صناعة
الجريمة الإلكترونية

القراصنة الفرديون يقيمون أعمالا ناضجة

تاماس غيدوش

أصبحت الجريمة الإلكترونية الآن صناعة ناضجة تقوم على مبادئ تتشابه كثيرا مع مبادئ الأعمال المشروعة سعيا إلى تحقيق الربح. ومكافحة انتشار الجريمة الإلكترونية يعني إعاقة نموذج أعمال يستخدم أدوات سهلة الاستخدام لتوليد أرباح عالية بمخاطر منخفضة.

وقد ولت منذ زمن بعيد أسطورة القراصنة الفرديين الذين ظهروا في أواخر ثمانينات القرن الماضي والذين كان تباهيهم بمهاراتهم المتقدمة جدا في استخدام الكومبيوتر هو السبب الرئيسي لاقتحام أجهزة كومبيوتر الآخرين. وأدى التحول إلى تحقيق الربح، الذي بدأ في تسعينات القرن الماضي، يسيطر تدريجيا على ساحة القرصنة لإنشاء صناعة الجريمة الإلكترونية التي نعرفها اليوم، والتي تتميز بجميع سمات الأعمال العادية، بما في ذلك الأسواق والتبادلات والمشغلون المتخصصون ومقدمو الخدمات الخارجيون وسلاسل الإمداد المتكاملة، وما إلى ذلك. واستخدمت العديد من الدول التكنولوجيا نفسها لتطوير أسلحة إلكترونية عالية الفعالية لجمع المعلومات الاستخباراتية والتجسس الصناعي وتعطيل البنى التحتية الضعيفة للأعداء.

التطور

انتشرت الجريمة الإلكترونية على الرغم من أن العدد المتاح من المتخصصين ذوي المهارات العالية لم يواكب وتيرة زيادة التقدم التقني المطلوب لنجاح القرصنة المربحة والإفلات من العقاب. وقد أدى تطور الأدوات والتشغيل الآلي إلى سد هذه الفجوة. فقد تطورت أدوات القرصنة تطورا هائلا على مدى العقدين الماضيين. ففي تسعينات القرن الماضي، انتشر في المهنة ما يطلق عليه اسم اختبار الاختراق من أجل إيجاد مواطن ضعف في أي نظام حاسوبي. وكانت معظم الأدوات المتاحة في ذلك الوقت بسيطة، وكثيرا ما كانت مصممة لغرض بعينه، ويتطلب استخدامها معرفة كبيرة بالبرمجة وبروتوكولات الشبكات والخصائص الداخلية لنظم التشغيل وغيرها من الموضوعات الأخرى التقنية للغاية. ونتيجة لذلك، لم يكن بوسع إلا عدد قليل من المهنيين اكتشاف مواطن ضعف يمكن استغلالها والاستفادة منها.

ومع تحسن الأدوات وزيادة السهولة في استخدامها، بدأ الشباب الأقل مهارة ولكن الأكثر حماسا — الذين يطلق عليهم الاسم الساخر «أطفال البرمجيات» في استخدام تلك الأدوات بنجاح إلى حد ما. والآن، أصبح إطلاق عملية التصيد الاحتيالي — أي الممارسة الاحتيالية المتمثلة في إرسال بريد إليكتروني يبدو من مُرسِل موثوق به لخداع الناس بحيث يكشفوا عن معلومات سرية — لا يتطلب إلا فهما بسيطا للمفاهيم والاستعداد وبعض الأموال النقدية. فقد أصبحت القرصنة سهلة التنفيذ (راجع الرسم البياني).

ومن الصعب للغاية تحديد حجم المخاطر الإلكترونية من الناحية الكمية. فبيانات الخسارة شحيحة وغير موثوقة، ويرجع ذلك في جزء منه إلى ضعف الحافز على الإبلاغ عن خسائر الجرائم الإلكترونية، ولا سيما إذا لم تؤد الحادثة إلى تصدر عناوين الأخبار أو إذا لم يكن هناك تأمين يغطي الخسائر الإلكترونية. ويجعل الطابع المتطور بسرعة للتهديدات البيانات التاريخية أقل أهمية في توقع الخسائر في المستقبل.

وتؤدي النماذج القائمة على السيناريوهات التي تحسب تكاليف الحوادث المحددة جيدا التي تؤثر على بعض الاقتصادات إلى تقديرات تصل إلى عشرات أو مئات المليارات من الدولارات. وتشير تقديرات شركة لويدز القائمة في لندن إلى أن خسائر انقطاع الخدمة السحابية لمدة يومين ونصف إلى ثلاثة أيام في الاقتصادات المتقدمة قدرها ٥٣,٠٥ مليار دولار. وتشير عملية إعداد النماذج في الصندوق إلى أن الخسائر الإجمالية السنوية تبلغ في الحالة الأساسية ٩٧ مليار دولار في المتوسط، وتصل في سيناريو أسوأ الحالات إلى حوالي ٢٥٠ مليار دولار.

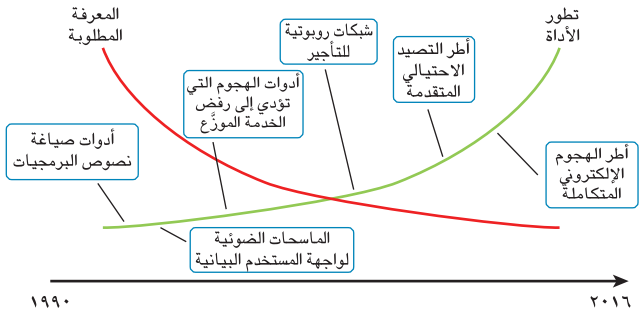
الأسباب والانعكاسات

عادة ما تكون الجريمة في العالم المادي — بهدف كسب المال — مدفوعة بمجرد تحقيق ربح أكبر من الذي تحققه الأعمال المشروعة، وهو ما يراه المجرمون كتعويض على

الرسم التوضيحي: VAIREEEL/ISTOCK/UGURHAN

لـعبة أطفال

تتطلب القرصنة معرفة فنية أقل مع تطور الأدوات، وأصبح الآن من الأسهل بكثير نجاح القرصنة.



المصدر: جامعة كارنيغ ميلون.

تحمل المخاطر العالية. وفي عالم الجريمة الإلكترونية، يمكن تحقيق أرباح مماثلة أو أعلى بمخاطر أقل بكثير: احتمال أقل أن يتم إلقاء القبض عليك ونجاح محاكمتك وتقريبا لا توجد مخاطر إطلاق النار عليك. وتشير التقديرات إلى أن أرباح التصيد الاحتيالي تصل إلى مئات أو حتى أكثر من ألف نقطة مئوية. ولا يمكن أن نتوقع إلا الأرباح الناجمة عن سرقة الملكية الفكرية والتي ترتكبها الجهات الأكثر تطورا التي تطلق التهديدات الإلكترونية. إلا أن الأساسيات مماثلة: تنشئ الأدوات الفعالة والنسبة الضخمة للمخاطر إلى المكافأة حالة مقنعة وتفسر في النهاية الزيادة الحادة في الجريمة الإلكترونية وتحولها إلى صناعة.

وتؤدي الجريمة الإلكترونية إلى مخاطر نظامية في كثير من الصناعات. وبينما تتأثر الصناعات المختلفة بطرق مختلفة، فمن المرجح أن تكون أكثر الصناعات عرضة للجريمة الإلكترونية هي القطاع المالي. وهناك تهديد جديد نسبيا من القائمين بالهجمات بدافع التدمير. فعندما يسعون إلى زعزعة استقرار النظام المالي، فإنهم ينظرون إلى أكثر الأهداف الواعدة. وتعتبر البنية التحتية للسوق المالية هي الأكثر ضعفا بسبب دورها المحوري في الأسواق المالية العالمية. ونظرا لاعتماد القطاع المالي على مجموعة صغيرة نسبيا من النظم التقنية، يمكن أن تنتشر التأثيرات غير المباشرة الناتجة عن التخلف أو التأخر عن السداد بسبب نجاح الهجمات، مما يمكن أن يكون له انعكاسات على النظام نفسه.

وبالنظر إلى الارتباط المتأصل بين المشاركين في القطاع المالي، فإن انقطاع نظم المدفوعات أو المقاصة أو التسوية — أو سرقة المعلومات السرية — يمكن أن يسفر عن تداعيات واسعة النطاق ويهدد الاستقرار المالي.

ولحسن الحظ، فإننا لم نشهد حتى الآن هجمة إلكترونية أثرت على النظام بأكمله. غير أن قلق صناع السياسات والهيئات التنظيمية للقطاع المالي آخذ في الازدياد في ضوء الحوادث التي وقعت في الفترة الأخيرة التي عطلت عمل شبكات أجهزة الصرف الآلي والهجمات التي وقعت ضد النظم المالية القائمة على الإنترنت والبنوك المركزية ونظم المدفوعات.

وقد اعتمد القطاع المالي على تكنولوجيا المعلومات لمدة عقود واحتفظ على مر التاريخ ببيئات قوية لضوابط تكنولوجيات المعلومات المفروضة بموجب القواعد التنظيمية. وبينما قد يكون القطاع المالي الأكثر عرضة للهجمات الإلكترونية، فإن هذه الهجمات تنطوي أيضا على زيادة المخاطر للمجرمين الإلكترونيين، ويرجع ذلك في جزء منه إلى زيادة الاهتمام من جانب القائمين بإنفاذ القانون (شأنها شأن سرقات البنوك بالطريقة القديمة). ويقوم القطاع المالي أيضا بعمل أفضل في مجال دعم إنفاذ القانون — على سبيل المثال عن طريق الاحتفاظ بسجلات كثيرة مفيدة في التحقيقات الجنائية. ويمكن أن تؤدي الميزانيات الكبيرة في كثير من الأحيان إلى حلول فعالة بشأن الأمن الإلكتروني. (من الاستثناءات البارزة مؤخرا شركة Equifax التي يقال إن القرصنة التي تعرضت لها كانت نتيجة القواعد التنظيمية الإلكترونية التي لم تكن متناسبة مع المخاطر التي تتعرض لها).

ويختلف الوضع في مجال الرعاية الصحية. فباستثناء أغنى الدول، عادة ما يفتقر قطاع الرعاية الصحية إلى الموارد اللازمة للدفاع الإلكتروني الفعال. ويتضح ذلك مثلا من الهجمات ببرمجيات طلب الفدية التي حدثت هذا العام واستهدفت نظم الحاسوب في شركة السجلات الصحية الإلكترونية Allscripts ومستشفيين إقليميين في الولايات المتحدة. وعلى الرغم من أن قطاع الرعاية الصحية يخضع أيضا إلى تنظيم شديد وقواعد صارمة بشأن حماية البيانات، فإنه لم يعتمد على تكنولوجيا المعلومات بنفس القدر الذي اعتمد عليه القطاع المالي وبالتالي لم تتطور فيه نفس ثقافة الضوابط الصارمة بشأن تكنولوجيا المعلومات. وهذا ما يجعل أيضا قطاع الرعاية الصحية أكثر عرضة للاختراقات الإلكترونية. والأكثر مدعاة للقلق إزاء هذا الضعف هو أنه على خلاف القطاع المالي، يمكن أن تُفقد الأرواح إذا ضرب القائمون بالهجمات نظم الحاسوب التي تعمل على الحفاظ على الحياة.

ويشار كثيرا إلى قطاع المرافق، وخاصة شبكات الكهرباء والاتصالات، على أنه القطاع التالي الذي يمكن أن يكون للهجمات الإلكترونية واسعة النطاق عواقب وخيمة عليه. غير أن الشاغل الرئيسي في هذه الحالة هو تعطيل النظم أو

التعاون الدولي في مجال مكافحة الجريمة الإلكترونية والملاحقة القضائية لمرتكبيها يتأخر كثيرا عن الطابع العالمي للتهديد.

اختراقها من جانب الدول المتنافسة، إما بطريقة مباشرة أو من خلال منظمات بديلة. وعلى النحو الذي أظهره المثال الشهير للهجمة الضخمة على البنية التحتية للإنترنت في إستونيا في عام ٢٠٠٧ — التي عطلت الخدمات المالية ووسائل الإعلام والوكالات الحكومية القائمة على الإنترنت — كلما كان الاقتصاد متقدما وقائما على الإنترنت، كلما يمكن أن تكون الهجمات الإلكترونية مدمرة. وإستونيا من أكثر المجتمعات الرقمية في العالم (راجع «إستونيا الإلكترونية تنطلق» في عدد مارس ٢٠١٨ من مجلة التمويل والتنمية).

التدابير المضادة

إذا تعرضت البنية التحتية الحيوية — مثلا شبكات الطاقة أو الاتصالات أو النقل — لهجمة أو أدت هجمة ما إلى تعطيل الحكومة عن تحصيل الضرائب أو تقديم الخدمات الضرورية، يمكن أن يلي ذلك اضطرابات كبرى ذات انعكاسات نظامية اقتصادية ومن المحتمل أن يؤدي ذلك إلى أخطار للصحة العامة والأمن. وفي مثل هذه الحالات، يمكن أن تتجاوز المخاطر الإجمالية التي يتعرض لها الاقتصاد العالمي مجموع المخاطر الفردية بسبب الطابع العالمي لشبكات ومنصات تكنولوجيا المعلومات، أو الطابع الوطني لهياكل الاستجابة، أو التعاون غير الفعال على المستوى الدولي، أو حتى وجود دول بين مرتكبي الهجمات.

والتعاون الدولي في مجال مكافحة الجريمة الإلكترونية والملاحقة القضائية لمرتكبيها يتأخر كثيرا عن الطابع العالمي للتهديد. وأفضل طريقة لمكافحة الجريمة الإلكترونية تتمثل في الهجوم على نموذج أعمالها الذي يعتمد على النسبة الضخمة للمخاطر إلى المكاسب والتي تصاحبها الملاحقة القضائية غير الفعالة. وفي هذا السياق، يجب رفع مخاطر أعمال الجريمة الإلكترونية بشكل كبير، ولكن هذا غير ممكن إلا بتعاون دولي أفضل.

ويمكن أن تمتد عمليات الجرائم الإلكترونية عبر الكثير من مناطق الاختصاص مما يجعل من الصعب مكافحتها وملاحقة مرتكبيها. وتكون بعض مناطق الاختصاص بطيئة أو غير فعالة أو تكون مجرد غير متعاونة في مكافحة الجريمة الإلكترونية. ومن شأن التعاون الأكثر قوة أن يزيد من سرعة تتبع المشتبه بهم وتوجيه التهم إليهم وأن يجعل التتبع أكثر فعالية.

وفي القطاع المالي، طورت الهيئات التنظيمية معايير محددة للتقييم، ووضعت توقعات ومعايير مرجعية قابلة للإنفاذ، وشجعت تبادل المعلومات والتعاون بين الشركات والهيئات التنظيمية. وتضطلع الهيئات التنظيمية المعنية بالمصارف بفحوص تكنولوجيا المعلومات التي تدمج مدى استعداد الأمن الإلكتروني في اختبارات القدرة على تحمل الضغوط، وتخطيط عمليات التسوية، والسلامة والرقابة السليمة. وتقتضي بعض الهيئات التنظيمية إجراء عمليات محاكاة للهجمات الإلكترونية تكون مصممة تحديدا لكل شركة، استنادا إلى معلومات وخبرة من الحكومة أو القطاع الخاص، لتحديد القدرة على الصمود أمام أي هجمة. ورفعت الشركات أيضا الاستثمارات في مجال الأمن الإلكتروني وأدمجت الاستعداد للهجمات الإلكترونية في إدارة المخاطر. وبالإضافة إلى ذلك، لجأت بعض الشركات إلى تحويل بعض المخاطر عن طريق التأمين الإلكتروني.

ولا تزال ساحة الأمن الإلكتروني الحالية متفاوتة ولامركزية ويتم التعامل مع المخاطر أساسا على أنها مشاكل فردية محلية. وهناك بعض آليات التعاون، وتُضاعِف الحكومات والهيئات التنظيمية جهودها، ولكن يُحدد اختيار الأمن الإلكتروني إلى حد كبير بالحاجة المؤسسية — «الكل بمفرده.» ويجب أن يتغير هذا الوضع لبناء القدرة على مواجهة المخاطر الإلكترونية عموما. وهناك حاجة إلى تدابير وقائية قوية على مستوى القواعد التنظيمية وعلى المستوى التكنولوجي وعبر الصناعات. ومن أهم هذه التدابير هي الالتزام بحد أدنى من معايير الأمن الإلكتروني التي تنفذها الهيئات التنظيمية بشكل منسق. وسيساعد التدريب على زيادة الوعي بالأمن الإلكتروني في الدفاع ضد مواطن الضعف التقنية الأساسية وأخطاء المستخدمين التي تشكل مصدر معظم الاختراقات.

ويبدو أنه لا مفر من الهجمات الإلكترونية واختراقات الأمن الإلكتروني، ولذا علينا أن نركز أيضا على سرعة اكتشافنا للاختراقات، ومدى فعالية استجابتنا، والسرعة التي نعيد بها العمليات إلى مسارها الطبيعي. FD

تاماس غيدوش، كبير خبراء القطاع المالي في إدارة الأسواق النقدية والرأسمالية بصندوق النقد الدولي، وهو من المهنيين المعنيين بالأمن الإلكتروني ولديه خبرة تزيد عن ٢٠ عاما، بما في ذلك في فحص النظم المصرفية للعثور على مواطن ضعف إلكتروني. وتولى من قبل الدور القيادي في إدارة الإشراف على تكنولوجيا المعلومات في البنك المركزي في هنغاريا.