إذا كنا لا نثق في "كاسبرسكاي" فلماذا نثق في مايكروسوفت؟

كتبه هارون مير | 30 أكتوبر ,2017

ترجمة حفصة جودة

أوضحت الـ10 سنوات الماضية أن الإنترنت – سواء البرامج التي تشغله والبرامج التي تتحكم في برامج التشغيل – لعبة مناسبة للمهاجمين، وأوضحت الـ5 سنوات الماضية أنه لم يستوعب أحد تلك الرسالة حتى مجتمع الاستخبارات العالي، فقد أزاحت تسريبات سنودن الستار عن الجهود الضخمة التي بذلها التجمع الاستخباري "Five Eyes" في هذا الصدد، سواء عقد اتفاقات صامتة مع عمالقة الإنترنت أو التسلية بجميع الجهود مثل سرقة الصور الثابتة من محادثات الفيديو على "ياهو".

ردًا على تلك التسريبات، توقع العديد منا التهشم البطيء للإنترنت، فقد أصبح الكثير من الناس مدركين تمامًا لاعتمادنا على دولة واحدة في الحصول على جميع البرامج والخدمات التكنولوجية، وأدت حادثتان في الشهور الأخيرة إلى ظهور هذه الأفكار على السطح: فيروس "NotPetya" والاتهامات الموجهة إلى برنامج مكافحة الفيروسات الروسي العملاق "Kaspersky".

لنتحدث سريعًا عن "NotPetya"، كان نوتبيتيا عبارة عن حزمة محاسبة عادية تُسمى "MeDoc" (ميدوك) تُستخدم على نطاق واسع في أوكرانيا، لكنه أُسيء استخدامها للإيقاع بالضحايا، كانت الفيروسات عبارة عن مجموعة من الـ10 سنتات، لكن هناك العديد من الأشياء التي أدت إلى ظهور نوتبيتيا، بالنسبة للمبتدئين، فقد استخدم الفيروس ناقلات عدوى معاد استخدامها من تسربات

وكاله الأمن الوطني، ويبدو أنها كانت تستهدف أوكرانيا تحديدًا، وكان لهذا الفيروس آثار جانبية ملموسة في العالم الحقيقي (فقد ذكرت شركة "Maersk" للشحن أنها خسرت نحو 200 مليون دولار بسبب فيروس نوتبيتيا).

> كان استخدام التحديث نفسه لنقل الهجوم حيلة مثيرة

الأمر الأكثر إثارة بشأن نوتبيتيا كان ناقلات العدوى، فمن خلال الوصول إلى خوادم ميدوك المفتوحة واسعة النطاق، تمكن المهاجمون من بناء تحديث خبيث لتلك الحزمة، حمّل آلاف العملاء التحديث الجديد بشكل تلقائي، ففي هذه المرحلة يصبح التحديث التلقائي أمرًا آمنًا، لذا كان استخدام التحديث نفسه لنقل الهجوم حيلة مثيرة.

تطرقت قصة "كاسبرسكاي" بشكل عرضي إلى التحديثات الخبيثة أيضًا، فبينما كان الكثيرون من مجتمع الاستخبارات الأمريكي ينظرون طويلًا إلى شركة مكافحة الفيروسات الروسية وهي تكتسب شعبية كبيرة في الولايات المتحدة، استطاع "كاسبرسكاي" الأداء بشكل جيد بما فيه الكفاية ليكتسب حصة كبيرة في السوق، ظهر هذا الموضوع على السطح في شهر سبتمبر من هذا العام عندما أصدرت وزارة الأمن الداخلي الأمريكي توجيهات لجميع الإدارات الحكومية في الولايات المتحدة بإزالة برنامج كاسبرسكاي من أجهزة الحاسب، وفي الأيام التي تلت ذلك ظهرت سردية للقصة أكثر إثارة.

فوفقًا لعدة مصادر كان أحد موظفي وكالة الأمن الوطني يعمل على أدوات للقرصنة والهجوم، وقد حمل معه بعض من العمل إلى المنزل، حينها بدأ الحاسب في منزله (والذي يحتوي على برنامج كاسبرسكاي) بالتهام تلك الملفات.

ومثل جميع المعلومات الأمنية بدأ تشتيت الأمر وإدخاله في دراما فرعية تتضمن أشباح الإنترنت في "إسرائيل" وروسيا والولايات المتحدة، قال المدافعون عن كاسبرسكاي إن هذه الادعاءات مستحيلة، بينما قال المعارضون إن تواطؤهم مع الاستخبارات الروسية أصبح واضحًا، وهناك القليل من الأصوات الخجولة التي تنتظر ظهور المزيد من الأدلة، لكننا سنتجاهل هذا الجزء الدرامي تمامًا.

> ما نهتم به حقًا هو إمكانية إساءة استخدام تلك التحديثات من أجل مصالح دولة ما

ما نهتم به حقًا هو إمكانية إساءة استخدام تلك التحديثات من أجل مصالح دولة ما، بالنسبة لادعاءات الولايات المتحدة، بأن وكالة الاستخبارات الروسية ترسل تلك التحديثات بشكل انتقائي لبعض مستخدميها ثم تحول برامجهم إلى أدوات تجسس عملاقة، فهو أمر ممكن تمامًا من الناحية التقنية، استجاب كاسبرسكاي للقضية بنشر خطة من أجل تحسين الشفافية لكنها ربما تساعد وربما لا في الحفاظ على مكانتها بين عامة الناس.

لكننا بذلك نتجاهل حقيقة واضحة وهي أن أي برنامج يعمل في هذا المستوى، فنظامه الآمن يقع على بُعد خطوة تحديث واحدة من تحوله إلى نظام خبيث، سارع مناهضو كاسبرسكاي للإشارة إلى ذلك، فحتى لو كان كاسبرسكاي بريء اليوم فربما يتحول إلى برنامج خبيث غدًا (بضغط من المخابرات الروسية)، وأي تأكيدات من الشركة تعتمد على كونهم جيدين بدلًا من أن لديهم تحكم تقني.

بالنسبة لنا كغير مقاتلين نسبيًا في تلك الحرب فالسخرية لاذعة، فهذه الأصوات (معظم الأمريكيين) التي تقول إن المخابرات الروسية تشارك في اختيار الشركات، تدّعي أن الشركات الأمريكية لن تخضع أبدًا لضغط المخابرات الأمريكية لأن أي تهديد لوضعها الصناعي سوف تعلنه، في كلتا الحالتين ليس هناك أي اختلاف في التحكم التقني، يراهن المدافعون عن الولايات المتحدة أن المخابرات الأمريكية ستفعل الصواب ليس فقط اليوم ولكن في المستقبل أيضًا، هذا يقودنا إلى سؤال مهم: هل ستُطبق تلك القواعد في حالة دخول الولايات المتحدة في حرب رسمية (أو غير رسمية) مع دولة أخرى؟

في أثناء الحرب العالمية الثانية أممت ألمانيا الأصول البريطانية الموجودة في ألمانيا كما قامت بريطانيا العظمى بالمثل، يبدو هذا الأمر منطقيًا وربما يحدث في أي صراعات مستقبلية أيضًا، لكن أجهزة الحاسب والإنترنت غيرت تلك النظرية، ففي حرب تخيلية بين الولايات المتحدة وألمانيا تستطيع ألمانيا الاستيلاء على كل فروع ميكروسوفت في البلاد لكنها لا تستطيع حماية أجهزة الويندوز من تحديث واحد خبيث تنشره الشركة من مقرها الرئيسي في ريدموند بولاية واشنطون.

> هل ستكون أول خطوة تعطيل التحديث التلقائي للبرامج التي تمتلكها الدولة المنافسة؟

كلما فكرت في هذا الأمر أُصبت بالكثير من الرعب، فتحديث واحد خبيث تنشره مايكروسوفت قد يؤدي إلى تعطيل جميع الحكومات في كل أنحاء العالم، فكيف من الممكن أن نمنع ذلك؟ بالطبع لن يمنع ذلك التحكم التقني (إلا إذا بنيت نظام تشغيل وطني كما فعلت كوريا الشمالية).

هذا الوضع ليس له سابقة، فقدرة عدد صغير من البائعين على إغلاق بنية تحتية حكومية عن بعد أو الحصول على وثائق سرية أمر مرعب للغاية ويجعلك تلتف حول نفسك، يمكنك أن تتخيل ذلك بالإضافة إلى مدة الضغوط التي قد يتعرضون لها من حكوماتهم، لذا في الصراعات المستقبلية هل ستكون أول خطوة تعطيل التحديث التلقائي للبرامج التي تمتلكها الدولة المنافسة؟

بذلك سوف يطال الشر الجميع، فالإنترنت يصبح أفضل عندما يقوم كل شخص بالتحديث التلقائي، عندما يتأخر النظام البيئي عن إصلاح نفسه فإننا نُصاب جميعًا بالسوء، فمجرد إمكانية حدوث ذلك يقودنا إلى مكان مظلم، تمتلك كوريا الشمالية نحو 30% من سوق الهاتف في الولايات المتحدة (وتورد معظم مكوناتهم)، أما المصانع الصينية فتبني الأجهزة الصلبة

وتشحن البرامج الثابتة للأجهزة التي نعتمد عليها يوميًا، وسواء أعجبنا ذلك أم لا، فنحن جميعًا نعتمد على أن تقوم تلك البلاد بالتعامل كمواطنين دوليين جيدين، مع وجود القليل من أسلوب "الجزرة والعصا" لتشجيع السلوكيات الجيدة.

وهذا يزداد سوءًا بالنسبة إلى البلدان الأصغر، بالإضافة إلى أنه قد يكون هناك نوع من الصراع التدميري في التكنولوجيا بشكل متبادل بين الصين والولايات المتحدة، ولكن ماذا يحدث عندما تدخل جنوب إفريقيا على خط الصراع؟ وليس لديها ناقة ولا جمل في هذه المعركة؟ فهي ليست إلا مصدرًا للايين الدولارات لصالح الشركات الأجنبية، فيما لا تملك جنوب إفريقيا القدرة التفاوضية لفرض هذا السلوك المعتبر، ولا كذلك الأرجنتين وإسبانيا، ولكننا معًا قد نستطيع.

> أصبحت البرمجيات (والإنترنت) موارد مشتركة ضخمة تعتمد عليها بلدان العالم

وكذا يمكن وضع اتفاق بين جميع البلدان المشاركة، حيث يلتزم بلد بعدم استخدام نفوذه على شركة برمجيات محلية بما يؤثر سلبا على باقي الموقعين على هذا الاتفاق، وكذلك تتعرض البلدان التي تنتهك هذا الاتفاق إلى إعادة جميع البرامج التي تنتجها من بقية الدول الأعضاء، وبهذه الطريقة، فإن أي وكالة استخبارات تسعى إلى إساءة استخدام النفوذ على برنامج شركة واحدة تخاطر بذلك في حظر تعاملها مع جميع البرامج التي تنتجها تلك الدولة وكذلك جميع الدول الأعضاء، وهذا يخلق قبضة مشتركة تحافظ على أمان أكثر للجميع.

لكن يبدو واضحا أن هذا ليس الحل السحري للمسألة، فأي وكالة استخباراتية قد تستمر في قرصنة شركات البرمجيات لإيجاد ثغرة بها، وربما تنجح، ولكنهم فقط لا يمكن أن يفعلوا ذلك مع تعاون الشركة، وكذلك سيكون لدى الدول محكمة مركزية (مثل محكمة العدل الدولية) من شأنها أن تبحث في القضايا الميدانية لتحديد إذا ما كانت مؤامرة الاستخبارات قد تمت بموافقة شركة البرمجيات أو بدون موافقتها، ومثل اتفاقية جنيف ستظل قابلة للتنفيذ في أوقات النزاع أو الحرب.

ازدادت شركات البرمجيات غنى ببيع برامجها إلى البلدان في جميع أنحاء العالم، وأصبحت البرمجيات (والإنترنت) موارد مشتركة ضخمة تعتمد عليها بلدان العالم، وحتى لو لم تنتج هذه البرامج ما يكفي من التوزيع على الصعيد العالمي بحيث يكون لها مقعد على طاولة المفاوضات، فإن جميع البلدان تستحق ضمان معرفة أن البرامج التي تشتريها لن تستخدم ضدها، إن القضية ضد كاسبرسكاي توضح أن الولايات المتحدة تعترف بذلك، باعتباره تهديدا جديًا، وعليه تتخذ خطوات لحماية نفسها، وبالقياس فإن الاتفاق العالمي يحمي بقيتنا أيضًا.

المصدر: الجزيرة الإنجليزية

رابط المقال : https://www.noonpost.com/20507/