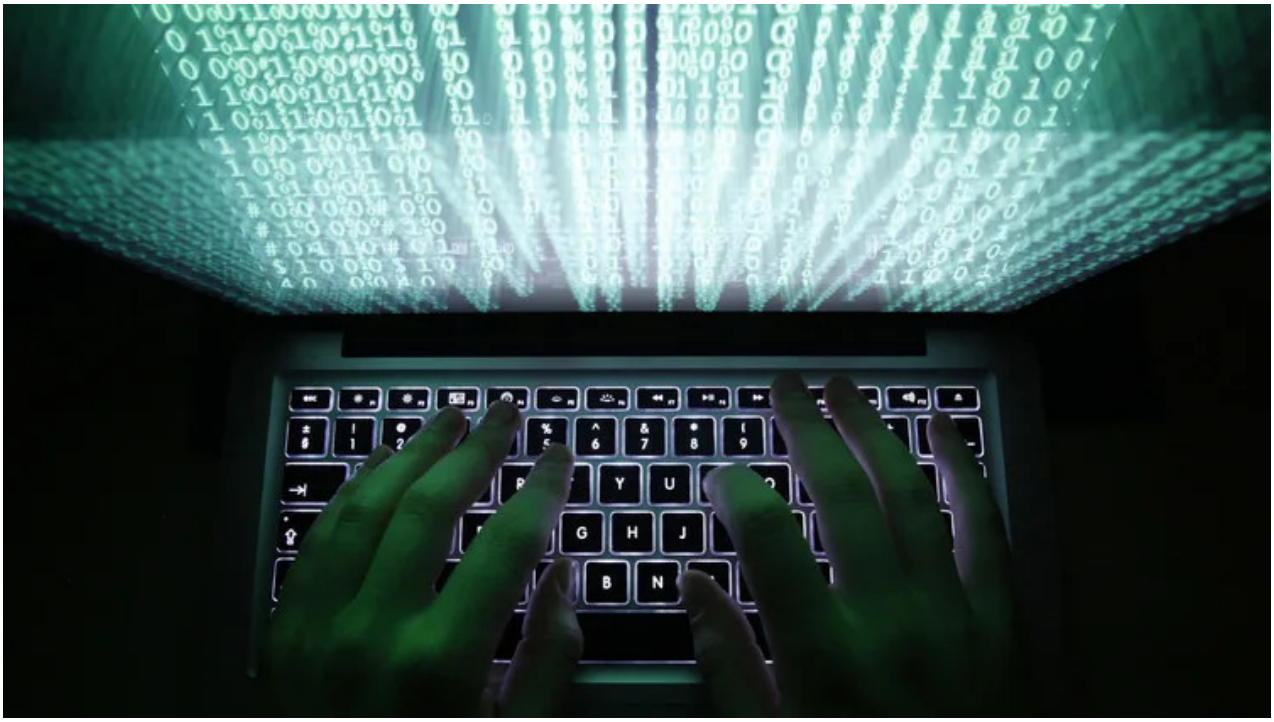
هل حلّ عصر الكوارث "السيبرانية"؟



ترجمة وتحرير: نون بوست

يوم الجمعة، ضربت العالم أحد أكبر الهجمات الإلكترونية في التاريخ الحديث، بعد أن أصاب "فيروس واناكري"، الذي يُطلق عليه أيضا اسم "رانسوموار الخبيث" العديد من الحواسيب حول العالم. ويعمل فيروس رانسوموار من خلال إرسال برمجيات دفع الفدية الخبيثة، التي تصيب الملفات في جهاز الحاسوب الشخصي حتى يدفع الضحايا مبلغا معينا (فدية) من المال للقراصنة.

من الناحية النظرية، يجب دفع الأموال عن طريق العملة الرقمية إلى مصدر غير معروف ليوفر الجاني للضحية مفتاح فك التشفير لإلغاء قفل النظام. والجدير بالذكر أن هذه البرمجية تستغل نقاط ضعف نظام "مايكروسوفت ويندوز" التي اكتشفتها من قبل وكالة الأمن القومي، ويبدو أنه تم تسريبها، في وقت لاحق، على الإنترنت.

وفي هذا الإطار، تعتقد المنظمة الدولية للشرطة الجنائية (الإنتربول) أن هذا الفيروس قد ضرب أكثر من 200 ألف شخص في أكثر من 150 بلدا. ويُتوقع أن تزداد الأمور سوءا، في الفترة المقبلة، حيث حذر الخبراء من أن العديد من العاملين في المكاتب يمكن أن يتفاجؤوا بقرصنة أجهزة الكمبيوتر الخاصة بهم في أي لحظة..

Here's what a London GP sees when trying to connect to the NHS network pic.twitter.com/lV8zXarAXS

— Rory Cellan-Jones (@ruskin147) May 12, 2017

هذا ما يراه الأشخاص عندما يحاولون الاتصال بشبكة هيئة الخدمات الصحية الوطنية

في الواقع، كان الهجوم حدثا عالميا لم يسبق له مثيل، إذ كانت المملكة المتحدة تعرضت أول بلد تعرض للاستهداف، حيث قام الفيروس بإغلاق أجزاء من برامج هيئة الخدمات الصحية الوطنية. في المقابل،

أفادت العديد من التقارير من جميع أنحاء العالم بتضرر الكثير من المستخدمين في الصين، وألمانيا، والهند، والولايات المتحدة.

في الساعات الأولى من الهجوم، كان العالم على وشك مواجهة اضطرابات تضرب صناعة السينما. بعد ذلك، وبمجرد أن بدأت عملية القرصنة السيبرانية، تم إيقاف العملية من قبل باحث الأمن السيبراني البريطاني، البالغ من العمر 22 سنة، الذي اكتشف "مفتاح تبديل القتل"، الذي يُمكنه وقف فيروس رانسوموار من الانتشار.

وعلى الرغم من النجاح النسبي الذي حققه هذا الباحث، إلا أن المخاطر لم تنته بعد. فيمكن لكل من يقف وراء الهجوم تحديث رانسوموار وإزالة مفتاح تبديل القتل. وفي الواقع، أشارت بعض التقارير الواردة حول هذه المسألة إلى أن هذا حدث بالفعل.

وفي شأن ذي صلة، تشير الدلائل إلى أن أهداف المهاجمين المجهولين كانت ربحية بحتة. وكانت الفدية المطلوبة من كل جهاز كمبيوتر مصاب لا تتجاوز 300 دولار أو نحو ذلك. ونتيجة لهذه الهجمة، أوصت السلطات بأن لا يدفع الضحايا، ولو حتى جزءا صغيرا من الفدية المطلوبة، التي من شأنها أن تتيح للمهاجمين جمع أموالا طائلة.

يمكن أن تكون هناك أهداف محتملة أخرى مثيرةً أكثر للقلق. يوم الأحد، لم ينفي وزير الدفاع البريطاني، مايكل فالون، الأنباء التي أفادت بأن الغواصات النووية البريطانية تستخدم نفس نسخة ويندوز التي جعلتها عرضة لهجمات هذه البرمجيات الخبيثة

وأيا كان الدافع، فإن النطاق الضخم للهجوم يدل على أن الأمن الإلكتروني يمكن أن يكون له عواقب جيوسياسية خطيرة. في بريطانيا، اضطرت بعض المستشفيات إلى صرف الكثير من المرضى وتأخير عملياتهم الجراحية. ونقلت هيئة الإذاعة البريطانية عن أحد العاملين في هيئة الخدمات الصحية الوطنية قوله إن هذا الهجوم كان بإمكانه أن يتسبب في "مجزرة كاملة" نظرا لأن "حياة المرضى، الذين كانوا سيخضعون لعملية قريبة الموعد، كانت على المحك، بسبب هذا الهجوم".

حتى اللحظة الراهنة، لم يتم التبليغ عن أي وفيات، ولكن هذا قد يتغير في أي لحظة. وفي هذا السياق، كتب مراسل صحيفة "فايننشال تايمز" تيم برادشو، يوم الأحد أن "تسجيل الوفاة الأولى التي تُعزى مباشرة إلى الهجوم إلكتروني قد تكون ممكنة في أي وقت". وأما إذا كان الهجوم قد نُفذ من قبل بلد معين وليس من قبل قراصنة مستقلين، فستعتبر الوفيات في تلك الحالة بمثابة "أعمال حرب".

في الحقيقة، يمكن أن تكون هناك أهداف محتملة أخرى مثيرةً أكثر للقلق. يوم الأحد، لم ينفي وزير الدفاع البريطاني، مايكل فالون، الأنباء التي أفادت بأن الغواصات النووية البريطانية تستخدم نفس نسخة ويندوز التي جعلتها عرضة لهجمات هذه البرمجيات الخبيثة. وتجدر الإشارة إلى أنه تم الإعراب عن مخاوف تعرّض أنظمة الكمبيوتر القديمة الخاصة بالغواصات، التي عفا عليها الزمن، إلى هجمة أخرى، إلا أن هذه الدعوات لم تلق استجابة من السلطات.

يمكن أن تؤدي هذه الهجمات إلى تفاقم التوترات بين الدول القومية. ففي روسيا مثلا، تعرضت وزارة الداخلية للهجوم من قبل واناكري، ويظن البعض أن الهجوم كان انتقاما أمريكيا للتدخل المزعوم لموسكو في الانتخابات الرئاسية

بالتالي، يجب على الأمريكيين أن يأملوا بأن تكون نظم القيادة والسيطرة النووية آمنة، ولكن من الممكن أن لا يكون ذلك مهما بالنسبة للولايات المتحدة. فعندما قام السيناتور بيل نيلسون بسؤال قائد القيادة الإستراتيجية الأمريكية، روبرت هيكلر، في سنة 2013، حول ما إذا كان بإمكان شخص ما اختراق نظام إطلاق الصواريخ النووية التابعة لروسيا أو الصين، حاول التهرب من الإجابة عن السؤال واكتفى بإجابة

غامضة قائلا "أنا لا أعرف...لا أعرف".

وحتى وإن لم تتحقق هذه السيناريوهات الكارثية، يُمثل الاستخدام واسع النطاق لبرمجية رانسوموار طريقا خطيرا يساهم في تمويل هذه الجماعات الإجرامية. وفي ذات هذا السياق، قال الخبير في إستراتيجية الأمن السيبراني في شركة بروفو بوينت، ريان كاليمبر، خلال لقاء أجراه السنة الماضية مع القناة الأمريكية "سي بي إس"، "لقد رأينا بعض الجماعات الإرهابية التي تمول منظماتها من خلال استخدام الجريمة السيبرانية وبرامج الفدية".

علاوة على ذلك، يمكن أن تؤدي هذه الهجمات إلى تفاقم التوترات بين الدول القومية. ففي روسيا مثلا، تعرضت وزارة الداخلية للهجوم من قبل واناكري، ويظن البعض أن الهجوم كان انتقاما أمريكيا للتدخل المزعوم لموسكو في الانتخابات الرئاسية، سنة 2016. وفي هذا الصدد، قال مدير معهد دراسات العولمة في روسيا ميخائيل ديلاجين، لصحيفة "نيويورك تايمز" إنه "يحترم أمانة الولايات المتحدة". وأضاف ديلاجين "لقد هدّدوا أمننا بالهجمات الإلكترونية، لذلك يجب أن يتوقعوا ردًا مماثلاً".

Thailand #WannaCry #Ranswomware #CyberSecurity
pic.twitter.com/uFfT99bv0x

— James McL □□□□□□□□□□□□□□□ □□□□ □□□□ (@JamesMcLeirigh) May 14, 2

لا شك أن واشنطن تتحمل جزء من المسؤولية في انتشار هذا الهجوم، نظرا لأن وكالة الأمن القومي كانت سباقة في اكتشاف ثغرة ويندوز الذي استغله رانسوموار. والجدير بالذكر أن مايكروسوفت أصدرت نشرة التصحيح عن الخلل بعد أن تم تسريب نقاط ضعف برمجية ويندوز هذه السنة، ولكن العديد من المستخدمين لم يقوموا بتحديث أنظمتهم.

وعلى ضوء هذه المعطيات، أشار مراسل التكنولوجيا في صحيفة واشنطن بوست، الذي يدعى براين فونغ، أن ما حصل كان درسا للسياسيين الذين يجب عليهم الاتعاظ. فضلا عن ذلك، إن مفهوم امتلاك وكالات تنفيذ القانون "الأبواب الخلفية" لبرامج ونظم الحاسوب، حتى لو كان ذلك لأسباب تتعلق بالأمن القومي، يزيد بشكلٍ كبيرٍ من خطر إيجاد الجماعات الإجرامية أو غيرها من الجهات الفاعلة السيئة لهذه الثغرات الأمنية.

وفي هذا الإطار، كتب فونغ في مقال نشره يوم السبت أن "الأمر سيكون مثل ترك المفاتيح تحت ممسحة الباب، مما يمكن أن يسمح للخيرين والأشرار باستخدامها". وقد أيّد رئيس مايكروسوفت، براد سميث، هذا الخط الفكري من خلال نشره لمدونة قوية يوم الأحد، أشار فيها إلى أن "هذا الهجوم يُظهر أن تخزين الحكومات لنقاط ضعف البرامج يُمثل مشكلة". ونتيجة لذلك، اقترح سميث أن يكون هناك شيء مثل "اتفاقية جنيف الرقمية" تعمل على تنظيم هذه القضايا.

إن لم تتخذ الحكومات إجراءات فورية، فإن العواقب قد تكون "غير متوقعة"، نظرا لأن هناك الكثير من الأشخاص والمؤسسات التي تعاني من ضائقة مالية؛ مثل هيئة الخدمات الصحية الوطنية، ولا تستطيع أن تفعل ذلك بمفردها

في حين، ذهبت الأكاديمية والكاتبة زينب توفيقي إلى أبعد من ذلك، مشيرة إلى أن العالم يحتاج إلى "إجراء إصلاح كامل لكيفية تشغيل وتعامل الشركات والحكومات والمؤسسات مع البرمجيات". فضلا عن ذلك، يتعين على الشركات مثل مايكروسوفت والوكالات الحكومية، مثل وكالة الأمن القومي أن تتخذ نهجا استباقيا للتعامل مع نقاط الضعف، وذلك وفقا لما كتبته في مقال في صفحات الرأي التابعة لصحيفة نيويورك تايمز الأمريكية.

وإن لم تتخذ الحكومات إجراءات فورية، فإن العواقب قد تكون "غير متوقعة"، نظرا لأن هناك الكثير من

الأشخاص والمؤسسات التي تعاني من ضائقة مالية؛ مثل هيئة الخدمات الصحية الوطنية، ولا تستطيع أن تفعل ذلك بمفردها. وفي الحقيقة، إن هجوم يوم الجمعة، يُظهر أن ما لا يمكن تصوره يمكن أن يكون حقيقة ملموسة.

المصدر: واشنطن بوست