الحرب الإلكترونية: ليس معنى أن رؤوس أموالك في البنوك أنها في مأمن

كتبه عماد عنان | 14 مايو ,2017

حين تسأل أي من أصحاب رؤوس الأموال: أين تضع أموالك؟ فيكون الرد الجاهز تلقائيًا: في البنك؟ وحين تعيد عليه السؤال: هل أنت بمأمن حين تضع أموالك داخل البنوك؟ بالفعل سيكون الجواب: نعم، أما عن السبب في ذلك فسيكون: هناك أجهزة تأمين تقنية عالية المستوى تحفظ الأموال داخل محافظ عالية الجودة والأمان، فضلاً عن سرية المعلومات الخاصة بالعملاء والتي لا يستطيع أي أحد أن يطلع عليها بحكم الاتفاق الضمني الذي بينهم وبين إدارات البنوك.

ربما هذا الكلام كان منطقيًا لفترة من الفترات لكن اليوم بات من الصعب اليقين به بصورة كاملة، إذ إن أموال البنوك والمؤسسات المالية، سواء كانت مؤسسات خاصة أو حكومية أو حتى دولية لم تعد بمأمن عن السرقة عبر أي من صور القرصنة أو الهجمات الإلكترونية التي باتت اليوم شيئًا عاديًا.

وبات بمقدور حفنة من محترفي القرصنة أن يعيدوا رسم خارطة رؤوس الأموال في العالم، فالدول الفقيرة التي تعاني مؤسساتها المالية المركزية من خواء ربما تصبح بين ليلة وضحاها من أغنى الدول، فقد تمتلئ خزائن تلك المؤسسات بالمال دون أن تدري، والعكس تمامًا، وبإمكان جماعة ما لا تملك قوت يومها أن تصبح في ثوانٍ معدودات من أكثر الكيانات العالمية ثراءً، ومن ثم بات الحديث عن

تأمين رؤوس الأموال هنا أو هناك بصورة كاملة دربًا خياليًا لا زال عاجزًا أمام التقدم الملحوظ في آليات الهجمات الإلكترونية التي تتطور يومًا بعد الآخر.. إذًا أين يقع الخلل؟

هجمات الجمعة والفدية الخبيثة

لم يكن يتخيل أكثر القلقين بشأن خطورة الهجمات الإلكترونية أن يحدث الذي حدث في الجمعة الماضية الثاني عشر من مايو الحالي، سواء من حيث الكم أو التأثير، ففي ثوانٍ معدودات تعرض أكثر من 75 ألف جهاز حاسوب في نحو 99 بلدًا مختلفًا إلى هجمات إلكترونية متزامنة، في هجوم يعد الأول من نوعه، وهو ما أصاب الجميع – حكومات وأفراد – بالقلق حيال ما تحمله الأيام القادمة.

البداية تعود إلى الهجوم على عشرات الآلاف من أجهزة الحاسوب في العالم عبر برمجيات "الفدية الخبيثة" من نوع ransomware (رانزوم وير) والتي حملت اسم WannaCry (وانا كراي)، والتي تصيب الحاسوب بالشلل التام، فتشفر الملفات كافة داخل الحاسوب وتخفيها عن أعين صاحبها، وتستهدف بشكل أساسي الحواسب الآلية التي تعمل بنظام ويندوز التابع لشركة "مايكروسوفت"، ثم تقوم هذه البرامج بطلب فدية في مقابل فك تشفير بيانات الجهاز التي أصابتها.

حين يصاب الجهاز بهذه البرامج الخبيثة تظهر على الشاشة فورًا طريقة الدفع من أجل استعادة الملفات المشفرة، وتكون البداية بـ300 دولار مع بيان طريقة الدفع والتي تكون عادة عبر عملة يطلق عليها "البتكوين" وهي المتعامل بها بين القراصنة، وفي حال تأخر الدفع عن المدة المحددة والتي لا تتجاوز ثلاثة أيام يتم مضاعفة الفدية إلى 600 دولار، وفي حال تصميم صاحب الملفات على عدم الدفع خلال سبعة أيام فإنه بذلك سيفقد ملفاته المشفرة بصورة نهائية.

الملاحظة الأخطر في هجوم الجمعة أنه لم يستهدف قطاعًا بعينه أو دولة محددة، إذ إنه شمل 99 دولة على رأسها الولايات المتحدة، فرنسا، بريطانيا، إسبانيا، روسيا، كما أنه أصاب جهات متباينة ما بين مستشفيات وهيئات قطار ونقل عام ووزارات الداخلية وعدد من الجامعات، فضلاً عن استهداف بعض الشركات الكبرى وعلى رأسها فيدكس للبريد.

منظمات العالم الخاصة بالأمن المعلوماتي وصفت هذا الهجوم بأنه كان "بمستوى غير مسبوق" ويتطلب "تحقيقًا دوليًا لمعرفة المذنبين"، وعلى الرغم من عدم التوصل حتى كتابة هذه السطور إلى الفاعل الحقيقي وراء هذه الهجمات، فإن هناك إشارات إلى أن الجاني واحد، وهو ما يثير القلق، فذلك يعني أن هناك جهات ومؤسسات ضخمة تقف وراء هذا الحادث، فليس من المعقول أن يكون وراءه شخص بمفرده، وهذا يدفع إلى العودة للوراء قليلاً وبالتحديد إلى أبريل العام الماضي.. لماذا؟

برمجيات "الفدية الخبيثة" تستهدف بشكل أساسي الحواسب الآلية التي تعمل بنظام ويندوز التابع لشركة "مايكروسوفت"، ثم تقوم هذه البرامج بطلب فدية في مقابل فك تشفير بيانات الجهاز التي أصابتها.

طريقة دفع الفدية عقب تعرض الحاسوب لبرمجية WannaCry الخبيثة

ذي شادو بروكر

في أبريل من العام الماضي 2016 تمكن بعض القراصنة أطلقوا على أنفسهم "ذي شادو بروكو" من سرقة أدوات للقرصنة وبرامج خبيثة من وكالة الأمن القومي الأمريكية والتي نجحت في تحديد نقطة ضعف في أنظمة "مايكروسوفت" يمكن استخدامها في الهجوم الإلكتروني على الأجهزة التي تعمل بنظام الويندوز التابع للشركة العالمية.

ويبدو أن صانع السم لا بد أن يتذوقه، وهو ما حدث بالفعل، فبعد سرقة القراصنة لهذه البرامج الخبيثة، جعلوها متاحة بشكل مجانٍ أمام الجميع، وهو ما مهد إلى هجوم الجمعة الماضية، حيث أصيبت العديد من المؤسسات الأمريكية بتلك البرمجية الخبيثة التي كانت تعدها واشنطن للقرصنة على جهات أخرى غير معلومة.

ما فعلته وكالة الأمن القومي الأمريكية بشأن امتلاك أدوات وبرامج قرصنة يقود إلى الإشارة إلى توجه عالمي جديد يهدف إلى خلق كيانات استخباراتية معلوماتية موازية للحروب العسكرية والسياسية، وهو ما دفع بعض القوى الدولية إلى بناء جيوش إلكترونية موازية تسعى من خلالها إلى التصدي لهجمات الدول الأخرى، فهناك الجيش الصيني الإلكتروني، الجيش الإيراني الإلكتروني، وبعض الميليشيات الإلكترونية التابعة لبشار الأسد والتي يستخدمها في الهجوم على مواقع المعارضة.

الحرب الافتراضية على الإنترنت لا تقل شراسة أو خطورة عن الحرب العسكرية في ميادين المعارك، وقاذفات القنابل لا تقل في تأثيرها عن حروف الكيبورد، وأجهزة الرادارات العسكرية لا تختلف كثيرًا عن شاشات الحاسوب، والجنود المدربون ليسوا أكثر فتكًا بالخصوم من القراصنة والمحترفين الإلكترونيين.

وبعيدًا عن الأبعاد العسكرية أو السياسية أو الاستخباراتية في مضمار الحروب الإلكترونية يمكن العودة إلى ما بدأنا به هذا الموضوع والتساؤل عن مصير ومستقبل رؤوس الأموال في ظل هذا الفضاء الملبد بسحب الصراعات والهجمات الافتراضية غير المرئية.

الصين تعزز أمنها بوحدات عسكرية إلكترونية أطلق عليها "الجيش الصيني الإلكتروني"

ما مصير رؤوس الأموال؟

من الواضح أن الأساليب المعتمدة في التأمين على رؤوس الأموال داخل البنوك المركزية والخاصة والكيانات المالية العالمية لا بد أن يعاد النظر فيها مرة أخرى، إذ إنها باتت هدفًا سهلاً وصيدًا ثمينًا أمام القراصنة، ومن يستطيع اختراق مؤسسات الدفاع والأمن القومي في دول عظام كأمريكا وروسيا لا يجد صعوبة مطلقًا في اختراق أنظمة بيانات بنكية.

نجاح القراصنة خلال السنوات الماضية في الوصول إلى حسابات بعض المودعين داخل البنوك والأرقام السرية الخاصة بالمؤسسات المالية والبريد الإلكتروني الخاص بالشركات والهيئات الحكومية والدولية أثار القلق لدى الجميع، أفراد وحكومات، خاصة فيما يتعلق بإمكانية تطوير ذلك مستقبلاً مما يسمح لهم بإحكام السيطرة على حركة رؤوس الأموال بالعديد من الطرق الابتزازية المعروفة.

وهنا يمكن استعراض أبرز أنواع الهجمات الإلكترونية التي يتعرض لها الأفراد والمؤسسات والتي تهدف إلى التربح المادي من قبل القراصنة، وذلك من خلال مستويين رئيسيين:

الأول: الأفراد.. ففي الوقت الذي باتت معاملات الفرد فيه مع العالم الخارجي محصورة بصورة رئيسية باستخدام الإنترنت سواء فيما يتعلق بإدارة أعماله أو تحويلاته المادية، بات من السهل تعرضه للعديد من صور الجرائم الإلكترونية، ومنها:

* سرقة بطاقة الائتمان الخاصة به.

* نقل الحسابات المصرفية.

* نقل ملكيته للأسهم.

* التلاعب في الفواتير لحساب جهات أخرى.

* تعرضه للاحتيال والابتزاز من خلال سرقة هويته أو بريده أو بعض بياناته الشخصية.

الثاني: البنوك والشركات.. والتي أصبحت تدار بطريقة إلكترونية على شبكة الإنترنت، سواء الخاصة أو الحكومية أو الدولية، لا سيما فيما يتعلق بالتواصل بين الشركات الكبرى والمؤسسات البنكية عبر مختلف دول العالم، وهو ما يجعلها عرضة لبعض الجرائم الإلكترونية وفي مقدمتها:

* السطو الإلكتروني.

* التلاعب في حسابات الأفراد والمؤسسات وسرقتها.

* إجراء بعض التحويلات البنكية لحساب الغير.

* الابتزاز والاحتيال من خلال سرقة الحسابات الرسمية وقواعد البيانات الخاصة بالمؤسسة أو البنك.

* اختراق الموقع الإلكتروني الخاص بالبنك أو المؤسسة.

> نجاح القراصنة خلال السنوات الأخيرة الماضية في الوصول إلى حسابات بعض المودعين داخل البنوك والأرقام السرية الخاصة بالمؤسسات المالية أثار القلق لدى الجميع

سجل حافل بالقرصنة

استطاع القراصنة خلال السنوات القليلة الماضية أن يدشنوا سجلاً حافلاً بالجرائم والسرقات التي ما

كان يمكن أن تدور بخلد أكثر المتشائمين والمشككين بالأساليب التأمينية المتبعة في المؤسسات المالية العالمية، إذ تعرضت كيانات ذات أسماء لا يمكن التشكيك في قدراتها التقنية التأمينية لهجمات إلكترونية كبدتها مليارات الدولارات كخسائر، ونستعرض هنا أبرز تلك العمليات.

***"بنك جي بي مورجان"**

في يوليو 2014 تعرض أكبر بنوك الولايات المتحدة الأمريكية "جي بي مورجان" لخروقات معلوماتية وعمليات قرصنة هي الأخطر في التاريخ كله، حيث تم اختراق بيانات أكثر من 83 مليون حساب مصرفي، لما يقرب من 76 مليون أسرة، بمعنى أن كل أسرتين من إجمالي ثلاث أسر أمريكية تعرضتا لسرقة بياناتهم البنكية، فضلاً عن بيانات 7 ملايين شركة صغيرة، ليتعرض البنك حينها لأكبر عملية ابتزاز في التاريخ.

الفريق الأمني للبنك أعتقد في بداية الأمر أن الهجوم قد انتهى مع بدء اكتشافه وسارت الأمور بعدها بروتينية طبيعية، إلا أن تم الكشف فيما بعد أن العملية استمرت قرابة شهرين كاملين دون أن يكتشف أحد هذا إلا في أواخر سبتمبر من نفس العام، مما كان له أثر سيء على نفوس المتعاملين بالبنك وعملائه.

83 مليون حساب مصرفي تم سرقتهم من بنك جي بي مورجان الأمريكي عام 2014

*** البنك المركزي لبنجلاديش**

في فبراير 2016 تعرض البنك المركزي لدولة بنجلاديش إلى عملية قرصنة إلكترونية تم بموجبها سرقة نحو 81 مليون دولار من حساب البنك وتم تحويلها لحساب البنك المركزي الأمريكي المعروف بـ"البنك الاحتياطي الفيدرالي" وذلك حسبما أكدت مؤسسة الاتصالات المالية بين المصارف حول

العالم.

*** وكالة الأمن القومي الأمريكي**

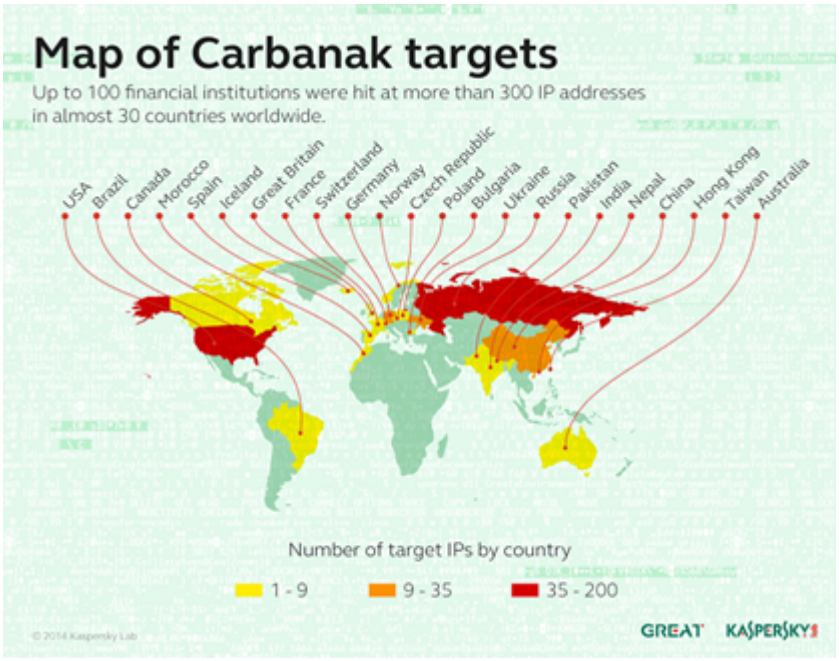
كما تم ذكره سابقًا، ففي أبريل عام 2016 تمكن مجموعة من القراصنة أطلق عليهم "ذي شادو بروكو" من سرقة أدوات للقرصنة وبرامج خبيثة من وكالة الأمن القومي الأمريكية، قيل حينها إن واشنطن تستخدمها في تخريب البرنامج النووي الإيراني.

وفي أغسطس من نفس العام تقدم القراصنة بعرض للحكومة الأمريكية مفاده تقديم ما بحوزتهم من البرامج الخبيثة المسروقة مقابل الحصول على 580 مليون دولار، لتقع وكالة الأمن الأمريكي هي الأخرى في فخ النصب والابتزاز.

*** Carbanak cybergang**

في فبراير 2015 تمكن بعض القراصنة من اختراق الأنظمة والحسابات المالية الخاصة بعدد من البنوك فيما يقرب من 30 دولة حول العالم منها الولايات المتحدة واليابان وروسيا وسويسرا، وذلك عبر استخدام برنامج قرصنة يطلق عليه "Carbanak cybergang" وقد تم تسمية العملية نسبة إلى هذا البرنامج.

العملية بدأت باختراق أجهزة الحاسوب واحد تلو الآخر، ثم يتم إرسال الأموال إلى أجهزة الصراف الآلي ليتم الحصول عليها بشكل أوتوماتيكي من قبل القراصنة، وقيل حينها إن هذه العملية انتهت بمحصلة قاربت المليار دولار واستغرقت نحو عامين تقريبًا.



خارطة بالبنوك التي استهدفتها عملية"Carbanak cybergang " عام 2015

*** SQL injections**

ما بين 2005 و2007 نجح فريق من القراصنة بقيادة "ألبرتو جونزاليس" في الاستيلاء على ما يقرب من 170 مليون رقم من أرقام الصراف الآلي وبطاقات الائتمان ثم إعادة بيعها في مزاد علني.

العملية أطلق عليها حينها اسم (SQL injections) ونجحت في تحقيق مكاسب مادية طائلة من وراء بيع هذه الأرقام، وحين ألقي القبض على جونزاليس عام 2008 أخبر المحكمة أنه يعمل لحساب جهاز الخدمات السرية الأمريكية، لكن المحكمة حينها لم تأخذ برأيه وحكمت عليه بالسجن 20 عامًا.

3 تريليون دولار خسائر

قد يرى البعض أن الخسائر الناجمة عن القرصنة الإلكترونية ربما لا تمثل شيئًا في حجم رأس المال العالمي، لكن حين نتتبع المنحنى العام لعلميات القرصنة نجد أن الأمر غاية في الخطورة لا سيما أنه سار في طريقه نحو الصعود رغم الجهود الأمنية والتأمينية التقنية المبذولة لتطويقه.

في "منتدى 2017" للأمن الاستخباراتي، كشف نائب مدير مركز رصد معلومات تابع لهيئة الأمن الفيدرالي الروسية، نيكولاي موراشوف، أن "خسائر العالم في السنوات الأخيرة، تقدر بحسب أساليب تقييم مختلفة، من 300 مليار إلى تريليون دولار" وأضاف "هذه المؤشرات تميل إلى طابع النمو المتزايد".

الخطير في تصريحات المسؤول الأمني الروسي أن الخسائر الناجمة عن القرصنة تشكل نسبة تقدر ما بين 4 – 5.1% من إجمالي الناتج العالمي، وهو ما يعد مؤشرًا كارثيًا يستوجب التدخل الفوري من دول العالم كافة على حد قوله.

أما عن توقعات ما يمكن أن تؤول إليه خارطة القرصنة الإلكترونية مستقبلاً فقد كشف عنه المدير التنفيذي لمؤسسة أوبن ثينكينغ للتدريب، إياد مرتضى، على هامش مشاركته في مؤتمر مكافحة الاحتيال بالشرق الأوسط في دبي العام الماضي، أن الخسائر الناجمة عن تلك العمليات قدرت بنحو 450 مليار دولار نهاية 2016.

الخبير المعلوماتي حذر من أن حجم تلك الخسائر من المرجح أن يصل إلى 3 تريليون دولار بحلول عام 2020، إذا لم تتخذ الحكومات التدابير اللازمة لمواجهة هجمات القرصنة الإلكترونية، متوقعًا أن يكون لدول الخليج نصيبًا كبيرًا من هذه العمليات لا سيما في قطاعات الخدمات المالية والنفط والغاز.

الخسائر الناجمة عن القرصنة تشكل نسبة تقدر ما بين 4 – 5.1% من إجمالي الناتج العالمي، وهو ما يعد مؤشرًا كارثيًا يستوجب التدخل الفوري من دول العالم كافة

العالم في خطر

ماذا لو نجحت الجماعات المسلحة التي تستهدف بعض الكيانات والحكومات في الحصول على تلك التقنية العالية التي تؤهلها للقرصنة والاستيلاء على الأموال من هنا أو هناك؟ وماذا لو زودت بعض الكيانات الاستخباراتية الدولية عددًا من تلك الجماعات بمثل هذه التقنية بهدف دعمها لتحقيق أهداف ما في منطقة معينة؟ هل يمكن بعدها أن يكون العالم في مأمن؟

إن المعضلة الأساسية التي تواجه تلك الجماعات تكمن في المقام الأول في التمويل المادي، وبالحصول على مثل هذه التقنية بات من السهل الحصول على المال اللازم لقيام الجماعات بالعمليات الخاصة بها، وهو ما يجب أن يوضع في الاعتبار، إذ إن الجهود العالمية المبذولة لمكافحة مثل هذه الكيانات المسلحة ستدخل نفقًا مظلمًا من التحديات التي قد لا تقوى على مجابهتها.

ومن ثم يبدو أن هجوم الجمعة الماضي لن يكون الأخير، لكنه جرس إنذار، ورسالة شديدة اللهجة، إذ إن الحرب الإلكترونية لم تعد خيارًا أمام الدول والحكومات، بل باتت أمرًا وقعيًا وعلى الجميع أن يعيد النظر في السياسات والإجراءات التأمينية المتبعة، حتى لا تجد الشعوب والكيانات الدولية نفسها ضحية مثل هذه العمليات.

رابط المقال : https://www.noonpost.com/17973/