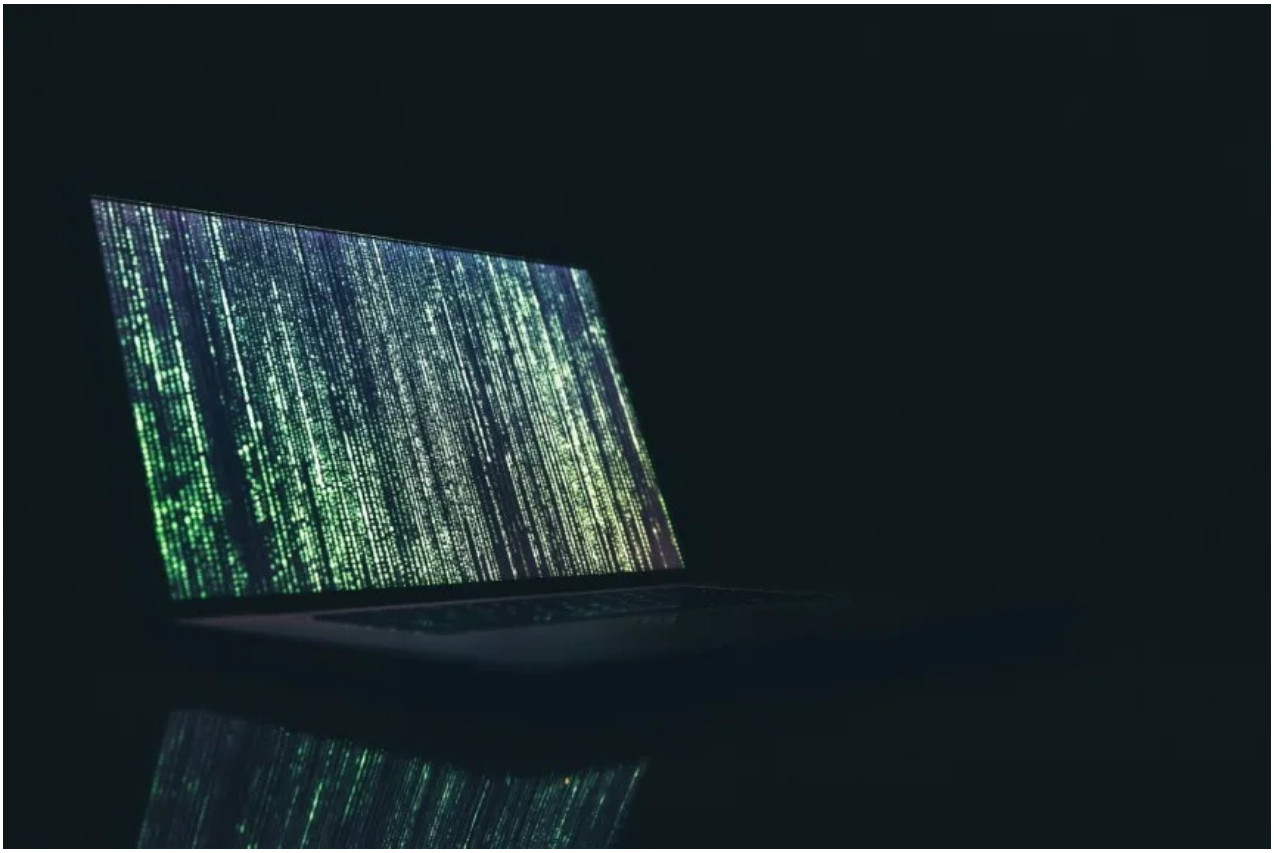
هكذا تخلق الهجمات الإلكترونية المشاكل السياسية



ترجمة وتحرير: نون بوست

تحدث رئيس شركة "فاير آي" الأمريكية المختصة في مجال الأمن الإلكتروني، كيفين مانديا، عن مساهماته في تشكيل ملامح السياسة الدولية. ففي سنة 2014، ألقى مانديا محاضرة تحدث فيها عن الأسباب التي دفعته إلى نشر تقرير يحتوي على 60 صفحة حول الهجمات الإلكترونية، التي تعرض لها جيش التحرير الشعبي الصيني.

في هذا الصدد، صرح رئيس شركة "فاير آي" قائلا: "تضم شركتنا أشخاصا عملوا في السابق في المجال العسكري. وبصراحة، يعلم كل شخص أن الهجمات الإلكترونية قد حصلت بالفعل، لكن لا أحد يجرؤ على الحديث عنها. لذلك، نشرتُ تقريرا بشأن هذه الهجمات حتى يكون الجميع على بيّنة بالأمر". وتجدر الإشارة إلى أن هذه الشركة الواقعة في كاليفورنيا، والتي يعمل فيها أكثر من 3000 موظف، مختصة في مكافحة الهجمات السيبرانية.

من خلال التحليل الذي أجرته بشأن عملية التجسس الصينية، حاولت هذه الشركة إجبار حكومات القوى العظمى على التدخل لمكافحة الهجمات الإلكترونية. وعلى الرغم من أن العديد من الصحف تطرقت إلى خبر الهجمات الإلكترونية التي استهدفت جيش التحرير الشعبي الصيني، إلا أن الحكومة الصينية فندت الأمر. ومن جهته، أعرب البيت الأبيض خلال عهد الرئيس الأسبق باراك أوباما عن قلقه بشأن هذه الهجمات خلال مفاوضاته مع شخصيات صينية رفيعة المستوى.

تُعتبر القرصنة أهم أداة تستخدمها الدول للتجسس

في الواقع، تعيش الشركات المختصة في الأمن الإلكتروني، التي تحلل هجمات القراصنة، وضعا

استثنائيا، حيث تنشر المعلومات لدى جهات ستتكتّم حتما عن الأمر على غرار الشركات المُخترقة، التي تخشى المساس بسمعتها، والدول المُخترقة التي تخشى أن يعلم مواطنوها ما حدث، فضلا عن القراصنة الذين يرغبون في العمل لصالح الأجهزة الاستخباراتية بشكل سري.

في هذا الصدد، اعترف موظف لدى شركة أمن إلكتروني بأن شركته قد تفضح ممارسات قراصنة الأجهزة الاستخباراتية أمام كل العالم.علاوة على ذلك، أفاد هذا الموظف بأنه "في حال بادرنا بتعقب آثار القراصنة، سيعد ذلك بمثابة رسالة تُعلمهم فيها بأننا تفطنّا لفعلتهم وبأننا نعلم كل نواياهم ودوافعهم. وبهذه الطريقة، نحذرهم من انكشاف أمرهم أمام العالم أجمع".

عموما، يجب علينا أن نطرح الأسئلة التالية: كيف تتصرف شركات الأمن الإلكتروني عندما تنشر التقارير بشأن الهجمات الإلكترونية؟ وأي دور سياسي تلعبه هذه التقارير؟ للإجابة على هذه الأسئلة، تحدثت صحيفة "زود دويتشه تسايتونغ" مع أكثر من 10 أشخاص. ومن بين هؤلاء، نذكر الباحث لدى مركز الدراسات الأمنية بالمعهد الفدرالي السويسري للتكنولوجيا في زيوريخ، فلوريان إيغلوف، الذي قال إن "التقارير التي تُعنى بالهجمات الإلكترونية تتناول البعد السياسي لهذه الهجمات".

فضلا عن ذلك، يجب علينا أن نطّلع على كل المستجدات بشأن الصراعات في العالم الرقمي". وفي السياق ذاته، أضاف إيغلوف قائلا: "جلّ معلوماتنا حول الصراعات في العالم الرقمي، محدودة. في المقابل، لا تكشف تقاريرنا سوى عن حقائق". وفي سياق متصل، أورد خبير آخر مختص في الأمن الإلكتروني أنه "لا يوجد أي شخص ساذج، حيث يعلم الجميع أن تقاريرنا لها تبعات سياسية".

أكبر مساوئ التجسس الرقمي: ترك آثار يمكن تقفيها

تُعتبر القرصنة أهم أداة تستخدمها الدول للتجسس. وعموما، تصل هذه الدول إلى المعلومات من خلال الثغرات الرقمية التي ترغب الحكومات والشركات في حمايتها. وتجدر الإشارة إلى أن ذلك يحمل في طياته أمرا إيجابيا، حيث لن تحتاج الدول لتجنيد مخبرين فعليين وإقناعهم بسرقة وثائق حساسة، ولن يتجاوز الأمر مجرد إسداء أوامر عن طريق لوحة المفاتيح. وسيتكفل أحد البرامج، على غرار برنامج حصان طروادة، بالاستيلاء على الوثائق بشكل سري.

بالإضافة إلى عمليات القرصنة، تحاول جهات فاعلة التأثير على الرأي العالم من خلال نشر أخبار كاذبة

في المقابل، يحمل التجسس الرقمي بعدا سلبيا يتمثل في ترك آثار على شبكات الشركات والدول. لذلك، يمكن للجهات المختصة في الأمن الإلكتروني، على غرار "فاير آي"، تتبع منفذي الهجمات. وعلى سبيل الذكر لا الحصر، حلل الفريق رقم 2672 لدى شركة "فاير آي"، منذ سنة 2006، الثغرات حتى يتمكن من إصدار التقرير المتعلق بتعرض الجيش الصيني للهجوم السيبراني. وعلى الرغم من أن التقارير حول الهجمات الإلكترونية تؤدي إلى اندلاع أزمات سياسية، إلا أنها تتسم بالشفافية. وفي الحقيقة، بفضل هذه التقارير، يتمكن الرأي العام من الاطلاع على طريقة عمل القراصنة.

مخبرو حرب المعلومات

في الكثير من الأحيان، تجري الشركات تحاليل على نوع آخر من الهجمات الرقمية، ألا وهو حرب المعلومات. فبالإضافة إلى عمليات القرصنة، تحاول جهات فاعلة التأثير على الرأي العالم من خلال نشر أخبار كاذبة. وفي بعض الحالات، تحدث الاختراقات الحكومية بالتزامن مع حملات ترويج الأخبار الكاذبة. فعلى سبيل المثال، روج مصنع "ترول" الروسي سيء السمعة، خلال الحملات الانتخابية الأمريكية في سنة 2016، أخبارا زائفة من شأنها أن تثير البلبلة في الولايات المتحدة الأمريكية.

يشرف الباحث لدى شركة "فاير آي"، المختصّة في مجال الأمن الإلكتروني، لي فوستر، على فريق محللين يعنى بالحملات التي تحاول التأثير على الرأي العام في دولة محددة عن طريق نشر مقالات

موجهة في وسائل الإعلام الرقمية. واكتشف فريق فوستر شبكة من الحسابات، التي وُصفت في التقرير الصادر عن شركة فاير آي على أنها "إيرانية" وتنشط خاصة في أمريكا اللاتينية والولايات المتحدة الأمريكية والشرق الأوسط.

من جهته، أكد فوستر أن التقرير لم يدن إيران نظرا لأن المحللين لم يجدوا أدلة تثبت تورط دولة ما بشكل مباشر. في هذا الصدد، أفاد فوستر، أن "موظفين أو ثلاثة موظفين فقط عملوا على إصدار التقرير"، في حين أن التحقيق فيما يتعلق بالهجمات الإلكترونية يحتاج أدلة دامغة. في هذا الإطار، صرح فوستر، قائلا: "لا يمكننا إصدار تقارير للعموم بمجرد تأكدنا من معلوماتنا، حيث يتطلب الأمر المزيد من البحث والتقصي. وغالبا، لا تقرر الشركات نشر تقاريرها إلا في حال كان الوقت مناسبا لذلك".

يقول خبير أمن تكنولوجيا المعلومات، يعمل ضمن واحدة من الشركات الثلاثين الكبرى المصنفة في مؤشر داكس للبورصة الألمانية، إنه لا يهتم بشكل شخصي بمن يقف وراء الهجمات بل المهم هو تحقيق الأمن

أصدرت شركة "فاير آي" التقرير حتى يتسنى للخبراء العمل عليه وإثرائه ليتم نشره فيما بعد. وفي وقت لاحق، بادرت شركتا غوغل وفيسبوك بنشر تقارير معمقة وجهت فيها أصابع الاتهام إلى طرف محدد. ووفقا لمعلومات خاصة، تتحمل الإذاعة الحكومية الإيرانية مسؤولية الهجمات الإلكترونية. على ضوء هذه المعطيات، أقدمت شركة غوغل على غلق 39 قناة على موقع يوتيوب وحظر 652 حساب وصفحة ومجتمع إلكتروني على موقع فيسبوك تورط أصحابها في الهجمات الإلكترونية.

الشركات تستفيد من هذه التقارير في مجال العلاقات العامة

بالطبع لا تقوم الشركات بهذه الأبحاث والتقارير بشكل مجاني، أو بهدف جعل العالم أكثر أمانا، حيث يقول خبير في أمن تكنولوجيا المعلومات، يعمل ضمن واحدة من الشركات الثلاثين الكبرى المصنفة في مؤشر داكس للبورصة الألمانية: "الجميع يستخدمون هذه التقارير كأسلوب للتسويق". كما أوضح هذا الخبير، الذي اشترط مثل غيره الحفاظ على سرية هويته، أن "كل الشركات تريد أن تظهر ما لديها من مهارات ومعلومات، وهذا جزء من اللعبة، ويعتبر أمرا شرعيا".

يبدو أن التقارير المثيرة للانتباه لا تمكن الشركة فقط من تصدر نشرات الأخبار، بل تجذب إليها زبائن جدد. وفي المقابل فإن التقارير التي تتم صياغتها بشكل غير احترافي، وتتضمن معلومات تعجز عن إثباتها أو تثبت شركات أخرى منافسة خطأها، فإنها تجعل أصحابها يبدون غير جديرين بالثقة، وتدفع الزبائن للابتعاد عنهم. ويتمثل هؤلاء الزبائن غالبا في شركات، تسعى لشراء تحليلات معمقة، تكون متاحة فقط لمن يقومون بالاشتراك مقابل مبلغ مالي. كما تمتلك شركات الأمن السيبراني أنظمة للمراقبة والتحكم في تدفق المعلومات، ومعدات مراقبة أخرى تقوم ببيعها للشركات التي تحتاجها.

يقول خبير أمن تكنولوجيا المعلومات، من الشركة المصنفة ضمن مؤشر داكس، إنه لا يهتم بشكل شخصي بمن يقف وراء الهجمات بل المهم هو تحقيق الأمن. حيث يقول: "بالنسبة لنا لا معنى ولا فائدة من تحديد مصدر الهجوم، ولا فرق لدينا إذا كان من المخترقون من الصين أو روسيا أو الولايات المتحدة، مهمتنا هي إيقاف هذا الهجوم وإنقاذ الضحية. وأحيانا حتى المسؤول في الشركة التي تعرضت للاختراق يعمد إلى إخفاء الوقائع عن مديريه، لأنه سيكون في موقف محرج ويتعرض للتوبيخ، وبعضهم يسألوننا بكل سذاجة، حول ما إذا كنا نستطيع الاتصال بسفارة الدولة التي جاء منها الهجوم، ليساعدونا على إيقافه".

يقول موظف في وكالة ألمانية لأمن المعلومات: "هنالك نوع من التحقق والتدقيق قد يستمر لمدة سنوات، حيث تقوم الشركات بإرسال المعلومات لأطراف رسمية، تقوم بدورها لتأكيد المعلومات أو

نفيها".

لكن بالنسبة لشركات الأمن السيبراني، فإن مسألة مصدر الهجوم والأطراف التي تقف وراءه تعد في غاية الأهمية في إعداد التقرير، حيث يقول شخص متخصص في كتابة هذه التقارير: "إن البعد السياسي لا يمكن إنكاره، فنحن نريد أن نعرف ما هو الدافع وراء المجموعة التي قامت بالاعتداء".

تبادل المعلومات بشكل غير رسمي بين الشركة والدولة

فيما يتعلق بالتقارير التي تنطوي على حساسية خاصة، فإنه تحدث أحيانا عمليات تواصل غير رسمي بين الشركات والسلطات الأمنية، وهو ما أكده لنا بشكل منفصل اثنان من خبراء أمن تكنولوجيا المعلومات. وعلى سبيل المثال يتم تنسيق جهود عدد من الخبراء، لأن بعضهم كان يعمل لدى الدولة قبل أن توظفه الشركات، وفي هذا السياق يقول موظف في وكالة ألمانية لأمن المعلومات: "هنالك نوع من التحقق والتدقيق قد يستمر لمدة سنوات، حيث تقوم الشركات بإرسال المعلومات لأطراف رسمية، تقوم بدورها لتأكيد المعلومات أو نفيها".

بعض الشركات الأخرى تذهب إلى حد إرسال أحد موظفيها للعمل مع السلطات الرسمية، وهذا يحدث غالبا في الدول الغربية، ومن بينها البلدان الناطقة بالألمانية. وبحسب أحد الخبراء في هذا المجال؛ فإن السبب وراء هذا الإجراء هو أن منتجات شركات أمن تكنولوجيا المعلومات تكون مثبتة على مئات الملايين من أجهزة الحواسيب حول العالم، لذلك فإن هذه الشركات الخاصة تعرف جيدا كيفية عمل القراصنة في منطقة معينة، وماهي المناطق أو السلطات أو الشركات التي يستهدفونها.

بعد التحقق من ملفاتهم، فإن هؤلاء الموظفين يمكنهم العمل في المؤسسات الحكومية بالاعتماد على البيانات التي جلبوها من شركاتهم، والتي لا تقدر الدولة على الوصول إليها. وفي المقابل فإن الوكالات الحكومية تقوم أحيانا بإصدار برمجيات تصفح إنترنت تحتوي على ثغرات للتجسس، ولكنها تسمح للشركات المتعاونة معها بتحذير زبائنها من هذه الثغرات.

تأجيج الخلافات الدبلوماسية

عمل جو سلوفيك أيضا في مجال الهجمات السيبرانية لفائدة البحرية الأمريكية. وهو يحذر من مغبة التقليل من خطورة التبعات السياسية لهذه التقارير. وفي الوقت الحالي يعمل سلوفيك كمسؤول على أمن تكنولوجيا المعلومات في شركة "دراغوس" لحماية منشآت البنية التحتية، وهي تقوم على سبيل المثال بتأمين شبكات الكهرباء، وهو يقول: "إن الشركات الخاصة نادرا ما تقوم هي بتحديد من يقف وراء الهجمات الإلكترونية، لأن مثل هذه القرارات يمكن أن تصب الزيت على النار المشتعلة أصلا في العلاقات الدبلوماسية".

عبر العديد من الباحثين في مجال أمن تكنولوجيا المعلومات عن شكوكهم في أن الحكومات تتأثر سياسيا بمحتوى التقارير

من الحالات التي توضح خطورة إلقاء اللوم على جهة معينة، يذكر لنا هذا الموظف قضية متعلقة بوكالة أمن ألمانية، تعرضت لهجوم من إيران، وقد قام القراصنة باستخدام منتج خاص بشركة لصناعة مضادات الفيروسات. وقد تمكنت هذه الشركة من موقعها من مشاهدة المهاجمين والضحية في نفس الوقت أثناء تنفيذ العملية. وبحسب جو سلوفيك فإن هذه القضايا تكون معقدة، خاصة إذا كان الرأي العام مقتنعا مسبقا بأن طرفا معينا يقف وراء الهجوم، إذ إن هذا يسلط ضغطا على شركات التحليل وعلى السلطات الرسمية، وقد يؤثر على أحكامها، لأنها لاشعوريا قد تخشى من اختلاف نتائجها النهائية عن توقعات الرأي العام.

حظا سعيدا إلى اللقاء

عبر العديد من الباحثين في مجال أمن تكنولوجيا المعلومات عن شكوكهم في أن الحكومات تتأثر سياسيا بمحتوى التقارير. حيث يقول أحد الموظفين السابقين في المخابرات الأمريكية: "إن موظفي الشركات ليسوا خبراء سياسيين، وعندما يقدمون تقاريرهم فإن الحكومة الأمريكية لا تعلق عليها، بل تستمع إليها وتقول لهم حظا موفقا وإلى اللقاء". ومن المؤكد أن العديد من الشركات مستعدة لفعل أي شيء، لمعرفة التفاصيل التي تمتلكها الحكومة الأمريكية، حول مجموعات القراصنة في العالم، ولذلك فإن الموظفين الحكوميين يكتفون بتعلم تقارير الشركات دون التعقيب عليها.

توجد قائمة تضم 150 من أشهر مجموعات القراصنة في العالم التي تقوم بعملها لفائدة الدول، وهي تنحدر أساسا من روسيا والصين وإيران. أما عن حقيقة وجود تقارير قليلة حول الهجمات التي تنطلق من الولايات المتحدة وأوروبا، فهو لا يدل على غياب تلك الهجمات، بل لأن القراصنة الأمريكيين ينشطون بشكل احترافي ولا يتركون أثرا وراءهم، ولأن شهرة الشركات ونجاحها يرتبط بالمناطق التي يتواجد فيها زبائنها.

في هذا الصدد، يشار إلى أن اثنين من التقارير حول وقوف الولايات المتحدة وراء هجمات سيبرانية، صدرت عن الشركة الروسية كاسبرسكي، والآن بدأت الشركات الصينية أيضا بنشر تقاريرها، ولكن لا تزال هناك معلومات شحيحة حول العمليات التي تقف ورائها أجهزة غربية، ولكن في المستقبل فإن الرأي العام سيصبح مطلعا على معلومات أكثر حول هذا الموضوع.

المصدر: زود دويتشه تسايتونغ

رابط المقال: https://www.noonpost.com/24990/