كيف كشفت هجمات الفدية الخبيثة عن ثغرات الأمن السيبراني العالمي؟

كتبه جيروم أوردو | 23 مايو ,2017

ترجمة وتحرير: نون بوست

بعد مرور 10 أيام على وقوع هجمات برمجيات الفدية الخبيثة، لا بدّ من توجيه أصابع الاتهام إلى العديد من الأطراف المسؤولة نسبيا عن هذا الهجوم. في الواقع، يجب الإشارة، أولا، إلى الدور الذي اضطلعت به وكالة الأمن القومي، حيث أنها كانت ملهمة للأطراف المسؤولة عن هذا الهجوم. بالإضافة إلى ذلك، لا بدّ من التنويه، ثانيا، بالدول التي ساهمت في خلق سوق من الثغرات الأمنية الالكترونية. كما لابدّ من الحديث، ثالثا، عن الشركات التي كانت قد حذّرت سلفا من وقوع هجوم مماثل.

استغرق مجموعة من الباحثين أسبوعا فقط لإحباط الفيروس واناكري، الذي تعرض له عشرات الآلاف من أجهزة الكمبيوتر في أكثر من 150 دولة حول العالم، يوم 12 أيار/مايو سنة 2017. ومؤخرا، أعلن باحثون أنهم توصلوا إلى وسيلة أطلقوا عليها اسم "واناكيوي"، تُمكّن الفنيين من فك تشفير أجهزة الكمبيوتر الخاصة بهم دون دفع الفدية التي يطلبها مجرمو الإنترنت. والجدير بالذكر أن ثلاثة فرنسيين هم من قاموا بتطوير هذا الفيروس المضاد لفيروس واناكري وهم؛ "أدريان غيني"، و"ماثيو سيشي"، و"بنيامين ديلي".

في يوم الجمعة 19 أيار/ مايو، قالت وكالة تطبيق القانون الأوروبية "يوروبول" انها اختبرت البرنامج الذي وضعه هذا الثلاثي من الباحثين، لعدة أيام وليال. وتجدر الإشارة إلى أن برمجية "واناكيوي" أصبحت متاحة مجانا لجميع مستخدمي الانترنت، حتى يتمكنوا من وضع حدّ لانتشار هذا الفيروس، وطي صفحة هذا الهجوم من تاريخ الأمن السيبراني.

في الحقيقة، ستكون جُملة من الدروس التي يجب أن نستخلصها من هجوم واناكري، الذي وُصف بأنه هجوم إلكتروني "لم يسبق له مثيل"، نظرا لما كشفه حول ثغرات الأمن الرقمي العالمي. فقد أدّت هذه البرمجية الخبيثة في إحداث ضجة إعلامية مثيرة، ساهمت بدورها في الإفراط في تقدير حجم الخطر الذي يشكله هذا الهجوم وإخفاء الثغرات الخطيرة التي خلقتها الجهات الفاعلة الرئيسية المسؤولة عن ضمان الأمن المعلوماتي في العالم.

> استهدفت برمجية الفدية الخبيثة العديد من الشبكات الحساسة في العالم على غرار؛ وزارة الداخلية، والبنك المركزي الروسي، ومجموعة الاتصالات الإسبانية "تيليفونيكا"، فضلا عن شركة السكك الحديدية الألمانية، "دويتشه بان"، وشركة خدمات توصيل البريد السريع، "فيديكس"

يوم الجمعة 12 أيار/مايو، انتشر فيروس واناكري كالنار في الهشيم، مما أدى إلى إصدار تنبيه عاجل في وقت مبكر من المساء، بأن وضع الأمن الإلكتروني العالمي مهدد، بعد إصابة آلاف الحواسيب في العالم. وقد ركزت العديد من وسائل الإعلام اهتمامها على المملكة المتحدة، حيث تأثرت العديد من المستشفيات، نظرا لأن هذا الهجوم أحدث العديد من الاضطرابات في أنظمة هيئة الخدمات الصحية الوطنية.

فضلا عن ذلك، استهدفت برمجية الفدية الخبيثة العديد من الشبكات الحساسة في العالم على غرار؛ وزارة الداخلية، والبنك المركزي الروسي، ومجموعة الاتصالات الإسبانية "تيليفونيكا"، فضلا عن شركة السكك الحديدية الألمانية، "دويتشه بان"، وشركة خدمات توصيل البريد السريع، "فيديكس".

في فرنسا، كانت شركة رينو الفرنسية أحد أول ضحايا هذا الهجوم الخبيث، حيث أنها اضطرت إلى إغلاق عدة مواقع إنتاج، "كتدبير وقائي لمنع انتشار الفيروس". وخلال يوم السبت 13 أيار/مايو، أعلنت يوروبول أن الهجوم وصل إلى مستويات غير مسبوقة. وتجدر الإشارة إلى أن جميع ضحايا هذا الهجوم تلقوا رسالة مماثلة جاء فيها: "عفوا، لقد تم تشفير الملفات الخاصة بك". بعبارة أخرى، تم تشفير الملفات الخاصة بهم من قبل برنامج خبيث ولا يمكنهم فكّ التشفير إلا عن طريق وضع كلمة مرور.

وللحصول على هذه الملفات، يجب دفع قرابة 300 عن طريق البيتكوين، التي تعتبر عملة المعماة الرئيسية. أما إذا لم يقم المستخدم بدفع الفدية فإنه سوف يفقد تدريجيا بياناته. وبعد مرور أسبوع، بدأ احتواء انتشار هذا الفيروس. فمنذ 13 أيار/مايو، اكتشف باحث شاب في مجال الأمن السيبراني

البريطاني "بالصدفة" ثغرة في شيفرة برمجية الفيروس نفسه، تُمكّن من الحدّ بشكل كبيرٍ من انتشاره.

من جهة أخرى، وبحسب البيانات التي قدّمتها شركة "كريبتوس لوجيك" لتحليل التهديدات، كانت نصف عناوين الإنترنت التي أُتلفت عالميًا بسبب "واناكراي" تقع في الصين وروسيا، مع نسبة بلغت 30 بالمائة في الأولى، و20 بالمائة في الأخرى، مقابل 7 بالمائة في الولايات المتحدة و2 بالمائة في فرنسا، وبريطانيا، وألمانيا.

والأمر الملفت للنظر، تعتبر الغنائم التي جمعها هؤلاء المجرمين الإلكترونيين ضئيلة جدا. ووفقا للأرقام التي ذكرتها وكالة رويترز، يوم الجمعة 19 مايو/أيار، كان قد تم دفع فدية لهؤلاء القراصنة تعادل 309 أي ما يعادل 94 ألف دولار. في الواقع، تبدو نتائج هذه "الهجمات الإلكترونية التي لم يسبق لها مثيل" ضعيفة جدا، مقارنة بالهجمات السابقة، وفقا لما أفاد به موقع ريفلي.

> في تاريخ الأمن السيبراني، أحدثت العديد من الهجمات أضرارا في أكثر من فيروس واناكري. ولا يتمثل الأمر المثير للقلق في هذه القضية في حجم الضرر الذي تسبب فيه هذا الفيروس، بل في حدوثه على الرغم من التحذيرات التي أطلقتها العديد من المؤسسات

منذ سنة 2000، تصدرت دودة "أي لاف يو" عناوين الصحف الدولية التي أصابت 10 بالمائة من أجهزة الكمبيوتر في جميع أنحاء العالم، وتسبب في خسائر تقدر بخمسة مليار دولار. وبعد ذلك الهجوم بسنة، ساهم فيروس "كود رد" في تعطيل تشغيل قرابة 359 ألف جهاز كمبيوتر، مما تسبب في خسائر تعادل قيمتها اثنين مليار دولار.

في تاريخ الأمن السيبراني، أحدثت العديد من الهجمات أضرارا في أكثر من فيروس واناكري. ولا يتمثل الأمر المثير للقلق في هذه القضية في حجم الضرر الذي تسبب فيه هذا الفيروس، بل في حدوثه على الرغم من التحذيرات التي أطلقتها العديد من المؤسسات.

كما كشفت هجمات الفدية الخبيثة عن ثغرات الأمن السيبراني العالمي. وفي السياق ذاته، قال الخبير المعلوماتي إيريك فيليول، المختص في علم التشفير وعلم الفيروسات إن "الهجوم الأخير لا يعتبر هجوما سيبرانيا، بل مجرد عمليات إجرامية مشبوهة لا يمكن أن يكون لها تأثير كبير. وحتى الآن، لا يمكن أن نقول أن هذا الهجوم لم يسبق له مثيل وخطير جدا. فإذا كان الهجوم من قبل فيروس من نوع كونفيكر، فلا أستطيع أن أتخيل ماذا يمكن أن يحدث في العالم".

من جانب آخر، يعتبر كونفيكر مثال آخر على أنواع الفيروسات الأكثر تدميرًا مقارنة بفيروس واناكري. وقد ظهرت دودة حاسوب كونفيكر سنة 2008. ووفقا للتقديرات، أصاب هذا الفيروس ما بين 3.5 و9 مليون جهاز كمبيوتر. والأهم من ذلك، انتشر كونفيكر في العديد من الشبكات الحساسة، منها وزارة الدفاع الأمريكية، وإدارات الدفاع البريطاني والفرنسي، فضلا عن أنه استهدف العديد من

الغواصات البريطانية، وطائرات الرافال الفرنسية.

أما فيما يتعلق بهجوم واناكري، فماذا يكشف عدد الشركات الكبيرة التي استهدفتها هجمات الفدية الخبيثة؟ منذ عدة أشهر، أعلن مدراء أمن تكنولوجيا المعلومات في جميع أنحاء العالم أنه يجب الاستعداد جيدا للهجمات المحتملة في المستقبل. وعلى الرغم من كل التحذيرات، إلا أن فيروس رانسوم وير تمكّن من الاستفحال في العديد من الأنظمة العالمية ولكن ليس عن طريق البريد الالكتروني، بل عن طريق إيجاد ثغرة أمنية في برامج مايكروسوفت.

ابتداء من شهر آذار/مارس، أصدرت شركة مايكروسوفت نشرة التصحيح للثغرات الأمنية الحرجة التي تقوم بالتأثير على كل نسخ نظام التشغيل ويندوز. وقد أطلقت مايكروسوفت هذه الإصلاحات في الوقت المناسب لأنه من الواضح، أنه تم رصد نقاط الضعف من قبل العديد من المستخدمين وخاصة من قبل وكالة الأمن القومي الأمريكي.

في 14 نيسان/ أبريل، نشرت مجموعة من القراصنة تُطلق على نفسها "وسطاء الظل" مجموعة من الأدوات التابعة لوكالة الأمن القومي الأمريكي، وقامت استغلال نقاط الضعف في برمجيات وثغراتها الأمنية خاصة غير المعروفة منها للعامة أو حتى مطوريها في شن هجمات إلكترونية أو ما يطلق عليه باسم "هجوم دون انتظار".

> لا يقتصر هذا الإهمال على هجوم واناكري. فهناك هناك مشكلة حقيقية ليس فقط في كيفية إدارة الهجمات بل حتى في ثقافتنا. وعلينا أن نتذكر اكتشاف ثغرة أمنية "هارتبليد" في سنة 2014، التي أثرت سلبا على تطبيق "أوبن إس إس إل"

علاوة على ذلك، قامت برمجية حاسوب "اتيرنال بلي" باستغلال نفس الخلل الذي وجده واناكري. وفي 13 أيار/ مايو، نشرت مايكروسوفت تنبيها طلبت من خلاله من المستخدمين تحديث البرامج الخاصة بهم. وبالتالي، فإن تجاهل المسؤولين عن الأمن السيبراني في الشركات للتحذيرات وفشلهم في تحديث برامجهم، يعدّ السبب الرئيسي الذي جعلهم عرضة لمثل هذا الهجوم.

في هذا الصدد، يقول إريك فيليول إن هذا الأمر مشين، وهو عبارة عن فضيحة. إني أرى اليوم المزيد من مدراء تقنية المعلومات الذين يقومون بشكل جيد في القاعات الإلكترونية على عكس مدراء أمن المعلومات الشركات الكبيرة. ومن جهة نظري، يجب طرد هؤلاء الأشخاص".

وتابع فيليول قوله "في الواقع، لا يقتصر هذا الإهمال على هجوم واناكري. فهناك هناك مشكلة حقيقية ليس فقط في كيفية إدارة الهجمات بل حتى في ثقافتنا. وعلينا أن نتذكر اكتشاف ثغرة أمنية "هارتبليد" في سنة 2014، التي أثرت سلبا على تطبيق "أوبن إس إس إل".

كما أضاف فيليول قائلا: "في ذلك الوقت، تصدرت هذه الثغرات الأمنية عناوين الصحف لمدة

سنتين. وقبل بضعة أشهر، كشفت عملية تدقيق أن قرابة 200 ألف خادم ما زالوا غير آمنين إلكترونيا! وهذا يعني أنه منذ سنة 2014، لم يفعل خبراء الأمن السيبراني أي شيء يُذكر لتصحيح هذه الثغرات الأمنية. وبالتالي، ماذا تتوقع إذا لم يقم الأشخاص المسؤولين عن الأمن الإلكتروني بعملهم الأساسي؟ بطبيعة الحال سوف تحدث كارثة".

"المواطنون في خطر محدق"

في الحقيقة، يجب تحميل المسؤولية، أو بالأحرى التقصير في حماية النظام المعلوماتي، للدول ووكالات مخابراتها، خاصة تلك الوكالات التي تنجز تقنيات إلكترونية جديدة لحماية المعلومات في العالم. وفي نفس الوقت، فضح باحثون وقراصنة إنترنت مدى ضعف نجاعة الأساليب المستعملة من قبل وكالات المخابرات الحكومية لحماية النظام المعلوماتي. وعلى ضوء ما ذكر آنفا، يبدو من الجليّ مدى ضعف قراصنة وكالات المخابرات في حماية الأنظمة المعلوماتية، حيث كثيرا ما وقع اختراق الأبواب الخلفية في نظام الحواسيب التي برمجها "هاكر" المخابرات.

من المفترض أن تبقى هذه الثغرات الإلكترونية طي الكتمان. ولكن ما تعرضت له مواقع عالمية من هجمات إلكترونية أثبت عكس ذلك. وللتوضيح أكثر، فإنه مع تعرض نظام ما إلى اختراقات إلكترونية، سيقوم أحد قراصنة المخابرات، أو المبلغين، أو المؤسسة الحكومية، باكتشافه مباشرة بهدف إما تحديد الثغرة والعمل على سدها مباشرة، أو تحويلها كأداة تستعمل لصالح الموقع المخترق.

> طرح إدوارد سنودن السؤال التالي: "ألم يسأل أحد منكم نفسه لماذا يتدخل دائما الباحثون وليس الحكومات في مجارات الفوضى التي تخلفها وكالة الأمن القومي داخل أنظمة الشبكات الإلكترونية؟"

في هذا الإطار، يعد إدوارد سنودن من بين أولئك الذين حذروا من مخاطر الأساليب التي تنتهجها وكالة الأمن القومي الأمريكية في حماية الأنظمة المعلوماتية. وفي هذا الصدد، نشر سنودن، يوم 13 أيار/ مايو الفارط، على حسابه في تويتر تغريدة سخر فيها من هذه الأساليب.وقد طرح إدوارد سنودن السؤال التالي: "ألم يسأل أحد منكم نفسه لماذا يتدخل دائما الباحثون وليس الحكومات في مجارات الفوضى التي تخلفها وكالة الأمن القومي داخل أنظمة الشبكات الإلكترونية؟"

وعزز هذا المتعاقد التقني السابق تغريدته بتقرير عن شركة "سيسكو سيستمز" المختصة في مجال المعدات الشبكية، حيث كشف من خلاله أن 90 بالمائة من النفقات التي تصرفها مختلف الوكالات الأمريكية لإنجاز البرامج الإلكترونية موجهة أساسا لتنفيذ هجمات قرصنة وليست منظومة دفاع إلكتروني.

علاوة على ذلك، فضح فيروس واناكري تقصير الحكومات في حماية الأنظمة المعلوماتية. وفي السياق ذاته، أشار مؤسس موقع "ويكيبيديا"، جيمي ويلز، إلى أنه "بإمكان وكالة الأمن القومي أن تعالج بسرعة أية ثغرة إلكترونية حاصلة بمجرد اكتشافها. بعد ذلك، تعلم الوكالة شركة "مايكروسوفت"

لتقوم بعملية الإصلاح بصفة سرية". وواصل جيمي ويلز حديثه منبها إلى "خطورة الأساليب التي تستعملها الوكالة لحماية الأنظمة المعلوماتية على حواسيب المدنيين".

من جهته، أكد رئيس شركة مايكروسوفت، براد سميث، في تقرير نشر بتاريخ يوم 14 أيار/ مايو، أن "اتفاقية جنيف الرقمية قد أصدرت بهدف حماية المواطنين من الهجمات الإلكترونية التي تطال حواسيبهم، كما تهدف أيضا إلى مساعدة الشركات على تحديد الثغرات الإلكترونية في أنظمتهم المعلوماتية".

ولكن هذه الاتفاقية لم ترق للخبير في الإلكترونيات، إيريك فيليول، الذي أكد أن "ما ذكرته شركة مايكروسوفت ليس سوى مجرد حبر على ورق، فلن تلتزم إدارتها بما جاء في الاتفاقية... ففي الحقيقة، كل ما يهم شركة مايكروسوفت هو تحقيق الربح على حساب الخبراء والباحثين في مجال المعلوماتية".

> تتمثل المعضلة الأساسية في أن اختراق الأنظمة المعلوماتية لم يعد حالة شاذة، بل أصبح أمرا متواترا بصفة رهيبة. وفي هذا الإطار، أضحت عمليات الاختراق سلعة متبادلة بملايين الدولارات

في الإطار ذاته، تتعاون كبار شركات عالم "النت" مع وكالات المخابرات إما تحت الإكراه أو بصفة طوعية. ونذكر من بينهم مؤسس شركة مايكروسوفت، بيل غيتس، حيث ركز بصفة طوعية على تطبيق الأبواب الخلفية في نظام الحواسيب التي تنتجها شركته. وعلى الرغم من أن بيل غيتس قد أنكر ذلك، إلا أن هذا التطبيق السري وقع كشفه سنة 2000 من قبل الحكومة الفرنسية عن طريق وزارة الدفاع.

من جهة أخرى، تتمثل المعضلة الأساسية في أن اختراق الأنظمة المعلوماتية لم يعد حالة شاذة، بل أصبح أمرا متواترا بصفة رهيبة. وفي هذا الإطار، أضحت عمليات الاختراق سلعة متبادلة بملايين الدولارات. وفي الحقيقة، يعد جزء من هذه العملية شرعيا وتحت إشراف مؤسسات أمريكية وفرنسية خاصة. في المقابل، يعد جزء آخر من هذه العمليات غير شرعي. ولكن ولئن اختلفت الطرق، إلا أن مصالح وكالات المخابرات والقراصنة تبدو متقاربة في بعض الأحيان.

من جهته، أشار إيريك فيليو إلى أن "الهجمات الإلكترونية تحتاج إلى ثغرات إلكترونية لكي تنجح في مهمتها". وواصل فيلول حديثه مؤكدا أن "الحكومات تعجز عن صد الهجوم الإلكتروني إذا كانت أجهزتها غير مؤمنة بالشكل الكافي". وبحسب رأيه، فإن ذلك يؤدي إلى تعرض عدة حواسيب حكومية إلى ما يسمى "بالهجوم دون انتظار" أي أن الهجمات الإلكترونية تستهدف مباشرة نقاط الضعف في البرمجيات، والتي بدورها تعجز عن حماية نفسها أو حتى الرد على هذا الهجوم.

وقد دعا هاكر وصحفي أمريكي في أحد تقاريره، الذي نشر بتاريخ 17 أيار/ مايو، إلى وضع حد لما اعتبره "غباء رقميا" من خلال تجريم بيع برامج الاختراق، كما دعا أيضا إلى تنزيل عقوبات صارمة

ضد الشركات والمؤسسات التي تعد مقصرة في في حماية أجهزتها الرقمية.وأضاف في تقريره مؤكدا أنه "من الضروري أيضا مساءلة الأشخاص الذين يتعمدون الولوج إلى الإنترنت وهم موقنون جيدا بأنها غير مؤمنة ويمكن أن تصبح عرضة للاختراقات".

وفي نهاية المطاف، يثير فيروس" واناكراي"، الذي يستهدف عادة أنظمة تشغيل مايكروسوفت ويندوز، قلق الكثير من الخبراء بما أنه يهدد برنامج الأمن السيبراني. ويجد هذا الفيروس أرضا خصبة في ضرب أهدافه عندما لا تتواصل الشركات والمؤسسات فيما بينها لتحقيق أمن معلوماتي مشترك، بالإضافة إلى تقصير مخترعي البرمجيات في حماية أنظمتهم الإلكترونية، دون أن ننسى طبعا تقصير الحكومات ووكالات استخباراتها. وبالنسبة لإيريك فيليول، فإن "عدم القدرة على تركيز نظام أمن معلوماتي ناجع تسبب في خلق عدة مشاكل، على غرار تقصير إدارة قسم تقنية المعلومات في القيام بمهمته التي أوكلت إليه".

> في الوقت الذي ننتظر فيه تنامي الحس بالمسؤولية تتواصل الجرائم الإلكترونية في الفتك بالمواقع الحكومية والخاصة. حيث أعلن موقع "وسطاء الظل" وضع يده على عدة أنظمة إلكترونية خاصة بوكالة الأمن القومي الأمريكي، تعمل على بيعها مع حلول شهر حزيران/ يونيو، في شكل "اشتراكات سنوية"

كذلك، إذا كانت مايكروسوفت الأكثر عرضة لفيروس "واناكراي"، فيجب أن نضع في الحسبان أن أغلب المؤسسات الفرنسية من وزارات الدفاع والتعليم وشركات تعمل ببرمجيات مايكروسوفت، ستكون بدورها عرضة للإصابة بفيروس واناكراي. وعلى الأرجح، سيتسبب ذلك في خلق مشاكل بين كلا من فرنسا والولايات المتحدة."

وأكد فيليول أيضا أن الحل لهذه المشكلة يكمن في تعزيز الوعي السياسي بخطورة الاختراقات الإلكترونية. ومن هذا المنطلق، تلوح في الأفق مسؤولية وكالات المخابرات. في المقابل، لا تتحمل كل من الحكومات ولا وكالات المخابرات مسؤولياتها بالقدر الكافي للحد من الهجمات الإلكترونية.

لذلك دعا فيليول إلى "توقيع اتفاقية عالمية لمجابهة الهجمات الإلكترونية، مشابهة للتي وقعت في أوتاوا بخصوص منع اعتماد الألغام المضادة للأشخاص، أو لاتفاقية باريس لحظر استعمال الأسلحة الكيميائية، فالهجمات الإلكترونية لا تقل خطورة عنهما".

وفي الوقت الذي ننتظر فيه تنامي الحس بالمسؤولية تتواصل الجرائم الإلكترونية في الفتك بالمواقع الحكومية والخاصة. وفي الموضوع نفسه، أعلن موقع "وسطاء الظل" وضع يده على عدة أنظمة إلكترونية خاصة بوكالة الأمن القومي الأمريكي، حيث تعمل على بيعها مع حلول شهر حزيران/ يونيو، في شكل اشتراكات سنوية".

المصدر: ميديا بار