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 لتنذر البشرية بالمستقبل القريب الكارثي الذي ينتظرنا ؟ حال لم تتحرك الأجهزة العالمية وع: كافة المستويات لاتخاذ الإجراءات والخطوات الحتمية اللازمة لمواجهة مثل هذه التهديدات بالغة الخطورة.

هذا ما أكده الخبير الأمني محمد أمين حاسبيني من "كاس؟س؟ لاب" ؟ حوار خاص مع البوابة العربية للأخبار التقنية قدم فيه تفصيلًا دقيقًا حول الحادثة وتأثيراتها، ومعلومات مهمة حول التهديدات الجدية التي حملتها، مشددًا ع: ضرورة التحرك الفوري من قبل الأجهزة المعنية العالمية للتصدي لسيناريوهات أخرى من شأنها الإطاحة ليس بشبكة الإنترنت فحسب، بل تهديد حياة مئات الآلاف من البشر.

ماذا حصل؟!

؟ صباح يوم الجمعة ٢١ أكتوبر ٢٠١٦- وبالتحديد ؟ حوالي الساعة ١١ صباحًا بتوقيت غرينتش- 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 إ َ توقف عدد كبير جًدا من المواقع والخدمات العالمية الشهيرة ع: الإنترنت وخروجها عن الخدمة بشكل كامل وتدريجي وفًقا لمواقعها الجغرافية.

كيف حصل ذلك تقنًيا؟

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

نتائج الهجمات؟

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

تشغيلًيا: لعل أبرز النتائج المباشرة التي يمكن لمثل هذه الهجمات أن تخلف وراءها تتمثل ؟ إيقاف عمليات الإنتاج ؟ الشركات، ولك أن تتخيل حجم الخسائر والكوارث الناجمة، ناهيك عن إلحاق الأذى بسمعة تلك الشركات وعلاماتها التجارية. أما مادًيا، فإنها بكل تأكيد بمثابة صفعة قوية جًدا 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 إ َ زوايا أكثر عمًقا، فإذا ما أخذنا بعين الاعتبار أن الهجمات استهدفت شركات أمريكية عريقة جًدا ؟ هذه المرة، ولك أن تتخيل التقدم التقني والعلمي الذي تتمتع به الولايات المتحدة الأمريكية ؟ هذا المجال مقارنة بغيرها من الدول والشركات الأخرى، فبإمكاننا حينئذٍ تصور مدى الخطورة البالغة التي يمكن لمثل هذه الهجمات أن تتسبب به ؟ حال استهدافها دول أخرى أقل تقدًما وذات إمكانات أقل!

وع: سبيل توضيح مدى الخطورة لهذه الهجمات، نذكر أن حجم البيانات المستخدمة ? شن أخطر هجمات DDoS (تحديًدا ? الإمارات) وصل ? حده الأق إ´ ٩٠ جيجابت ? الثانية، بينما نرى أن حجم البيانات المستخدمة ? الهجمات الأخ ع: شركة Dyn يصل إ´ ١,٥ ابت ? الثانية، أي أك؟ بحوا ١٥ مرة

السيناريوهات الكارثية المحتملة والأ خطورة؟!

بناًء ع: المعطيات الحالية، فإن من أ السيناريوهات خطورة لمثل هذه الهجمات تلك التي تبنى ? جوهرها ع: إحداث الضرر ع: نطاق أوسع وأشمل معتمدة ع: إن نت الأشياء، والتي تحظى بفرص كب ة لاسيما مع دخولنا ? حقبة المدن الذكية ومن ب تلك السيناريوهات: إيقاف الإن نت عن دول بأكملها، واستهداف المنشآت الحيو ة التي ترتبط ارتباط وثيق بحياة الإنسان مثل شبكات المواصلات ال؟ة والجو ة والبح ة، ومحطات الطاقة، وشبكات الكهرباء والمياه والصرف الصحي، واستهداف المنشآت النووية، وتعطيل الأنظمة المالية العالمية بما فيها المؤسسات المالية وأجهزة الصرف الآ وغ ها، واستهداف المستشفيات والمنظمات الطبية والإنسانية وغ ها ناهيك عن استغلال الوضع الراهن من قبل منظمات إرهابية، بالإضافة إ´ الك من السيناريوهات الكارثية والأ خطورة مما حدث يوم أمس

قبل أن تخرج الأمور عن السيطرة!

قال حاسبيني إن علينا تحديد من هو المسؤول عن تلك الهجمات الأخ ة، فأنا هنا لا أقصد من هي الجهة المسؤولة عن شن الهجوم، فبالرغم من تبني مجموعة قراصنةتطلق ع: نفسها اسم "قراصنة عالم جديد" Hackers World New عن الهجوم الإلك و الهائل الذيُشَّن يوم أمس الجمعة، إلا أنه لا يمكن تأكيد ذلك حتى الآن، وإنما أقصد من تسبب ? شن هذا الهجوم؟!

علينا أن لا نثقل كاهل المستخدم بالعبارات الرنانة والتوجيهات الطنانة، وإلقاء اللوم عليه ? كل الحالات لنثقل كاهله بما لا يطيق، ولا يخفى عليكم أنه ظهر مؤخًرا مصطلح عالمي يدعى "إرهاق المستخدم أمنًيا بما لا يطيق" Fatigue Security أخذنا الحادثة الأخ ة بع الاعتبار، فما حدث هو استغلال أجهزة تسجيل فيديو وكام رقمية صينية الصنع لشن الهجمات مستغلة ثغرات من المف ض أن تكون مسؤولة عنها الشركات المصنعة وليس المستخدم لوحده وهذا الأمر يتطلب تعاون تقني وأمني أك؟ بك ع: مستوى الدول والشركات المصنعة لسن تشر عات وقوان لضمان استمرارية الإن نت وتفادي هجمات أ خطورة

فمن المهم جًدا وبأسرع وقت أن تتوجه الحكومات نحو الحد الأق من التعاون مع شركات أمن المعلومات، والتي بإمكانها عندئذ إيقاف شبكات البوت نت، وتحديد مصادر الهجوم، والمساعدة ع: توف الحماية اللازمة ومن جهة أخرى، يتوجب ع: المجتمع الدو التوجه أيَضا نحو تعاون تقني وقانو أك؟ لسن وتطبيق تشر عات دولية تفرض عقوبات ع: ممارسات مماثلة مصدرها دول تسعى لتحقيق مكاسب سياسية أو عسك ة .

سيناريوهات ومخاطر جدية تلوح ? الأفق والحروب الإلك ونية باتت حديث الإعلام ? الآونة الأخ ة، والتهديدات الناجمة عن المنظمات الإرهابية، وممارسات غ قانونية لدول بعينها بدأت تتكشف معالمها يوما بعد يوم، والمدن الذكية وإن نت الأشياء ترسم ملامح الأيام والحقبة القر ة القادمة، والتحرك الفوري ع: كافة المستو ات بات ضرورة حتمية قبل أن تخرج الأمور عن السيطرة!

فالإن نت غابة بكل معنى الكلمة! والغابة تتطلب قوان وتشر عات ل؟ لا ي يوم يسود فيه قانون الغاب وتخرج الأمور عن السيطرة