تحديات

«إن الإصرار على منع سلطات تطبيق القانون من الاطلاع على الاتصالات والرسائل المشفرة يسهل على المقاتلين والمتعاطفين مع تنظيم الدولة الإسلامية مهاجمة الولايات المتحدة».

جيمس كومي
مدير مكتب التحقيقات الاتحادي الأميركي (أف بي آي)

هل تسهل «سي آي ايه» لروسيا التجسس على المسؤولين الأميركيين

● صمت الاستخبارات الأميركية عن ثغرات شركات التكنولوجيا يجعلها لقمة سائغة لدول معادية ● سلاح تجسس أميركا ينقلب عليها

سباق على اختراق شركات التكنولوجيا دون ضجيج

تصمت عمدا وكالات الاستخبارات الأميركية على ثغرات في برامج ينتجها عمالقة التكنولوجيا الأميركيون بهدف استغلالها في عمليات تجسس محلية ودولية. لكن الأميركيين ليسوا الجهة الوحيدة التي تستطيع استغلال هذه الثغرات، إذ تتربص دول معادية بانتظار أي نافذة تستطيع أن تدخل منها إلى غرف مغلقة يحتلها مسؤولون أميركيون يستخدمون تكنولوجيا هذه الشركات باطمئنان.

❑ لندن – يعتقد عميل "سي أي إيه" الجالس في مكتبه بضاحية لانغلي من ولاية فيرجينيا أنه الوحيد على الكرة الأرضية الذي يعلم بثغرات شركات التكنولوجيا العملاقة، ومن ثم يستطيع اختراقها.

لكن ربما لم يخطر على باله أن قدرته على استغلال ثغرات شركات مثل "أبل" و"غوغل" ربما يكون عملا سهلا بالنسبة إلى وكالات استخبارات معادية، تبحث عن أدق التفاصيل حول عمل مسؤولين رفيعي المستوى في واشنطن.

ونشر موقع ويكيليكس وثائق تصف أدوات سرية للتسلل الإلكتروني وأجزاء من أكواد كمبيوتر تستخدمها وكالة المخابرات الأميركية.

واختبر ويكيليكس برنامجا واحدا من بين برامج تجسس سي أي إيه على أنظمة تشغيل ميكروسوفت "ويندوز إكس بي، وفيستا، وويندوز 7. ويقوم هذا البرنامج بإدخال كود سري يمكن المخترق من الحصول على ذاكرة الجهاز ووسائط تحكم أخرى.

ولم ينشر ويكيليكس البرامج الكاملة اللازمة من أجل الاختراق الفعلي للهواتف وأجهزة الكمبيوتر وأجهزة التلفزيون المتصلة بالإنترنت.

ستيفن أفترغود

القاعدة هي أن الجميع يتجسس على الجميع، باستثناء وجود اتفاق بين طرفين على عدم التجسس على بعضهما البعض

ومن المؤكد أن عمالقة التكنولوجيا، الذين يمثلون إحدى أدوات الهيمنة الأميركية على سوق التكنولوجيا والإنترنت في العالم، قد تحولوا إلى هدف سهل في مرمى أجهزة الاستخبارات الروسية والصينية، بعدما قدمتها لهم وكالات الاستخبارات الأميركية على طبق من ذهب.

وبذلك أوقع مجتمع الاستخبارات الأميركي، الذي يتكون من أكثر من 70 ألف موظف ومتعاقد، بلاده في شرك دول معادية للولايات المتحدة دون أن يدري.

وفي ديسمبر الماضي حذرت شركة ياهو من أنها اكتشفت هجوما إلكترونيا ضخما قالت إنه شمل السطو على بيانات أكثر من مليار حساب للمستخدمين في أغسطس 2013، مما يجعله أكبر اختراق في التاريخ.

وبلغ عدد الحسابات المتضررة مثلي العدد المذكور في اختراق عام 2014 الذي أعلنته الشركة في سبتمبر، واتهمت قراصنة يعملون لصالح إحدى الحكومات بالمسؤولية عنه.

ولاحقا قالت ياهو إن الدولة التي كانت تشير إليها هي روسيا.

وتعزز استراتيجية أجهزة أمنية أميركية مازالت تعمل بعقلية تقليدية من فرص جعل شركات تكنولوجية عرضة لعمليات قد تؤدي بها إلى انهيار كامل، مثلما حدث مع ياهو.

ويخشى مسؤولون أمنيون في الولايات المتحدة من قوة التشفير في برامج وتطبيقات قد يستخدمها متشددون إسلاميون لتنسيق القيام بهجمات على الأراضي الأميركية.

ويقول جيمس كومي مدير مكتب التحقيقات الاتحادي الأميركي (آف بي آي) إن منع سلطات إنفاذ القانون من الاطلاع على الاتصالات المشفرة يسهل على المتعاطفين مع تنظيم الدولة الإسلامية مهاجمة الولايات المتحدة.

ويطالب المكتب شركات التكنولوجيا بالسماح لسلطات إنفاذ القانون بالاطلاع على الاتصالات المشفرة للتحقيق في الأنشطة غير القانونية. لكن الشركات تقاوم وتقول إن السماح بهذا سيقوض التشفير ويضعف الأنظمة في مواجهة المجرمين والمتسللين.

وكان كومي انتقد في السابق شركتي "أبل" و"غوغل" لتكثيفهما عملية التشفير.

ووسط إصرار الشركات على حماية مستخدميها، تلجأ وكالات الأمن الأميركية إلى استغلال ثغرات تظهر بين الحين والآخر في أنظمتها، وتتعمد عدم إخبار أغلب الشركات حتى لا تتمكن من وضع حدّ لها.

وما من مسؤول أو سياسي أميركي لا يستخدم أنظمة هذه الشركات؛ من هواتف "أيفون" من أبل أو أجهزة كمبيوتر مايكروسوفت التي تعمل بنظام تشغيل ويندوز، أو أجهزة أخرى من إنتاج شركة سامسونغ، التي تعمل بنظام التشغيل أندرويد.

وفي سبيل التجسس على مواطنين عاديين من أجل الحصول على معلومات قد تساعد في عرقلة أي هجمات محتملة، تسمح وكالات الاستخبارات الأميركية لدول معادية بالتسلل إلى أدق أسرار المسؤولين الأميركيين.

ويقول محللون في مجال التكنولوجيا إن الاستخبارات الأميركية "تقدم دون قصد كنزا استخباراتيا للروس بشكل غير معلن، بينما يقدم ويليام أسانج هذه المعلومات إلى العالم بأسره".

وفي أكتوبر الماضي اتهم عميل روسي باختراق موقع البحث عن الوظائف "لينكد إن"، إذ تمكن من تسريب بيانات أكثر من 117 مليون مستخدم. وبعد اعتقاله في التشيك، تدخلت السلطات الروسية لمنع ترحيله إلى الولايات المتحدة حيث تجرى المحاكمة.

عقاب أميركا بسلاحها

كان الهدف الرئيسي لوكالات الاستخبارات في العالم هو المسؤولين في دولة معادية تملك أجهزة استخبارات منافسة. ولم تكن ثمة طرق غير تقليدية للقيام بذلك.

يقول ستيفن أفترغود، مدير وحدة معنية بسرية أنشطة الحكومة في اتحاد العلماء الأميركيين، إن "القاعدة هي أن الجميع يتجسس على الجميع، باستثناء وجود اتفاق بين طرفين على عدم التجسس على بعضهما البعض... لكن في بعض الأحيان يحدث التجسس حتى مع وجود اتفاق".

واعتمدت أجهزة الاستخبارات على وحدات داخلية متقدمة تقوم بالأساس على عملاء من البشر، تعمل على زراعتهم بين صفوف العدو من أجل جمع المعلومات عن خطط وتحركات مسؤولين كبار قد تشكل تهديدا محتملا.

لكن اليوم بات الإنترنت هو العميل المشترك بين كل وكالات الاستخبارات في العالم، أو يمكن اعتباره "جاسوسا مزدوجا".

والإنترنت هو سلعة تجسس غير مكلفة، وتتوفر لدى كافة مسؤولي الاستخبارات بشكل متساو. وتتوقف قدرة كل جهاز على جمع أكبر قدر من المعلومات على مهارة فريق من القراصنة يشكل وحدة التجسس الإلكتروني.

وهذه الوحدة هي رأس الحربة في ضرب وكالات الأمن الإلكتروني التي تفطنت

> **اليوم بات الإنترنت هو العميل المشترك بين كل وكالات الاستخبارات في العالم، أو يمكن اعتباره وفق معايير الأمن «جاسوسا مزدوجا»**

دول غربية لإنشائها، وعززتها دول أخرى خصوصا بعد جدل كشف عن مساعدة فريق قراصنة روسي للرئيس الأميركي الجديد دونالد ترامب في الفوز بانتخابات الرئاسة، التي أجريت في نوفمبر الماضي.

ويقول جيرمي كيرك، الخبير في القرصنة التكنولوجية إن "روسيا تتعاقد مع مجموعة من القراصنة الذين يعملون بشكل مستقل كي يساعدوا في أنشطة الحكومة تجاه خصومها الخارجيين، وهذا ما جرّ لها اتهامات غير مسبوقة، ستشكل حجر عثرة في طريق العلاقات الروسية الأميركية في المستقبل".

وتُشكل جلسة الاستماع العلنية التي عقدت الاثنين، لمدير مكتب التحقيقات الفيدرالي جيمس كومي ومدير وكالة الأمن القومي مايك روجرز، محط آمال بتقديم توضيحات لمسائل تعكر صفو الحياة السياسية الأميركية منذ أسابيع، من بينها اتهامات الرئيس لسلفه بالتنصت عليه وعلاقات فريقه بروسيا.

وهذه هي المرة الأولى التي يتحدث فيها كل من كومي وروجرز علنا عن المسألتين الحساستين أمام لجنة الاستخبارات في مجلس النواب.

وفي يناير خلصت الاستخبارات الأميركية بالإجماع إلى أن قراصنة يعملون لصالح روسيا تمكنوا من اختراق رسائل البريد الإلكتروني لكبار المسؤولين الديمقراطيين ونشروا المحرجة منها بهدف مساعدة ترامب في الفوز على منافسته الديمقراطية حينها هيلاري كلينتون.

لكن الكشف الذي أظهره موقع ويكيليكس لم يدع مجالا لأي شك في أن الولايات المتحدة تمتلك إمكانيات تمكنها من القدرة على التجسس على أي دولة في العالم، مهما بلغت قوتها الأمنية والعسكرية والسياسية.

التكالب على عمالقة التكنولوجيا

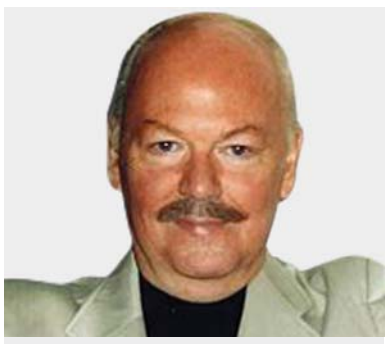
يقول جيمس بامفورد، وهو كاتب متخصص في شؤون الاستخبارات الوطنية الأميركية، إن "كل الدول لديها أسلحة للتجسس، لكن كل هذه الأسلحة لا تتعدى بندقية جيب، مقارنة بما تملكه الولايات المتحدة". وأضاف "بمعايير التجسس، الولايات المتحدة تملك سلاحا نوويا".

وقال أفترغود "نحن نلتقط صورا ونتنصت على الكون بأكمله".

قال أسانج في مؤتمر صحافي في وقت سابق عبر خدمة فيسبوك لايف "في ضوء ما نعتقد أنها أفضل طريقة للمضي قدما وبالاستماع لتلك الدعوات من بعض المصنعين، قررنا العمل معهم لمنحهم بعض الاطلاع الحصري على التفاصيل الفنية الإضافية التي لدينا حتى يتسنى لنا تطوير عمليات إصلاح (نقاط الضعف) وتنفيذها حتى يكون الناس في أمان".

وإصلاح الثغرات في شركات التكنولوجيا سيغلق بابا كبيرا أمام أجهزة الاستخبارات الأميركية على وجه الخصوص، ويجعلها عاجزة عن زرع أعينها وآذانها داخل غرف صنع القرار في أغلب عواصم العالم.

ولا يعني هذا أن الاستخبارات الأميركية ستستسلم للأمر الواقع، إذ توظف سي آي إيه ووكالة الاستخبارات الوطنية موظفين تنحصر مهامهم في ممارسة لا نهائية للعبة القط والفأر مع موظفين متخصصين في الأمن، يعملون لدى "أبل" و"غوغل" على وجه الخصوص.



جيمس بامفورد

بمعايير التجسس، كل دولة تملك بندقية جيب، والولايات المتحدة تملك سلاحا نوويا

فاختراق أجهزة التلفزيون والهواتف الذكية وأجهزة الكمبيوتر المحمول قد تمتد إلى أجهزة منزلية أخرى تشمل غسالات الملابس وخزانتها وماكينة صنع القهوة وساعة المنبه.

وهذا يعني أن استخبارات معادية للولايات المتحدة لن تقف كي تتفرج.

ويقول محللون في الأمن إن الاستخبارات الروسية تسعى إلى اختصار الطريق، إذ تحاول الوصول إلى مصدر المعلومات الأساسي داخل خزانة سي آي إيه وأجهزة أميركية أخرى، تكون قد حصلت على معلوماتها عبر اختراق شركات التكنولوجيا.

وبهذا تصبح شبكة التجسس معقدة تماما، إذ "تقوم الاستخبارات الغربية باصطياد الفريسة، ثم تأتي الاستخبارات الروسية لتسطو عليها وتلتهمها".