بنك الاستثمار القومي
قطاع الاستثمار والموارد
الدعم الفني للاستثمار

دراسات دورية

العدد التاسع

الهجمات السيبرانية

إعداد
هبة أحمد عبدالدايم
منار محمد شعبان

يوليو ٢٠١٧

سلسلة دراسات دورية

تصدر سلسلة دراسات دورية عن الإدارة المركزية للدعم الفني للاستثمار بقطاع الاستثمار والموارد، بنك الاستثمار القومي. وتهتم هذه السلسلة بإلقاء الضوء على أهم الموضوعات التي تساهم في إثراء المعلومات في جميع المجالات بما يعود بالنفع وزيادة الثقافة والمعلومات العامة. وتصدر بشكل دوري.

جميع الآراء الواردة في هذه السلسلة هي مجرد تحليلات واجتهادات بحثية، ولا تعبر بأي حال عن الرأي الرسمي لبنك الاستثمار القومي، ويجب أخذها في إطارها البحثي فقط.

المحتويات	الصفحة

فيروسات الكمبيوتر

ما هي الفيروسات

بحسب جريدة القبس الالكترونية فيروسات الكومبيوتر هي برامج تتم كتابتها بطريقة معينة بغرض إلحاق الضرر بكمبيوتر آخر، أو السيطرة عليه. سُمّيت بالفيروسات، لأنها تشبه تلك الكائنات المتطفلة في صفتين رئيسيتين :

(١) تحتاج دائماً إلى عائل تعيش متسترة فيه

فالفيروسات، دائماً تتستر خلف ملف آخر، ولكنها تأخذ زمام السيطرة على البرنامج المصاب. بحيث أنه حين يتم تشغيل البرنامج المصاب،فإنه يتم تشغيل الفيروس أولاً.

(٢) تستطيع أن تنسخ نفسها

تتم كتابة هذه البرامج المؤذية بحيث تقوم بنسخ نفسها فوراً بمجرد تشغيل البرنامج المصاب. وهي تنسخ نفسها للأقراص المدمجة (CD's) الأخرى، فإذا كان الكومبيوتر مصاباً ووضعت فيه أسطوانة (CD)، يتم نسخ الفيروس أوتوماتيكيا للاسطوانة. ونظراً لهذه الخاصية في الفيروسات، تجد أن ال CD المصاب يعطيك علامة أنه ممتلئ تماماً برغم أنك لم تقم بتخزين غير ملفات ذات حجم صغير.

ما الفرق بين الدودة Worm و الترجان Trojan horses و الفيروس Virus ؟

الدودة (Worm): تصيب الدودة الكمبيوترات الموصلة بالشبكة بشكل أوتوماتيكي و من غير تدخل الإنسان و هذا الأمر يجعلها تنتشر بشكل أوسع و أسرع عن الفيروسات . و الديدان لا تقوم بحذف أو تغيير الملفات بل تقوم بإستهلاك موارد الجهاز و استخدام الذاكرة بشكل فظيع مما يؤدي إلى بطء ملحوظ جدا للجهاز ، و من المهم تحديث نسخة النظام المستخدمة في الجهاز كي يتم تجنب الديدان.

ومن المهم عند الحديث عن الديدان الإشارة إلى تلك التي تنتشر عن طريق الإيميل. حيث يرفق بالرسالة ملفاً يحتوي على دودة، و عندما يشغّل المرسل إليه الملف المرفق، تقوم الدودة بنشر نفسها إلى جميع الإيميلات الموجودة في دفتر عناوين الضحية.

الترجان (Trojan horses): وهو عبارة عن برنامج يغري المستخدم بأهميته أو بشكله أو باسمه إن كان جذاباً، و في الواقع هو برنامج يقوم بفتح باب خلفي بمجرد تشغيله ، و من خلال هذا الباب الخلفي يقوم المخترق باختراق الجهاز وبإمكانه التحكم بالجهاز بشكل كبير حتى في بعض الأحيان يستطيع القيام بأمور ، صاحب الجهاز نفسه لا يستطيع القيام بها ، و هذا لا يرجع لملف التروجان ، لكن ملف التروجان هو الذي فتح للمخترق الباب إن صح التعبير بتشغيله إياه.

الفيروس(Virus): عبارة عن برنامج صمم لينشر نفسه بين الملفات و يندمج أو يلتصق بالبرامج. عند تشغيل البرنامج المصاب فانه قد يصيب باقي الملفات الموجودة معه في القرص الصلب (Hard Disk) أو الأقراص المدمجة (CD's)، لذا يحتاج الفيروس إلى تدخل من جانب المستخدم كي ينتشر ، بطبيعة الحال التدخل عبارة عن تشغيله بعد أن تم تحميله من الإيميل أو تنزيله من الانترنت أو من خلال تبادل الأسطوانات أو أنواع وسائط التخزين المختلفة

كيف تعمل الفيروسات؟

يقوم الفيروس في حالة إصابة الملف بإضافة نفسه في بداية أو نهاية الملف المصاب، دون أن يقوم فعلياً بأي تغيير في مكوّنات الملف الأصلية. وعند استدعاء البرنامج فإنه يعمل بشكل طبيعي بينما يقوم الفيروس بلصق نفسه في البرنامج دون أن يغير في محتويات الملف شيئاً. وطريقة اللصق تكون، إما أنه يقوم بلصق نفسه في بداية البرنامج، بحيث يتم تشغيله هو قبل البرنامج نفسه وقد تكون طريقة التحاق الفيروس بالملف بأن يضع نفسه في نهاية البرنامج المصاب. ويضع علامة في بدايته، فيختبئ في نهاية الملف المصاب، ويضع في مقدّمة البرنامج مؤشّراً بحيث أنه عندما يتم استدعاء البرنامج وتشغيله، يحوّل السيطرة للفيروس بدلاً من تشغيل البرنامج . ويسبب أضراراً جسيمة للجهاز

أنواع الفيروسات

هناك الآف من الفيروسات المنتشرة عبر الانترنت ، لكن اغلبها ما يقع تحت هذه النقاط الستة :

(١) فيروسات بدء التشغيل أو Boot Sector Virus

تعتبر من أقدم الفيروسات المعروفة لدى المستخدمين حيث تستطيع ان تصيب القرص الصلب (Hard Disk) والأقراص المدمجة (CD's) وتنتشر عن طريقها من مستخدم الى آخر وتكمن خطورة هذا النوع من الفيروسات في قدرتها على اصابة جزء أساسي من أي قرص صلب أو مدمج وهو الجزء المخصص لتوجيه الجهاز في كيفية تحميل برنامج نظام التشغيل ويقوم هذا الفيروس بتحميل نفسه للذاكرة في كل مرة يتم فيها تشغيل الجهاز

وهذا النوع من الفيروسات يصيب قطاع الإقلاع (The boot sector) في الجهاز، و هو المكان المخصص الذي يتجه إليه الكمبيوتر في بداية تشغيل الجهاز. و هذا النوع من الفيروسات قد يمنع المستخدم من الوصول إلى النظام ويمنعه من إقلاع الجهاز

(٢) فيروس الملفات أو File Virus

هذا النوع من الفيروسات يلحق نفسه كملف في أي برنامج تنفيذي و يتميز هذا النوع من الفيروسات بقدرته على الإنتشار بعدة طرق و بسرعة كبيرة منها وسائط التخزين المختلفة (Storage media) و الأقراص المدمجة (CD's) ورسائل البريد الإلكتروني (Email messages) كملف ملحق كما يمكنه الإنتقال من البرامج المجانية و المتوفرة في الإنترنت و تكمن خطورته في قدرته على الانتشار السريع واصابة بقية الملفات الموجودة في البرامج التنفيذية الأخرى ويصيب البرامج عادة ، وينتشر بين الملفات الأخرى و البرامج الأخرى عند تشغيله

(٣) فيروس المايكرو أو Macro Virus

هذا النوع أيضا سريع الانتشار بين المستخدمين خاصة أنه قادر على الانتشار بكل الطرق كوسائط التخزين المختلفة (Storage media) و الأقراص المدمجة (CD's) ورسائل البريد الإلكتروني (Email messages) و البرامج المجانية و كذلك أثناء تحميل أو تنزيل البرامج من الأجهزة الخادمة (Servers) و من الجدير بالذكر أن هذا النوع لا يصيب الا البرنامج التطبيقي التي صمم ليصيبه أساسا فمثلا لو كان هناك فيروس مصمم ليصيب برنامج تحرير الكلمات والنصوص فإنه لا يستطيع الحاق الأذى ببرنامج آخر مثل برنامج قواعد المعلومات و هكذا و لكن يستطيع أن يصيب أي ملف تم انشاؤه بواسطة البرنامج المستهدف

وهذه الفيروسات عادة تصيب برامج الميكروسوفت أوفيس (Microsoft Office) مثل الوورد (Word) و الإكسل (Excel)، و تعتبر ذات انتشار واسع جدا تقدر بـ ٧٥% من الفيروسات الموجودة. يقوم هذا النوع من الفيروسات بتغيير بعض المستندات الموجودة في القرص الصلب و خصوصا الوورد، قد تجد بعض التصرفات الغير منطقية في بعض الأحيان مثل طلب باسوورد (Password) لفتح ملف تعرف انك لم تضع عليه باسوورد ، و أيضا تجد بعض الكلمات قد تغير مكانها و أضيفت كلمات جديدة لا علاقة لها بالموضوع . هي أساسا ليست ضارة، لكنها مزعجة نوعاً ما وقد تكون مدمرة أحيانا!

(٤)الفيروس المتعدد الأجزاء Multipartite Virus

و هو الذي يقوم بإصابة الملفات مع قطاع الإقلاع (boot sector) في نفس الوقت و يكون مدمراً في كثير من الأحيان إذا لم تتم الوقاية منه

(٥) الفيروس المتطور Polymorphic Virus

هي فيروسات متطورة نوعا ما حيث أنها تغير الشفرة كلما انتقلت من جهاز إلى آخر. نظريا يصعب على مضادات الفيروسات (Antivirals) التخلص منها لكن عمليا و مع تطور المضادات فالخطر أصبح غير مخيف

(٦) الفيروس المختفي

تخفي نفسها بان تجعل الملف المصاب سليما و تخدع مضادات الفيروسات بان الملف سليم و ليس مصاباً بفيروس. مع تطور مضادات الفيروسات أصبح من السهل كشف هذا النوع.

ما هي العلامات الشائعة لوجود فيروس في الجهاز

- بطء الجهاز الشديد، بما لا يتناسب مع عدد البرامج التي تعمل في نفس الوقت
- امتلاء القرص بما لا يتناسب مع عدد و حجم الملفات الموجودة عليه
- ظهور مربّعات حوار غريبة أثناء العمل على الجهاز
- إضاءة لمبة القرص الصلب (Hard Disk) أوالأقراص المدمجة (CD's)، دون أن تقوم بعملية فتح أو حفظ ملف

لابد أن تعرف أن هذه العلامات لا تعني بالضرورة وجود فيروس، فقد يكون بعضها بسبب مشكلة في عتاد الجهاز مثلاً

الأمن السيبراني

الأمن السيبراني هو تعريب لكلمة cyper security، فكلمة cyper هي مرتبطة في الأساس بأجهزة الكمبيوتر والمحمول، أي بتكنولوجيا المعلومات والاتصالات. وهو عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير مصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين من المخاطر في الفضاء السيبراني.

الأمن السيبراني في مصر

أصدر رئيس مجلس الوزراء إبراهيم محلب فى ١٦ ديسمبر ٢٠١٤ قرارا بإنشاء مجلس أعلى لـ"الأمن السيبراني"، المعروف بأمن البنية التحتية للاتصالات وتكنولوجيا المعلومات.

ماذا يشمل هذا النوع من الأمن؟

الحماية من اختراق شبكات المعلومات في البلاد، بالذات تلك التي تحتوي معلومات سرية، والحماية من هجمات التعطيل والهجمات الإلكترونية للهاكرز، والحماية من الجريمة الإلكترونية، والحماية من تهديدات فيروسات الـ"سوفت وير" (software)، وكذلك الحماية من اختراق ترددات المكالمات.

اختصاص المجلس الأعلى للأمن السيبراني

وضع استراتيجية لمواجهة الأخطار والهجمات السيبرانية والإشراف على تنفيذ تلك الاستراتيجية وتحديثها.

ممن يتشكل؟

يرأسه وزير الاتصالات، بعضوية ممثلين عن ٩ وزارات "الدفاع، والخارجية، والداخلية، والبترول، والكهرباء، والصحة، والموارد المائية، والتموين، والاتصالات"، بالإضافة إلى ممثلين عن البنك المركزي، وجهاز المخابرات العامة، و٣ مختصين يرشحهم المجلس ويعينهم الوزير.

ما القوانين المختصة بموضوع أمن المعلومات في مصر قبل صدور هذا القرار؟

بالإضافة لقانون العقوبات وما يقرره عند ارتكاب جرائم، والذي تسري أحكامه على جرائم الفضاء الإلكتروني وقانون حماية الملكية الفكرية وقانوني المرافعات المدنية والتجارية والإثبات في المواد المدنية والتجارية، فإن هناك قانونين أساسيين لتنظيم الموضوع هما قانون تنظيم الاتصالات، وقانون التوقيع الإلكتروني ولائحته التنفيذية.

قانون التوقيع الإلكتروني

قانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠١٤ نص على إنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، ونص على أنه من مهامها تنظيم نشاط خدمات التوقيع الإلكتروني وغيرها من الأنشطة في مجال

المعاملات الإلكترونية وصناعة تكنولوجيا المعلومات، ومن مهام مجلس إدارتها وضع القواعد التي تكفل احترام تقاليد المهنة في مجال المعاملات الإلكترونية وتكنولوجيا المعلومات والاتصالات.
كما وضع القانون عقوبة على استعمال محررات الكترونية مزورة وشهادات التصديق المزورة، وأعطى القانون صفة الضبطية القضائية للعاملين بالهيئة فيما يخص الجرائم الإلكترونية المنصوص عليها فيه.

قانون تنظيم الاتصالات

قانون تنظيم الاتصالات، رقم ١٠ لسنة ٢٠٠٣ حتى الآن هو القانون الأساسي للتعامل مع هذا الموضوع، ونص على إنشاء جهاز تنظيم الاتصالات، ومن مهامها تنظيم مرفق الاتصالات بما يضمن الأمن القومي. وكذلك ما يتعلق بحماية وضمان كفاءة الخدمة، ورغم كونه لم يتحدث عن أمن المعلومات تحديدا، لكنه حدد في مادته الأولى الاتصالات بأنها "أية وسيلة لإرسال أو استقبال الرموز، أو الإشارات، أو الرسائل، أو الكتابات أو الصور، أو الأصوات، أيا كانت طبيعتها، وسواء كان الاتصال سلكيا أو لا سلكيا، ما يجعله يشمل كل أنواع الاتصالات والتواصل الإلكتروني بما في ذلك استخدام أجهزة الكمبيوتر أو الهاتف المحمول.
كما أعطى هيئته الحق في وضع قواعد وشروط منح التراخيص بما يضمن حقوق المستخدمين، خاصة حقهم في ضمان السرية التامة طبقا للقانون، وبما لا يمس بالأمن القومي والمصالح العليا للدولة ومعايير التخطيط العمراني والمعايير الصحية والبيئية.

أسباب صدور القرار؟

بالإضافة لأهمية إنشاء جهاز متخصص مماثل للموجود في بلدان أخري لتحقيق هذا الغرض، فإن هناك سبب آخر هو انتشار عمليات الاختراق الإلكتروني وانتشار اختراق مجال ترددات بعض الاتصالات.
وقد يكون قرار إنشاء هذا المجلس خطوة نحو تعديل قانون لتنظيم الاتصالات بما يلائم المتغيرات الجديدة، وخطوة نحو إصدار تشريعات حديثة في هذا المجال عموما.

عملة البيتكوين

البتكوين هو نوع جديد من العملة أو المال.
البتكوين عملة رقمية تعتمد علي التشفير "Cryptography" و هي ايضا عملة لا مركزية أي ان لا أحد يتحكم بها غير مستخدميها، فهم من يقومون بصنعها و استخدمها دون الحاجة الي وسيط او رقيب عليهم مثل حكومة او مصرف مثل باقي العملات الموجودة بالعالم. و عن نشأة البتكوين، في عام ٢٠٠٨ قام شخص يلقب ب "ساتوشي ناكاموتو" "Satoshi Nakamoto" بنشر دراسة يشرح بها ما هو البتكوين و كيف يعمل البتكوين و في عام ٢٠٠٩ قام "ساتوشي" باطلاق شبكة البتكوين للعالم.

كيفية عملها البيتكوين

البتكوين يعمل بنظام الند للند "peer-to-peer" و نظام الند للند يمكن المستخدمين من التعامل مباشرة بين بعضهم البعض دون الحاجة الي وسيط، بمعني ان البيانات التي تستقبلها انت علي جهاز الكمبيوتر الخاص بك هي قادمة من مستخدم اخر لشبكة البتكوين و ليست قادمة من "سرفير" و هذا يعطي شبكة البتكوين ميزة بان لا احد يمكنه ان يهاجم الشبكة او يحاول ان يغلقها او يقوم بالحجز علي البتكوين الخاصة بأي مستخدم.

هل من الممكن استخدام البتكوين فى خدمات البيع و الشراء؟

بالطبع، يمكنك استخدام البتكوين في بيع و شراء ما تريد. هنالك آلاف من المواقع والمتاجر الالكترونية التي تتعامل بالبتكوين وهي في تزايد يومي ومستمر وهنالك ايضا متاجر وفنادق ومطاعم حول العالم تتعامل بالبتكوين.

الاعتراف الدولى الرسمى بالبيتكوين

تعد ألمانيا الدولة الوحيدة التي اعترفت رسمياً بعملة بِتْكُويْن نوعاً من النقود الإلكترونية. وبهذا، اعتبرت الحكومة الألمانية أنها تستطيع فرض الضريبة على الأرباح التي تحققها الشركات التي تتعامل بـ «بِتْكُويْن»، في حين تبقى المعاملات المالية الفردية معفية من الضرائب.
وكان قاضٍ فدرالي في الولايات المتحدة قد حكم أخيراً بأن بِتْكُويْن هي عملة ونوع من أنواع النقد، ويمكن أن تخضع للتنظيم الحكومي، لكن الولايات المتحدة لم تعترف بالعملة رسمياً بعد.

الهجمات الإلكترونية

اجتاحت سلسلة من الهجمات الإلكترونية عددًا من دول العالم، يوم الجمعة ١٢ مايو ٢٠١٧، باستخدام فيروس خبيث يُعرف باسم "انتزاع الفدية" (Grab the ransom)، فيما أرجعها خبراء أمن الكمبيوتر إلى ضعف البرمجيات التي زعموا أن وكالة الأمن القومي الأمريكية استغلته في وقت سابق.
وسجّل خبراء في الأمن المعلوماتي وقوع أكثر من ٤٥ ألف هجوم في أكثر من ٩٩ دولة، من بينها بريطانيا وروسيا وأوكرانيا وتركيا واليابان والهند والصين وإيطاليا وأستراليا وبلجيكا وفرنسا وألمانيا والمكسيك وإسبانيا والفلبين، كما أنه تم إعلان مصر واحدة من الدول التي ضربها الفيروس العالمي الأشرس على الإطلاق وفقًا لشركة الأمن السيبراني الروسية "كاسبرسكاي لابس"(Kaspersky Labs).
من بين الشركات والهيئات الحكومية التي ألحقت بها الهجمات الإلكترونية اعتداءات جسيمة، كانت شركة فيديكس (FEDEX) الأمريكية العملاقة لتوصيل الطلبات، ودائرة الصحة الوطنية البريطانية (إتش إن سي)، ووزارة الداخلية الروسية.

ما الذى نعرفه عن الهجمات الالكترونية ؟

- استغل القراصنة ثغرة في نظام التشغيل "ويندوز" (Windows) في مايكروسوفت، اكتشفتها وكالة الأمن القومي الأمريكية (NSA)، واتاحتها مجموعة قرصنة تطلق على نفسها "وسطاء الظل" (Shadow Brokers) على الإنترنت ١٤ أبريل ٢٠١٧.

(وسطاء الظل (TSB) هم مجموعة من القراصنة ظهروا لأول مرة في صيف عام ٢٠١٦ ونشروا العديد من التسريبات التي تحتوي على أدوات القرصنة من وكالة الأمن القومي (NSA) ولا يزال مبتكروا هذا الجزء من فيروس الفدية غير معروفين، لكن "وانا كراي" هو محاولتهم الثانية في الابتزاز الإلكتروني؛ حيث كان قد تم اكتشاف نسخة مبكرة تحت مسمى "وي كراي" (WeCry) في فبراير ٢٠١٧، وطلبوا من المستخدمين قيمة ٠,١ من العملة المشفرة، (تساوي حاليا ١٧٧ دولاراً لكن مع قيمة متغيرة)، لإعادة فتح الملفات والبرامج.)

- حدّد خبراء الأمن البرنامج الخبيث بأنه بديل لفيروس انتزاع الفدية المعروف باسم "وانا كراي"(WanaCry) أو "واناكريبتور" (WanaCrypt0r)، التي تستغل نقاط الضعف في أنظمة مايكروسوفت ويندوز.

(فيروسWanaCrypt0r 2 هو البرنامج الضار الذي أصاب شركة تليفونيكا في إسبانيا و جهاز الصحة الوطنية في بريطانيا. رصد جزءا من فيروس الفدية لأول مرة من قبل الباحثين الأمنيين في فريق "Malware Hunter Team" في الساعة العاشرة إلا ربع من صباح يوم الجمعة ١٢ مايو٢٠١٧، وبعد أقل من ٤ ساعات، أصاب الفيروس أجهزة كومبيوتر جهاز الصحة وانتشر بعد ذلك عبر الشبكات الداخلية لجهاز الصحة)

- تضرّر ما لا يقل عن ١٦ مستشفى بريطاني، الأمر الذي حال الأطباء دون الوصول إلى ملفات المرضى، وأجبر غرف الطوارئ على تحويل المرضى. وقالت رئيسة الوزراء تيريزا ماي "لا يوجد دليل على تعرّض بيانات المرضى للاختراق."
- تلقّى العاملون في المنظمات التي ضربتها هجمات "انتزاع الفدية" (Grab the ransom) رسالة على أجهزة المراقبة خاصّتهم، مفادها: "عفوًا، لقد شُفّرت ملفاتكم!"، وطالبوهم بدفع ٣٠٠ دولار أمريكي بُعملة بيتكوين الافتراضية.

ما هو "انتزاع الفدية" الخبيثة (Grab the ransom) ؟

عندما يشن القراصنة هجومًا باستخدام فيروس "الفدية" الخبيث، يُرسلون إلى ضحاياهم بريدًا إلكترونيًا يحتوي على رابط يبدو للوهلة الأول عنوان ويب غير ضار أو ملف مُرفق عبر البريد. غير أنه في حقيقة الأمر يحتوي الرابط على ملفات مضغوطة مُشفّرة، تُصعّب من اكتشاف أهدافهم الشائنة.

ما إن يضغط الضحية على الملف المُرفق، حتى يُصاب حاسوبه بالفيروس الخبيث. وحينها يتم تشفير الملفات والمجلدات ومحركات الأقراص على جهازه. والأخطر من هذا هو "عدم اكتشاف المُستخدمين تعرّض أجهزتهم للاختراق، وأنه لم يعد بإمكانهم الوصول إلى بياناتهم، سوى بعد إرسال القراصنة رسالة تُعلِمهم بأمر الهجوم وتُطالبهم بدفع فِدية مقابل فكّ التشفير"، بحسب مكتب التحقيقات الفيدرالي.

تنطوي الرسائل التي يتلقّاها الضحايا على إرشادات لطريقة دفع الفدية. وعادة ما يطلب الهاكرز الدفع باستخدام عملة "بيتكوين" الافتراضية.

وكانت شركة مايكروسوفت اكتشفت ثغرة مُحتملة في خوادمها، مكّن فيروس "الفدية" وفيروسات خبيثة أخرى من التوغّل بداخل شبكاتها.

في فبراير ٢٠١٧، تعرّضت مستشفى في لوس أنجلوس لهجوم مماثل، اضطرت على إثره دفع ١٧ ألف دولار بعُملة بيتكوين.

ما الذى لا نعرفه عن الهجمات الإلكترونية؟

من يقف وراء الهجوم؟

بالرغم من أن قراصنة "وسطاء الظل" أفصحوا عن إحدى الأدوات المستخدمة في الهجوم، إلا أنه لا يزال من غير الواضح من هو المسؤول الحقيقي عن الهجمات. كما أنه لم يتبيّن على وجه الدقة "من هم قراصنة وسطاء الظل". ويقول خبراء الأمن إن "توقيت القرصنة غالبا ما يتماشى مع المصالح السياسية لبعض الدول."

هل دفع أي شخص الفدية؟

وفي هذا الصدد قال خبراء أمنيون إن الفدية التي طلبها القراصنة من الضحايا الذين وقعوا في فخّ الفيروس الخبيث كانت "قليلة نسبيًا". وأشار الباحث الأمني المعني بفيروسات الفدية، جيسون ريبهولز، إلى إمكانية البحث عن خدمة فكّ تشفير البيانات على الإنترنت، إلا أنها لا تكون "مُجدية" في الهجمات المتطورة التي يتخذ خلالها مجرمو الإنترنت إجراءاتهم لتحصين عمليات التشفير.

هل تعرّض أحد لأذى؟

ما من معلومات متوافرة حول تعرّض أي شخص لإصابات أو وقوع وفيات جراء الهجمات، بخلاف ما ورد عن تعطّل غرف الطوارئ ومكاتب الأطباء وسيارات الإسعاف في بريطانيا، وتأثر الاتصالات في بلدان أخرى.

الهجمات الإلكترونية وأكثر دول العالم تعرضاً لها

لم تعد الحروب بين الدول مقتصرة على استخدام القوة العسكرية في الهجوم المباشر على المواقع المادية لتدمير الحصون و الجيوش المعادية، فمثلما تطورت الوسائل العسكرية من السيوف و الدروع إلى الطائرات و الصواريخ نتيجة لتغير الزمن و التقدم التكنولوجي، حدث نفس التطور مؤخراً و لكن على

مستوى آخر؛ نتيجة لظهور شبكة الإنترنت، و تحول نظم الإدارة و الصناعة و المعلومات في معظم دول العالم من النظام الورقي المكتبي الأرشيفي إلى الأنظمة المعلوماتية على شبكات الكمبيوتر، فظهر مفهوم الهجمات الإلكترونية .. ثم الحروب الإلكترونية إلى الوجود.

ما هي الحرب الإلكترونية ؟

إن الحرب الإلكترونية هى انعكاس للصراع بين الدول المختلفة على كافة مستويات الصراع؛ من صراع سياسى إلى صراع استخباراتى إلى صراع إقتصادى...

حيث يتم التعبير بالحرب الإلكترونية عن قيام دولة ما بشن هجمات إلكترونية على بيانات و برمجيات دولة أخرى عن طريق مجموعة من المتخصصين فى هذا المجال، و ذلك لعدة أهداف و هى:

- الاستغلال
- الخداع
- إحداث الفوضى
- تدمير المعلومات و نظمها
- تعطيل البنية التحتية و شلّها مثل: البنوك و شبكات الكهرباء و المرور و المياه و الأنظمة المالية و إيقاف الإنترنت و غيرها.

معلومات لتقدير مدى خطورة الهجمات الإلكترونية

- قامت وزارة الدفاع الأمريكية (البنتاجون) بتصنيف الإنترنت على أنه الميدان الرابع من ميادين الحروب بعد الجو والبحر والبر.
- اعتبرت استراتيجية رئيس وزراء بريطانيا (ديفيد كاميرون) الهجمات الإلكترونية واحدة من أكبر أربعة تهديدات لبريطانيا.
- قامت الصين بتخصيص قسماً عسكرياً كاملاً لعمليات التجسس الإلكتروني.
- لدى إسرائيل برنامج عسكري يسمى (تلبيوت)، يتم تجنيد نخبة من أذكى الخريجين به لإتقان أساليب الدفاع والهجوم الإلكترونية.
- طبقا لتقرير شركة (مكافي) المتخصصة فى الأمن المعلوماتى الصادر فى بداية يناير ٢٠١٥ فإن عدد الهجمات الإلكترونية وصل فى أواخر عام ٢٠١٤ إلى ٣١٧ تهديداً فى الدقيقة الواحدة !! .. هذا بعد أن كانت الهجمات الإلكترونية قد ارتفعت فى عام ٢٠١٣ عن عام ٢٠١٢ بنسبة ١٤%
- فى الولايات المتحدة الأمريكية تتم إجراء مناورة سنوية تحت اسم سيبر ستورم لاختبار جاهزيتها لمواجهة أى هجمات إلكترونية معادية و يشارك بها ١١٢ جهاز أمنى أمريكى.

أكثر دول العالم تعرضاً للهجمات الإلكترونية

إن الهجمات الإلكترونية ربما يقوم بها أفراد كمجموعات الهاكرز و ربما تقوم بها دول حيث تسمى بالحرب الإلكترونية. و بالنسبة لهجمات الهاكرز الفردية فإنها عادةً –و ليس دائماً- تستهدف الدول

الصغيرة و الفقيرة في أساليب الحماية المعلوماتية، كما أن المعلومات المتوفرة عن هذه الهجمات عادة ما تكون ضئيلة و غير واضحة، و تعتبر الهند و الصين من أكثر مصادر الهجمات الإلكترونية للأفراد.
أما بالنسبة للهجمات التي تقوم بها الدول و المعبر عنها بالحرب الإلكترونية فإنها تكون بين دولتين، أحدهما معتدية على الأخرى، أو أنهما يتبادلان الاعتداء

روسيا / أستونيا عام(2007)

تعتبر هذه الحرب الإلكترونية من أولى الحروب الإلكترونية في العالم، حيث تم استخدام الهجمات الإلكترونية من قبل روسيا ضد أستونيا .. ووقف القانون الدولي حائراً .. هل يعتبر هذه الهجمات من ضمن الهجمات المسلحة فيوقع عقوبات على روسيا أم لا ؟ و في النهاية لم يعترف بها لصعوبة تحديد المصدر القائم بشن الهجمات، وما إن كان حكومي أو شخصي و ذلك إلى الآن.

روسيا / جورجيا(2008)

شكلت الهجمات الإلكترونية بين روسيا و جورجيا حرباً إلكترونية موازية للحرب التقليدية التي كانت قائمة بين البلدين.

الصين / الولايات المتحدة الامريكية

تعد الحرب الإلكترونية الدائرة بين الصين و أمريكا واحدة من أكبر و أطول الحروب الإلكترونية القائمة بالعالم.
و لكن أهداف كلا من البلدين متباينة تمام التباين، فأهداف الولايات المتحدة هي أهداف سياسية تجسسية بحته، أما أهداف الصين فهي أهداف صناعية في المقام الأول، فهجمات الصين الإلكترونية تتعلق بالأسرار الصناعية و التجارية و حقوق الملكية الفكرية .. و الدولة الصينية تعتبر ذلك نوع من أنواع الأنشطة المشروعة لبناء البلاد.
و لعل من أوضح الأمثلة على ذلك ما قامت به مجموعةapt1 ، و هي مجموعة حكومية صينية تعمل من شنغهاى، هاجمت ١٤١ شركة أمريكية في مختلف المجالات الصناعية، و حصلت على خرائط تقنية و حقوق ملكية فكرية و خطط أعمال مشاريع كاملة في حجم كمية مسروقة تساوى ٥٠ ضعف للمعلومات الموجودة في مكتبة الكونجرس مما كلف أمريكا ملايين الدولارات.

إيران / الولايات المتحدة و إسرائيل

حيث قام إيران بهجمات إلكترونية قاسية على عدد من المؤسسات المالية الامريكية رداً على ما تم فرضه عليها من عقوبات دولية .. حيث تعرضت مجموعة من البنوك الأمريكية الكبرى لعدة موجات من الهجمات، وبلغ عدد البنوك المستهدفة في الموجة الثالثة ٢٠ بنكاً.
أما من الجانب الأمريكي الإسرائيلي فلقد تم استهداف المنشئات النووية الإيرانية، ولقد كانت إحدى هذه الهجمات عن طريق نشر برمجيات خبيثة وكان من أبرز المتضررين منشأة نطانز النووية الإيرانية الشهيرة، حيث تم تعطيل ألف جهاز طرد مركزي.

إيران / العالم العربي

مؤخرا تم الهجوم إلكترونياً على بعض المنشئات النفطية العربية، مثل شركة (راس غاز) في قطر عن طريق فيروس شيمون، وتوجهه أصابع الاتهام نحو إيران.
يتبين إلينا أن هناك بعض الدول التي تُهاجم أكثر من غيرها مثل أمريكا والصين وبعض دول الخليج وإيران.
و هكذا نرى أن هناك حروباً إلكترونية في غاية القوة قائمة بالفعل في عالمنا الحالي، و لكننا كعالم عربي نعتبر الجانب الأضعف في أي من تلك الصراعات، إن مهمة تأمين نظمنا المعلوماتية لا بد أن تتم من داخلنا بدون الاستعانة بأي جهة خارجية، لأننا بذلك سنسلمها كل مفاتيحنا بأنفسنا.

اليوروبول (Europol) يدعو إلى تحقيق دولي في الهجمات الالكترونية الأخيرة

دعت وكالة الشرطة الأوربية، المعروفة باسم اليوروبول، إلى إجراء تحقيق دولي واسع النطاق للوصول إلى المسؤولين عن موجة الهجمات الإلكترونية التي طالت بلدان عديدة في العالم.
وقالت اليوروبول إن هذه الهجمات الإلكترونية الضخمة التي جرت "لم يسبق لها مثيل، وتستدعي تحقيقا دوليا معقدا لتحديد الجناة".
وقد تأثر نحو ١٣٠ ألف نظام إلكتروني في أكثر من ١٠٠ بلد بتلك الهجمات ببرمجيات ضارة، بحسب أحدى شركات الأمن الإلكتروني.
ونقلت وكالة فرانس برس (AFP) عن ميكو هايوبنين، رئيس الباحثين في شركة أف سيكيور (F-Secure) للأمن الالكتروني، ومقرها هلسنكي، قوله إنه "أكبر تفشٍ لبرمجيات خبيثة للمطالبة بفدية في التاريخ".
واضاف أن روسيا والهند كانتا الأكثر تضررا بهذه الهجمات لأن نظام تشغيل مايكروسوفت ويندوز أكس بي ما زال يستخدم على نطاق واسع في البلدين.
وقالت شركة مايكروسوفت إن الوضع "مؤلم" وإنها ستتخذ كل الاجراءات الممكنة لحماية زبائنها".
وأصدرت إرشادات لمستخدميها لحماية أنظمتهم الالكترونية.
وكانت تلك الهجمات قد استهدفت أجهزة كمبيوتر في مختلف أنحاء العالم باستخدام خلل برمجي يُعتقد أنه كان جزءا من أدوات مراقبة سرقت من وكالة الأمن القومي الأمريكية.
وقالت وكالة أفاست (Avast Agency) المتخصصة في أمن الإنترنت إنها اطلعت على ٧٥٠٠٠ حالة من حالات استخدام برنامج "رانسوم وير" (Ransom Ware) وهو برنامج كمبيوتر يمنع الأجهزة من العمل أو يمنعها من استرجاع معلومات حتى تدفع فدية معينة.
وتظهر صور على شاشة كومبيوتر الضحية تطالب بدفع فدية (مبلغ ٣٠٠ دولار) عبر العملة الافتراضية المعروفة باسم بيتكوين، مع عبارة أن "ملفاتك قد شُفرت"، ثم رسالة تطالب بتسديد الفدية خلال ثلاثة أيام وإلا فإنها ستتضاعف، وتهدد بحذف الملفات كليا إذا لم تدفع الفدية خلال سبعة أيام.

وضربت الهجمات نحو ١٠٠ بلد ومن ضمنها روسيا والهند والصين وبريطانيا وفرنسا، إذ تعطلت أنشطة وزارة الداخلية الروسية والاتصالات الإسبانية وهيئة الرعاية الصحية العامة في إنجلترا واسكتلندا.
وذكرت تقارير أن روسيا كانت الأكثر عرضة لهذه الهجمات الإلكترونية، إذ تضررت وزارتا الداخلية والصحة، وشركة القطارات الروسية الحكومية، وثاني أكبر شركة للهواتف المحمولة بالإضافة لبنوك محلية روسية.
وقالت وزارة الداخلية الروسية إن ١٠٠٠ كمبيوتر تعطل، لكنها أضافت أن مسؤولي تكنولوجيا المعلومات تعاملوا مع الوضع بسرعة، كما أن المعلومات الحساسة التي تخزنها الوزارة لم تتضرر.
الأطباء في مراكز الرعاية الصحية البريطانية استخدموا الورق والأقلام في عملهم بعد تعطل جميع نظم الكمبيوتر والهواتف
كما أن نحو ٤٠ منظمة محلية تابعة لنظام هيئة الرعاية الصحية البريطانية وبعض العيادات تعرضت لهجمات بحيث اضطرت هذه المؤسسات الطبية إلى إلغاء عمليات جراحية .
وقال عاملون في هذه المرافق الطبية إنهم شاهدوا برمجيات خبيثة "تنتشر مثل النار في الهشيم"، وأغلقت أجهزة الكمبيوتر "واحدا تلو الآخر".
كما تعرض عدد من الشركات الإسبانية الضخمة من قبيل تيليفونيكا (Telefonica) وشركة الطاقة إيبيردرولا (Iberdrola) وشركة غاز ناتورال (NATURAL) لهجمات إلكترونية، وقيل للعاملين فيها أن يغلقوا أجهزتهم التي يعملون عليها.
وقالت شركة صناعة السيارات الفرنسية رينو (Renault)، إنها ضُربت بموجة الهجمات الإلكترونية، الأمر الذي أجبرها على ايقاف عملياتها الانتاجية في عدد من المواقع لمنع انتشار الفيروس في كل اجهزتها الإلكترونية.
وبعث عاملون في مؤسسات أخرى تغريدات أظهرت صورا لآلة التذاكر المحلية المعطلة في ألمانيا ومختبر جامعي للكمبيوترات في إيطاليا.
كما تضررت بسبب هذه الهجمات الإلكترونية شركة تيليكوم البرتغالية، وشركة فيديكس لنقل الرسائل.
ولم تعلق الصين رسميا بشأن تعرضها لأي هجمات إلكترونية محتملة، لكن التعليقات المنشورة على وسائل التواصل الاجتماعي ذهبت إلى أن مختبرا جامعيا للكمبيوترات تضرر

كيف يعمل البرنامج الخبيث ومن يقف خلفه؟

يبدو أن البرنامج الخبيث يعتمد على فيروس ينتشر من تلقاء نفسه في أجهزة الكمبيوتر الموجودة في المكان.
وتعتمد معظم البرامج الخبيثة على الإنسان بغية الانتشار من خلال الضغط على ملفات مرفقة تحتوي على كلمة السر لبدء الهجوم الإلكتروني.
لكن في المقابل عندما يتمكن البرنامج من التسلل إلى منظمة ما، فإنه يستهدف الكمبيوترات القابلة للاختراق والهشة ويعطلها.

ويرى خبراء أن الهجوم الحالي يستهدف تحديد نقطة ضعف في أنظمة مايكروسوفت سبق أن حددتها وكالة الأمن القومي الأمريكية

وسرق جماعة قراصنة يطلقون على أنفسهم اسم "ذي شادو بروكورز" (The Shadow Brokers) برنامجا خبيثا، وجعلوه متاحا بشكل مجاني في أبريل ٢٠١٧، مضيفين أنه يستهدف الاحتجاج على الرئيس الأمريكي ، دونالد ترامب .

وقالت مايكروسوفت إنها ستجِّدث النسخ القديمة من برامجها والتي "لم تعد تستقبل الدعم العام" الذي تقدمه مثل وندووز إكس بي والتي تستخدمها هيئة الصحة البريطانية على نطاق واسع ووندووز ٨ ووندووز سيرفر ٢٠٠٣.

ويبدو أن عدد الهجمات الإلكترونية أخذ في التباطؤ في أعقاب تفعيل زر إيقاف للطوارئ .

حقائق ومعلومات حول الهجمات السيبرانية العالمية الأخيرة

ماذا تفعل البرمجية المستخدمة؟

– تعمل البرمجية المستخدمة في الهجمات الأخيرة على إغلاق الأقراص الصلبة بحيث لا يتمكن المستخدم من الوصول لبياناته، ومن ثم يطلب منه دفع فدية قدرها ٣٠٠ دولار في صورة عملات رقمية مثل "بتكوين".

– تم حظر البريد الإلكتروني المرتبط بهذه البرمجية، لذلك حتى لو دفع الضحايا الفدية فإنهم لن يحصلوا على ملفاتهم مرة أخرى.

كيف تنتشر؟

– يقول الباحثون إن الفيروس المستخدم، يصيب الشبكات بطريقة العدوى حيث ينتقل من حاسوب إلى آخر.

– يستخدم المهاجمون أداة قرصنة تدعى "EternalBlue" والتي تستغل نقطة ضعف في نظام التشغيل "ويندوز".

– رغم أن شركة "مايكروسوفت" أصدرت تحديثًا لنظام التشغيل في مارس الماضي، إلا أن أغلب الشركات لم تفعله حتى الآن.

– تعد "إترنال بلو" مجموعة من أدوات القرصنة التي تم تسريبها في وقت سابق هذا العام، ويعتقد أنها من تطوير وكالة الأمن القومي الأمريكية.

من المتضرر؟

– تضررت شركات كبرى في أوروبا والولايات المتحدة وآسيا، جراء الهجمات الأخيرة، ومن بينها، شركة النفط والغاز الروسية "روسنفيت" (Rosneft) وشركة الشحن الدنماركية "مولر ميرسك" (Mueller Maersk) وشركة المواد الدوائية الأمريكية "ميرك" (Merck) وغيرها.

– كما تضررت شركة التجزئة الفرنسية "أوشان" (Auchan) ووحدة الأعمال العقارية التابعة لبنك "بي إن بي باريبا"، بالإضافة إلى عدد من المنشآت الحيوية الأوكرانية.
– من جانبها قالت شركة "موندليز" (Mundles) إن منشأتها التصنيعية في أستراليا ونيوزيلندا أصيبت جميعًا لكن بعضها ما زال قادرًا على تنفيذ عمليات محدودة.
– تم إغلاق منشأة "مولر ميرسك" لشحن الحاويات في مدينة مومباي الهندية.

هل مستخدمي الإنترنت الأفراد عرضة لهذه الهجمات؟

– يقول الخبراء إن المستخدمين المنتظمين الذي فعلوا التحديثات الجديدة لنظام التشغيل "ويندوز" في مأمن من هذه الهجمات.
– مع ذلك فإن أي حاسوب لم يتم تحديث نظام تشغيله، فمن الممكن أن يصيب الأجهزة الأخرى المتصلة به.

من يقف وراء هذه الأفعال؟

– من السابق لأوانه الجزم بوقوف جهة بعينها وراء هذه الهجمات.
– لكن وكالات استخبارات وباحثين ربطوا هجمات "وانا كراي" الشهر الماضي بمجموعة ذات صلة بكوريا الشمالية، لكن إلى الآن لم يتم الإشارة لوقوف أي طرف وراء الهجمات الأخيرة.

الهجمات الالكترونية على أجهزة الحاسب الآلى الشخصية تعدت مرحلة كونها مجرد اختراق لبعض الاجهزة الالكترونية لبعض الاشخاص او الجهات ووصلت إلى أنها أصبحت تمثل اختراقا للحياة على سطح الكرة الارضية وذلك بعد تعرض أكثر ٤٥ الف جهاز كمبيوتر في أكثر من ٩٠ دولة لهجوم الكتروني خبيث أدى إلى توقف العمل فيها ، مما أدى إلى تعطيل بعض مظاهر الحياة العامة بها وتأثرت مجالات المال والأعمال فيها بشكل كبير.
ويقوم الفيروس الجديد من خلال برنامج خاص بتشفير جميع الملفات المحملة على الأجهزة الالكترونية والحواسب الآلية برقم سري ، ويشترط البرنامج دفع الأموال (فدية) لفك هذا التشفير عن طريق حساب "البيتكوين".
ويرى نائب الرئيس التنفيذي للجهاز القومي لتنظيم الاتصالات لشئون الأمن السيبراني المصري أنه من المبكر في الوقت الحالي تقدير حجم تأثر مصر بالهجمات الإلكترونية. ولكن تم اتخاذ اجراءات الأمان والتحصين
وبحسب ما أعلنت عنه إحدى الشركات الأمنية السيبيرية الفرنسية، فإن هذا الهجوم يشل عمل الأجهزة الالكترونية ويستغل ثغرة موجودة في نظام تشغيل "ويندوز" ، وتبقى النصيحة الذهبية لتجنب مثل هذا الهجوم على الأجهزة التي تعمل بنظام ويندوز هو تحميل جميع التحديثات على ملفات جديدة منفصلة.
كما حذّر مركز الأمن الإلكتروني السعودي من الفيروس الذى اجتاح العالم ويسمى (الفدية).
وقال مركز الأمن الإلكتروني عبر حسابه الرسمي في "تويتر"، إنه لاحظ انتشار فيروس "فدية" للأجهزة العاملة بنظام "ويندوز"، ونصح بعمل بعض الخطوات بشكل عاجل جدًا.

ومن أبرز الخطوات التي نصح بها إغلاق المنافذ المتصلة بالإنترنت "١٣٥، ١٣٩، ٤٤٥" وتثبيت التحديث "MS17-010" من أجل إغلاق الثغرة المستغلّة في هذا الهجوم.

حقائق هامة حول الهجمات الإلكترونية

- تشير التقديرات إلى أن القطاعات التجارية تتكبد ما يزيد عن ٤٠٠ مليار دولار أمريكي سنوياً كخسائر مادية نتيجة الهجمات الإلكترونية.
- يتراوح عدد الحوادث المتعلقة بالأمن الإلكتروني ما بين ٨٠ – ٩٠ مليون حادثة سنوياً.
- 20 % من الشركات الصغيرة والمتوسطة تعرضت لجرائم إلكترونية مختلفة
- ترصد شركة مايكروسوفت يومياً أكثر من ١٠ مليون محاولة لمهاجمة خدماتها المختلفة. (تُعد كحادثة واحدة)
- العام الماضي، كان قطاع الرعاية الصحية هو الأكثر تعرضاً لهجمات القراصنة
- 40 % من ضحايا الجرائم الإلكترونية تعرضوا لعمليات احتيال مرتبطة ببطاقات الائتمان بأنواعها المختلفة .
- كمعدل، فإن مجرمي الإنترنت لديهم حوالي ٢٠٠ يوم قبل أن يتم اكتشاف هجماتهم
- 70% من الهجمات الإلكترونية لا يتم اكتشافها ويبقى فاعلوها مجهولين
- الشبكات الاجتماعية المختلفة تعتبر الهدف المفضل بالنسبة للقراصنة لمهاجمة الضحايا

وتعتمد بعض محاولات التصيّد الإلكتروني الموجّهة على إنشاء عنوان بريد إلكتروني لموظف وهمي في المؤسسة واستخدامه لطلب معلومات عن الشركة من موظفين آخرين في المؤسسة، وعندها لن يتردد الموظفون في إرسال هذه المعلومات ظنًا منهم بأن مصدر الرسالة هو زميل لهم في المؤسسة.

وهناك نوع سائد من الهجمات الإلكترونية تعرف بـ (watering hole)، ويقوم المخترقون في هذه الحالة بوضع برمجية خبيثة ضمن الكود البرمجي المستخدم في أحد مواقع الإنترنت المنتشرة على نطاق واسع، وفي حال قام أحد الموظفين بفتح هذا الموقع من كمبيوتر الشركة فستكون شبكة الشركة بأكملها عرضة للخطر الذي تحمله البرمجية الخبيثة.

والهجمات الإلكترونية على الشركات الصغيرة والمتوسطة تعود إلى ٣ عوامل رئيسية، أولها افتقار الشركات الصغيرة والمتوسطة إلى الحماية، إذ لا تطبق معظم هذه الشركات معايير مناسبة للحماية من الهجمات الإلكترونية، ثم إن غالبية هذه الشركات لا تنوي زيادة استثماراتها في حلول الحماية الأمنية رغم ازدياد الهجمات الإلكترونية التي تستهدفها.

ولقد رصدت شركة ديل خلال عام ٢٠١٤ حوالي ٣٧ مليون برمجية خبيثة، وهي تقريبًا ضعف كمية البرمجيات الخبيثة التي تم الكشف عنها في العام ٢٠١٣، وإذا ما وصلت هذه البرمجيات إلى أحد مواقع الإنترنت فبإمكانها إلحاق الأذى بكافة الشركات، سواء كانت كبيرة أو متوسطة أو صغيرة، وإذا أخذ

بعين الاعتبار ضعف مستويات الحماية المتوفرة في الشركات الصغيرة والمتوسطة فإنها ستكون بالتأكيد الأكثر تأثرا بتلك الهجمات.

ومن العوامل الرئيسية للهجمات الإلكترونية هو أن الشركات الصغيرة والمتوسطة هي بوابة عبور لشركات أكبر، وقد حصلت في السابق هجمات كبيرة على مؤسسات كبيرة انطلاقًا من الشركات الصغيرة والمتوسطة التي تم اختراقها، ومن أبرزها الهجمة الشهيرة التي حصلت في الولايات المتحدة على منافذ بيع شركة Target والتي تم من خلالها شن هجوم أوسع على مزوّد الخدمة لهذه الشركة وتسريب بيانات بطاقات الاعتماد لأكثر من ٤٠ مليون عميل.

وبهذه المناسبة، قال مارك مورلاند، المدير الإقليمي لشركة SecureWorks (التابعة لشركة ديل) لمنطقة الشرق الأوسط: "تسبب الاختراقات الأمنية للمؤسسات الصغيرة والمتوسطة خسائر بالغة، وفي ظل عدم وجود نسخة احتياطية عن البيانات فستكون لهذه الهجمات عواقب وخيمة على سمعة الشركة وسير العمليات فيها، أضف إلى ذلك الأضرار المرتبطة بإمكانية ضياع أو فقدان أحد الأجهزة التي يستخدمها موظفو هذه الشركات".

ويوجد بعض الإجراءات التي يمكن اتباعها لتعزيز حماية الشركات الصغيرة والمتوسطة من محاولات الاختراق ومن الأضرار الناجمة عن ضياع أو فقدان أحد الأجهزة التي يستخدمها موظفو هذه الشركات.

ومن أبرز هذه الإجراءات تشفير البيانات، فقد بات من الممكن اليوم استخدام هذه الطريقة لحماية البيانات بغض النظر عن مكان وجودها، سواء كانت على الكمبيوتر المكتبي أو الجوال أو وسائط التخزين المحمولة أو في السحاب، ودون أن يشعر المستخدم بوجود إجراءات أمنية مزعجة تعرقل سير العمل.

ومن الإجراءات أيضًا تقنيات المصادقة أو التعرّف المتقدمة والتي تجمع عدّة نماذج للتعرّف على المستخدمين والمصادقة على صلاحياتهم معًا، وذلك للتأكد من هوية المستخدمين الذين يحاولون الوصول إلى بيانات الشركة.

كما ينبغي احتواء الهجمات، ووقف البرمجيات الخبيثة التي تصيب أنظمة الشركات وشبكاتها ومنعها من الانتشار. وتقوم برامج الاحتواء بتوجيه المستخدمين لتشغيل التطبيقات المستهدفة في بيئات افتراضية لضمان حمايتها، ففي هذه الحالة إذا زار المستخدم إحدى الصفحات التي تحتوي على برمجية خبيثة فإن هذه البرمجية لن تتمكن من العمل وإلحاق الأذى بجهاز المستخدم.

نصائح لتبقى بعيداً عن الفيروسات والبرمجيات الخبيثة

اعتمادك على برنامج قوي لمكافحة الفيروسات والبرمجيات الخبيثة يُعد من الوسائل المفيدة للحماية وتجنب المشاكل الأمنية على جهازك.

لكن للأسف فإن هذه الوسيلة لن تضمن لك حماية أمنية كاملة، فهناك بعض البرمجيات الخبيثة التي يُمكنها تجاوز برامج الحماية دون الكشف عنها.

لذلك فإن الوقاية دائماً أفضل من العلاج، والوقاية في هذه الحالة تكمن في الحذر الدائم أثناء استخدام الهاتف الذكي أو الحاسب الشخصي حتى في حال تثبيت برنامج لمكافحة الفيروسات.
فيما يلي بعض النصائح لتُساعدك على تجنب الفيروسات والبرمجيات الخبيثة:

تحديث نظام التشغيل والمتصفح (Operating system and browser)

لأن الكثير من الفيروسات تأتي هذه الأيام من خلال تصفحك لبعض المواقع، فإن اعتمادك على متصفح قوي ومحدث لآخر إصدار سيساعدك في تجنب الكثير من المشاكل الأمنية، أبرزها عدم منح المخترقين إمكانية الوصول إلى تسجيلات الدخول التي قمت بها على المتصفح.
نفس الأمر ينطبق على نظام التشغيل، سواءً للهاتف الذكي كأندرويد (Android) و آي أو إس (IOS)، أو للحواسيب الشخصية كويندوز وماك فاعتمادك على متصفح محدث لآخر إصدار في نظام تشغيل قديم يعتبر مجازفة أمنية كبيرة.
لذلك احرص دائماً على تحديث المتصفح أولاً بأول ولا تهمل هذه النقطة، فالتحديثات الجديدة للمتصفح تشمل دائماً بعض الإصلاحات والتحسينات الأمنية، وذلك إلى جانب تحديث نظام التشغيل إلى آخر إصدار.

فحص الملفات الجديدة

إن كنت تعتقد أن الخطورة كامنة في الملفات المخزنة على فلاشات USB فقط، فيجب أن تعيد النظر في ذلك.
أي ملف جديد من جهة خارجية ترغب بتخزينه على جهازك يجب أن تقوم بفحصه عبر برنامج لمكافحة الفيروسات، سواء الملفات الجديدة التي ترغب بنقلها من الفلاش وأقراص التخزين الخارجية أو تلك التي تقوم بتلقيها عبر الإنترنت مثل المرفقات في رسائل البريد الإلكتروني أو من خلال تطبيقات التواصل الفوري.
فمثلاً إن كنت ترغب بإضافة بطاقة تخزين مايكرو إس دي إلى هاتفك الذكي فاحرص على فحصها ببرنامج لمكافحة الفيروسات قبل استخدامها، وكذلك الحال بالنسبة للأقراص المستخدمة على الحاسب الشخصي.
نفس الأمر ينطبق على الملفات التي تقوم بتنزيلها من الإنترنت، فهي أيضاً يجب أن تخضع للفحص قبل أن تقوم بتشغيلها.

تجنب أزرار التنزيل الوهمية والنوافذ المنبثقة

قد تزور موقع معين، لتفاجئ بنوافذ لإعلانات منبثقة مثل تلك التي تخبرك بأنك الزائر رقم مليون وأنك سعيد الحظ للفوز بالجائزة الكبرى، طبعاً إن انخدعت بمثل هذه الأساليب فستصبح تعيس الحظ الأكبر في العالم بعد أن يتم حقن جهازك بالبرمجيات الخبيثة.
هذا الأمر يتكرر أيضاً مع أزار التنزيل الوهمية، فمثلاً إن كنت تزور المواقع المتخصصة بتنزيل البرامج أو الكتب أو الألعاب ستلاحظ وجود أزار التنزيل في كل مكان وهي للأسف أزار وهمية يُمكن أن تؤدي

إلى تنزيل برمجيات ضارة على جهازك، لذا كن حذراً من هذه الممارسات ولا تعاود زيارة المواقع التي تتبع هذه الأساليب.

يُمكنك أن تفحص موثوقية المواقع من خلال أداة جوجل التي تعمل على اكتشاف المواقع غير الآمنة، فكل ما عليك فعله هو نسخ رابط الموقع ولصقه في الخانة المخصصة وستخبرك الأداة إن كان الموقع يتضمن محتويات غير آمنة.

أيضاً تتوفر خدمة مشابهة من نورتن لفحص سلامة المواقع من الناحية الأمنية

اعتمد على المصادر الموثوقة

كلنا يحتاج إلى تنزيل البرمجيات على حسابه الشخصي أو هاتفه الذكي، فهي مسألة لا يُمكن المفر منها. ولكي تضمن تجربة تنزيل آمنة لهذه البرامج، فيجب عليك أن تعتمد على المصادر الرسمية فقط مثل الموقع الرسمي لمطور التطبيق أو من خلال متاجر التطبيقات الآمنة والموثوقة فقط، وتجنب التنزيل من المصادر المجهولة أو غير الآمنة مهما كانت الأسباب.

وأيضاً يجب مراعاة التالي:

- لابد من موجود برنامج حماية من الفيروسات في جهازك
- لابد أن تقوم بتحديثه بشكل دوري، وإلا فلا فائدة من وجوده
- لا تقم بفتح المرفقات في أي أيميل لا تعرف مرسله
- لا تقم بفتح المرفقات في إيميلات أصدقائك إذا وجدتها تنتهي بـ exe أو bat أو أي امتداد لا تعرفه
- لا تقبل ملف من شخص لا تعرفه أبداً
- إذا قبلت ملفاً من شخص تعرفه، افحصه أيضاً ببرنامج الحماية، فقد يكون صديقك نفسه ضحية
- احرص على فحص جميع البرامج التي تقوم بتنزيلها من الإنترنت، أو تشغيلها من الأقراص المدمجة (CD's) قبل أن تشغّلها
- داوم على زيارة المواقع التي تهتم بالحماية من الفيروسات، للاطلاع على كل ما هو جديد في هذا المجال

البرامج المضادة للفيروسات

هي البرامج التي تقوم بحمايتك من هجمات الفيروسات وبقية البرامج التي تشكل تهديدا امنيا على معلوماتك وتستطيع أن تحدد هذه الملفات الضارة القادمة من أي مصدر مثل الأقراص المدمجة و الرسائل الإلكترونية و كذلك يمكنها رصد هذه البرامج في القرص الصلب وتتمكن هذه البرامج من مسح أو تعطيل عمل البرامج المهددة لسلامة الجهاز و ملفات البرامج الموجودة على جهازك و يتكون برنامج مضاد الفيروسات من جزئين مختلفين

التشغيل المباشر عند الدخول

وهذا الجزء يعمل تلقائيا عند تشغيل(الدخول) البرامج أو تنزيل الملفات من الإنترنت وهو ما يعرف ب On Access element

التشغيل عند الطلب

وهذا الجزء يعمل عندما تطلب أنت منه ذلك وهو متخصص بالكشف عن الفيروسات في القرص الصلب والأقراص المدمجة وهو ما يعرف ب On Demand element

كيفية عملها

ان البرامج المضادة للفيروسات عبارة عن تقنية مسح ورصد للبرامج المشبوهة التي تتميز بخصائص معينة أو تحتوي على صيغة معينة من البرمجة عبارة عن مجموعة من الأرقام الثنائية وهي التي تعرف ب (التوقيع) ويتم ذلك بالطريقة التالية :

يقوم البرنامج المضاد بالنظر الى كل الملفات و البرامج ذات الطبيعة التنفيذية

تتم مقارنة التوقيع الموجود على كل ملف بالتواقيع المخزنة في قاعدة المعلومات الخاصة بالبرنامج المضاد للفيروسات

و الجدير بالذكر أن كل برنامج مضاد للفيروسات يحتوي على توقيع أكثر من ٤٠٠٠٠ نوع من الفيروسات و أكثر من عشرة الاف من تواقيع التروجان و الديدان كما أن كل شركة منتجة للبرامج المضادة للفيروسات تقوم بتحديث و اضافة المزيد من هذه التواقيع كل يوم

بعد عملية المقارنة يقوم البرنامج المضاد باكتشاف الفيروس أو حصان طروادة (التروجان) و يقوم بإعلام المستخدم عنه

يقوم البرنامج المضاد بتخيير المستخدم بين مسح أو تعطيل الفيروس أو بإصلاح الخلل بطريقة آلية

تكنولوجيا الكشف

يقوم مصنعي و مبرمجي الفيروسات عادة بتعديل أو تحريف التوقيع الأصلي لبعض البرامج الشهيرة و ذلك لتضليل المستخدم و البرنامج الأصلي و تقوم تكنولوجيا الكشف عن هذا التزوير و التعديل بواسطة المقارنة السريعة بين التواقيع الأصلية و المزيفة

مدى الاعتمادية على هذه البرامج

ليس هنالك برنامج مضاد للفيروسات قادر على حمايتك مائة في المائة و لكن اذا قمت بالتحديث المستمر لبرنامجك كل اسبوع فإنك سوف تحصل على حماية تصل الى ٩٥% و ذلك لأن هنالك أكثر من ستمائة من الفيروسات الجديدة و أحصنه طروادة تظهر كل شهر

مفاهيم خاطئة عن برامج الحماية من الفيروسات

لعل من أكثر المفاهيم الخاطئة بين المستخدمين على مستوى العالم هي الاعتقاد بأن اقتناء برنامج مضاد للفيروسات يمنع و يحمي من هجوم الهاكرز و المخترقين وهذا طبعا ليس صحيح حيث أن هذه البرامج تحميك فقط من الفيروسات و الديدان و تستطيع التعرف على معظم أحصنه طروادة (التروجان) و لكن لا تقوم بغلق المنافذ و المعابر الموجودة في جهازك و التي تمكن المخترقين من الوصول الى جهازك ومعلوماتك و لذلك فإنه من الضروري أن تقوم بالحصول على برنامج متخصص يعرف بجدران اللهب (Fire Wall)

المصادر

http://kenanaonline.com/users/tamer2011-com

/https://alqabas.com/160012

http://www.dotmsr.com/details/158509/

http://www.bitcoinbuz.com/2017/03/bitcoin.html

https://al-ain.com/article/nhs-ransomware-cyber-attack

http://www.masrawy.com/News/News_PublicAffairs/details/2017/5/13

https://www.tasawk.com.sa

http://www.bbc.com/arabic/science-and-tech-39907190

https://www.an7a.com/304257

http://www.elbalad.news/2760492

https://aitnews.com/2016/05/14