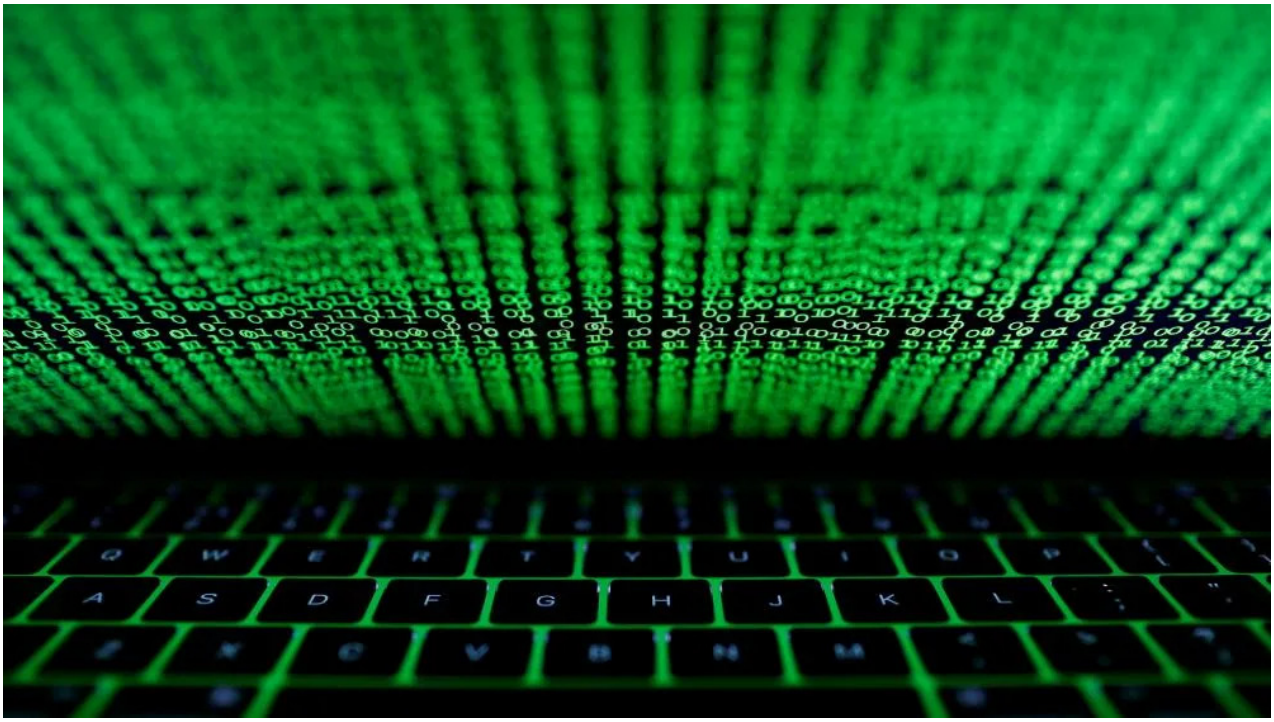
بروس شينير | نشر في ٥ يونيو ٢٠١٧,

لماذا تجعلنا وكالة الأمن الوطني أكثر عرضة للهجمات السيبرانية؟



ترجمة حفصة جودة

لقد تم إلقاء الكثير من اللوم على هجوم "واناكراي" وبرمجية دفع الفدية التي انتشرت على الإنترنت الشهر الماضي، الأمر الذ أدى إلى تعطيل العمل في المستشفيات والمصانع والشركات والجامعات، أولا؛ هناك كتاب البرامج الخبيثة والذين منعوا الضحايا من الدخول على أجهزتهم حتى دفع الفدية، ثانيا؛ هناك المستخدمين الذين لم يقوموا بتثبيت برامج الحماية على أجهزتهم والتي كانت لتمنح هذا الهجوم، القليل من اللوم يقع على عاتق مايكروسوفت والتي كتبت شفرة غير آمنة في المقام الأول، ويمكن للمرء أن يدين بالتأكيد وسطاء الظل وهم مجموعة من القراصنة لهم علاقة بروسيا وقاموا بسرقة ونشر أدوات الهجوم من وكالة الأمن الوطني والتي استخدموها في هذا الهجوم، لكن قبل ذلك كله؛ هناك وكالة الأمن القومي "NSA" والتي اكتشفت هذا الضعف منذ عدة سنوات وقررت استغلاله بدلا من الكشف عنه.

تحتوي جميع الرمجيات على أخطاء في الشفرات، لكن بعض هذه الأخطاء له آثار أمنية، حيث يسمح للمهاجم بالوصول غير المصرح به أو التحكم في جهاز الكمبيوتر، هذه الثغرات تنتشر في جميع البرامج التي نستخدمها، لكن برمجية كبيرة ومعقدة مثل مايكروسوفت ويندوز تحتوي على مئات من الثغرات وربما أكثر، هذه الثغرات لها استخدامات إجرامية واضحة والتي يمكن إبطال مفعولها مع التصحيح المستمر، يتم تصحيح البرمجيات الحديثة طوال الوقت، إما باستخدام جدول زمني ثابت مثل مرة شهريا بالنسبة لمايكروسوفت أو عندما يتطلب الأمر كما يفعل متصفح كروم.

كل سلاح هجومي هو ثغرة محتملة في دفاعنا والعكس صحيح

عندما اكتشفت حكومة الولايات المتحدة وجود ثغرة في إحدى البرمجيات كان أمامها أن تقرر بين خيارين، إما أن تحتفظ بهذا السر وتستخدمه لجمع استخبارات أجنبية، والمساعدة في تنفيذ أوامر التفتيش ونقل برمجيات خبيثة، أو أن تقوم بتنبيه بائع البرمجيات لإصلاح الثغرة وحماية الدولة والعالم

كله من هجمات مشابهة من حكومات أجنبية أو مجرمي الإنترنت، يقول جاك غولدسميث –مساعد النائب العام الأمريكي السابق-: "كل سلاح هجومي هو ثغرة محتملة في دفاعنا والعكس صحيح".

هذه خطوة جيدة على الأرض؛ في عام 2010 قامت حكومة الولايات المتحدة بتطبيق عملية المساواة بين نقاط الضعف في الوكالات (VEP) لتحقيق التوازن في عملية المقايضة، كانت التفاصيل سرية بشكل كبير، لكن في عام 2014 نُشرت مدونة لمنسق الأمن السيبراني الخاص بالرئيس باراك أوباما؛ مايكل دانيل، أوضح فيها المعايير التي تستخدمها الحكومة لتقرر عدم الافصاح عن عيب برمجي معين، لم يكن محتوى المنشور مفاجئًا لكه طرح الكثير من الأسئلة مثل: "إلى أي مدى يُستخدم النظام الضعيف في البنية التحتية الأساسية للإنترنت، وفي أنظمة البنى التحتية الأخرى وفي الاقتصاد الأمريكي وفي أنظمة الأمن القومي؟" و"هل يؤدي هذا الضعف في حالة عدم معالجته إلى حدوث مخاطر كبيرة؟" "هل نحتاج بشدة إلى تلك المعلومات التي قد نحصل عليها من استغلال نقاط الضعف تلك؟"، من ناحية أخرى لاحظ دانيل أن حكومة الولايات المتحدة تكشف للبائعين الغالبية العظمى من نقاط الضعف التي تكتشفها –حوالي 91%- وفقًا لما قاله مدير وكالة الامن مايكل روجرز.

تحتوي أنظمة البنية التحتية على الكثر من نقاط الضعف التي تشكل مخاطرة كبيرة في حالة عدم إصلاحها

كانت نقطة الضعف الخاصة بواناكراي شفرة تسمى " EternalBlue"، والتي اكتشفتها الولايات المتحدة –وكالة الأمن القومي على الأرجح- في وقت ما قبل عام 2014، ذكرت واشنطون بوست في تقريرها أن الثغرة كانت مفيدة في الهجوم وأن وكالة الأمن القومي كانت قلقة من استخدام أشخاص آخرين لهذه الثغرة، هذا القلق يبدو معقولا فالأمن الوطني وأنظمة البنية التحتية الأساسية تحتوي على الكثير من نقاط الضعفة البرمجية والتي تمثل مخاطرة كبيرة في حالة تركها دون إصلاح، وبالفعل كانت متروكة دون إصلاح.

هناك الكثير لا نعرفه عن عملية " VEP"، تقول واشنطون بوست أن وكالة الأمن القومي استخدمت " إذا واضحا يكن لم ،2010 عملية بعد شفتُاكة أنها يعني هذا ،سنوات خمس من لأكثر "EternalBlue ما كانت كل نقاط الضعف تحظى بهذا الاهتمام أو أن أي خلل يُراجع بشكل دوري لتحديد إذا ما كان ينبغي الكشف عنه أم لا، هذا يعني أن أي عملية تسمح لشيء خطير مثل " EternalBlue" أو " Cisco" –والذي كشف عنه وسطاء الظل في أغسطس الماضي وقالوا أنه ظل بلا إصلاح لعدة سنوات- لم يكن يخدم الأمن القومي بشكل جيد، وكما قال موظف سابق في وكالة الأمن القومي فإن قيمة ونوعية الاستخبارات التي تم جمعها لم تكن واقعية وكذلك الضرر المحتمل، ينبغي أن تتوقف وكالة الأمن القومي عن تجميع نقاط الضعف.

ربما اعتقدت وكالة الأمن القومي أن لا أحد سواها قد يكتشف " EternalBlue"، هذه هي أحد معايير دانيل الأخرى: "هل من المرجح أن يكتشف شخص آخر نقاط الضعف؟ عادة ما يُشار إلى ذلك بكلمة " ضعف نقاط تكتشف أن القومي الأمن لوكالة يمكن هل ،"سوانا أحد لأ" لجملة اختصار وهي "NOBUS لا يستطيع غيرها اكتشافها؟ أو أليس من المرجح أن نقاط الضعف التي تكتشفها وكالة استخبارات ما قد يكتشفها آخرون أو مجرمي الإنترنت؟

تعرض وكالة الأمن القومي ووكالة المخابرات المركزية للسرقة بسهولة أمر مرعب

في الأشهر القليلة الماضية، توصلت شركات التكنولوجيا إلى بعض البيانات بخصوص تلك الأسئلة، في إحدى الدراساتا؛ تمكنت مع اثنين من زملائي بهارفرد من فحص أكثر من 4300 نقطة ضعف في برامج عامة وخلصنا إلى أن حوالي 15 إلى 20% منهم أعيد اكتشافهم خلال عام، بشكل منفصل؛ قام الباحثون في مؤسسة "راند" بالبحث في بيانات مختلفة وأصغر حجما وانتهوا إلى أن أقل من 6% من نقاط

الضعف تلك أعيد اكتشافهم خلال عام، هذه الأسئلة التي يتناولها البحثان مختلفة قليلا والنتائج غير قابلة للمقارنة بشكل مباشر، لكن يبدو واضحًا أننا بحاجة لمزيد من البحث.

عارض الأشخاص داخل وكالة الأمن القومي هذه الدراسات سريعا، وقالوا أن تلك البيانات لا تعكس حقيقتهم، وقالوا أن هناك فئات كاملة من نقاط الضعف التي تستخدمها وكالة الأمن القومي وليست معروفة في عالم الأبحاث مما يجعل إعادة اكتشافها أقل احتمالا، قد يكون هذا الأمر صحيح؛ لكن الأدلة التي حصلنا عليها من وسطاء الظل تقول بأن نقاط الضعف التي تحتفظ بها وكالة الأمن القومي سرا لا تختلف باستمرار عن تلك التي يكتشفها الباحثون، ونظرا لتعرض أدوات وكالة الأمن القومي ووكالة المخابرات المركزية للسرقة بسهولة مرعبة، وإعادة اكتشافها ليست مقتصرة على الأبحاث الأمنية المستقلة.

من الضروري مراجعة نقاط الضعف المُحتفظ بها لأغراض دفاعية بشكل دوري

وحتى لو كان من الصعب إصدار بيانات نهائية حول إعادة اكتشاف نقاط الضعف، فمن الواضح أن نقاط الضعف كثيرة، أي نقاط ضعف يتم اكتشافها واستخدامها في الهجوم ينبغي أن تظل سرية لفترة قصيرة من الوقت إن أمكن، وقد اقترحت أن تظل سرية لمدة 6 أشهر مع الحق في التمديد لـ6 أشهر أخرى في الظروف الاستثنائية، يجب على الولايات المتحدة الوفاء بمتطلباتها الدفاعية من خلال النشر المستمر لنقاط الضعف المكتشفة حديثًا؛ والتي عند إصلاحها تساعد في تحسين دفاع البلاد.

لابد من إعادة إصلاح " VEP" وتقويتها كذلك، في تقرير العام الماضي قام به آري شوارتز وروب كناك –عمل كلاهما سابقا في سياسة الأمن السيبراني بمجلس الأمن القومي بالبيت الأبيض- قدما بعض الاقتراحات الجيدة حول كيفية إضفاء صبغة رسمية على العملية وزيادة شفافيتها والرقابة عليها، وضمان المراجعة الدورية لنقاط الضعف المُحتفظ بها في سرية لأغراض دفاعية، هذا أقل ما يمكن القيام به، وهناك مشروع قانون قدم مؤخرا لمجلس الشيوخ ومجلس النواب يدعو إلى تلك الاقتراحات وأكثر.

في حالة " EternalBlue" كان لعملية " VEP" آثار إيجابية، فعندما أدركت وكالة الأمن القومي أن وسطاء الظل سرقوا هذه الأداة قاموا بتنبيه مايكروسوفت والتي أصدرت التصحيح في مارس، هذا الأمر منع وقوع كارثة عندما قام وسطاء الظل بنشر نقطة الضعف على الإنترنت، وكانت الأنظمة غير المصححة فقط هي المعرضة لهجوم "واناكراي" بعد ذلل بشهر ومن ضمن ذلك نسخ الويندوز القديمة والتي لم تعد مايكروسوفت تدعمها، وبالرغ من أن وكالة الأمن القومي ينبغي أن تتحمل نصيبها من المسؤولية –بغض النظر عن جودة عملية " VEP" أو عدد نقاط الضعف التي أبلغت عنه الوكالة ليقوم بإصلاحها البائعون- فإن الأمن لن يتحسن إلا عندما يقوم المستخدمون بتحميل وتثبيت التصحيحات،وينبغي على المنظمات أن تتحمل مسؤولية الحفاظ على برامجها وأنظمتها محدّثة حتى اللحظة، هذه هي أحد أهم الدروس التي ينبغي أن نتعلمها من "واناكراي".

المصدر: فورين أفيرز