإسرائيلية في مجال التراسل الفوري : برنامج ICQ من شركة Mirabilis وبرنامج Gooey من شركة Hypernix الذي يتوقع أن يحصل على نجاح يعادل نجاح ICQ.

التبعية العربية

إذا نظرنا إلى حلول أمن المعلومات المطبقة في الأنظمة المعلوماتية والشبكات التي تعتمدها كثير من الحكومات العربية، مثل جدران النار سنجدها جميعاً مصنعة خارجياً، كذلك سنجد أن العشرات منها تعتمد على حلول أمنية مصنعة في إسرائيل، ما يزيد على ذلك هو جهل القائمين على هذه الشبكات العربية التابعة للقطاع الحكومي بهذه الحقيقة.

فالاعتماد الكلي على تقنيات أجنبية للحفاظ على أمن معلوماتنا وتطبيقها على الشبكات الرسمية التابعة للدول العربية، هو تعريض للأمن الوطني والقومي لهذه الدول للخطر، ووضعه تحت سيطرة دول غريبة بغض النظر عما إذا كانت هذه الدول عدوة أم صديقةّ، الدول تتجسس على بعضها بغض النظر عن نوع العلاقات بينها، هذه حقيقة قائمة لا يمكن نفيها، تطورت أساليب التجسس في هذا العصر، أصبحت الأسلحة المعتمدة هي الوسائل الإلكترونية، خاصة عبر الإنترنت.

لا يقتصر الأمر على التجسس على المعلومات لأهداف عسكرية وسياسية بل يتعداه إلى القطاع التجاري فنحن نعلم جلياً الآن أن الشركات العاملة في مجال تقنية المعلومات تتجسس على بعضها البعض وعلى مستخدمي منتجاتها(مثلما فعلت شركة RealNetworks وإنتل ومايكروسوفت وغيرها بالإضافة إلى شبكات ومواقع الإنترنت عديدة) للحصول على معلومات تعطيها الأفضلية على منافستها في الأسواق أو لصالح جهات حكومية معينة ما الذي يضمن إذاً ألا تتجسس الشركات الإسرائيلية وغير الإسرائيلية المقدمة للحلول الأمنية، التي تضع أمن البيانات تحت سيطرتها على شبكات الدول العربية أو الأنظمة المعلوماتية المختلفة التي تعتمد هذه الحلول لهذا السبب شددنا على ضرورة تطوير حلول أمن المعلومات محلياً أو على الأقل وضع الحلول الأمنية الأجنبية التي نرغب باستخدامها تحت اختبارات مكثفة ودراسات معمقة والتأكد من استقلاليتها وخلوها من الأخطار الأمنية.

أسلحة هجومية جديدة تهدد شبكة الويب

لعل توفر مجموعة من التقنيات الحديثة وارتفاع نصيب شركات أعمال الإنترنت في الأسواق يوضحان سبب انقطاعات عدد من أبرز مواقع شركات الإنترنت الرائدة عن الخدمة.

فقد توفرت و لفترات طويلة أسلحة بدائية تستخدم في تنفيذ هجوم "حجب الخدمة" denial of service الذي يشل مواقع الويب لكن خبراء الأمن يقولون إن عدداً من أسلحة الاعتداء الفعالة التي تساعد على أتمتة إطلاق تلك الهجمات ظهرت في الآونة الأخير.

باستخدام برامج مثل Tribal Flood Network, Trinno و Stacheldralnt يمكن استغلال أجهزة الكمبيوتر البريئة المرتبطة بالشبكة العالمية في إطلاق طوفان كبير من الرسائل والطلبات باتجاه المواقع التي تستهدفها هذه الأسلحة.

يمكن للمهاجمين الذين يستخدمون هذه البرامج اقتحام عشرات ومئات أجهزة الكمبيوتر المرتبطة بالشبكة وتركيب ما يشبه القنبلة الموقوتة التي يصعب اكتشافها فيها، يمكن للمهاجم في وقت لاحق أن يُرسل أمراً لكافة الأجهزة التابعة التي زرع فيها قنابله يجعلها تطلق سيلاً من المعلومات يؤدي لانسداد الشبكة المستهدفة.

على الرغم من أن ضحايا الهجمات التي وقعت حديثاً على مواقع مثل CNN.com,Buy.com Amazon.com, eBay, Yahoo لم يتأكدوا من أن المهاجمين استخدموا هذه التقنيات إلا أن معظم المحللين يتوقعون أن تصبح سلاحاً هجومياً في الحروب الرقمية في الوقت الذي تتزايد فيه الحصص الاقتصادية والمعارك للسيطرة على الإنترنت بشكل سريع فإن وجود مثل هذه الأسلحة قد يكون مغرياً لبعض من يرتكبون مثل هذه الهجمات.

يقول روب إندلر المحلل لدى مؤسسة Giga Information Systems "تشير هذه الهجمات إلى إمكانية وقوع هجمات أشرس مما يتطلب من الشركات وضع خطط للعمل وتجهيز نفسها".

كانت السلطات القانونية و منظمات الإنترنت قلقة بشأن انتشار تقنيات الاعتداءات الجديدة لبعض الوقت حيث أطلق مكتب التحقيق الفيدرالي الأمريكي FBI والمعهد الأمريكي للمواصفات والتكنولوجيا NIST و مركز الطوارئ التابع لشركة Garnegie-Mellon's تحذيرات بهذا الخصوص في الأشهر الأخيرة.

كان أول المواقع التي تعرضت لمثل هذا الهجوم الشامل هو موقع جامعة مينيسوتا الذي أغلق فعلياً واستخدم في تلك الحادثة 227 كمبيوتراً لإمطار نظام الجامعة بوابل من الحركة ارتبط بعضها بنظام الإنترنت 2 الأكاديمي عالي السرعة.

لم يؤكد أحد أن هذه الأدوات أو ما يشبهها التي استخدمت فعلاً في الموجة الجديدة من الهجمات على مواقع الويب الرئيسية إلا أن خبراء الأمن يقولون إن ما استخدم في هذه الهجمات يشبه إلى حد كبير تلك الأدوات ما يعني ذلك أن هذا النوع من "الإرهاب الشبكي" سيستمر.

يقول جيم ماجديش مدير أبحاث الأمن لدى مؤسسة PGP Security: "إذا كان من قام بتلك الهجمات شخص لديه عدد كبير من أجهزة الكمبيوتر التابعة التي تنتظر الأوامر بالهجوم فبإمكان ذلك الشخص أو المجموعة إطلاق الهجمات واحدة تلو الأخرى".

يراهن العديد من محللي الشؤون الأمنية أن شخصاً واحداً، أو مجموعة منظمة، هي المسؤولة عن الأحداث التي وقعت حديثاً، لكن ذلك لا يعني أن هجمات مخططة أخرى تحوم في الأفق.

يقول الخبراء إن الحصول على الأدوات المستخدمة في هذه الهجمات سهل و متاح في الإنترنت أما وكالة FBI فتقول إنها وجدت آثاراً لأدوات الهجوم منتشرة بشكل واسع في عدد من الشبكات ما يزيد احتمال وقوع المزيد من الهجمات.

يقول مديرو الشبكات أنه يوجد عدد قليل من الدفاعات ضد مثل هذه الهجمات إلا أن العديد من المحللين قالوا إنهم لا يرون في هذه الهجمات تهديداً قوياً للتجارة الإلكترونية على المدى البعيد.

كانت الهجمات التي تعرضت لها المواقع البارزة على الإنترنت حديثاً سبب الانقطاع لفترات قصيرة بحيث لا تؤدي إلى اكتشاف مرتكبيها علاوة على أن بعضها يتحلى بدرجة عالية من التنظيم كتلك التي تعرض لها موقع Yahoo مثلاً و يقول مجديش: " يمكن لهذه الهجمات أن تستمر لأيام إلا أن ذلك يعرض مرتكبيها للاكتشاف".

من الناحية النظرية كانت المواقع الشهيرة على الإنترنت عرضة للهجوم منذ فترة، للدلالة على ذلك فقد تعرض موقع شركة eToy للهجوم بواسطة مستخدمين أرادوا أن يعبروا عن احتجاجهم على جهود قانونية قامت بها الشركة لإلغاء اسم نطاق مجموعة فنية هو etoy أيضاً.

تعبر عدة مواقع عسكرية كالتي تديرها البحرية الأمريكية ووكالة الفضاء الأمريكية من ضحايا هجمات من هذا النوع.

إلا أن الهجوم الأخير على المواقع البارزة رفع من حدة الشعور المعادي والحادثة التي تعرض لها موقع Yahoo مثلاً تضمنت ما يقرب من 50 جهازاً تعمل بالتبادل، قامت بإرسال حجم كبير من الجيجابايتات في الثانية لتعطيل النظام.

قال بعض المراقبين إنهم يلحظون ارتباطاً بين الهجوم على ياهو والوقت الذي عُقد فيه مؤتمر مزودي خدمة الشبكات إذ قدمت مجموعة North American Network Operators Group ورقة عمل حول الهجمات التي تسبب في حجب الخدمة في الوقت الذي تم فيه مهاجمة موقع Yahooما يثير التكهنات بأن الهكرة أرادوا توصيل رسالة واضحة للمجتمعين، يعتقد دانييل تود مدير الخدمات العامة في شركة System Keynote أيضاً بأن الأمر ليس مصادفة.

لم تُعلن أي جهة، مسؤوليتها عن هذه الهجمات على الرغم من اجتماع ضباط مكتب FBI بمسؤولي موقع Yahoo لمناقشة هذا الموضوع لكن برزت مؤشرات ربما تؤدي للوصول إلى المهاجمين الهكرة بغض النظر عن حجم هذه الهجمات أو الدوافع الكامنة خلفها فالهجمات التي تتسبب في قطع الخدمة قد تكون الآن من حقائق العصر الرقمي الذي نعايشه.

يقول بيتر نيومان محلل الشؤون الأمنية لدى SI International: "يبدو سهلاً القيام بمثل هذه الهجمات كما يبدو صعباً في الوقت ذاته اتخاذ الدفاعات المناسبة لكن ذلك ليس مدعاة للقلق فقد تعرضنا لهجمات أقسى مثل الهجوم على " بيرل هاربر" في الماضي".

الاستيلاء على 2500 بطاقة ائتمان عن طريق الاختراق

ما مدى سهولة الاستيلاء على أرقام بطاقات الائتمان على شبكة الإنترنت استطاعت شبكة NSNBC خلال بضع دقائق عرض قوائم تحتوي على حوالي 2500 رقم بطاقة ائتمان تخزنها سبعة مواقع للتجارة الإلكترونية صغيرة الحجم باستخدام تعليمات أولية زودتها بها إحدى الجهات كانت هذه القوائم إما غير محمية بكلمات مرور أو كانت كلمات المرور الموجودة في الموقع مكشوفة.

قفزت مسألة سرقة بيانات بطاقات الائتمان هي إحدى المشاكل المرتبطة بالتجارة عبر الإنترنت إلى واجهة الأحداث التي تهم المستخدمين حين تمكن أحد المتطفلين الذي أطلق على نفسه اسم "ماكسس" من اقتحام قاعدة بيانات بطاقات ائتمان المستخدمين التابعة لشركة CD Universe، ما زالت التكهنات تتضارب حول الطريقة التي تمكن بها من القيام بذلك.

لعل ماكسس لم يكن بحاجة لبذل جهد كبير لتحقيق ذلك فقد تمكنت شبكة MSNBC، هي شبكة إخبارية تملكها كل من مايركوسوفت وشبكة NBC من عرض ما يقارب 2500 رقم بطاقة ائتمان

وبيانات أخرى بمجرد تصفح مواقع التجارة الإلكترونية على شبكة الويب باستخدام أدوات قواعد بيانات متوفرة تجارياً بدلاً من استخدام متصفح للشبكة، كانت تلك المواقع تخزن بطاقات الائتمان على شكل نص عادي، في قاعدة بيانات متصلة بالشبكة، تستخدم أسماء العملاء الافتراضية بدون كلمة مرور أحياناً.

اكتشفت هذه الثغرات الأمنية شركة Strategy LLC الروسية للبرمجيات، يقول أناتولي بروكوروف كبير مديريها التنفيذيين أبلغ تلك المعلومات لشبكة MSNBC أنه حاول في البداية الاتصال مع شركات أخرى إلا أنها لم تستجب له.

يقول بروكورف: " يدل هذا الأمر في رأينا على درجة عالية من عدم الاحتراف، ليس له ما يبرره " و تكتب شركة Stategy LLC برامج تساعد المستخدمين على مقارنة الأسعار عبر مواقع تجارة إلكترونية متعددة، اعتاد لذلك المطورون العاملون فيها على بنية البيانات الموجودة في مئات المواقع التي تتعامل بالتجارة الإلكترونية، لم يكن المطورون العاملون يبحثون عن الثغرات الأمنية على وجه التحديد إلا أنهم عثروا عليها عن طريق الصدفة ووصف بروكوروف الوضع بأنه " باب مفتوح" دهشنا لوجوده"، لكن خبراء الأمن لم يدهشوا! فمع السرعة اللازمة للنجاح في اقتصاد الإنترنت ذي الأهمية المتزايدة أصبحت الشركات على عجلة من أمرها لنشر مواقع عمل لها على الشبكة، هو ما يجعلها تهمل المسائل المتعلقة بالأمن.

يقول إلياس ليفي صاحب موقع "SecurityFocus.com " يعتبر ما وجده بروكوروف نموذجاً مصغراً لما هو قائم بالفعل، ليس بإمكاننا إلا أن نتخيل ما كان سيجده المتطفلون لو كانت أغراضهم سيئة، فالمشكلة التي نحن بصددها مترامية الأطراف"، كان موقع SecurityFocus.com هو أول من أبلغ عن اختراق قاعدة بيانات شركة CD Universe .

ليست الثغرات الأمنية التي اكتشفها بروكوروف مجرد وسيلة سهلة لسرقة بطاقات الائتمان إذ تضمنت المواقع السبعة التي تمكن MSNBC من عرض كماً كبيراً من المعلومات الشخصية للمستخدمين التي تشمل: عناوين إرسال الفواتير وأرقام الهواتف وأرقام الضمان الاجتماعي للموظفين أحياناً.

أرسل بروكوروف لشبكة MSNBC قائمة بعشرين موقعاً على الشبكة بتعليمات أولية للدخول إليها لمشاهدة أرقام بطاقات الائتمان، لم توفر هذه المواقع التي كانت كلها تشغل برنامج SQL Server من مايكروسوفت حماية بكلمات المرور لمزودات قواعد بياناتها فيما وفر بعضها كلمة مرور لكن اكتشافها كان سهلاً، كانت عملية الدخول إلى تلك المواقع سهلة إذ لم تتطلب أكثر من تشغيل مزود و فتح اتصال مع الموقع على شكبة الويب.

هذه المواقع هي : Softwarecloseouts.com, PIMWeb.com, computerparts.com eExpressmicro.com, EPCdeals.comK Sharelgic.net, Directmicro.com قد تم الاتصال بالمواقع السابقة وتنبيهها إلى ضرورة سد الثغرة الأمنية.

على الرغم من أن وجود الثغرت الأمنية أمر مؤكد إلا أن تعيين السبب الحقيقي قد لا يكون هيناً فالمخاوف تزداد من تعرض الشركات الصغيرة خاصة للاختراقات الأمنية لأن معظمها لا تشغل خبراء في الكمبيوتر بين صفوفها، يلجأ بعض أصحاب الشركات أحياناً لقبول عروض إنشاء مواقع منخفضة التكلفة من مطورين يعدون بتوفير الأمن على الموقع إلا أنهم يخفقون في ذلك لأسباب مختلفة يضاف إلى ذلك الظهور المستمر للمشاكل الأمنية في البرمجيات التي تساعد على وقوع الاختراقات الأمنية.

يمكن في بعض الحالات الاطلاع على الشيفرة الموجودة في الكمبيوتر المزود والمتضمنة في صفحة الويب إذا أدخل المستخدم عبارة "::$DATA" مباشرة بعد كتابة عنوان الموقع ضمن مستطيل العنوان

في المتصفح، هذا إذا كان العنوان ينتهي بالامتداد (asp.)، يمكن أن يؤدي ذلك إلى الكشف عن أسماء المستخدمين أو كلمات المرور أو أي معلومات أخرى عن الكمبيوترات المرتبطة بالمزود على الرغم من اكتشاف هذه الثغرة وتصحيحها إلا أن MSNBC وجدت أربعة من المواقع المعرضة للاختراق التي يستضيفها مزود ويب واحد لم تعمل على سد تلك الثغرة كان يمكن للثغرة أن تكون داخل البرمجيات.

قال روس كبور خبير الأمن الذي يدير قائمة البريد NTBugTraq أنه يفضل الحصول على أكثر من رأي عند بناء موقع للتجارة الإلكترونية.

أوصى كوبر بوضع شرط في عقد بناء الموقع ينص على وجوب اجتياز الموقع الاختبارات الأمنية التي يجريها طرف ثالث، قال إن المشكلة الأساسية هي عدم مسؤولية المطورين عن الثغرات التي يتركونها بعد بناء مواقع التجارة الإلكترونية، على الرغم من أن التجار مسؤولون عن دفع تكلفة أي بضائع مسروقة إلا أن معظم عقود المطورين تنص على أنهم غير مسؤولين عن عما يحدث للمواقع التي يبنونها و ينتهي لذلك الأمر بحصول كثير من الشركات على موقع يعمل لكنه غير آمن.

ليس لدى المستخدم العادي وسيلة لمعرفة مدى حماية معلوماته الشخصية بعد تسليمها لموقع معين على شبكة الويب، قال ليفي: " يقع اللوم على أكثر من شخص فلا يمكن التعجل في بناء موقع للتجارة الإلكترونية بصرف النظر عن الأموال التي يخطط لجنيها فالكثير من الأشخاص لا يأبهون بمسائل الأمن.

من الأخطاء الأساسية في كافة المواقع السابقة في عدد آخر من المواقع تخزين معلومات العملاء الخاصة بنص عادي على الرغم من توفر أساليب التشفير التي تضمن عدم القدرة على قراءة هذه المعلومات يقر الخبراء أن هذا التصرف غير مقبول.

قال ويزلي وايلهيلم مستشار منع الاحتيال في مجلس Internet Fraud Prevention Advisory Council: "نصيحتي هي إبقاء المعلومات الخاصة بالمستخدمين بمنأى عن الوصول إليها عن طريق الشبكة إن لم نضمن أمنها ".

أما المستهلكون فليس لديهم ما يفعلونه للتأكد من الطريقة التي يحمي بها موقع الويب بياناتهم الشخصية، يقترح بعض الخبراء استخدام بطاقة ائتمان واحدة للتسوق عبر الإنترنت و الاستمرار في التدقيق في فواتير البطاقة التي يلفقونها لضمان عدم استخدامها من قبل آخرين.

نشاط الهكرة في مواقع الإنترنت العربية

استهدفت هجمات "الهكرة" أخيراً مواقع عربية خاصة وحكومية على الإنترنت كان معظمها في بلدان الخليج العربية، تفيد آخر الأنباء بوقوع هجومين جديدين: أحدهما في الرياض دولة الإمارات العربية المتحدة تحديدا إمارة الشارقة.

تصاعدت حدة الهجمات التي يقوم بها مخترقو أنظمة الكمبيوتر والموجهة لمواقع الإنترنت الحكومية خاصة في الدول العربية خلال الفترة الأخيرة، قد أبلغ عن احتراق موقعين في منطقة الخليج.

تعرض موقع شركة MBCE المتخصصة في الأعمال الهندسية والاستشارية مقرها الرياض للاختراق ثلاث مرات خلال خمسة أسابيع من قبل مجموعة أو أكثر من المخترقين، يعتقد أنهم موجودون في البرازيل، موقع الشركة هو (www.mbce.com.sa) ما زال يتعرض للاختراق.

غير المخترقون الصفحة الرئيسية للموقع و ظهرت فيه رسالة مكتوبة باللغة البرتغالية تعلن عن إنشاء ما يُسمى بفريق النخبة "Elite Team" للهكرة ، وصفت المجموعة نفسها بأنها مجموعة جديدة لعصر جديد، كما سخرت الرسالة من مدير الموقع لعدم قدرته على حماية مزودات الموقع تفاخرت الرسالة بقدرات و مهارات أعضاء الفريق، تم ترجمة نصًا تضمنته الرسالة التي تركها الهكرة على موقع الشركة يقول :"من كانت لديه المعرفة يجب أن يكون قادراً، من كانت لديه سلطة فهو يمتلك زمامها".

تعرَض موقع المكتبة العامة في مدينة الشارقة في الإمارات العربية المتحدة (http://shjlib.gov.ae) للاختراق وترك الهكرة على الموقع رسالة مسيئة استمرت لمدة طويلة إلى أن منع المشرفون على الموقع وصل الزوار إليه.

تابع فريق IIT هجمات المخترقين على مواقع موجودة في الشرق الأوسط قبل حوالي عام لكنها كانت تستهدف في تلك الفترة الصفحات الشخصية على شبكة الويب إلا أن شدة الهجمات تزايدت خلال الأشهر الماضية من قبل مجموعات دولية ومحلية من المخترقين صغار السن الذي انضموا إلى اللعبة.

كانت مواقع الويب في المملكة العربية السعودية هدفاً مفضلاً للمخترقين، تعرضت بعض المواقع الخاصة للاختراق بالإضافة إلى موقع وزارة الشؤون الخارجية الحكومي الذي لم يعد ممكناً الوصول إليه.

من المواقع الأخرى التي تم اختراقها في المنطقة خلال الأشهر القليلة الأخيرة كل من موقع مطار الكويت الدولي وهيئة كهرباء ومياه دبي في الإمارات العربية المتحدة وهيئة الاستثمار الكويتية وشركة DigiSys اللبنانية للبرمجيات والعتاد لكن تم إصلاح هذه المواقع، لم يعد فيها أثر للتخريب حالياً، سبق أن تعرضت مؤسستا إنترنت قطر وجلوبال ون" في الأردن لهجمات مماثلة.

لم تقتصر عمليات الاختراق على المواقع العربية فقد تعرضت كبرى مواقع الإنترنت العالمية لعمليات اختراق، أو تخريب ومنها eBay,amazon, ZDNet,Yahoo وغيرها، يعود السبب الرئيسي وراء تزايد الهجمات على مواقع الويب العربية إلى ارتفاع عدد هذه المواقع بشكل كبير خلال العام الماضي قد يكون لارتفاع أسعار النفط خلال الأشهر الماضية دور في الهجوم على المواقع الخليجية تحديداً يمكن أن نستشعر هذا من بعض رسائل الحسد التي تركها المخترقون في بعض هذه المواقع.

إختراق الشبكات اللاسلكية

تعتبر أولى خطوات الإختراق البحث ثم إيجاد شبكة إيصال لاسلكية، هناك عدة برامج تستخدم لهذا الغرض الأشهر و المستخدم من قبل الهاكرز والمتطفلين برنامجين هما:

Nets tumbler

يعتمد هذا البرنامج على الويندوز في تشغيله، يستطيع بكل سهولة تحسس وإيجاد الشبكات اللاسلكية في حدود نطاق بحثه أخذا في الاعتبار المسافة بين الجهاز ومصدر بث الشبكة كذلك يستطيع تحديد قوة الإرسال ومستوى الضوضاء لإشارات تلك الشبكة المستهدفة التي تكون أسبابها عادة الأجسام التي تعترض نطاق بث الشبكة كالجدران مثلا، كذلك الأجهزة التي تصدر إشارات قد تتداخل مع إشارات الشبكة اللاسلكية، هذه المعلومات عن الشبكة تستخدم لإجراء مسح لجودة الشبكة.

Kismet

مايميز هذا البرنامج أنه يملك القدرة في رصد وكشف الشبكات التي تبث بالخفاء مما يعني أن معظم أجهزة الشبكات اللاسلكية أكسس بوينت، تكون مزودة بخاصية البث المخفي التي تمنع إظهار اسم الشبكة أو الـ SSID مما يمنع ظهورها في نتائج بحث أجهزة الكمبيوتر أو المحمول اللاسلكية عن شبكات في حدود نطاق البث والاستقبال، لن يستطيع جهاز كمبيوتر مكتبي أو محمول مزود بخاصية إتصال لاسلكي من رصدها أو إظهارها لإنه لايملك اسم الشبكة، هذا البرنامج يستطيع إيجادها حتى لو كانت مخفية، هذا ما يجعله من الأدوات الخطرة حينما تسقط بيد عابث. إذا كانت تلك الخطوة الأولى إيجاد الشبكة أو الشبكات المستهدفة الخطوة التي تتبع عادة تكون محاولة الإيصال بتلك الشبكة، إذا كانت تلك الشبكة غير مشفرة فبكل بساطة نستطيع تأسيس إتصال معها، لكن إذا كانت تلك الشبكة مخفية، باستعمال الـ Kismet يستطيع بناء أو عمل بروفايل للشبكة المراد استهدافها، في حال كانت تلك الشبكة مشفرة بإحدى طرق التشفير المستخدمة في معظم الشبكات authenticationأو encryption فقد نحتاج لأدوات مساعدة لفك التشفير، من أشهر البرامج التي تستخدم هذه الرموز(****) رمز أو مفتاح أو كود التشفير التالي:

Airsnort

مايميز هذا البرنامج سهولته فلسنا بحاجة أن نكون خبراء لكي نتقن عمله، يستخدم للتجسس على الشبكة المستهدفة ، من ثم مفتاح أو كود التشفير و الذي يستخدمه الكثير من الناس في حماية شبكاتهم اللاسلكية، بالتأكيد استخدام التشفير للحماية أفضل من استخدام لاشيء ، ما يلاحظ على أداء هذا البرنامج أنه يحتاج لبعض الوقت لكي يقوم بتحليل الإشارات الصادرة من الشبكة المستهدفة ذلك بإرسال كميات من الحزم اللاسلكية للشبكة المستهدفة و استقبال الرد منها، من ثم تحليلها واستخراج مفتاح التشفير، يعاب على هذا البرنامج بطئه بعض الشيء، هناك بعض الحيل والإستراتيجيات التي تستخدم لتقليل مدة التجسس وإستخراج مفتاح التشفير الخاص بالشبكة، لكن هذه الخاصية غير متاحة مع هذا البرنامج.

CowPatty

هذه الأداة أو البرنامج تستخدم قوة لإجبار الشبكة على الكشف عن رموز التشفير، حيث يقوم بتجربة حزم كبيرة جدا من الرموز بسرعة فائقة مغيرا النسق، مستفيدا من معجم إنجليزي يحويه بين أحشائه حتى يصطاد فريسته، من ثم يظهرها يشابهه في عمله برامج كشف الأرقام السرية لبطاقات الائتمان.

AsLeap

هذا البرنامج مصمم لرموز أو مفتاح التشفير للشبكات التي تستخدم نظامLeap هذا النظام غير مشهور أو مستخدم بكثرة لحماية الشبكات لكونه ضعيف وسهل الاختراق لكن عمله و طريقته مشابهة إلى نظامي authenticationو encryption .

سواء خلال الاتصال بالشبكة اللاسلكية أم لا، كانت الشبكة في وضع البث وحدود النطاق هناك كميات من المعلومات مازالت تحلق في الهواء في أي لحظة، يحتاج المتطفل(المتسلل) لبعض الأدوات لكي يرى تلك المعلومات، هذا ما يرمز عليه باستنشاق المعلومات، من أشهر برامج "الاستنشاق" هو:

Ethereal

يتميز بقدرته الهائلة، تميزه عن بقية البرامج المنافسة له، هذا البرنامج يستطيع البحث عن المعلومات التي تبث لاسلكيا أو عن طريق الإيثرنت، هذا ما يزيد من جبروته ثم يعود بمعلومات مرشحة (مصفاة) جبارة عن تلك الشبكة يستطيع كذلك استخراج رمز حماية إدارة الشبكة "Admin Codes" مما يمكن المتسلل من التحكم في الشبكة وتغيير ما يشاء في خصائصها وإعداداتها، كذلك يستطيع رصد الشبكات المخفية.

ما يتوجب عمله كإجراء دفاعي ضد تلك البرامج أو السلاح الذي يجب استخدامه في وجه كل برنامج على حدهبرنامج NetStumbler

باستخدم نظام البث المخفي المشفر، فهذا البرنامج ضعيف أمام هذه الخاصية.

برنامج Kismet

لا يمكن فعل الكثير لمواجهة رصد الشبكة اللاسلكية مع هذا البرنامج، لإنه سواء كانت مخفية أو لا فهو يرصدها، لذلك كل ما يتوجب فعله هو تشفير الشبكة بأحد نظامي authentication أو encryptionالمطور وتحديث الـ firmware الخاص بالجهاز باستمرار متى ما صدر جديد.

برنامج Airsnort

للقضاء على خطر هذا البرنامج ينصح باستخدام أحد نظامي التشفير authentication أو encryption و استخدام نموذج الـ 128 bit- الذي يتيح عمل مفتاح أو كود للتشفير بحدود 40 خانة، ليس نظام الـ 40 bit- الذي يستخدم مفتاح أو كود حماية في حدود 8 خانات استخدام نظام أل 128-bitسيجعل عملية إيجاد رمز أو مفتاح التشفير أطول بكثير لمستخدم هذا البرنامج، كما انه في حالة كانت الأجهزة تدعم تقنية التشفير المطورة التي يشار إليها بـ WPA أو WPA2 بدلا من نظام WEP فمن الأفضل استخدامها، "بعض الأجهزة قد تحتاج لترقية أو تحديث برنامج التشغيل firmware أو software.

Cowpatty

ينصح هنا باستخدام رموز تشفير معقدة أي عدم استخدام كلمات سهلة فالمعجم المستخدم في هذا البرنامج يستطيع إيجادها بسرعة فائقة، لذا يجب أن يكون رمز التشفير في الغالب مكون من كلمات أو أحرف أو خليط ما بينهم طويلا ما أمكن و ينصح باستخدام تقنية الـ 128. bit كما أن هذا الإجراء مهم جدا لأصحاب الشبكات الكبار التي يوجد بها أكثر من مركز إدار ة للشبكة أكثر منAdmin واحد.

ASLeap

إستخدام رمز تشفير معقد و طويل ما أمكن و ينصح بالترقية للنظام الجديد من Eap الذي يشار إليه بـ EAP-FAST أو إلى أي نظام جديد من EAP.

Ethereal

استخدام نظام تشفير authentication أو encryption بخاصية الـ 128 bit- دائما حتى يقوم بعمل تشفير للبيانات الصادرة والقادمة إلى الشبكة فهذا البرنامج يستنشق المعلومات الصادرة من الشبكة وإليها.

اختراق الأجهزة العاملة بتقنية البلوتوث Flexilis مجموعة من الهاكرز سموا أنفسهم فليكسيليس، تعتبر خاصية البلوتوث(Bluetooth) أو البندقية التي صممت لاختراق الأجهزة العاملة بتقنية البلوتوث أطلقوا عليها اسم Blue Sniper بلو سنايبر. يمكن لهذه البندقية استهداف أي جهاز جوال يدعم خاصية البلوتوث على مسافة تصل إلى ميل و نصف وسرقة البيانات الموجودة على الهاتف الضحية كدفتر العناوين والرسائل وغيرها، كما يمكنه زرع رسائل داخل الجهاز. الخطير في الأمر أن المهاجم يستطيع استخدام الهاتف الضحية لإجراء اتصال إلى أي هاتف آخر دون أن يشعر صاحب الجهاز، تخيل أنك جالس مع شخص ما في مطعم وهاتفك في جيبك أو على الطاولة وقام المهاجم بالتحكم في جهازك للقيام بمكالمة إلى هاتفه دون أن تشعر، عندما يرد المهاجم سيصبح هاتفك جهازاً للتصنت يمكن المهاجم من الاستماع إلى كل ما يدور بينك وبين صديقك في المطعم، معظم الهجمات يمكن أن تتم بدون ترك أي أثر للمهاجم.

قبل فترة قام باحث ألماني بتطوير برنامج سماه Blue bug يمكنه التحكم في الأجهزة الجوالة العاملة بنظام البلوتوث وتحويلها إلى أجهزة تصنت عن بعد، مثلاً من خلال كمبيوتر محمول يمكن تشغيل البرنامج للتحكم في الهاتف النقال للقيام بمكالمة إلى المهاجم دون أن يشعر الضحية بذلك و بالتالي يستطيع المهاجم التصنت على المحادثات التي تتم بالقرب من الهاتف الجوال بالطبع سيظهر رقم هاتف المهاجم في فاتورة الضحية، لكن بعد فوات الأوان، من الصعب أن يتذكر الضحية حينها هل اتصل أم لا بذلك الرقم و في ذلك الوقت.

يمكن أن يستخدم المهاجم شريحة جوال مؤقتة حتى لا تدل على شخصيته في حال اكتشاف الرقم يمكن للمهاجم أيضاً التجسس على مكالمات الضحية مع الأشخاص الآخرين وتسجيلها كما يمكنه إرسال رسائل من هاتف الضحية إلى أطراف أخرى دون أن ينتبه لذلك صاحب الجهاز.

تكون الهواتف الجوالة عرضة للهجوم والاختراق في حالة تمكين البلوتوث وضبطها على الوضع "discoverable" أو "visible" حيث أن الهاتف في هذا الوضع يكون مرئياً من قبل الأجهزة المتوافقة الموجودة ضمن مجال الاتصال، يسمح لها ذلك بالاتصال ببعضها و تبادل البيانات فيما بينها، يمكن للمستخدم بالطبع أن يقوم بإيقاف و تعطيل هذا الوضع إلى "Off" لكن بعض أجهزة نوكيا يمكن اختراقها حتى لو كانت على وضع التعطيل، فكل ما يحتاجه المهاجم هو عنوان البلوتوث للجهاز الضحية هو ما يمكن اكتشافه باستخدام بعض برامج الاختراق المتوفرة على الإنترنت.

من خلال التقارير المنشورة ظهر أن أسوأ الأجهزة في مقاومة هذه الهجمات هي أجهزة نوكيا سوني و اريكسون، ظهرت بعض المشاكل في أجهزة موتورولا أيضاً بينما كانت أجهزة سيمنس أقوى الأجهزة في الحماية ضد هذه الهجمات. قام مخترعو هذه البندقية بإجراء تجربة حية لإثبات إمكانية عملية الاختراق بواسطة بندقيتهم المزودة بهوائي موصل بجهاز كمبيوتر محمول يدعم بلوتوث (يمكن وضعه في حقيبة على الظهر) حيث قام أحدهم بتصويب البندقية من نافذة في الطابق الحادي عشر لأحد الفنادق في مدينة لاس فيجاس إلى موقف لسيارات الأجرة في الشارع المقابل، تمكن من جمع دفاتر العناوين من 300 جهاز هاتف نقال، بدأت معظم الشركات المنتجة للهواتف النقالة بتحديث أجهزتها لمعالجة هذه المشكلة الأمنية.