التجسس الالكتروني.. سلاح امريكي فتاك يثير قلق العالم

2015-02-22عبد الامير رويح

عمليات التجسس والقرصنة الالكترونية اصبحت اليوم كما يقول بعض الخبراء من اهم وأخطر الاسلحة بيد العديد من الدول والحكومات، التي تسعى من خلال هذه العمليات الى الكشف عن معلومات اضافية تمكنها من تحقيق انتصارات جديدة خصوصا مع اتساع رقعة الخلافات والازمات الدولية التي افقدت العالم الثقة بكل شيء تقريباً.

والتجسس الإلكتروني كما يقول بعض المراقبين هو نوع جديد من حروب السيطرة على الأشخاص والدول، ازدادت وتيرته بشكل كبير في ظل التطور التقني الهائل الذي نعيشه. وتتعدد أساليب القرصنة لتواكب زمن حرب المعلومات التي وصلت إلى ذروتها مطلع القرن الحادي والعشرين، ويلاحق القراصنة أهدافهم لجمع المال وسرقة معلومات هامة، وبعضها الآخر وهو الأهم تقف وراءه دوافع سياسية غايتها اختراق الأنظمة الدفاعية، والتجسس على الشخصيات المستهدفة.

ويرى بعض المراقبين ان برامج التجسس الأمريكية التي كشف عنها في السنوات الاخيرة تعد من اكبر البرامج، التي اثارت القلق والخوف في جميع انحاء العالم دون استثناء، خصوصا وان تلك العمليات التجسسية قد شملت اقرب الحلفاء، الامر الذي تسبب بحدوث أزمات أمنية ودبلوماسية، دفعت العديد من الحكومات والدول و الشركات الى اعتماد اساليب جديدة في حماية نفسها ومواطنيها من عمليات التجسس التي تقوم بها الحكومات وغيرها من عمليات سرقة البيانات. يضاف الى ذلك انها قد ولدت ردود افعال مختلفة تمثلت بإجراء عمليات مضادة وبنفس الاسلوب وهو ما قد يزيد من حدة الخلافات الدولية.

طفرة في برمجيات التجسس

وفي هذا الشأن فقد قال باحثون في الأمن الإلكتروني وعملاء سابقون إن وكالة الأمن القومي الأمريكية توصلت إلى كيفية إخفاء برمجيات تجسس في أعماق محركات الأقراص الصلبة التي

تنتجها شركات وسترن ديجيتال وسيجيت وتوشيبا وغيرها من كبار المصنعين مما وفر للوكالة الوسائل للتجسس على أغلبية أجهزة الكمبيوتر في العالم. وكانت هذه المقدرة المنشودة منذ وقت طويل والتي تخضع لحراسة مشددة جزءا من مجموعة برامج تجسس اكتشفتها شركة كاسبرسكي لاب لأمن البرمجيات ومقرها موسكو والتي كشفت سلسلة من عمليات التجسس الإلكتروني الغربية.

وقالت كاسبرسكي إنها اكتشفت أن أجهزة الكمبيوتر الشخصي في 30 دولة مصابة ببرنامج تجسس واحد على الأقل. وحدثت أغلب الإصابات في إيران تليها روسيا وباكستان وأفغانستان والصين ومالي وسوريا واليمن والجزائر. وتشمل الأهداف منشآت حكومية وعسكرية وشركات اتصالات وبنوكا وشركات طاقة وباحثين نوويين ووسائل إعلام ونشطاء إسلاميين.

ورفضت الشركة الكشف عن اسم الدولة التي تقف وراء حملة التجسس لكنها قالت إنها على صلة وثيقة مع السلاح الإلكتروني ستوكسنت الذي تتحكم فيه وكالة الأمن القومي الأمريكية واستخدم في مهاجمة منشأة إيرانية لتخصيب اليورانيوم. والوكالة مسؤولة عن جمع معلومات المخابرات الإلكترونية لحساب الولايات المتحدة.

وقال موظف سابق في الوكالة إن تحليل كاسبرسكي صحيح وإن الناس الذين ما زالوا يعملون في وكالة التجسس يعطون قيمة كبيرة لهذه البرامج التجسسية على نفس قدر ستوكسنت. وأكد ضابط مخابرات سابق آخر أن الوكالة طورت التقنية المرغوبة لإخفاء برمجيات التجسس في محركات الأقراص الصلبة لكنه قال إنه لا يعرف جهود التجسس التي تعتمد عليها. ورفضت المتحدثة باسم وكالة الأمن القومي الأمريكية فاني فاينز التعليق.

ونشرت كاسبرسكي التفاصيل الفنية لبحثها في خطوة ينبغي أن تساعد المؤسسات المصابة ببرمجيات التجسس على اكتشافها وبعضها يرجع إلى عام 2001. ويمكن للكشف أن يسبب مزيدا من الضرر لقدرات المراقبة لدى وكالة الأمن القومي الأمريكية التي تضررت بالفعل من تسريبات كبيرة عن طريق المتعاقد إدوارد سنودن. وألحقت تسريبات سنودن ضررا بعلاقات الولايات المتحدة مع بعض الحلفاء وأبطأت بيع منتجات تكنولوجية أمريكية في الخارج.

ويمكن للكشف عن تلك الأدوات الجديدة للتجسس أن يؤدي إلى رد فعل أكبر ضد التكنولوجيا الغربية وخاصة في دول مثل الصين التي سنت بالفعل لوائح تستلزم من أغلب موردي التكنولوجيا للبنوك تقديم نسخ من شفرات البرامج الخاصة بهم لسلطات تفتيش. وقالت كاسبرسكي إن الجواسيس حققوا طفرة تكنولوجية بمعرفة كيفية زرع البرمجيات الخبيثة في الشفرة الغامضة المسماة نظام التشغيل الذي يعمل في كل مرة يجري فيها تشغيل الكمبيوتر.

ويعتبر الجواسيس وخبراء الأمن الإلكتروني نظام تشغيل لمحرك القرص الصلب ثاني أهم الأصول بالنسبة للمتسللين في جهاز الكمبيوتر الشخصي. ولا يفوقه أهمية سوى شفرة نظام الادخال والاخراج الاساسي (بيوس) الذي يعمل بصورة آلية لدى تشغيل الجهاز. وقال كوستن ريو الباحث في كاسبرسكي "مكونات الكمبيوتر ستكون قادرة على إصابة الجهاز مرارا وتكرارا." وأضاف أن المسؤولين عن حملة التجسس التي ما تزال مستمرة كان يمكنهم السيطرة على الآلاف من أجهزة الكمبيوتر الشخصي مما يعطيهم القدرة على سرقة ملفات أو التجسس على أي شيء يريدونه لكن الجواسيس كانوا انتقائيين وحققوا سيطرة كاملة عن بعد فقط على أجهزة تخص أكثر الأهداف الأجنبية جاذبية.

وقال إن كاسبرسكي لم تعثر سوى على القليل من أجهزة الكمبيوتر ذات القيمة العالية بصورة خاصة بين الأجهزة التي أصيبت محركات الأقراص الصلبة بها بالبرمجيات الخبيثة. وأعادت كاسبرسكي بناء برمجيات التجسس مما أظهر أنها يمكن أن تعمل في محركات اقراص تبيعها أكثر من عشر شركات بما يغطي السوق بالكامل بصورة اساسية. وتشمل تلك الشركات وسترن ديجيتال وسيجيت تكنولوجي وتوشيبا وآيبيإم ومايكرون تكنولوجي وسامسونج الكترونيكس. وقالت وسترن ديجيتال وسيجيت ومايكرون إنها لا تعرف بمثل هذه البرمجيات. ورفضت توشيبا وسامسونج التعليق. ولم ترد آيبيإم على طلبات للتعليق.

وقال ريو إن مصممي برامج التجسس لابد أنهم توصلوا إلى شفرة المصدر المحمية بالملكية والتي توجه حركات محركات الاقراص الصلبة. ويمكن لهذه الشفرة أن تعمل كخارطة طريق لنقاط الضعف بما يسمح لمن يدرسونها بتنفيذ هجمات بسهولة أكبر. وأضاف ريو "الفرصة معدومة لتمكن شخص من إعادة كتابة نظام التشغيل (لمحرك القرص الصلب) باستخدام معلومات عامة."

وتفاقمت المخاوف بشأن الوصول إلى شفرة المصدر بعد سلسلة من الهجمات الإلكترونية البارزة على شركة جوجل وغيرها من الشركات الأمريكية في 2009 والتي ألقي باللوم فيها على الصين. ويقول المحققون إنهم عثروا على دليل على أن المتسللين توصلوا إلى شفرة المصدر الخاصة بالعديد من الشركات التكنولوجية والدفاعية الأمريكية الكبرى. ولم يتضح كيف حصلت وكالة الأمن القومي الأمريكية على شفرات المصدر لمحركات الأقراص الصلبة. وقال ستيف شاتوك المتحدث باسم وسترن ديجيتال إن الشركة "لم تقدم شفرة المصدر الخاصة بها إلى وكالات حكومية."

ولم تكشف الشركات الأخرى لصناعة محركات الأقراص الصلبة عما إذا كانت أطلعت وكالة الأمن القومي على شفرات المصدر الخاصة بها. وقال كليف اوفر المتحدث باسم سيجيت إن لديها "إجراءات مؤمنة لمنع التلاعب أو القيام بهندسة عكسية لبرنامج تشغيلها وغيره من التقنيات." وقال دانييل فرانشيسكو المتحدث باسم مايكرون إن الشركة تتعامل بجدية مع أمن منتجاتها "ولا نعرف بأي أمثلة لشفرة خارجية." بحسب رويترز.

وقال ضباط مخابرات سابقون إن وكالة الأمن القومي الأمريكية لديها طرق عدة للحصول على شفرة المصدر من الشركات التكنولوجية منها الطلب مباشرة والتظاهر بمظهر مطور برمجيات. وإذا ارادت شركة بيع منتجات للبنتاجون أو وكالة أمريكية حساسة أخرى يمكن أن تطلب الحكومة مراجعة أمنية للتأكد من سلامة الشفرة الأمنية. وقال فنسنت ليو الشريك في مؤسسة بيشوب فوكس الاستشارية الأمنية والمحلل السابق في وكالة الأمن القومي الأمريكية "إنهم لا يعترفون به لكنهم يقولون ‘سنجري تقييما.. نريد شفرة المصدر’." وأضاف "من المعتاد أن تجري وكالة الأمن القومي التقييم وانه استنتاج صغير جدا أن نقول انهم سيحتفظون بتلك الشفرة."

وزارة الخارجية الاميركية

الى جانب ذلك اوردت وسائل الاعلام الاميركية ان وزارة الخارجية اضطرت الى وقف شبكتها المعلوماتية غير السرية بعد ادلة على حصول قرصنة تقنية. وكتبت الوزارة في بريد الكتروني ان الاغلاق تم ضمن اعمال صيانة مقررة على شبكتها الرئيسية غير السرية وسيؤثر على الرسائل الالكترونية والوصول الى المواقع العامة.

الا ان تقارير وردت حول وجود ادلة بان احد القراصنة اخترق الحماية الامنية في بعض نواحي النظام المتعلقة بالرسائل الالكترونية غير السرية. واشار مسؤول كبير لصحيفة "واشنطن بوست" الى "اعمال مثيرة للقلق" لكن ايا من الاقسام السرية للنظام لم يتعرض لخطر. ولو كانت وزارة الخارجية تعرضت للقرصنة، فستكون الادارة الاخيرة ضمن سلسلة من الوكالات الحكومية التي تواجه اختراقات امنية، مع ان اي رابط لم يتضح بين تلك العمليات.

واعلنت هيئة البريد الاميركية ان قراصنة سرقوا معلومات شخصية حساسة في ما يشكل عملية اختراق امني كبيرة كما تم الاستيلاء على معلومات حول بعض الزبائن ايضا. وقال متحدث باسم هيئة البريد ان الاختراق شمل قرابة 800 الف شخص يتلقون اجورا من الوكالة من بينهم موظفون ومتعاقدون. واضاف المتحدث ان القراصنة اخترقوا انظمة الدفع في مكاتب هيئة البريد وعلى الانترنت حيث الزبائن يدفعون لقاء الخدمات. بحسب فرانس برس.

وتعمل الوكالة مع مكتب التحقيقات الفدرالي (اف بي اي) وغيره من الاجهزة الامنية للتحقيق في الامر. وفي وقت سابق، اشار البيت الابيض الى اختراق لشبكته المعلوماتية غير السرية. وقام البيت الابيض بفصل بعض المستخدمين لديه مؤقتا عن الشبكة لكن لم تسجل اي اضرار في الشبكة او الانظمة، بحسب مسؤول. ونقلت صحيفة واشنطن بوست عن مصادر بان الشبهات تدور حول قراصنة يعملون لحساب الحكومة الروسية.

طائرات لجمع البيانات

على صعيد متصل أفادت تقارير أن الحكومة الأمريكية تستخدم طائرات تطير فوق الولايات المتحدة مزودة بمعدات لجمع بيانات من ملايين الهواتف المحمولة. ووفقا لتقرير نشرته صحيفة "وول ستريت جورنال" الأمريكية فأن الحكومة تستخدم أجهزة تسمى "ديرت بوكس" تحاكي أبراج إرسال الهواتف النقالة، ومن خلالها يجري نقل بيانات عن موقع المستخدم وهويته الخاصة. وتنقل تلك الأجهزة بيانات جميع الأشخاص، ففي الوقت الذي تستخدم تلك الأجهزة لتعقب المشتبه بهم في منطقة ما، فإن جميع الهواتف تستجيب للإشارة التي ترسلها أجهزة جمع المعلومات.

ورفضت وزارة العدل الأمريكية تأكيد أو نفي هذا التقرير. وقالت وول ستريت جورنال إنها حصلت على معلومات من مصادر مطلعة على البرنامج، أكدت أن طائرات من طراز سيسنا مجهزة بمعدات "ديرت بوكس" كانت تنطلق من خمسة مطارات أمريكية على الأقل. وقالت الوزارة إنها تعمل ضمن القانون الفيدرالي. وتطلق أجهزة "ديرت بوكس" إشارات مماثلة لتلك التي تنقلها أبراج الهاتف النقال التي تستخدمها شركات الاتصالات، وتلتقطها الهواتف بصورة عادية.

وعندما يحدث هذا فإن الهواتف ترسل بيانات حول معلومات التشغيل الخاصة بالشخص ومكان وجوده. وفي الوقت الذي تستخدم فيه هذه العملية لمراقبة شخص أو مجموعة صغيرة في منطقة معينة، فإن جميع الهواتف الموجودة في تلك المنطقة سوف تخضع للمراقبة. وقال الخبير الأمني البروفيسور آلان وودوارد: "إن تلك الأجهزة تعمل بنفس طريقة تشغيل "ستينغراي"، أحد الأدوات الشائعة لمراقبة الهاتف النقال". وأضاف: "الحكومة تستخدم "ستينغراي" المتاح للاستخدام حاليا من أجل التجسس على الهواتف النقالة، لكن الحكومة ليست هي الجهة الوحيدة، فمقابل 2000 استرليني يمكن الحصول على (هذه التقنية) واستخدامها". بحسب رويترز.

والأدوات أمثال "ستينغراي" و"ديرت بوكس" تعرف أيضا باسم كاشف (هوية مشترك الهاتف الدولي)، لأنها تجمع بيانات الهوية الخاصة التي يرسلها كل جهاز فردي إلى الشبكة. وعن طريقة عملها أوضح وودوارد: "انها تحاكي في جوهرها الشبكات بالتظاهر أنها برج إشارة هاتف نقال، وتوقف تشغيل التشفير ثم يمكن استخلاص جميع أنواع المعلومات مثل المكالمات التي جرت ومتى وأين، وغيرها". وأشار وودوارد إلى أنه غير متفاجئ من سماع استخدامها. مضيفا :"إنها سهلة الاستخدام، واستخدامها من الجو هو أفضل مكان لفعل هذا، لكن السؤال هو تحت أي تشريع يفعلون هذا وماذا يفعلون بالبيانات".

تحريات أمنية

في السياق ذاته ذكرت صحيفة نيويورك تايمز إن مئات الموظفين الذين لهم صلات خارجية ويعملون مع مكتب التحقيقات الاتحادي الأمريكي يخضعون لما يصفونه بتحريات استفزازية غير عادلة عن خلفياتهم تجبر بعضهم على قطع الاتصال بافراد عائلاتهم في الخارج. ويخضع كل موظفي

مكتب التحقيقات الاتحادي لفحص أمني ولكن وفقا لهذه الرواية فإن الموظفين الذين يتقنون لغات أجنبية ومن لهم عائلات أو أصدقاء في الخارج يجدون أنفسهم يواجهون مقابلات أكثر حدة وأكثر تكرارا واختبارات على أجهزة كشف الكذب ومراجعات للسفريات الشخصية والاتصالات الالكترونية وتحميل الملفات.

وقال مايكل كورتان المتحدث باسم مكتب التحقيقات إنه يؤكد التعليق الذي أدلى به لنيويورك تايمز. وقال كورتان للصحيفة إن مكتب التحقيقات يسعى إلى حماية المعلومات الوطنية الحساسة والسرية في الوقت الذي يأخذ في اعتباره أي تأثير على أي موظف. وأنشأ مكتب التحقيقات الاتحادي برنامجا بعد هجمات 11 سبتمبر أيلول 2001 يعرف اختصارا باسم "بارم" يهدف إلى مراقبة الموظفين والمتعاقدين الذين قد تشكل خلفياتهم أو أنشطتهم أو علاقاتهم خطرا أمنيا. ودفع إلى هذه الخطوة مخاوف من احتمال إرغام جواسيس أو منظمات أجنبية تصنف على أنها إرهابية الموظفين والمتعاقدين الذين لهم صلات بالخارج لكشف معلومات سرية تتعلق بالأمن القومي. بحسب رويترز.

ومن بين العاملين الذين وضعوا ضمن برنامج بارم مسلمون وآسيويون تعاقد معهم مكتب التحقيقات كلغويين أو للقيام بأدوار آخرى لمواجهة معلومات المخابرات أو لمكافحة الإرهاب. وبحلول عام 2012 زاد مكتب التحقيقات تعاقده مع لغويين بنسبة 25 في المئة واعتبرت العربية والصينية والفارسية من بين اللغات التي تحتل أولوية قصوى. ويقول موظفون غاضبون في مكتب التحقيقات إن البرنامج متحيز ويحول دون تقدمهم الوظيفي وغالبا ما يستخدم لمعاقبتهم. وقال مسؤولون بمكتب التحقيقات لم تنشر أسماؤهم إن البرنامج يحمي البلاد بالاضافة إلى الموظفين ولا يفرق في المعاملة ضد هؤلاء العاملين أو يعرقل تدرجهم الوظيفي.