

كيف استغلت الاستخبارات الروسية شركات التكنولوجيا لديها في الحرب السيبرانية؟

كتبه خافيير إسكاليرا | 20 أكتوبر, 2017



ترجمة وتحرير: نون بوست

“لا نتحدث عن بوتين، واستخدم برمجية روسية”، هذه أوامر موسكو التي تفرضها على مجموعة المتصيدين أو ما يعرف “بالتروول”، الذين يتلقون دفوعات تصل إلى حوالي ألفي يورو شهريا، خلال الحرب السيبرانية. في الغالب، تسلط الأضواء على شركات الإنترنت الروسية، سواء داخل أو خارج البلاد.



الرئيس الروسي، فلاديمير بوتين، في زيارة له إلى مدينة أورينبورغ، خلال مناورات عسكرية داخلها قم بتحسين هذا التحرير باللغة الإنجليزية، أو استلهم جملة من الأفكار من سلسلة “بيت من ورق”، أو لا تضيعوا الوقت في الحديث عن بوتين وروسيا، أو قوموا بإحداث أكبر قدر ممكن من

الفوضى والجدل... عموماً، تعد هذه العبارات من بين التعليمات التي يتلقاها "التربول" الروسي بعد انتهاء الحصة الأولى من دوامه، خلال استراحة القهوة. وتجدر الإشارة إلى أن هؤلاء المتصيدين يتقاضون ما يصل إلى حدود ألفي يورو في الشهر.

كشف ماكسيم، أحد المتصيدين الذي عمل لمدة 18 شهراً في "شركة متصيدين" مقرها في سانت بطرسبرغ، لقناة "دوشت" الروسية خلال سنة 2015، أن مهمته كانت تقتضي نشر أخبار تفيد أن هيلاري كلينتون كانت غنية. ومن مهامه الأخرى أيضاً، نشر أخبار حول "رسائل البريد الإلكتروني التي تم نشرها بعد اختراق حساب كلينتون، وإظهار أن عائلة كلينتون هي التي تقود الولايات المتحدة الأمريكية منذ فترة". وأضاف ماكسيم أن "مهمة المتصيدين كانت تتمثل في الدخول على أي منصة كانت، وعدم الدفاع عن أية جهة...".

من جانب آخر، ساهم الكشف عن هذه التحركات على شبكة الإنترنت، في تنامي حالة عدم الثقة بين مختلف الأطراف الدولية. ففي خضم هذه "الحرب الإعلامية الباردة"، اعتبرت روسيا أن فيسبوك ويوتيوب، وانستغرام، وتويتر، وريديت، وغوغل بمثابة أسلحة بين يدي الغرب. لكن في الوقت ذاته، كانت هذه الوسائل الذخيرة التي اعتمدها القراصنة الروسيون في حرب "الصواعق"، التي شنوها على جهات مختلفة ومتعددة على غرار الانتخابات في الولايات المتحدة الأمريكية أو الانتخابات العامة الألمانية. وبناء على ذلك، أصبحت شركات الإنترنت الروسية في دائرة الضوء، سواء داخل البلاد أو خارجها.

راودت الولايات المتحدة الأمريكية جملة من الشكوك حول إمكانية عمل مكافح الفيروسات الروسي، كاسبيرسكي، بطريقة غير مباشرة لصالح أجهزة الاستخبارات التي تسيطر عليها موسكو.

في الوقت الراهن، باتت جهات الحروب الإعلامية المفتوحة، أكثر عدداً من أي وقت مضى. وفي خضم هذه الصراعات، يقع الكثير من "المقاتلين" في مصيدة الخلط بين الإعلانات الكاذبة التي تنشر على موقع فيسبوك، وبين بوتات الإنترنت التي تنشر أخباراً تدعم النزعة الانفصالية الكتالونية، أو الإشاعات التي راجت حول الانتخابات الفرنسية في نهاية الحملة الانتخابية.

من جانب آخر، يواجه "جنود الخفاء الروس" نوعاً آخر من الخلط. ففي الوقت الذي يتلقون فيه تعليمات بتعزيز صفوفهم وحشد المزيد من القوات، أمر الرئيس الروسي فلاديمير بوتين الشركات التكنولوجية باستعمال البرمجيات الروسية لا غير، وإلا ستفقد هذه الشركات دعم الدولة. وفي الأثناء، تعجز المؤسسات الحكومية الروسية عن استعمال برمجية أجنبية، نظراً لأنها تمثل خطراً على الأمن السيبراني الوطني.

في هذا السياق، كشف "إيليا. آل"، وهو مسؤول اعتاد التعامل مع المعلومات المتعلقة بالأجهزة الأمنية، أن "الشركات الروسية، في حقيقة الأمر، لا تزال تستخدم بشكل رئيسي التكنولوجيا

المستوردة. في المقابل، أصبحت موسكو اليوم تعتبر التكنولوجيا الأجنبية بمثابة حسان طروادة". في الواقع، لا تتبنى روسيا فقط هذا الموقف. فوجهة نظر موسكو ليست إلا ردا على حالة عدم الثقة الشائعة على الجانب الآخر من المحيط الأطلسي.

على امتداد العديد من السنوات، راودت الولايات المتحدة الأمريكية جملة من الشكوك حول إمكانية عمل مكافح الفيروسات الروسي، كاسبيرسكي، بطريقة غير مباشرة لصالح أجهزة الاستخبارات التي تسيطر عليها موسكو. وفي الفترة الأخيرة، تأكدت المخاوف الأمريكية. وقد تجلّى ذلك من خلال الأوامر التي وجهتها وزارة الداخلية الأمريكية لجميع وكالاتها بالتوقف عن استخدام أي منتجات تابعة لشركة كاسبيرسكي. في الواقع، اتخذت الداخلية الأمريكية هذه الإجراءات، على خلفية لعب برمجية شركة أمن الحواسيب الروسية، كاسبيرسكي، دورا في سرقة برمجيات وكالة الأمن القومي الأمريكية. وفي هذا الصدد، يشتبه أن قرصنة روسيين، هم من نفذوا هذه العملية.

صورة لانعكاس ظل رجل يشاهد شعار وكالة الأمن القومي الأمريكية، في سرايفو.

في بعض الأحيان، تلجأ أجهزة الاستخبارات الأمريكية، وحتى وكالة الأمن القومي، إلى اعتماد الفيروسات بهدف الوصول إلى أجهزة كمبيوتر أفراد آخرين، أي تماما مثل ما يفعل القراصنة. وقد اكتشفت هذه الحقيقة خلال سنة 2015، عندما وقع التجسس على حاسوب خاص تابع لأحد المتعاونين الخارجيين مع أجهزة الاستخبارات الأمريكية. وبالتالي، يمكن القول إن بعض القراصنة يستولون على المعلومات التي استحوذ عليها أحد “السارقين” خلال قيامه بنفس عملهم.

في ظل هذه المعطيات، انتشرت المخاوف في صفوف الأفراد على نطاق أوسع، حيث توقفت العديد من الشركات الأمريكية عن التعامل مع برنامج كاسبيرسكي. في المقابل، تحولت هذه الشركة إلى ضحية للنزاع الجيوسياسي بين روسيا والولايات المتحدة الأمريكية.

من المؤكد أن شركة كاسبيرسكي تخفي بين صفوف العاملين فيها موظفين كانوا في السابق جزءا من جهاز الاستخبارات الروسي. ويمثل هذا المعطى سببا كافيا حتى تضع الولايات المتحدة الأمريكية هذه الشركة تحت مراقبة أمنية. لكن يبقى السؤال المطروح: ما الدور الذي يلعبه مكافح الفيروسات في إطار عمليات التجسس أو القرصنة؟ عموما، يستطيع مكافح الفيروسات القيام بمختلف الأمور والمهام، نظرا لأن جميع الملفات الموجودة في الحاسوب “والحوسبة السحابية” متاحة له.

في شأن ذي صلة، تعد الأوامر القانونية للدول أمرا بالغ الأهمية. وقد كشف أندري سولداتوف، أحد مؤلفي كتاب “الشبكة الحمراء”، الذي يتطرق إلى عن الضغوط التي تمارسها روسيا على شبكة الإنترنت؛ أن “البيئة التي تنشط فيها شركات أمن الحواسيب في روسيا شهدت تغييرات جذرية، خاصة منذ سنة 2014”.

اعتبر مؤسس شركة تيليغرام، بافيل دوروف، أن “أجهزة الاستخبارات الروسية ترغب في أن يسمح لها بالوصول إلى المراسلات الخاصة، إلا أن ما تقوم به يعد محاولة لتوسيع نفوذها على حساب الحقوق الدستورية للمواطنين”

وأضاف سولداتوف أن “الكرملين باتت منذ ذلك التاريخ أكثر تشددا، في حين أصبحت التشريعات تتدخل في الأوضاع الداخلية للشركات والأفراد، وتسمح لأجهزة الاستخبارات بالوصول إلى البيانات وحتى دخول مكاتب الشركات”. وأورد الكاتب أن “ثلة من الشركات مثل كاسبيرسكي، تتعرض لضغوط هائلة في روسيا وفي الولايات المتحدة الأمريكية على حد سواء، مع العلم أن الوضع السائد قد تغير وبشكل كبير في هذه البلدان”. من جهته، لا يستبعد مؤسس الشركة، يوجين كاسبيرسكي، أن تستفيد أجهزة الاستخبارات الروسية من الثغرات الأمنية الموجودة في برامج شركته.

من جهة أخرى، تم تضييق الخناق أيضا على شركة روسية أخرى، وهي تيليغرام. وفي مطلع هذا الأسبوع، قامت محكمة موسكو بتغريم شركة تيليغرام، على خلفية رفضها مد أجهزة الأمن الروسية مفاتيح التشفير من أجل التمكن من الوصول إلى رسائل بعض المستخدمين. وفي ظل عزوفها عن القيام بواجبها المتمثل في “تقديم المعلومات اللازمة لأجهزة الأمن”، ستضطر هذه الشركة إلى دفع

من جانبه، اعتبر مؤسس شركة تيليغرام، بافيل دوروف، أن "أجهزة الاستخبارات الروسية ترغب في أن يسمح لها بالوصول إلى المراسلات الخاصة، إلا أن ما تقوم به يعد محاولة لتوسيع نفوذها على حساب الحقوق الدستورية للمواطنين". وقد تعهد دوروف بمواصلة حربه القانونية ضد هذه الضغوط، مع الأمل أن يفوز فيها. في حقيقة الأمر، خسر بافيل دوروف معارك قانونية في السابق. وفي سنة 2014، قرر مؤسس شركة تيليغرام مغادرة روسيا بعد أن ندد بالضغوط التي تمارسها ضده الأجهزة الأمنية من أجل الكشف عن محادثات لمعارضين روسيين يستخدمون موقع فكونتاكتي، الذي أسسه سنة 2006، للتراسل فيما بينهم.

صورة لخدمة تيليغرام خلال مؤتمر صحفي في جاكرتا.

على العموم، تتهم العديد من الدول تطبيق تيليغرام، بتسهيل الاتصالات بين عناصر تنظيم الدولة.

فضلا عن ذلك، جعلت قدرته على الوصول إلى عدد غير محدود من الأشخاص، بعض الحكومات تحكم مراقبتها عليه، معتبرين إياه وسيلة مثالية للتخريب والقيام بعمليات خفية. وعلى العموم، اعتبرته العديد من الحكومات وسيلة تدعم التمرد بجميع درجاته ومستوياته.

على سبيل المثال، يتم تنظيم ما يسمى “بلجان الدفاع عن الاستفتاء” في كتالونيا للذهاب إلى الشوارع “والنضال من أجل إنشاء جمهورية كتالونية”، والتنسيق بين مختلف المجموعات، عن طريق تطبيق تيليغرام. وينطبق الأمر ذاته على المجموعات الشابة المعارضة لنظام بوتين، الذين ينضمون مظاهراتهم من خلال هذه الخدمة. وبالتالي، يعد الوجود المستمر لخدمة التراسل “تيليغرام” عائقا أمام الحكومة الروسية.

في الوقت الراهن، لا تفكر موسكو في حجب خدمة التراسل الفوري تيليغرام في روسيا، وهو ما أكده المتحدث باسم الكرملين، ديمتري بيسكوف. في المقابل، تشعر روسيا أنها موجودة بالفعل في قلب دائرة ضوء الحرب السيبرانية، خاصة بعد عملية إجلاء أكثر من 300 ألف شخص في جميع أنحاء البلاد على خلفية موجة الأخبار الكاذبة التي استمرت على مدى أسبوعين، حول بعض التفجيرات في المنطقة.

في الحقيقة، وردت التحذيرات من خارج روسيا، وتمت عبر الإنترنت، وهو ما مثل عائقا أمام تتبع المسؤولين عن هذه العملية بشكل فعال. وفي هذا السياق، أورد فرانتس كلينتسيفيتش، عضو مجلس الشيوخ الروسي وعضو لجنة الدفاع في مجلس الاتحاد الروسي، أن “هذه العملية تعد بمثابة “حرب إلكترونية على نطاق واسع”، محذرا من رد فعل روسيا المؤكد. من هذا المنطلق، لسائل أن يسأل: ما إذا سيكون الرد الروسي عن طريق تعزيز موجة الضغوط على شركاتها أو عن طريق هجوم آخر تتكفل بتنفيذه “شركة المتصيدين” الواقعة في شارع سانت بطرسبورغ.

المصدر: [صحيفة الكونفدنسيال الإسبانية](#)

رابط المقال : <https://www.noonpost.com/20357/>