نور علوان | نشر في ٢٨ يونيو ٢٠١٧,

"الحرب لم تنته بعد" هجوم إلكتروني عالمي جديد

بعدما أصبح العالم الافتراضي الأساس المعتمد في جميع جوانب الحياة، لا سيما كبنية تحتية لتبادل وحفظ وتخزين المعلومات والبيانات في سرية تامة وبأحجام كبيرة، خاصة ضمن أعمال حكومات وأجهزة الدول، إلا أن هذه المساحة التقنية تحولت إلى ميدان حرب تُستهدف فيها هيئات استراتيجية مثل الجيوش العسكرية والمصارف والشركات العالمية العملاقة، لدوافع غالبًا ما تكون سياسية واقتصادية وبأهداف تخريبية.

ومن الواضح أن هذه الحروب الإلكترونية هي الطابع السائد على حروب القرن الواحد والعشرين، فهي السلاح الأكثر استخدامًا والثغرة الأقل أمانًا في الوقت الحاضر، وتبعًا لاحتمالية الاختراق والهجوم العالية واشتداد الضربات بين جهات مختلفة، فإن الدول العظمى في العالم تجتهد في تطوير برمجيات وأنظمة دفاع لتحصين بياناتها والتصدي لأي هجمات متوقعة أو فجائية.

كما تشير بعض التقارير إلى ازدياد الأعمال الهجومية الإلكترونية في العالم، والتي يقوم بها مجموعات وحكومات، وتتدرج عمليات الاستهداف من أبسط المستويات إلى أكثرها تعقيدًا وتدميرًا.

حرب تخريبية

تعددت التعاريف والمفاهيم لهذا النوع من الحروب الحديثة، واجتمع المعرفون الخبراء على أن ميدان هذه الحرب هو شبكة الإنترنت وهدفها تخريب وتعطيل أنظمة وشبكات تابعة لدول الخصم.

وأهداف هذه الحرب واضحة، فهي لا تكف عن اختراق المواقع الرسمية لتسريب معلومات معينة أو لسرقة بيانات سرية وربما تعديلها وتعطيلها، أما الموجة الأخيرة من الهجمات الإلكترونية، فكانت بهدف "الابتزاز" وطلب فدية مالية مقابل المعلومات التي تم إلغاؤها وإزالتها من قبل المخترق.

هذا النوع الجديد من الهجمات الإلكترونية أثار قلق العالم عامةً وخبراء المعلوماتية خاصةً، ففي الشهر الماضي ضُربت عدة مؤسسات وشركات في الولايات المتحدة الأمريكية وروسيا وبعض الدول الأوروبية.

البرنامج الخبيث يتسلل لأجهزة الحاسوب ويمنع المستخدم من الوصول إلى الملفات الخاصة به، حتى تبدأ المساومات ويضطر أن يدفع 300 دولار.

وتبعًا لهذه الحادثة المثيرة للقلق، حذر مركز معلومات مجلس الوزراء المصري من الهجمات التي تحدث عبر هذا الفيروس، وأوضح أن فيروس "بيتيا" الخبيث يخترق أجهزة الحواسيب ويسرق البيانات الموجودة عليها، عن طريق اختراق ثغرة موجودة في أنظمة التشغيل ويندوز، المعروفة باسم أتيرنال بلو.

كما ذكر المركز أن مبلغ الفدية هو 300 دولار ولا أحد مستثنى من هذه السرقات الإلكترونية، وحذر مضيفًا ألا يتم تحميل تطبيقات أو استلام ملفات من أشخاص مجهولين، وألا يتم الدخول على روابط غير معروفة، مع ضرورة حفظ نسخ احتياطية عن المعلومات خارج منظومة الإنترنت.

وبدورها قالت الشركة المسؤولة عن الكشف عن محاولات الاختراق، جروب أي بي: "البرنامج الخبيث يتسلل لأجهزة الحاسوب ويمنع المستخدم من الوصول إلى الملفات الخاصة به، حتى تبدأ المساومات ويضطر أن يدفع 300 دولار".

هذه الاختراقات الإلكترونية "هجوم دولي" يستهدف عدة دول ومنظمات.

ويذكر أن ضحايا هذا الابتزاز الإلكتروني هي شركات نفط واتصالات وشركات طبية توزعت بين أوكرانيا

وروسيا والولايات المتحدة الأمريكية وبريطانيا وألمانيا وإسبانيا خلال الشهر الماضي.

وتعليقًا على هذه الهجمة الإلكترونية التي شملت دول عدة، قالت رئيسة الوزراء البريطانية، تيريزا ماي، إن هذه الاختراقات الإلكترونية "هجوم دولي" يستهدف عدة دول ومنظمات.

جيوش إلكترونية

حذرت سلطات الدول من موجة القرصنة الإلكترونية وخاصة من الهجمة الابتزازية الأخيرة التي تطالب بفديات مالية مقابل استرجاع المعلومات الخاصة بالمؤسسات أو الشركات، وناشدتهم بعدم دفع أموال لهم، كما أوصت الوكالة البريطانية للأمن المعلوماتي بتحديث برامج الحاسوب المكافحة للفيروسات الإلكترونية لتجنب أي هجمة ممكنة.

تم إرسال 5 ملايين رسالة في الساعة تحمل فيروسات خبيثة، وفقًا لشركة فورسبوينت سيكيوريتي لابس.

وبهذا الخصوص، أشارت وزارة الأمن الداخلي الأمريكي إلى خطورة دفع هذه الفدية مقابل البيانات، لأن هذا الأمر لا يضمن الوصول إلى المعلومات، وإنما يضمن استمرار أعمال القرصنة في العالم.

كما قال مسؤول في شركة أفاست المعلوماتية، جاكوب كروستيك: "لقد رصدنا أكثر من 75 ألف هجوم في نحو 1000 بلد"، كما تم إرسال 5 ملايين رسالة في الساعة تحمل فيروسات خبيثة، وفقًا لشركة فورسبوينت سيكيوريتي لابس، فعمليات الاختراق لا تستثني أحدًا.

نتيجة لهذه الحوادث الكارثية، فإن الدول تعمل على تدريب نفسها على عمليات الاختراق والقرصنة لتنفيذها ضد العدو والتسبب بأضرار لهم في شبكاتهم وأنظمتهم المعلوماتية، نتيجة لهذا القلق العام، يفيد مركز الدراسات الاستراتيجية والدولية 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.

تنشط كل من روسيا والصين والولايات المتحدة وإنجلترا وفرنسا ودولة الاحتلال "إسرائيل" في بناء صفوف من الخبراء والمتدربين على تطوير أنظمة وأجهزة تكون فعالة في الحروب الإلكترونية، كما يذكر أن الهند وباكستان وكوريا الشمالية وإيران من دول العالم الثالث التي تطور نفسها في هذا المجال بعيدًا عن أعين العالم.

شملت عمليات القرصنة الإلكترونية عشرات المستشفيات في إنجلترا، حيث تأثرت كل أجهزة الحاسوب في المستشفى مما سبب في إغلاقها وضياع سجلات المرضى والأدوية والفواتير.

هذه الحرب الإلكترونية تشبه الحرب التقليدية في أهدافها ودوافعها، لكن ما يجعل هذا النوع من الحروب صعب هو عدم القدرة على تحديد مصدر الهجمات وفي حال إن أمكن تتبع مصدر هذه الهجمات فإن الكشف عنها يتطلب شهورًا خاصة لو كان المسؤولون عن الاختراق أفرادًا غير قانونيين ليس لديهم أصول أو قواعد بيانات للرد عليهم.

في الحرب التقليدية قد تكون مناطق الاستهداف متوقعة ويمكن أخذ تدابير الحيطة والحذر من بعض الهجمات، إلا أن الحرب على شبكات الإنترنت تكون مليئة بالمخاطر، فكل مواقعها الحكومية والعسكرية والاقتصادية مستهدفة ومعرضة لأي تعطيلات مادية حقيقية في نظام حركة الدولة، مما يكبدها خسائر مالية فادحة.

كما أنها غير أخلاقية أبدًا، فلقد شملت عمليات القرصنة الإلكترونية عشرات المستشفيات في إنجلترا، حيث تأثرت كل أجهزة الحاسوب في المستشفى مما سبب في إغلاقها وضياع سجلات المرضى والأدوية والفواتير، كما صرح مدير مستشفى دهارمايس لوكالة رويترز الإخبارية.

تستنفد الصين طاقاتها في تطوير قدراتها الإلكترونية، الأمر الذي أصبحت الأشهر به والأقوى خاصة عندما أتيح لها أن تعرف نقاط ضعف خصومها في هذا المجال.

ما يميز هذه الحرب، عدم وجود إطار قانوني يحكمها، ولا توجد هوية لمنفذ الهجمات، إلا أنه في بعض الأحيان يمكن أن تعكس هذه الهجمات صفات النظام الذي قام بهذه الأعمال الهجومية.

على سبيل المثال، غالبًا ما يتم نسب معظم الهجمات الإلكترونية التي تحدث إلى الروس والصينيين، هذا لأن هجماتهم ذات نزعة واضحة وتكون أعمالهم الاختراقية منظمة بشكل كبير ومستمر، فهي تقوم باختراق آلاف المواقع في كل عام، لهذا تعد الصين وروسيا أشهر الدول في مجال الاختراق الإلكتروني.

كما تعتبر الصين خاصة من أبرز الدول التي تعمل على تطوير أجهزتها وأساليبها الهجومية والدفاعية في ذات الوقت يرى البعض أن الصين تفتقر لمواطن القوة في المجالات الأخرى ولذلك تستنفد طاقاتها في تطوير قدراتها الإلكترونية، الأمر الذي أصبحت الأشهر به والأقوى خاصة عندما أتيح لها أن تعرف نقاط ضعف خصومها في هذا المجال.

أما روسيا، فاسمها لا يفارق اسم الصين في هذا المجال، إذ تعد مسؤولة عن أكبر الهجمات الإلكترونية في العالم، لكن دون دليل إدانة مادي ضدها، وربما تلجأ روسيا لهذه الطريقة التخريبية في شن الحروب أو افتعال الأزمات بسبب تفوق الدول الأخرى عسكريًا عليها.

الجهات المخترقة

تم الذكر مسبقًا أن ليس هناك جهة دولية أو حكومية أو خاصة مستبعدة من هذا الاختراق، فالهجمات الإلكترونية تصيب المصارف والمؤسسات المالية والمستشفيات وشركات اتصالات وشركات نفطية وحسابات شخصية أيضًا.

الجهات الأكثر استهدافًا هي المصارف والمنشآت الحيوية مثل قطاعات الطاقة والنفط والصحية والبرامج النووية.

وفقًا لهافينتغتون بوست عربي، فإن الدول الأكثر عرضة للتهديدات الإلكترونية هي جمهورية مصر العربية، وأكثر الجهات المعرضة لهذه الهجمات الإلكترونية هي الحسابات والصفحات الشخصية وتاليها الأجهزة والمواقع الحكومية ومن بعدها أجهزة ومواقع الشركات الخاصة.

ما يحدث بعد الهجمة

ولأن كل حرب لها عواقبها الكارثية، على الدول عامة، لأن الجميع يعتمد على شبكة الإنترنت في تنظيم وإدارة الأمور، يقول مدير مشاريع شركة بوز ألن هاملتون، إن الخسائر الناتجة عن الهجمات الإلكترونية العالمية غير مسبوقة من ناحية الحجم ووتيرة السرعة، فهي تقوم بتشفير الآلاف من أجهزة الحاسوب.

وتبعًا لمصادر معهد بونيمون، فإن متوسط الخسائر السنوية للشركات من الهجمات الإلكترونية في العالم تجاوز 7.7 مليون دولار لكل مؤسسة، إذ أنفقت المؤسسات في جميع أنحاء العالم 73.7 مليار دولار في العام الماضي على الأمن المعلوماتي الإلكتروني وذلك وفقًا لما صرحته منظمة البيانات العالمية.

ومن المتوقع في الأعوام المقبلة، أن تكون الجهات الأكثر استهدافًا هي المصارف والمنشآت الحيوية

مثل قطاعات الطاقة والنفط والصحية والبرامج النووية.