

خبراء الأمن يقرعون ناقوس الخطر العالمي! ويكشفون تفاصيل الهجمات التي أطاحت بنصف الإنترنت!



الأحد 23 أكتوبر 2016 06:10 م

حملت الهجمات الإلكترونية - التي أطاحت يوم أمس الجمعة بما يعتقد أنه نصف شبكة الإنترنت العالمية - تهديدًا واضحًا وصريحًا لحياة الإنسان ع: كوكب الأرض، وجاءت لتندثر البشرية بالمستقبل القريب الذي ينتظرنا في حال لم تتحرك الأجهزة العالمية وع: كافة المستويات لاتخاذ الإجراءات والخطوات الحتمية اللازمة لمواجهة مثل هذه التهديدات بالغة الخطورة

هذا ما أكدته الخطة الأمنية محمد أم حاسبيني من "كاس؟س؟ لاب" في حوار خاص مع البوابة العربية للأخبار التقنية قدم فيه تفصيلًا دقيقًا حول الحادثة وتأثيراتها، ومعلومات مهمة حول التهديدات الجديدة التي حملتها، مشددًا ع: ضرورة التحرك الفوري من قبل الأجهزة المعنية العالمية للتصدي لسيناريوهات أخرى من شأنها الإطاحة ليس بشبكة الإنترنت فحسب، بل بتهديد حياة مئات الآلاف من البشر

ماذا حصل؟!

في صباح يوم الجمعة ٢١ أكتوبر ٢٠١٦ - وبالتحديد في حوال الساعة ١١ صباحًا بتوقيت غرينيتش- بدأ هجوم شرس من نوع "دي دوس" والمعروف اصطلاحًا بـ "الهجمات الموزعة للحرمان من الخدمة" - ع: نظام أسماء الإنترنت DNS التابع لشركة Dyn العالمية، مما أدى إلى توقف عدد كبير جدًا من المواقع والخدمات العالمية الشبكية ع: الإنترنت وخروجها عن الخدمة بشكل كامل وتدرجي وفقًا لمواقعها الجغرافية

كيف حصل ذلك تقنيًا؟

نعلم جميعًا ما حصل في الفلة الأخيرة، وبالتحديد إتاحة الشيفرة المصدرية لشبكة البوت نت botnet المعروفة باسم "ميراي" Mirai، وهي عبارة عن شبكة مؤلفة من حوال ١٤٥ ألف من أجهزة تسجيل الفيديو الرقمية والكاميرات الرقمية المصنعة في الصين، وهي مرتبطة مع بعضها ومتصلة بالإنترنت وقد تم تسخيرها واستغلالها في شن هجمات متتالية من نوع نظام أسماء الإنترنت DNS التابع لشركة Dyn العالمية، والتي تعتمد عليه معظم المواقع والخدمات العالمية الرائدة

نتائج الهجمات

تقنيًا، أدت تلك الهجمات الشرسة والمتوالية إلى توقف عدد كبير جدًا من المواقع والخدمات العالمية الرائدة وتعذر الوصول إليها تدريجيًا من قبل المستخدمين حول العالم وشملت القائمة الطويلة جدًا للشركات المتأثرة بالهجمات كل من تويتر، باي بال، وسبوتيفاي، وساندكلود، وشوبيفاي، وغتهاب، وإير بي إن بي، وريديت، وفيسبوكس، وفوكس ميديا، والقائمة تطول جدًا لتطال واتس اب وبعض خدمات جوجل السحابية وغيرها الكثير من شبكات ومنصات التواصل الاجتماعي، وبوابات الدفع الإلكترونية، والمواقع الخدمية، وغيرها

تشغيليًا: لعل أبرز النتائج المباشرة التي يمكن لمثل هذه الهجمات أن تخلف وراءها تتمثل في إيقاف عمليات الإنتاج في الشركات، ولك أن تتخيل حجم الخسائر والكوارث الناجمة، ناهيك عن إلحاق الأذى بسمعة تلك الشركات وعلاماتها التجارية أما ماديًا، فإنها بكل تأكيد بمثابة صفة قهوة جدًا ع: الصعيد المادي، لا سيما بالنسبة للشركات الكبيرة التي من المتوقع أن تعلن عن خسائر فادحة بسبب توقفها ع: العمل حتى لو كان ذلك لفترات محدودة

حجم المخاطر لما حصل؟

لتحديد حجم الخطر الكامن ومدى خطورة هذه الهجمات، علينا أن ننظر إلى زوايا ألق عققا، فإذا ما أخذنا بع الاعتبار أن الهجمات استهدفت شركات أمريكية عريقة جدًا في هذه المرة، ولك أن تتخيل التقدم التقني والعلمي الذي تتمتع به الولايات المتحدة الأمريكية في هذا المجال مقارنة بغيرها من الدول والشركات الأخرى، فبإمكاننا حينئذ تصور مدى الخطورة البالغة التي يمكن لمثل هذه الهجمات أن تتسبب به في حال استهدافها دول أخرى أقل تقدمًا وذات إمكانات أقل!

وع: سبيل توضيح مدى الخطورة لهذه الهجمات، نذكر أن حجم البيانات المستخدمة في شن أخطر هجمات DDoS (تحدثًا في الإمارات) وصل في حده الأقصى إلى ٩٠٠ جيجابايت في الثانية، بينما نرى أن حجم البيانات المستخدمة في الهجمات الأخيرة: شركة Dyn يصل إلى ١,٥ تيرابايت في الثانية، أي أكبر بحوالي ١٥ مرة.

السيناريوهات الكارثية المحتملة والأخطار خطورة؟!

بناءً على المعطيات الحالية، فإن من أخطر السيناريوهات خطورة لمثل هذه الهجمات تلك التي تبنى في جوهرها على إحداث الضرر على نطاق أوسع وأشمل معتمدة على الإنترنت الأشياء، والتي تحظى بغرض كفة لاسيما مع دخولنا في حقبة المدن الذكية ومن ثم تلك السيناريوهات: إيقاف الإنترنت عن دول بأكملها، واستهداف المنشآت الحيوية التي ترتبط ارتباط وثيق بحياة الإنسان مثل شبكات المواصلات الجوية والبحرية، ومحطات الطاقة، وشبكات الكهرباء والمياه والصرف الصحي، واستهداف المنشآت النووية، وتعطيل الأنظمة المالية العالمية بما فيها المؤسسات المالية وأجهزة الصرف الآلي وغيرها، واستهداف المستشفيات والمنظمات الطبية والإنسانية وغيرها. ناهيك عن استغلال الوضع الراهن من قبل منظمات إرهابية، بالإضافة إلى الكلفة من السيناريوهات الكارثية والأخطار خطورة مما حدث يوم أمس.

قبل أن تخرج الأمور عن السيطرة!

قال حاسبيني إن علينا تحديد من هو المسؤول عن تلك الهجمات الأخيرة، فأنا هنا لا أقصد من هي الجهة المسؤولة عن شن الهجوم، فبالرغم من تبني مجموعة قراصنة تطلق على نفسها اسم "قراصنة عالم جديد" Hackers World New عن الهجوم الإلكتروني الهائل الذي شن يوم أمس الجمعة، إلا أنه لا يمكن تأكيد ذلك حتى الآن، وإنما أقصد من تسبب في شن هذا الهجوم؟!

علينا أن لا ننقل كاهل المستخدم بالعبارة الرنانة والتوجيهات الطنانة، وإلقاء اللوم عليه في كل الحالات لننقل كاهله بما لا يطيق، ولا يخفى عليكم أنه ظهر مؤخرًا مصطلح عالمي يدعى "إرهاق المستخدم" أمليًا بما لا يطيق "Fatigue Security" أخذنا الحادثة الأخيرة بعين الاعتبار، فما حدث هو استغلال أجهزة تسجيل فيديو وكاميرات رقمية صينية الصنع لشن الهجمات مستغلة ثغرات من المفترض أن تكون مسؤولة عنها الشركات المصنعة وليس المستخدم لوحده. وهذا الأمر يتطلب تعاون تقني وأمني أكبر بكثير: على مستوى الدول والشركات المصنعة لشن تشبهات وقواطع لضمان استمرارية الإنترنت وتفادي هجمات أخطار خطورة.

فمن المهم جدًا وبأسرع وقت أن تتوجه الحكومات نحو الحد الأقصى من التعاون مع شركات أمن المعلومات، والتي بإمكانها عندئذ إيقاف شبكات البوت نت، وتحديد مصادر الهجوم، والمساعدة على توفير الحماية اللازمة ومن جهة أخرى، يتوجب على المجتمع الدولي التوجه أيضًا نحو تعاون تقني وقانوني أكبر: لسن وتطبيق تشبهات دولية تفرض عقوبات على ممارسات مماثلة مصدرها دول تسعى لتحقيق مكاسب سياسية أو عسكرية.

سيناريوهات ومخاطر جدية تلوح في الأفق والحروب الإلكترونية باتت حديث الإعلام في الآونة الأخيرة، والتهديدات الناجمة عن المنظمات الإرهابية، وممارسات في قانونية لدول بعينها بدأت تتكشف معالمها يوما بعد يوم، والمدن الذكية وإنترنت الأشياء ترسم ملامح الأيام والحقبة القريبة القادمة، والتحرك الفوري على كافة المستويات بات ضرورة حتمية قبل أن تخرج الأمور عن السيطرة!

فالإنترنت غابة بكل معنى الكلمة! والغابة تتطلب قواطع وتشبهات لئلا يضلّ يوم يسود فيه قانون الغاب وتخرج الأمور عن السيطرة.