المستقبل
للأبحاث والدراسات المتقدمة

اسم الموضوع : تمدد عالمي:

عنوان الموضوع : اقتصاديات الجريمة السيبرانية.. الملامح ودورة العوائد

تاريخ النشر : 08/07/2018

اسم الكاتب : مروان صالح

الموضوع :

إلى أن متوسط تكلفة اختراق البيانات سيتجاوز 150 مليون دولار بحلول عام 2020، (Juniper) تُعد الجريمة السيبرانية من أكبر التحديات التي تواجه العالم، حيث تشير شركة جونيبر وستكلف الجريمة السيبرانية الشركات أكثر من 2 تريليون دولار بحلول عام 2019، أي بزيادة أربعة أضعاف عن عام 2015. وتهدد الجريمة السيبرانية الملايين من المستخدمين على شبكة الإنترنت، خاصة وأن العدد الإجمالي للهجمات ينمو عامًا بعد عام، ومعه يزداد الضرر المحتمل من الهجمات السيبرانية. وقد أصبح تخطيط وتنفيذ هجمات القرصنة أكثر سهولة بسبب اهتمام ومتابعة القراصنة للتطورات السريعة في مجال الأمن السيبراني وأسلحته الرقمية، وتحول الجريمة السيبرانية إلى اقتصاد إجرامي ذي عائد ضخم ومخاطر منخفضة نسبيًّا مقارنة بأشكال الجريمة الأخرى.وقد تركز الاهتمام في البداية على آليات الجريمة السيبرانية وتقنياتها، والثغرات الأمنية وكيفية التصدي لها، بيد أنه في الآونة الأخيرة تزايد الاهتمام بالأبعاد الاقتصادية لهذا الأمر، لأنه يلقي الضوء على كيفية توليد عائدات الجريمة السيبرانية، ويساعد على فهم أفضل لتلك الأنظمة التي تدعم الجريمة السيبرانية وتساهم في تمددها.عائدات ضخمة:تطورت الجريمة السيبرانية إلى حد أنها أصبحت منظومة اقتصادية مستقلة لها ديناميات مشابهة للقطاعات الاقتصادية. وترصد دراسة مولتها شركة "برورميوم" تعقيد مكونات اقتصاد الجريمة السيبرانية، فهي تشمل: عمليات القرصنة التي ينتج عنها إيرادات، Surrey، "الأمريكية بالتعاون مع الدكتور "مايكل ماجواير" المحاضر في جامعة "سري واستخدام العملات الرقمية وأدوات صرفها، بالإضافة إلى وجود مجموعة من الوكلاء المتخصصين مثل المنتجين والموردين للبرمجيات الخبيثة ومقدمي خدمات القرصنة، وتوافر القدرة على استخراج وتبادل البيانات، ووجود أسواق مخصصة ليس فقط للمواد غير المشروعة مثل المخدرات والأسلحة النارية والبيانات المسروقة أو الأسرار التجارية بل أيضًا للسلع والخدمات المزيفة والهويات المسروقة إلى درجة تصل إلى وجود أشخاص يتولون صناعة الأخبار الكاذبة بما يخدم هذه الجريمة.وتقدر الدراسة عائدات الجريمة السيبرانية بما يعادل 1.5 تريليون دولار على الأقل سنويًّا، وهو ما يعني أن إيراداتها تتجاوز عائدات الشركات الكبرى، وتعتبر الأسواق الرقمية غير المشروعة والتي يوجد معظمها على الشبكة المظلمة أكثر الأسواق ربحية، حيث يقدر حجم أرباحها بحوالي 860 مليار دولار، وتليها إيرادات سرقة الأسرار التجارية والصناعية والملكية الفكرية بما يقدر بحوالي 500 مليار دولار، وتجارة بيانات المستخدمين المسروقة بحوالي 160 مليار دولار، ثم خدمات القرصنة بحوالي 1.6 مليار دولار وبرمجيات الفدية بما يعادل مليار دولار.وتُشير الدراسة إلى عددٍ من الإحصائيات الهامة. فعلى سبيل المثال، تتراوح أرباح بيع معلومات بطاقات الائتمان ما بين 250 ألف دولار إلى مليون دولار أمريكي، وأن سرقة المحتوى من المواقع يحقق ما يقرب من 227 مليون دولار، بالإضافة إلى أن ذلك يحقق للقراصنة حوالي 521 ألف دولار سنويًّا من بيع أجهزة البث التي توفر الوصول إلى الأفلام والمسلسلات التلفزيونية وغيرها بشكل غير قانوني. وتُشير بعض التقديرات إلى أن القراصنة المحترفين من ذوي الدخل المرتفع يحصلون على ما يقارب 166 ألف دولار أمريكي شهريًّا، فيما يتراوح دخل القراصنة الأقل احترافًا ما بين 75 ألف دولار إلى حوالي ثلاثة آلاف دولار شهريًّا.كما تؤكد الدراسة أن عوائد جرائم الإنترنت يشكل وبحد أدنى من 4٪ إلى 10٪ من إجمالي الأموال التي يتم غسلها في العالم، حيث تصل قيمتها إلى حوالي 200 مليار دولار، ويلجأ القراصنة في غسيل أموالهم الناتجة عن الجريمة السيبرانية إلى عدة طرق، منها: الاستخدام غير المشروع للنظام المصرفي، حيث يمكن للقراصنة استغلال البنوك كأحد الطرق لغسيل مكاسبهم بسبب تعاون بعض موظفي البنوك معهم، واستخدام الشركات الوهمية التي تزايد عددها في مناطق كثيرة حول العالم. بالإضافة إلى الاستثمار في العقارات أو الأراضي أو حتى في بعض الصناعات الحيوية. كما يستغل القراصنة نوادي القمار التقليدية والإلكترونية وأنظمة الدفع الإلكتروني ومواقع الألعاب الإلكترونية في إخفاء مصادر أرباحهم غير المشروعة.الدورة الاقتصادية: توجد أربع مراحل -حسب تصنيف الخبراء- تعمل من خلالها أسواق الجريمة السيبرانية. تتمثل المرحلة الأولى في تطوير ونشر البرمجيات الخبيثة، ويتم ذلك عن طريق صناعتها، أو إعادة تحوير وتعديل برامج موجودة حاليًّا، أو سرقة البرمجيات والأدوات التي تطورها بعض الأجهزة الأمنية والشركات الخاصة في عدد من الدول. ومن الجدير بالذكر أن أكثر البرمجيات خطورة وانتشارًا في الآونة الأخيرة هي برامج الفدية، وهي برامج تهاجم أجهزة المستخدمين وتشفر بياناتهم وتطالبهم بفدية لفك والتي تستغل قدرات أجهزة وهواتف Cryptomining بالإضافة إلى انتشار برمجيات تعدين العملات الرقمية الخبيثة، WannaCry، التشفير، وأشهر مثال على ذلك برنامج الفدية المستخدمين بدون علمهم في جني العملات الرقمية.وتتمثل المرحلة الثانية في الترويج لخدمات القرصنة عن طريق التسعير التنافسي، وتقديم فرص لتجربة السلع المعروضة، وعرض تقييمات المستخدمين للبائعين، وتقديم ضمانات لجودة الخدمات والبرمجيات، وعمل تخفيضات على المشتريات بالجملة، وحتى تقديم خدمات ما بعد البيع في بعض الأحيان على غرار ما تفعله الشركات المحترفة، كما يتم التسويق للبرمجيات وخدمات القرصنة على شبكات التواصل الاجتماعي ومنتديات القرصنة ومواقع بيع الممنوعات، وفي مرحلة الشراء يحاول كل من البائع والمشتري البقاء مجهول الهوية قدر المستطاع حتى لا يتم تعقب أي منهما. فعلى سبيل المثال، قد يقوم المشتري بالتواصل مع البائع عن طريق بريد إلكتروني وهمي أو غرف دردشة خاصة للمفاوضة على القيمة المادية والحصول على طريقة تشغيل المنتج والخدمة ومعرفة ميعاد وطريقة الدفع، وتأتي المرحلة الرابعة بعد إتمام الصفقة، وتشمل عمليات غسيل الأموال التي تم جمعها من مبيعات أسواق القرصنة أو تلك التي تمت سرقتها من المستخدمين.ولكي تستمر المنظومة الاقتصادية للجريمة السيبرانية بالعمل لا بد من استقطاب المزيد من الأفراد، ويشير الخبراء إلى سعي القراصنة لجذب المواهب الجديدة بالاعتماد على الشبكة المظلمة، وتتمثل أهم المهارات التي يبحثون عنها في الفرد الذي يرغبون بضمه في: إجادة عدد من اللغات، والقدرة على تعلم أساليب الاختراق المختلفة، ووجود معرفة واسعة عن الشبكات والأنظمة داخل المؤسسات، وتأدية كل ما يستجد من مهام القرصنة، ومن الممكن أن يطلب من المرشحين اختراق موقع أو القيام بأي نشاط إجرامي خلال مدة زمنية محددة ليتم تقييم مهاراتهم، وبعد تحديد المرشحين المناسبين يتم التواصل معهم عن طريق برامج المحادثة، ولكن هناك مخاطرة بأن يكون المرشح من أجهزة الأمن ويعمل بشكل متخفٍ، لذا فمن أجل حماية المشاركين تكون تلك المكالمات بدون فيديو، وقد تستخدم مبادلات الصوت الرقمية لإخفاء هويات المشاركين، كما يتم التواصل داخل الشبكة المظلمة بشكل مشفر. وقد وجد الخبراء أيضًا أن هناك اهتمامًا مستمرًا باستغلال نقاط الضعف الأساسية والتي يتم استخدامها لأكثر من عقد من الزمان ولا تزال شائعة وفعالة، مثل أساليب مهاجمة المواقع وإيقاف عملها وتشويهها وتخريب قواعد البيانات.خسائر الدول: لا تزال تقديرات تكلفة الخسائر الناجمة عن الجريمة وهي شركة متخصصة في الأمن، McAfee السيبرانية تتباين بشكل ملحوظ نظرًا لصعوبة حصر كافة حوادث الاختراق وتحديد قيمة خسائرها بدقة، وتقدر دراسة أعدتها شركة أن التكلفة العالمية للجريمة السيبرانية قد تصل إلى 600 مليار دولار، كما يترتب عليها فقدان CSIS، الإلكتروني ومكافحة الفيروسات بالتعاون مع مركز الدراسات الاستراتيجية والدولية الملكية الفكرية والمعلومات السرية التجارية والبيانات الشخصية، وتزايد الاحتيال الرقمي والجرائم المالية والتي غالبًا ما تكون نتيجة استغلال للمعلومات الشخصية المسروقة، وتوسع هامش التلاعب المالي باستخدام المعلومات التجارية المسروقة الحساسة حول صفقات الدمج المحتملة، وتعطيل الخدمات والمنتجات بكافة صورها وفقدان الثقة في التعامل عبر شبكة ودفع تكاليف التعافي من الهجمات السيبرانية، cyberinsurance، الإنترنت، ورفع تكلفة تأمين الشبكات، واضطرار الشركات والمؤسسات إلى شراء بوليصات التأمين السيبراني بالإضافة إلى تضرر سمعة الشركات المخترقة وتعرضها للمساءلة القانونية، وتأثر أسعار أسهمها في أسواق البورصة. كما أن تكلفة الجريمة السيبرانية تتوزع بشكل غير متساوٍ بين جميع دول العالم، فكلما كان البلد أكثر ثراء كانت تكلفة الجريمة السيبرانية فيه أكبر، ولكن العلاقة بين دول العالم النامي والجريمة السيبرانية معقدة بسبب أن الهواتف الذكية سهلت على ملايين المستخدمين الوصول إلى شبكة الإنترنت، لكن العائد من وراء عمليات القرصنة التي تستهدف هؤلاء المستخدمين قليل، وبالتالي فإن القراصنة يوجهون هجماتهم إلى الدول الأكثر ثراء. وطبقًا للدراسة فإن توزيع تكاليف القرصنة جغرافيًّا كالآتي: منطقة شرق آسيا والمحيط الهادئ بقيمة تتراوح ما بين 120 إلى 200 مليار دولار، وتليها منطقة أوروبا ووسط آسيا بتكلفة تتراوح ما بين 160 إلى 180 مليار دولار، ثم منطقة شمال أمريكا بتكلفة تتراوح ما بين 140 إلى 175 مليار دولار، ومنطقة جنوب آسيا بتكلفة مقدارها 2.9 مليار دولار، ومنطقة أمريكا اللاتينية بتكلفة مقدارها 5.3 مليارات دولار، ومنطقة الشرق الأوسط وشمال إفريقيا بتكلفة مقدارها 3.1 مليارات دولار، ومنطقة جنوب الصحراء الكبرى بإفريقيا بتكلفة مقدارها 1.5. مليار دولار