المستقبل
للأبحاث والدراسات المتقدمة

اسم الموضوع : :"قراصنة " الويندوز

عنوان الموضوع : كيف كشفت هجمات "الفدية الخبيثة" ثغرات الأمن السيبراني؟

تاريخ النشر : 14/05/2017

اسم الكاتب : د. فاطمة الزهراء عبدالفتاح

الموضوع :

يُعد الهجوم الضخم الذي تعرضت له عشرات آلاف أجهزة الكمبيوتر في أكثر من 100 دولة حول العالم في 12 مايو 2017، تحولا جوهريًّا في نوعية تهديدات الأمن السيبراني، إذ في تعطيل تعاملات وخدمات مؤسسات متعددة وإعطاب شبكاتها وأجهزتها الإلكترونية، مما تسبب ،(Wanna Cry) التي يطلق عليها (Ransomware) تسببت برمجية الفدية الخبيثة في خسائر مالية ضخمة. ويكتسب هذا الهجوم طابعًا استثنائيًّا، ليس فقط لخطورة الهجمات التي وصفتها وكالة تطبيق القانون الأوروبية بأنها "لم يسبق لها مثيل"، وإنما أيضًا لما أفصحت عنه من دلالات بشأن ثغرات الأمن الرقمي العالمي.هجمات متوقعة!على الرغم من الضجة العالمية التي أثارتها الهجمات، إلا أن الواقع يكشف عن أنها لم تكن مفاجئة، وأن جماعة القرصنة المسؤولة عن الهجمات والتي تطلق على نفسها اسم "وسطاء الظل" سبق أن أعلنت في أغسطس 2016 أنها اخترقت وكالة الأمن القومي الأمريكي، واستحوذت على "أسلحة إلكترونية" قدّرتها بقيمة 500 مليون دولار، عارضة تلك البرمجيات الخبيثة للبيع في مزاد تحت اسم "مزاد الأسلحة السيبرانية لمجموعة التسوية".وعادت المجموعة مرة أخرى في إبريل 2017 لتبعث برسالة احتجاج ضد الرئيس الأمريكي "دونالد ترامب"، وتتيح مجموعة من الأدوات التجسسية التي سبق وأعلنت عنها مجانًا، كما أفصحت عن تفاصيل جديدة بشأن استحواذها على برمجيات استخدمتها وكالة الأمن القومي الأمريكية للتجسس على التحويلات المالية، مستغلة ثغرات في نظام تشغيل ويندوز، ما دفع شركة مايكروسوفت المنتجة للنظام للقول بأنها قامت بمعالجة تلك الثغرات الأمنية قبل بيان "وسطاء الظلال"، نافية إبلاغ وكالة الأمن الأمريكي أو أي جهة حكومية أخرى لها بشأن تلك الثغرات، ولكنها -في الوقت نفسه- لم لتضرب أجهزة الكمبيوتر في مختلف دول "Wanna Cry" تعلن عن مصدر اكتشافها لها.وعقب البيان الذي نشره "وسطاء الظل" على مدونة إلكترونية بنحو شهر، انطلقت هجمات العالم، وهو ما كان "متوقعًا" وفق وصف "ريان كاليمبر" الخبير المتخصص بشركة بروفبوينت للأمن السيبراني بعد التسريبات التي كشفت عنها المجموعة. ورغم تقديم مايكروسوفت تحديثات لعلاج الثغرات حثت المستخدمين على تحميلها، إلا أن العاملين بمجال الأمن تأكدوا من عدم إمكانية تحميل تلك التحديثات على نطاق كبير، خاصة مع انتشار استخدام نسخ أقدم من برمجيات الفدية الخبيثة التي تمنع الأجهزة من العمل أو استرجاع العمل حتى تدفع فدية معينة، حيث تظهر للمستخدم "Wanna Cry" مثل ويندوز "إكس بي".حجم الخسائر:يُعد واجهة إلكترونية تحمل عبارة "ملفاتك قد تم تشفيرها"، ورسالة تطالبه بتسديد فدية بمقدار 300 دولار باستخدام العملة الإلكترونية "بت كوين"، وذلك خلال ثلاثة أيام، وفي حال عدم الدفع يتم مضاعفة المبلغ مع التهديد بحذف الملفات كليًّا حال عدم الدفع خلال سبعة أيام.ووصل معدل انتشار الهجمات إلى خمسة ملايين رسالة في الساعة، وفق شركة "فورسبوينت سيكيوريتي" الأمنية، ومع نهاية اليوم الأول فقط من الهجمات أعلنت شركة "أفاست للأمن المعلوماتي" أنها رصدت أكثر من 75 ألف هجوم في 99 بلدًا، وهو العدد الذي تجاوز مائة دولة فيما بعد.ووفق هيئة الإذاعة البريطانية، شملت الهجمات دولاً من ضمنها: روسيا، والهند، والصين، وبريطانيا، وفرنسا، وإيطاليا، وألمانيا، والبرتغال، وفيتنام، وتايوان، ودولا أخرى، وهو ما اعتبره ميكو هايوبنين، رئيس الباحثين في شركة إف سيكيور للأمن الإلكتروني، أكبر تفشٍّ لبرمجيات الفدية الخبيثة في التاريخ، وفق وكالة الأنباء الفرنسية.وفي روسيا، تضررت وزارتا الداخلية والصحة، وشركة القطارات الروسية الحكومية، وثاني أكبر شركة للهواتف المحمولة، بالإضافة إلى بنوك محلية مختلفة. كما تعرضت 40 منظمة محلية بريطانية تابعة لنظام هيئة الرعاية الصحية وبعض العيادات لهجمات، وهو ما أسفر عن إلغاء بعض العمليات الجراحية. وتعرض عدد من الشركات الإسبانية الضخمة، مثل: تيليفونيكا، وشركة الطاقة إيبردرولا، وشركة غاز ناتورال، لهجمات. كما تضررت شركة تيليكوم البرتغالية وسكك الحديد الألمانية، فضلا عن مدارس وجامعات في الصين ومستشفيات في إندونيسيا.وفي فرنسا، أُجبرت شركة رينو لصناعة السيارات على إيقاف بعض خطوط إنتاجها إثر الهجمات، ما يُثير احتمالات مطالبة هذه الشركات "مايكروسوفت" بدفع تعويضات لزبائنها جراء الأضرار التي تكبدوها بسبب عيوب في أنظمتها.وبينما سادت حالة الطوارئ دول العالم لمعالجة تداعيات الهجمات، جاءت مواجهتها من مصدر غير متوقع، وهو باحث شاب مجهول الهوية يبلغ حيث اكتشف اعتماد القراصنة على نطاق غير مسجل، قام هو بشرائه بمبلغ 10.69 ،(Malware tech) من العمر 22 عامًا -وفق شبكة "سي إن إن"- بنشط على الإنترنت تحت اسم وهو خادوم يوفر تقنية للتضليل تعتمد على توفير بيانات خاطئة بشأن نطاق معين، ما يؤدي إلى فشل عملية الوصول إليه، (Sinkhole) دولارات فقط، ثم أعاد توجيهه إلى ما يُسمى الأمر الذي يجعله فعالا في الحد من البرمجيات الخبيثة.وعلى الرغم من بساطة هذا الإجراء، إلا أنه لعب دورًا كبيرًا في الحد من انتشار البرمجية الخبيثة، أخذًا في الاعتبار أنه أوقف فيما لا تزال هناك إصدارات أخرى من برمجية الفدية الخبيثة لا تتواصل مع ذلك النطاق الذي تم تضليله، ما يعني بقاء خطر التعرض ،(Wanna Cry) إصدار واحد من برنامج قائلا، إنه منع حدوث 100 ألف هجوم محتمل، إلا أنه أشار (Malware tech) للهجمات قائمًا.وقد نوّه مركز الأمن السيبراني البريطاني إلى أهمية دور الإجراء المضاد الذي ساهم فيه -في الوقت نفسه- إلى عدم قدرته على إصلاح آثار الهجمات التي حدثت بالفعل، لافتًا إلى ضرورة اتباع الاحترازات الأمنية ضد برمجيات الفدية الخبيثة التي سبق أن أصدر بشأنها دليلا في أكتوبر الماضي بعدما شهد النصف الأول من عام 2016 زيادة بمقدار ثلاثة أضعاف تقريبًا في برمجيات الفدية الخبيثة مقارنة بعام 2015 كاملا.الدلالات الأمنية:تحمل هجمات "وسطاء الظل" مجموعة من الدلالات الكاشفة عن ثغرات الأمن الرقمي العالمي، والتي يمكن عرضها فيما يلي:1- معضلة الدفاع السيبراني: على الرغم من الإمكانات الضخمة التي تتمتع على المستخدم الفرد الذي يقوم بفتح ،(ICANN) بها الدول العظمى، إلا أن أنظمتها الدفاعية الرقمية وقفت عاجزة أمام تلك الهجمات التي تعتمد في انتشارها، وفق منظمة الآيكان الدولية الرسائل الحاملة للفيروس. وفيما شن الهجمات جماعة قرصنة غامضة فقد استطاع مجابهته ناشط غامض أيضًا، فيما وقفت الأجهزة الأمنية الغربية عاجزة أمام الهجوم، لتعلن امتنانها للباحث الشاب، ما يكشف الفجوة الكبيرة بين أجهزة الحماية من جانب، وقراصنة الجريمة من جانب آخر.2- تهديدات احتكار المعلومات: اعتماد الهجمات على برمجيات تم تطويرها من قبل وكالة الأمن القومي الأمريكي اعتمادًا على ثغرات اكتشفتها في نظام تشغيل ذي انتشار عالمي، أثار الجدل بشأن مشروعية احتكار مثل تلك المعلومات التي لها تبعات مدمرة على الأمن العالمي، خاصة في ظل احتمالات تعرض تلك الجهات الأمنية للاختراق، ووقوع مثل تلك المعلومات في أيدي الجماعات الإجرامية كما هو الحال في تلك الهجمات. وقد أشار إدوارد سنودن، المتعاقد السابق مع وكالة الاستخبارات الأمريكية، إلى ذلك في تعليقه على الهجمات، والتي ألقى اللوم فيها على وكالة الأمن القومي الأمريكي التي لم تكشف عن الثغرات المتسببة فيها لحظة اكتشافها.3- مخاطر العملات الإلكترونية: على الرغم من التفاؤل بشأن دور تلك العملات في رواج الاقتصاديات الرقمية، إلا أن المجهولية وغياب الرقابة التشريعية والتنظيمية عن تلك المعاملات المشفرة يثير المخاوف بشأنها، لا سيما بعدما باتت وسيلة لتحصيل الفدية في حالة الهجمات الخبيثة، وأداة أيضًا لتمويل الجماعات الإرهابية، الأمر الذي يزداد خطورة مع تصاعد قيمتها حتى بلغت أعلى معدل لها هذا العام، بما يزيد عن 1758 دولارًا للكوين الواحد، لتتجاوز قيمة الذهب، مما يجعلها ملاذًا آمنًا للتعامل النقدي العابر للحدود، ومربحًا أيضًا لتلك الجماعات الإجرامية.4- استهداف المؤسسات الصحية: فالمنشآت التي تضررت لم تكن منشآت سياسية أو أمنية ودفاعية، وإنما تضررت منشآت اقتصادية بل وإنسانية مثل المستشفيات من جراء تلك الهجمات، الأمر الذي يحمل دلالات خطيرة بشأن الانهيارات الاقتصادية المحتملة لهجمات من هذا النوع ضد الأسواق المالية، أو المؤسسات المصرفية العالمية، وكذلك المخاطر البالغة حال استهداف بيانات المستشفيات والمراكز الطبية بهجمات إرهابية. يدعم ذلك ما أشار إليه تقرير آي بي إم – إكس فورس للأمن الرقمي لعام 2016، الذي كشف أن مؤسسات الرعاية الصحية باتت هي الأعلى تعرضًا للهجمات الرقمية. وقد أشار في وقت مبكر الباحث "بريان فولتز" إلى مخاطر استهداف المؤسسات المدنية على هذا النحو حينما افترض في دراسة له عام 2004 سيناريو لهجمة رقمية على بيانات مستشفى تتلاعب فقط ببيانات فصائل دم المرضى، مما يُودي بحياة المئات.5- دوافع مالية: على الرغم من الاتهامات بشأن وجود دوافع سياسية وراء هجمات وسطاء الظلال، إلا أن الأمر قد يكون ببساطة متعلقًا بالحصول على الأموال، أي غياب الدوافع الإرهابية أو المعارضة السياسية، وصعود دوافع التربح والابتزاز عبر جرائم رقمية، ويتسق ذلك مع ما أشار إليه تقرير قسم الجرائم الحاسوبية وقضايا الملكية الفكرية الأمريكي، من أن هناك 4000 هجوم من برمجيات الفدية الخبيثة يحدث يوميًّا منذ بدء عام 2016، وكذلك تقرير فيروزن للابتكار الرقمي حول التحقق من اختراق البيانات لعام 2016، والذي تضمن تحليل 100 ألف واقعة و2260 اختراقًا في 82 دولة، وقال إن 89% من الهجمات الإلكترونية تتضمن دوافع مالية أو تجسسية.6- هيمنة الشركات الكبرى: أحد أسباب الانتشار الكبير للبرنامج هو الاستخدام العالمي واسع النطاق لنظام ويندوز الذي تنتجه شركة مايكروسوفت، ما قد يؤشر إلى مخاطر الاحتكارات وسيادة نظم تشغيل واحدة في العالم، وهي الاتهامات التي طالما واجهتها الشركة بالفعل.التداعيات المستقبلية:أشار تقرير شركة ديل السنوي للتهديدات الأمنية في عام 2016 إلى أن البرمجيات الخبيثة تضاعف عددها إلى 8.19 مليارات، فيما أصبحت أنظمة أندرويد والذي يُغرق (DDOS) هي الأكثر استهدافًا، وفي أكتوبر 2016 تعرضت مواقع إنترنت كبرى -مثل: تويتر، وأمازون، وريديت- لهجوم من نوع الهجمات البرمجية لحجب الخدمات الخوادم بحركة مرور عالية تؤدي لتوقفها.وتدل تلك الهجمات المتسعة من حيث النطاق والمتنوعة الأهداف على تصاعد حدة الهجمات الرقمية حول العالم، وذلك عن طريق البرمجيات وشفرات حصان طروادة وغيرها، وهو ما قد يرجع لعدة أسباب، أهمها التوسع في استخدام الوسائط ،DDOS الخبيثة، مثل: الفيروسات الدودية، والهجمات البرمجية لحجب الخدمات الرقمية، سواء لتخزين المعلومات، أو إتمام المعاملات المالية، أو غيرها، وهو ما يجعل من المعلومة أمرًا قيمًا يستدعي الاستهداف، الأمر الذي واكبه تزايد في المهارات الرقمية لدى الجماعات الإجرامية.ويحمل ذلك التصاعد عدة تداعيات مستقبلية يُمكن استقراؤها في ظل ما كشفت عنه هجمات "وسطاء الظل"، أهمها احتمالات الاتجاه العالمي للضغط من أجل تفعيل تبادل المعلومات الأمنية الرقمية، وإعمال قواعد دولية للإفصاح حال وجود مخاطر محتملة واسعة النطاق، فضلا عن التزايد المحتمل للاستثمارات الموجهة لأبحاث الأمن الرقمي، سواء من جانب الحكومات أو الشركات التكنولوجية التي باتت تهددها مخاطر التعويضات، فضلا عن تدعيم التشريعات التي تجرم مثل تلك الهجمات، مع إدماج النشطاء الرقميين والشركات التكنولوجية والرواد التقنيين في تلك العمليات، والتي تفتح مجالا عريضًا أمام مخاطر أمنية جسيمة تستدعي تعزيز أواصر التعاون الإقليمي والدولي في مجال مكافحة الجريمة الإلكترونية في إطار من تشارك المعلومات وتبادل الخبرات دون تأثير على استقلالية القرار وأولوية المصلحة الوطنية.وعلى الرغم من أن ردود الفعل السائدة بشأن الهجمات تدعو إلى حتمية التعاون، وأهمية الإفصاح والتشارك؛ إلا أن عقبات السياسة والتصارع ستقف حتمًا عائقًا أمام ذلك الاتجاه، مما يؤكد أهمية الضغوط المجتمعية من أجل حث الحكومات على تجاوز حواجز الصراع بما يحد من هجمات تُنبئ كافة المؤشرات أنها في طريقها إلى الازدياد.