نور علوان | نشر في ٢٤ يونيو ٢٠١٩,

القرصنة الأخلاقية.. مهنة مستقبلية ونوع من النضال الوطني

عندما بات العالم الافتراضي أساسًا معتمدًا ومحوريًا في جميع جوانب الحياة، أصبحت الهجمات الإلكترونية جزءًا رئيسيًا من بنية هذه المنصة، فهي وحدة من أكثر الأسلحة استخدامًا وقوة وأقل الثغرات أمانًا، إذ تحولت هذه التقنية إلى ميدان حرب تتعارك فيه المصارف والشركات العالمية العملاقة والجيوش العسكرية مع القراصنة الإلكترونيين، حمايةً لبياناتها السرية ودفاعًا عن أنظمتها من أي هجمات تخريبية وفجائية، ولذلك نجد أن دول العالم العظمى تجتهد في تطوير أدواتها وبرمجياتها.

إذ تشير التقديرات العامة بأن 15 دولة في العالم من الدول التي تمتلك ميزانيات عسكرية ضخمة، تستثمر في المجالات المتخصصة في تسديد ضربات إلكترونية ضد العدو ودمج هذه القدرة التقنية في العمليات العسكرية، مثل روسيا والصين والولايات المتحدة وإنجلترا وفرنسا ودولة الاحتلال "إسرائيل"، ومن دول العالم الثالث، تصطف الهند وباكستان وكوريا الشمالية وإيران بجانبهم.

على صعيد آخر وبجانب الهيئات الإستراتيجية والحكومات، تتحكم مجموعات مستقلة أو أفراد بهذه الهجمات، إما بهدف الابتزاز وطلب فدية مالية مقابل عدم نشر معلومات معينة، أو بهدف تسريب محتوى سري، أو لسرقة بيانات وربما تعديلها وتعطيلها، وبصرف النظر عن الغايات، تثير هذه الانتهاكات المزعجة الكثير من الفوضى، ولكن في بعض الحالات، قد تكون هذه القرصنة أخلاقية.

أصحاب القبعات البيضاء: مهنة يتقنها خبراء الأمن

عام 2017، قد تكون سمعت عن الانتهاكات الإلكترونية التي حدثت عبر فيروس "بيتا" الخبيث الذي اخترق أنظمة شركات نفط واتصالات وشركات طبية توزعت بين أوكرانيا وألمانيا وبريطانيا وإسبانيا والولايات المتحدة الأمريكية في شهر واحد، وكان أكثرها تسببًا بالضرر، عمليات القرصنة التي شملت

اختراق عشرات المستشفيات في إنجلترا، حيث تأثرت كل أجهزة الحاسوب، ما أدى إلى إغلاقها وضياع سجلات المرضى والفواتير.

يطلق على قراصنة الهجمات الأخلاقية "أصحاب القبعات البيضاء"، وهم الخبراء الأمنيون الذين يركزون على حماية الأنظمة الإلكترونية بدًلا من اختراقها عبر معالجتها وسد ثغراتها الأمنية كي لا تكون هدفًا للخصوم، ويتم ذلك بطريقة قانونية ومشروعة

أثارت هذه الحادثة سخط واستياء العديد من الأفراد الذين اعتبروا أن هذه التقنية تشكل تهديدًا مباشرًا لأمنهم وحياتهم وسجلاتهم الرقمية، لكن في الجهة المقابلة، ورغم تكرر هذه الحالة، رأى البعض الآخر أن هذه التقنية سلاح ذو حدين، فكما تستخدم لأغراض شريرة ومضرة، يمكن استغلالها أيضًا لتحقيق أهداف أخلاقية بحتة وبعيدة عن الغايات الاستفزازية والمثيرة للفوضى والخراب.

إذ يطلق على قراصنة الهجمات الأخلاقية "أصحاب القبعات البيضاء"، وهم الخبراء الأمنيون الذين يركزون على حماية الأنظمة الإلكترونية عبر اختراقها بنفس عقلية المتسللين الأشرار لكن بهدف معالجة وسد الثغرات الأمنية كي لا تكون هدفًا للخصوم، ويتم ذلك بطريقة قانونية ومشروعة، وفي بعض الأحيان قد يقتحمون الأنظمة الأخرى بناءً على مبدأ الواجب الإنساني، وتعبيرًا عن موقف معين، أو دعمًا لقضية ما، وعكس ذلك، فهو المعنى الكامل للمتسللين غير الأخلاقيين أو أصحاب القبعات السوداء.

ووفقًا للمجلس الأوروبي، فإن تعريف القرصان الأخلاقي يتلخص كالتالي: "الشخص الذي يعمل مع منظمة ويمكن الوثوق به لاختراق الشبكات أو الأنظمة الحاسوبية باستخدام نفس الأساليب والتقنيات التي يستخدمها المتسلل الخبيث أو الشرير". المثير للاهتمام، ليس فقط أهمية هؤلاء القراصنة في إغلاق التصدعات وعرقلة التطفلات غير الشرعية، وإنما في الشهادات المهنية والجوائز العالمية التي يتلقونها كأحد "القراصنة الأخلاقيين" المعتمدين، فلقد جعلت شركات تكنولوجيا المعلومات شهادة CEH التي تغطي أكثر من 270 تقنية، مؤهلاً إلزاميًا للوظائف ذات الصلة بالأمان الإلكتروني.

من المرجح أن تصل الأضرار المتعلقة بجرائم الإنترنت إلى 6 تريليونات دولار سنويًا بحلول عام 2021

جدير بالإشارة أن مجال القرصنة الأخلاقية كان موجودًا منذ السبعينيات، ولكنه في الوقت الحاليّ فقط،

يشهد نموًا سريعًا، فخلال السنوات الخمسة ما بين 2012 و2017، زادت قوائم وظائف الأمن السيبراني بنسبة هائلة بلغت 75%. وتقدر دخولهم السنوية بين 80 ألف و95 ألف دولار أمريكي، ووفقًا لمصادر أخرى، قد تتراوح بين 50 ألف و100 ألف دولار في السنوات الأولى من العمل. وبحسب إحدى الدراسات، فإن 72% من مجتمع القراصنة الأخلاقيين تتراوح أعمارهم بين 18 و29 عامًا، وتعلم 43% منهم كيفية الاختراق عبر المدونات والمصادر الإلكترونية، و41% تعلموا من الأشخاص الخبرة من حولهم.

تنبع أهميتهم من المؤشرات التي تدلل على زيادة المخاطر الأمنية بشكل سنوي، فبحسب الإحصاءات، تعتقد 70% من المؤسسات أن مخاطرها الأمنية زادت بشكل كبير منذ عام 2017، ومن جهة أخرى، من المقدر أن يحدث هجوم ابتزازي على الشركات كل 14 ثانية في العام الحاليّ، وذلك مقارنة مع كل 40 ثانية في عام 2016، كما من المرجح أن تصل الأضرار المتعلقة بجرائم الإنترنت إلى 6 تريليونات دولار سنويًا بحلول عام 2021.

وتبعًا لهذه الأرقام، من المتوقع أن ينمو سوق أمن المعلومات بنسبة 8.7% عام 2019 إلى 124 مليار دولار، ويعود ذلك جزئيًا إلى الإنفاق على خدمات الاستشارية والمتعلقة بحماية البيانات وتشريعات الخصوصية، مثلما فعلت شركة جوجل.

شركات تكنولوجية عملاقة تستغل مهارات القراصنة الأخلاقيين

عام 2015، أعلنت شركة محرك البحث الشهير جوجل، بأنها أنفقت 1.5 مليون دولار على أكثر من 200 هاكر من أصحاب القبعات البيضاء الذين ساعدوا الشركة في العثور على الثغرات الأمنية في منتجاتها، وهو النهج الذي بدأت الشركة باتباعه منذ عام 2010، بحثًا عن الأخطاء والعيوب التي تختبئ في أنظمتها ومن الممكن أن تستغل من الخصوم، وأحد هؤلاء القراصنة كان شابًا يبلغ من العمر 17 عامًا فقط، وتلقى مكافأة مادية بقيمة 150 ألف دولار، وانتهى به الأمر كمتدرب في قسم الأمان الإلكتروني في جوجل.

20% من المؤسسات في منطقة الشرق الأوسط تعترف بعدم معرفتها ما إذا كانت قد وقعت ضحية لجرائم الإنترنت خلال العامين الماضيين، ما يدلل بشكل أو بآخر أن بعض دول هذه المنطقة ليست واعية كفاية بأهمية ومخاطر هذا المجال

جوجل ليست الشركة التقنية الوحيدة التي تكافئ أصحاب القبعات البيضاء، إذ تلجأ إليهم أيضًا شركة فيسبوك وتويتر ومايكروسوفت وآبل وتسلا، وبحسب التقارير، تدفع الأخيرة من ألف دولار إلى 15 ألف دولار، وذلك على حسب المشكلة ومدى تعقدها وشدتها، ومع وجود ثغرة أمنية واحدة على الأقل في 77% من التطبيقات الإلكترونية، فإنه ليس من المستغرب أن تلجأ الشركات الكبيرة لهذه المكافآت المادية من أجل تحفيز القراصنة الأخلاقيين والعثور على نقاط الضعف، وذلك ما يفسر أيضًا المؤشرات التي تتوقع وجود 3.5 مليون وظيفة في مجال الأمن الإلكتروني بحلول عام 2021.

أما فيما يخص المنطقة العربية، تشير الأرقام الصادرة عن دراسة الجريمة الاقتصادية العالمية إلى أن الجرائم الإلكترونية في عام 2016 كانت ثاني أكثر الجرائم الاقتصادية التي أبلغت عنها منظمات الشرق الأوسط، حيث تم استهداف 30% من الشركات، لكن من المثير للدهشة أن أكثر من 20% من المؤسسات تعترف بعدم معرفتها ما إذا كانت قد وقعت ضحية لجرائم الإنترنت خلال العامين الماضيين، ما يدلل بطريقة ما أن بعض دول هذه المنطقة ليست واعية كفاية بأهمية ومخاطر هذا المجال.

القرصنة العربية والنضال الإلكتروني

في أكثر من مرة، اخترق المغاربة العديد من المواقع والمؤسسات الحكومية الإسرائيلية مثلما فعلوا عام 2013، حين اخترقوا تقريبًا 350 موقعًا في غضون 45 دقيقة، منها وزارة الاستيعاب والكنيست والبورصة وجهاز المخابرات وهيئة الأوراق المالية وموقع المحاكم الإسرائيلية، وغيرها الآلاف من حسابات الإسرائيلين على موقع فيسبوك.

الكثير من القراصنة العرب يشاركون في هذه العمليات من السعودية ولبنان والجزائر، مؤكدين أن الحرب الإلكترونية ساحة جديدة من ساحات المقاومة ضد الانتهاكات الإسرائيلية وجرائمها على أرض الواقع

وغالبًا ما يعمل القراصنة المغاربة بشكل كثيف وممنهج ضمن شبكة "أنونيموس" – أي مجهولي الهوية -، دعمًا للقضية الفلسطينية واحتجاجًا على ممارسات دولة الاحتلال ضد الفلسطينيين وحرمانهم من أبسط حقوقهم، وأحيانًا تكون هجماتهم ردًا لحظيًا ومباشرًا على الغارات الإسرائيلية على قطاع غزة.

على سبيل المثال، قالت الجماعة في بيان لها ذات مرة "فلتعلموا يا أهالي غزة أن أنونيموس تقف إلى جانبكم، سنقوم بعمل كل ما نستطيع لمنع القوات الإسرائيلية الغاشمة من الاصطفاف ضدكم. سنقوم بتوظيف جميع إمكاناتنا كي نتأكد بأنكم ستظلون قادرين على الاتصال بالإنترنت وعلى نقل معاناتكم إلى العالم".

وهو ما دفع التليفزيون الإسرائيلي لوصف هذا الهجوم بـ"الهجمة الإلكترونية الأكبر ضد البلاد"، مع العلم أن الكثير من القراصنة العرب يشاركون في هذه العمليات من السعودية ولبنان والجزائر، مؤكدين أن الحرب الإلكترونية ساحة جديدة من ساحات المقاومة ضد الانتهاكات الإسرائيلية وجرائمها على أرض الواقع.

رابط المقال: https://www.noonpost.com/28267/