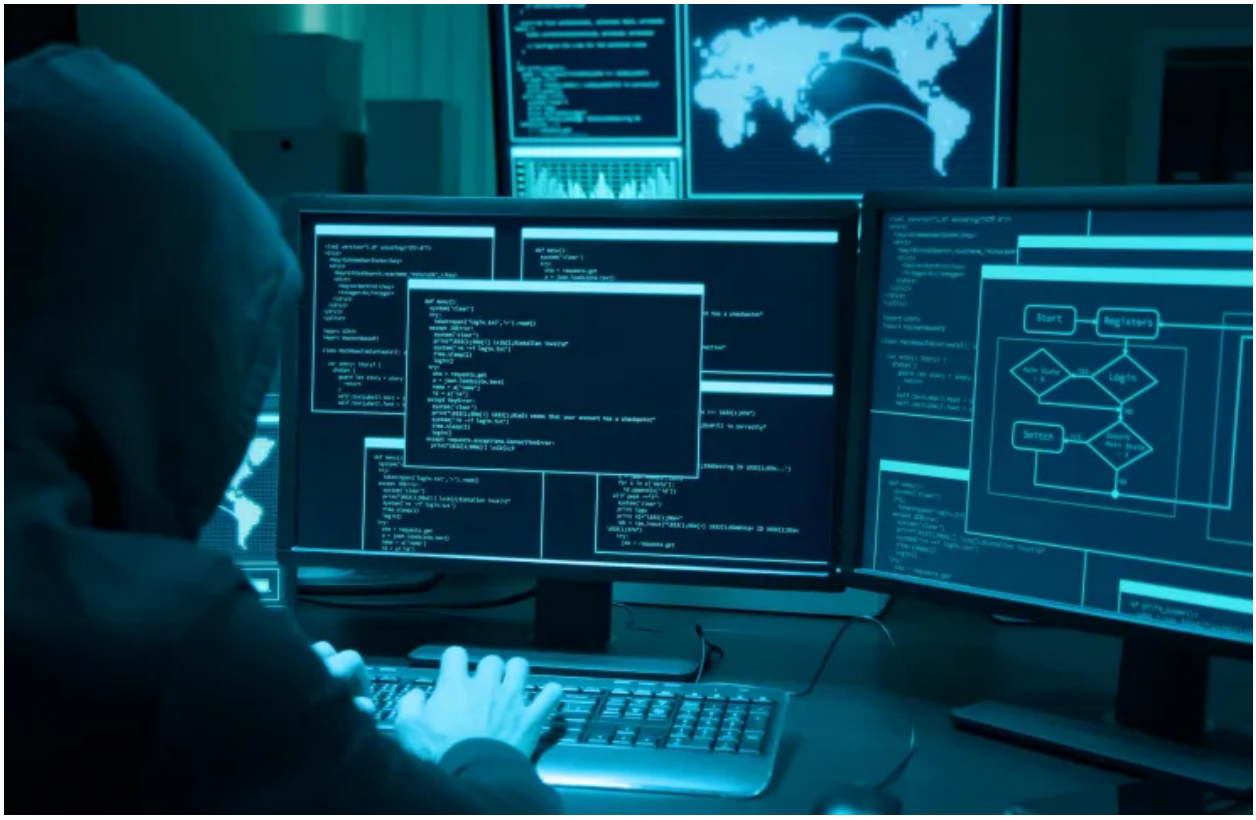
تحقيـق.. شركـات إسرائيليـة تُطـور أداة تجسس "مجنونة"

كتبه عومر بن يعقوب | 18 سبتمبر 2023,



ترجمة وتحرير: نون بوست

"نحن نعيش تحت المراقبة" باتت هذه حقيقة معترف بها عالميًا بشأن هذا العصر الرقمي؛ حيث تعرف شركات التكنولوجيا والإعلانية كل شيء تقريبًا عنا: أين نحن، وماذا نشتري، والتطبيقات التي ننزلها وكيف نستخدمها، وتاريخ بحثنا ومشترياتنا السابقة، وحتى ميولنا الجنسية والأنشطة التي نمارسها؛ لكن هناك شيء واحد فقط لا يستطيع المعلنون أن يصلوا إليه: وهو هويتنا، فمن المفترض أن يكون عالم الإعلانات والبيانات الذي يقف وراءه مجهولاً للعموم.

كلنا قرأنا منشور أحد الأصدقاء الذي عاد للتو من الإجازة، وبعد ساعات قليلة يظهر على شاشتنا إعلان عن فندق، ويلاحقنا مثله لأيام، يتابعنا عبر المواقع ووسائل التواصل الاجتماعي؛ لكن القليل منا لديه فكرة كيف أو لماذا يحدث هذا.

كلما فتحنا تطبيقًا أو موقعًا إلكترونيًا على هاتفنا، دون أن نلاحظ ذلك، تحدث عملية سريعة من المفاوضات الجماعية، وينشأ سوق معقد وقوي يجسد اقتصاد الإنترنت بأكمله: في جزء من الثانية – أو جزء صغير من اللحظة التي تنقضي حتى تفتح الصفحة التي نريدها – تحدث عملية تقديم

العطاءات التلقائية بين مئات الآلاف من المعلنين المختلفين؛ حيث إنهم يقاتلون من أجل تقديم الإعلان لنا بالضبط في هذه اللحظة بالذات، وكلما كانت المعلومات التي يمتلكها المعلنون عنا أكثر دقة، وكلما كانت البيانات مجزأة ومستهدفة، زاد احتمال نقرنا فعليًا؛ وبالتالي يرتفع سعر الإعلان.

لكن البعض لديه القدرة على استغلال هذا الجزء من الثانية لأداء مهمة أكثر ضررًا: إرسال إعلان مميز إلى الأشخاص؛ حيث يبدو بريئًا ولكنه يحتوي على برامج تجسس متقدمة. على الرغم من أن الإعلان يبدو عاديًا تمامًا، إلا أنه في الواقع سلاح إلكتروني قادر على التسلل إلى الهاتف أو الكمبيوتر.

في الماضي؛ كان يُعتقد أن أجهزة استخبارات الدولة فقط هي التي تمتلك هذه القدرة، حيث تستغل عالم الإعلانات الرقمية، الذي من المفترض أن يكون مجهول الهوية تمامًا، لتجاوز آليات الأمان الخاصة بشركة آبل وغوغل ومايكروسوفت وتثبيت برامج تجسس متقدمة على أجهزتنا.

ويقول مصدر مطلع على هذه التكنولوجيا: "يمكن لهذه القدرات أن تحول أي إعلان إلى نوع من السلاح الرقمي".

وقد بدأت التكنولوجيا الجديدة أيضًا في الانتشار إلى سوق الدفاع التجاري؛ حيث اكتشف تحقيق أجرته مجلة هاآرتس ومكتب التحقيق الوطني والأمن السيبراني التابع للصحيفة أنه في ظل جائحة الفيروس التاجي – عندما تم تطوير ونشر أدوات معينة لتتبع انتشار الفيروس – ظهرت صناعة تجسس إلكترونية جديدة ومثيرة للقلق في إسرائيل، وطوّرت عدد من الشركات الإسرائيلية تقنيات قادرة على استغلال الإعلانات لجمع البيانات ومراقبة المواطنين؛ حيث يمكن مراقبة مئات الآلاف – إن لم يكن الملايين – من الأشخاص بهذه الطريقة.

ويكشف التحقيق، الذي يستند إلى مقابلات مع أكثر من 15 مصدرًا من الصناعات السيبرانية والأمنية والدفاعية الهجومية الإسرائيلية، أن مجموعة صغيرة من نخبة الشركات قد نقلت هذه التقنيات إلى مستوى أعلى: فقد ابتكرت تكنولوجيا تستخدم الإعلانات لأغراض هجومية وتثبيت برامج التجسس. وبينما تتنافس ملايين الإعلانات على الحق في اختراق شاشاتنا، تبيع الشركات الإسرائيلية بشكل سري التكنولوجيا التي تحول هذه الإعلانات إلى أدوات مراقبة – أو حتى إلى أسلحة قادرة على اختراق أجهزة الكمبيوتر أو الهواتف الخاصة بنا.

إحدى هذه الشركات هي "إنساينت"، التي يتم الإعلان عن وجودها في هذا التقرير لأول مرة، وكما يوحي اسمها، فهي تمتلك قدرات جنونية، وفقًا لمصادر في هذه الصناعة. وتأسست الشركة على يد عدد من رجال الأعمال المعروفين في مجالات الاستخبارات السيبرانية والرقمية الهجومية، وهي مملوكة لأعضاء سابقين رفيعي المستوى في مؤسسة الدفاع، بما في ذلك الرئيس السابق لمجلس الأمن القومي، داني أرديتي. ويكشف التحقيق أن الشركة طورت تقنية تستغل الإعلانات للتتبع والتجسس، وليس من قبيل الصدفة أن تقوم الشركة بتسمية منتجها باسم "شيرلوك".

ونجح موظفو الشركة في الحصول على تصريح من وزارة الدفاع لبيع التكنولوجيا الخاصة بهم على مستوى العالم؛ حيث باعت "إنساينت" بالفعل التكنولوجيا إلى دولة غير ديمقراطية.

ووفقًا لنتائج التحقيق، فإن هذه هي الحالة الأولى في العالم التي يتم فيها بيع نظام من هذا النوع كتقنية، وليس كخدمة. وقامت شركة إسرائيلية أخرى، وهي "رايزون"، بتطوير منتج مماثل وحصلت هذه السنة على موافقة من حيث المبدأ لبيعه لعملائها في الدول الغربية، على الرغم من أن هذا لم يحدث بعد من الناحية العملية.

لكن الأمر الأكثر إثارة للقلق هو أنه لا توجد حاليًا أي دفاعات ضد هذه التقنيات، وليس من الواضح ما إذا كان من الممكن حظرها على الإطلاق. على مر السنين، منعت شركات التكنولوجيا مثل آبل وغوغل مئات الاختراقات التي تمكنت من خلالها برامج التجسس مثل بيغاسوس من التسلل إلى الأجهزة. وفي هذا الأسبوع فقط؛ تم استغلال المحفظة الرقمية لشركة أبل لإرسال رسالة إلى أجهزة آيفون الخاصة بالمستخدمين تحتوي على صورة تحتوي على رمز ضار، وعلى خلفية ذلك تم حظر هذا الخرق الأمني. ولكن حتى أذكى الدفاعات وأكثرها تقدمًا لدى آبل وغوغل و مايكروسوفت تفتقر حاليًا إلى القدرة على درء هذا النوع من الاختراق. فحتى اليوم، كانت أنظمتهم الإعلانية، التي تحتوي على عدد لا يحصى من آليات الدفاع، تعتبر آمنة تمامًا.

ويكشف هذا التحقيق عن التكنولوجيا التي تتجاوز قيود الأمان والخصوصية التي تفرضها آبل وغوغل، وتتسلل إلى الهواتف من خلال الاستخدام المتطور للمعلومات الإعلانية وكيفية تحول الإعلانات إلى أدوات حرب في ساحة المعركة الرقمية. تكشف القصة عن العلاقة الخطيرة بين عالم التجسس والسوق الخاصة، وتقدم مثالًا مناسبًا لما يشار إليه باسم "رأسمالية المراقبة": وهو كيف تستغل الدول المعلومات التي يتم جمعها لأغراض تجارية لأغراض استخباراتية وتحولها – من خلال التعاون مع رواد الأعمال الإسرائيليين في مجال التكنولوجيا الفائقة – إلى منتج أمني، يمكن أن يصبح سلاحًا يستهدف المواطنين العاديين.

في البداية كانت هناك شعارات. ففي سنة 1994؛ اشترت شركة "آي تي أند تي" أول إعلان على الإنترنت من موقع "هوت وايرد"، ويسأل ذلك الموظف الذكي الذي عمل لصالح تلك الشركة، "هل سبق لك أن نقرت بالفأرة هنا؟"ويجيب على سؤاله بحزم "سوف تفعل". ووفقا للمعلومات التي جمعها الموقع للمعلنين الجدد، فإن ما يقارب من نصف أولئك الذين شاهدوا الإعلان جعلوا النبوءة تتحقق ذاتيًّا.

بعد مرور ثلاثين سنة؛ ما زلنا ننقر على تلك الإعلانات، لكن عالم الإعلان الرقمي تغير تمامًا. اليوم؛ لا تتسم الإعلانات التي نراها على هواتفنا الذكية بطابع عشوائي على الإطلاق: فهي تعرف الكثير عنا ويمكنها، على سبيل المثال، تحديد موقعنا الجغرافي وحتى الشارع، ومطابقة المعلومات مع سجل البحث الخاص بنا.

لقد أصبح الإعلان الرقمي اقتصادًا ضخمًا تبلغ قيمته مئات الملايين من الدولارات وآلاف الشركات وعشرات الآلاف من أنواع الخدمات لجمع البيانات وتحليلها وتقسيمها وتحسينها من أجل استهداف المستخدمين. ويشار إليه مجتمِعًا باسم "تكنولوجيا الإعلان"، وهو اقتصاد ثانوي ضخم نشأ أيضًا حول الإعلان الرقمي للأجهزة المحمولة والتطبيقات التي تعمل عليها؛ حيث يتنافس المعلنون على وقت شاشاتنا من خلال عمليات العطاءات المعقدة والآلية التي تغذيها بياناتنا وتستنير

بها.

والجدير بالذكر أننا نمثل المنتج المجاني وعمليات تبادل الإعلانات (التي تسمى منصات جانب الطلب) وأسواق البيانات الإعلانية التي تقف خلفها هي المكان الذي يتم فيه بيع المنتج الذي نمثله كسلعة.

لكن كل هذه المعلومات من البيانات لا تخدم مصالح المعلنين فقط. فقبل بضع سنوات؛ اكتشف الناس أن البيانات التي تم جمعها للإعلان والاحتياجات التجارية يمكن استخدامها أيضًا لأغراض أخرى، وأن هذه التبادلات يمكن استخدامها أيضًا للتتبع الجغرافي ومراقبة موقعنا. ويسمى هذا المجال غير المعروف باسم (الإعلان الاستخباراتي) والذي يهدف إلى تحويل البيانات والمعلومات المجمعة لأغراض دعائية إلى معلومات استخباراتية.

يوضح أحد الأشخاص العاملين في صناعة الإعلان الاستخباراتي في إشارة إلى الشركتين اللتين تعمل أنظمة التشغيل الخاصة بهما على تشغيل معظم الهواتف الذكية: "بمعنى ما، أنشأت شركتا غوغل و آبل سوقًا للتجسس"، وأضاف قائلًا "لقد كانوا يأملون فقط ألا يفهم الناس أن المعلومات التي يجمعها المعلنون يمكن أن تكون أيضًا بمثابة ذهب استخباراتي. هناك طريقة أخرى للتفكير في الأمر وهي أن آبل وغوغل هما بحد ذاتهما من إحدى شركات التجسس. هناك ببساطة بعض الذين يعرفون كيفية استغلال ذلك".

هذه ليست محاولة لاختراق جهاز من الباب الخلفي، ولكن للسماح لشيء ما بالدخول إليه بذكاء من خلال النافذة الأمامية، وهي نافذة مفتوحة على مصراعيها بفضل عالم الإعلانات الذي يدعم اقتصاد الإنترنت بأكمله.

على ضوء حساسيتها المحتملة، من المفترض أن تكون المعلومات الإعلانية، وخاصة المعلومات المتعلقة بهواتفنا الذكية، مجهولة المصدر؛ حيث يحتوي كل هاتف ذكي على رقم تعريف إعلاني فريد، والذي يبدو من المستحيل مطابقته مع رقم هاتفنا أو اسمنا. الهدف واضح: منع استخدام بيانات الإعلان للتجسس على الأشخاص، وعدم السماح للمعلنين باستغلال معلوماتنا الخاصة. ويحظر قانون الخصوصية الرقمية في الاتحاد الأوروبي، والمعروف باسم اللائحة العامة لحماية البيانات، ذلك بشكل واضح.

ولكن حتى المعلومات المجهولة المتوافقة مع قوانين الخصوصية هذه يمكن أن تكون ذات قيمة كبيرة من منظور استخباراتي. فعلى سبيل المثال؛ بمساعدة تكنولوجيا الإعلان، من الممكن وضع علامة رقمية على جميع الهواتف المحمولة الخاصة بالأشخاص الذين مروا عبر مطار معين في وقت محدد، ويمكن استخدام هذه الأداة الإعلانية البسيطة، على سبيل المثال، لإجراء تتبع الاتصال ومراقبة سلاسل العدوى أثناء الجائحة. أولًا؛ يتم جمع كافة معرفات الإعلانات الخاصة بالأجهزة التي كانت موجودة في المطار. إنها عملية بسيطة: في كل مرة نلتقط فيها هاتفنا ونفتح تطبيقًا يعرض الإعلانات، يرسل الهاتف مكان تواجدنا إلى المعلنين من أجل تحسين فعالية الإعلانات التي يرسلونها إلينا. يؤدي تحديد موقع هذه المعرفات إلى إنشاء قائمة بالأشخاص الذين كانوا في المطار في وقت معين. قد لا يعرف المعلنون أسماء هؤلاء الأشخاص، ولكن يمكن تصنيفهم كجزء من الجمهور المستهدف، والذي

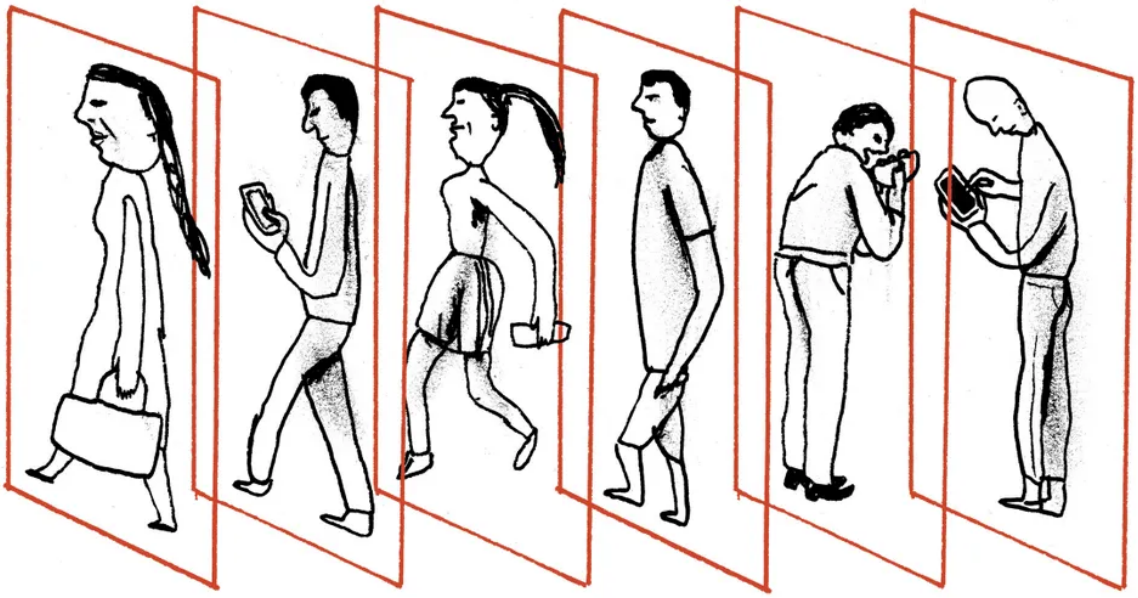
يمكن استهدافه بشكل مستمر من خلال قصفهم بوابل من الإعلانات، التي من خلالها يمكن تتبع تحركاتهم في جميع أنحاء العالم.

هذه هي الطريقة التي ظهرت بها إلى حيز الوجود صناعة جديدة من الإعلانات الاستخباراتية، في ظل أزمة فيروس كورونا؛ حيث عرضت شركة أسسها "إريك بانون"، أحد رواد الهجوم السيبراني في إسرائيل، على جهاز الأمن الشاباك خدمة مراقبة تعتمد على الإعلانات. وكما ذكر "جور مجيدو" في صحيفة "ذا ماركر" العبرية؛ كان الهدف هو إجراء هندسة عكسية للمعلومات حول المستخدمين في شبكات الإعلانات الكبيرة لأغراض استخباراتية. وفي هذه الحالة، كان الهدف هو المشاركة في مراقبة جماعية لتتبع انتشار الجائحة.

تُعرف هذه الشركة باسم "أنتلوس" ويسمى منتجها "أدهوك"، الذي يُسوق لوكالات إنفاذ القانون والعملاء من رجال الأعمال على حد السواء. ولا تعتبر منتجات الشركة ذات صلة بالأمن وبالتالي لا تخضع للتنظيم، وتجدر الإشارة إلى أن هناك صناعة كاملة من الشركات المماثلة.

بشكل عام؛ لا تخضع المراقبة الجغرافية المجهولة عبر الإعلانات حاليًا لإشراف وزارة الدفاع لأنها تعتمد فقط على معلومات الملكية التي يمكن الحصول عليها تجاريًا. ومع ذلك؛ يمكن أيضًا استخدام هذه التقنيات لأهداف أمنية، مثل مراقبة الأهداف المشتبه بها، حتى دون معرفة معلومات شخصية عنها. ويمكن للمرء أن يتخيل، على سبيل المثال، حملة إعلانية موجهة نحو جمهور من العلماء النوويين من أصل إيراني الذين تتراوح أعمارهم بين 35 و65 عامًا والذين مروا عبر مطار طهران خلال السنة الماضية. وبعد تحديد هوية هؤلاء الأفراد وتلقي الإعلانات الأولى، يمكن الاستمرار في استهدافهم بمرور الوقت؛ وبالتالي، يمكن لهذه لتكنولوجيا تحديد أين سافروا ومتى.

في الواقع؛ ما بدأ كتتبع جماعي للاتصالات توسع بسرعة ليشمل مجالات إضافية للأمن الداخلي. فعلى سبيل المثال – ووفقًا للوثائق التي حصلت عليها صحيفة هاآرتس – تقدم "شركة كوب ويبز" الإسرائيلية، المتخصصة في الاستخبارات مفتوحة المصدر، تكنولوجيا مدنية يمكنها تحديد موقع جهاز محمول. وتبرز الشركة قدراتها من خلال استهداف أحد الإيرانيين، حيث يمكن رؤية كيف يتتبع البرنامج تحركات الهدف في الشارع.



يسلط مثال إيران الضوء على القيمة الاستخباراتية الفريدة التي تمتلكها صناعة الإعلان الاستخباراتي: فبينما تعتمد معظم أنواع المعلومات الاستخبارية الرقمية والسيبرانية الهجومية على الوصول المباشر إلى المعلومات والشبكات والبنى التحتية – البيانات التي من المفترض أن تمتلكها الدولة فقط – يعتمد الإعلان الاستخباراتي على المعلومات التي تعتبر مفتوحة، ويمكن العثور عليها من مصادر تعتبر تجارية. وفي هذه الحالة؛ يتم دمجهم معًا لتلبية الاحتياجات الاستخباراتية.

يمكن الحصول على المعلومات من قواعد البيانات الخاصة المختلفة – على سبيل المثال تلك المرتبطة بالمعلنين أو منصات جانب الطلب – أو من خلال طرق أكثر إبداعًا. فمن أجل العثور على موقع شخص ما، على سبيل المثال، لا تحتاج إلى أي شيء أكثر من المعلومات التي يمكن الوصول إليها من خلال تبادل الإعلانات الخلوية.

ووفقًا لمصادر في الصناعة، فإن اسم اللعبة في مجال الذكاء الاستخباراتي هو الاندماج، أو المطابقة المتبادلة لعدد كبير من مصادر المعلومات. وحتى مجرد المشاركة في عملية تقديم العطاءات يمكن أن يوفر معلومات جغرافية للمعلن؛ سواء كان معلنًا حقيقيًا أو معلنًا تستخدمه شركات استخباراتية.

ويقول مصدر في الصناعة: "من أجل الحصول على معلومات استخباراتية باستخدام الإعلان، ينبغي توفير بنية تحتية إعلانية ضخمة، ويجب أن تكون متصلًا بطريقة أو بأخرى بأنظمة الإعلانات المختلفة حتى تتمكن من تنفيذ ما لا تريد أبل وغوغل مطلقًا أن تكون قادرًا على القيام به: وهو تتبع الأشخاص أو استخدام الملفات الشخصية الإعلانية بحثًا عن العدوى".

لهذا السبب؛ ترتبط الشركات في هذا المجال بشكل عام بشركات إعلانية. وفي بعض الحالات؛ يقومون فعليًا بتشغيل شركة إعلانية خاصة بهم أو يعملون مع واحدة منها، مما يوفر غطاءً لنشاطهم الاستخباراتي والوصول إلى المعلومات التي يحتاجون إليها.

يُظهر التحقيق أن هناك عددًا من الشركات الإسرائيلية التي تقدم معلومات من هذا النوع للعديد من أنواع العملاء المختلفة. وإحدى هذه الشركات هي "رايزون"، والتي تعتبر رائدة في هذا المجال وقد صاغت بالفعل مصطلح الإعلان الاستخباراتي. ويطلق على منتجها، اسم "إيكو"، الذي لا يخضع لإشراف الدولة لأنه يستخدم أيضًا معلومات تعتبر مفتوحة. يباع هذا المنتج لجهات خاصة، لكن هيئة إسرائيلية رسمية أبدت أيضًا اهتمامًا بشرائه بغرض محاولة مراقبة الفلسطينيين في إسرائيل.

يوضح أحد الأشخاص العاملين في صناعة الإعلان الاستخباراتي: "بمعنى ما، أنشأت غوغل وآبل سوقًا للتجسس. لقد كانوا يأملون فقط ألا يفهم الناس أن المعلومات التي يجمعها المعلنون يمكن أن تكون أيضًا بمثابة ذهب استخباراتي".

تقدم الشركات الأخرى منتجات أقل تقدمًا؛ حيث تقوم إحداها، التي تعرف باسم "بسايتفول"، بتسويق قدراتها للعاملين في عالم الإعلان الخاص. ووفقًا لمصادر في هذا المجال، يعتمد نشاط الشركة على مطابقة بيانات التصفح والمصادر الأخرى للمعلومات المتاحة تجاريًّا والتي يمكن شراؤها أو استخراجها أو استخلاصها بطريقة أخرى من الويب. وقد تم الاستحواذ على الشركة من قبل شركة إلكترونية أخرى، هي "كوغنايت"، التي تقدم خدمات مماثلة، ولكن للدول والقوات المسلحة. بمعنى آخر؛ نفس المعلومات ونفس التقنيات، ولكن مع استخدامات مختلفة: أحدهما تجاري والآخر استخباراتي.

لكن بعض الشركات لا تستخدم الإعلانات لأغراض المراقبة فقط، ويذهبون إلى أبعد من ذلك، حيث يقومون بإنشاء أدوات تستخدم الإعلانات لاختراق الهواتف وأجهزة الكمبيوتر.

كيف يعمل ذلك؟ يتم تجميع ملف تعريف إعلاني للجمهور المستهدف. بعد ذلك، يتم إنشاء حملة إعلانية مصممة خصيصًا للجمهور، ويتم ملؤها بالإعلانات، مما يسمح بالمراقبة الجغرافية الجماعية. بعد ذلك، يتم وضع برامج التجسس أو البرامج الضارة في الحملة.

وبمساعدة أحد المعلنين أو البنية التحتية للإعلان؛ يتم تحميل الإعلان المستهدف إلى تبادل الإعلانات وتبدأ المزايدة، حتى يتلقى الهدف الإعلان وتتسلل التعليمات البرمجية الضارة إلى الجهاز.

وتقول مصادر في الصناعة إنه كان من الواضح لهم منذ البداية أن التكنولوجيا سوف تصبح بسرعة منحدرًا كبيرًا، ويقول أحد هذه المصادر: "يعد "الذكاء الإعلاني" مجالًا مشروعًا، طالما ظل ضمن نطاق التتبع العام، وأولئك الذين يحولونها إلى سلاح يلعبون بالنار. كل ما هو مطلوب هو لغط واحد، وحالة إساءة واحدة، حتى يتم حرق التكنولوجيا بأكملها".

لقد انخرطت الجهات الحكومية وعمالقة التكنولوجيا منذ فترة طويلة في لعبة القط والفأر. فقبل خمسة عشر سنة؛ عندما تحولنا جميعًا إلى الهواتف المحمولة، فقدت أجهزة الاستخبارات القدرة على التنصت على الناس عبر الخطوط الأرضية، وأصبحت الأجهزة المحمولة أكثر ذكاءً، والأهم من ذلك، أكثر تشفيرًا.

وعلى الرغم من أن شركات "أبل" و"غوغل" و"ميتا" تتعاون عادةً مع الطلبات القانونية التي

تقدمها الهيئات الأمنية للحصول على المعلومات، خاصة في الولايات المتحدة والاتحاد الأوروبي، إلا أنها لا تسمح لهم بالوصول الكامل إلى مكالماتنا أو أجهزتنا. وهناك سبب فني وسياسي لذلك: من الناحية الفنية، يعمل التشفير الشامل ولا يمكن اختراقه. ومن الناحية السياسية، لا ترغب شركات التكنولوجيا الكبرى في السماح للدول باستخدام هواتفنا للمراقبة، حتى لو كان ذلك قانونيًا، خاصة في ضوء الحالات التي تم فيها إساءة استخدام المراقبة لاستهداف الصحفيين ومنتقدي الحكومة ونشطاء حقوق الإنسان.

لكن هيئات الاستخبارات في العالم تتوق رغم ذلك للوصول إلى أجهزتنا، وقد قدمت الصناعة السيبرانية الهجومية لفترة طويلة مجموعة من الحلول على وجه التحديد للبلدان غير القادرة على تطوير هذه القدرات بمفردها. فلقد بدأت منذ ما يزيد قليلًا عن عقد من الزمن مع القرصنة والمراقبة عبر الشبكات الخلوية، واستمرت في شكل خروقات عبر الإنترنت اللاسلكي (واي فاي)، وتقدمت إلى المتصفحات وتطبيقات الهواتف الذكية والرسائل النصية الموبوءة بالبرامج الضارة.

إن القدرات الأكثر تقدمًا، والتي تم الإبلاغ عنها في السنوات الأخيرة والتي أثارت انتقادات شديدة، هي تلك التي طورتها شركات إسرائيلية مثل "إن إس أو" و"كانديرو". وبمساعدة برامج التجسس الخاصة بها، وأشهرها برنامج "بيغاسوس" التابع لشركة "إن إس أو"، يمكن اختراق أجهزة مثل أيفون عبر عمليات استغلال بدون نقرات. وبعبارة أخرى؛ يتم إصابة جهاز الشخص دون علمه بذلك أو حتى اتخاذ أي إجراء.

تقوم برامج التجسس مثل "بيغاسوس" باختراق الهواتف الذكية من خلال استغلال الثغرات الأمنية في نظام تشغيل أيفون، لكننا نتحدث عن شيء مختلف هنا، فهذه ليست محاولة لاختراق جهاز عبر الباب الخلفي، ولكن للسماح لشيء ما بالدخول إليه بذكاء من خلال النافذة الأمامية، وهي نافذة مفتوحة على مصراعيها بفضل عالم الإعلانات الذي يدعم اقتصاد الإنترنت بأكمله.

في الواقع؛ تخلق هذه التقنية "ناقلًا" جديدًا في الجهاز لأولئك القادرين على تطوير برامج التجسس بأنفسهم، أو للعملاء الحاليين لشركات مثل "إن إس أو". وإذا كانت "بيغاسوس"، كما يقول البعض، هي القنبلة النووية للعصر الرقمي، فيمكن تشبيه هذه القدرات الجديدة بالصاروخ الموجه الذي يُطلق عليه "الرأس الحربي النووي الرقمي".

ولسبب وجيه؛ حاولت عدد من شركات الإنترنت الإسرائيلية في السنوات الأخيرة تطوير التكنولوجيا الهجومية التي تستغل الإعلانات ليس فقط للمراقبة ولكن أيضًا للإصابة ببرامج التجسس. وفي الواقع؛ شهدت السنوات الخمس الماضية سباق تسلح في الصناعة السيبرانية، شاركت فيه شركات مثل "كانديرو"، "باراغون" "نيميسيس"، "كوادريم"، وشركة "إن إس أو" نفسها.

ووفقًا للمصادر، أنشأت "إن إس أو" أيضًا منتجًا مسيئًا، يسمى "ترومان" يستخدم الإعلانات. ومع ذلك، مثل معظم هذه الشركات، لم تتمكن "إن إس أو" من الحصول على تصريح لبيع البرنامج؛ فقط "إنساينت" تمكنت من بيع منتجها.

تأسست "إنساينت" في سنة 2019 من قبل مجموعتين من رواد الأعمال. الأولى المؤلفة من رواد الأعمال السيبرانيين المخضرمين، ومن بينهم آرييل آيزن وروي ليمكين وداني أرديتي، والذين توصلوا إلى الاستثمار اللازم. ويعرف الثلاثة كمسوقين لشركات مثل "إن إس أو" (في الماضي) و"باراغون" (حاليًا) في أوروبا الغربية وآسيا، ويتمتعون بعلاقات ممتازة مع أجهزة المخابرات والأمن في إسرائيل وكذلك في تلك الأجزاء من العالم.

وتألفت المجموعة الثانية من رواد أعمال شباب، بعضهم لديه خلفية في الوحدات السيبرانية العسكرية الإسرائيلية، والذين قدموا الفكرة. وقبل تأسيس "إنساينت"، قاموا بتأسيس شركة متخصصة في تكنولوجيا الإعلانات، والتي باعوها منذ عدة سنوات.

وبالاعتماد على الخبرة التي اكتسبتها المجموعة الأخيرة في مؤسسة الدفاع الإسرائيلية وفي صناعة الإعلان، قاموا بتطوير أداة "شيرلوك"، وهي أداة تستغل نظام الإعلانات لاختراق أجهزة الكمبيوتر والأجهزة الخلوية.

ولتسويق المنتج؛ قامت الشركة بدراسة إمكانية التعاون مع شركات إلكترونية هجومية أخرى؛ حيث عرضت وثيقة "كانديرو" التسويقية لسنة 2019، والتي تم الكشف عنها في سنة 2020 بواسطة أميتاي زيف في صحيفة "ذا ماركر" العبرية؛ حيث عرض برنامج "شيرلوك" لعميل محتمل إلى جانب برنامج التجسس للكمبيوتر الشخصي الخاص بالشركة.

وأظهرت الوثيقة أن هذه القدرة كانت مكلفة للغاية: فاستخدام "شيرلوك" للفيروس سيكلف العميل 6 ملايين يورو إضافية (6.7 مليون دولار).

وكشفت الوثيقة أيضًا أن "شيرلوك" يمكنه اختراق أجهزة الكمبيوتر التي تعمل بنظام ويندوز بالإضافة إلى أجهزة آيفون وأندرويد. وحتى الآن؛ تخصصت شركات مختلفة في اختراق الأجهزة المختلفة، وبينما ركزت "كانديرو" على أجهزة الكمبيوتر الشخصية، في حين تمكنت "إن إس أو" من اختراق أجهزة آيفون، وكان منافسوها متخصصين في أجهزة أندرويد. ولكن مع هذا النظام، كما تظهر الوثائق، يمكن اختراق كل جهاز بشكل فعال.

ويوضح دونشا أو كيرهيل، الذي يرأس مختبر أمن التكنولوجيا التابع لمنظمة العفو الدولية، الوحدة التكنولوجية التابعة لمنظمة حقوق الإنسان، أن "هذا تطور جديد خطير للغاية"، مضيفًا: "قد تسمح القدرة الموصوفة للمهاجمين باستهداف الأفراد بناءً على الخصائص الديموغرافية والسلوكية التي تجمعها شبكات الإعلانات وبالتالي استهداف أشخاص من مجموعة عرقية معينة أو إعادة استهداف الأفراد الذين زاروا موقعًا إعلاميًا مستقلًا ينتقد الحكومة".

وعلى الرغم من المخاوف؛ تم بيع منتج "إنساينت" بشكل قانوني وبترخيص من دولة إسرائيل؛ حيث حصلت الشركة في البداية على موافقة واسعة نسبيًا من وزارة الدفاع، على الأقل فيما يتعلق بالأسلحة الإلكترونية الحساسة. وبهذه الموافقة، تمكنت "إنساينت" من إكمال صفقة رئيسية واحدة على الأقل.

ولكن بعد ذلك تم تخفيض التصريح بشكل كبير؛ حيث تقول مصادر في الصناعة إن التغيير في السياسة كان مرتبطًا بثلاثة مخاوف حقيقية: الخوف من تسرب القدرات، والخوف من الغضب الأمريكي، والخوف من غضب عمالقة التكنولوجيا، الذين هم على أي حال في طريق الحرب ضد إسرائيل في مجال صناعة الإنترنت (فيسبوك وأبل، على سبيل المثال، يقاضيان شركة "إن إس أو").

تم تقليص ترخيص شركة "إنساينت"؛ ولكن من الممكن الآن بيع "شيرلوك" كمنتج عسكري هجومي ـ وإن كان ذلك في ظل ظروف مقيدة للغاية وللدول الغربية فقط. وحتى لتقديمها إلى عميل محتمل في الغرب، يجب الحصول على تصريح محدد من وزارة الدفاع، ولا يتم منحه دائمًا.

إن حالة "إنساينت" وامتداد هذه التكنولوجيا إلى سوق الدفاع العام، هي قصة إسرائيلية كلاسيكية: روح تكنولوجية متطورة لريادة الأعمال تتحدى – وتستغل – آليات الرقابة التي تقادمت والتي لا تستطيع مواكبة العالم الذي لا يحبّذ الرغبة في تقنيات التجسس الرقمي المتقدمة. ويشعر العاملون في الصناعة بالقلق من أن القدرة على تقييد استخدام هذه التقنيات التي يحتمل أن تكون خطرة تتضاءل بسرعة. وبعضهم مقتنع بأن الصناعة قد خرجت عن نطاق السيطرة بالفعل.

منذ عدة سنوات؛ يقوم رجال الأعمال في هذا المجال باختبار المسؤولين عن الإشراف عليهم في وزارة الدفاع، وهناك جدل يدور حول مسألة ما إذا كانت تقنية "الذكاء الإعلاني" التي يعتمد الكثير منها على مصادر المعلومات المفتوحة، هي تقنية مدنية أم عسكرية.

حتى الآن، لم تكن الشركات التي عرفت نفسها على أنها تعمل فقط على أساس المصادر المفتوحة، للعملاء المدنيين، خاضعة لأي إشراف من الدولة. وفي المقابل؛ كانت الشركات السيبرانية تخضع لرقابة مشددة من قبل وزارة الدفاع.

ومع ذلك؛ فإن الحدود ليست واضحة دائمًا والقيود لم تنجح دائمًا. فعلى سبيل المثال؛ بعد رفض تصريح شركة "إن إس أو" بتصدير منتجها في هذا المجال، ومُنع موظفو الشركة من مجرد إخبار العملاء المحتملين عن وجودها، قامت الشركة بدراسة إمكانية دمج التكنولوجيا داخل شركة "بيغاسوس"، وربما قامت شركات أخرى بمحاولات مماثلة.

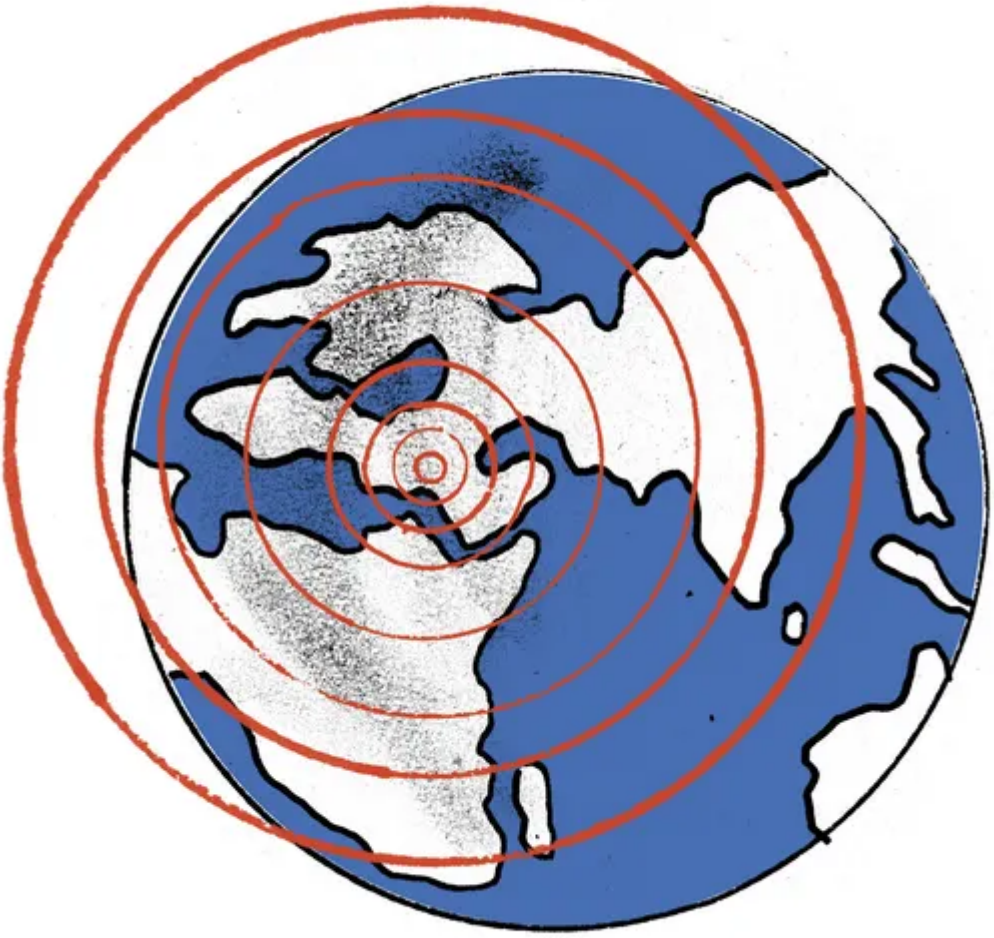
القيود المفروضة على التصريح الممنوح لشركة "إنساينت" لم توقف الشركة أو منافسيها. وفي الأشهر التي تلت تقييد نشاطها، أجرت الشركة محادثات مع شركات الإنترنت الهجومية التي تم رفض الترخيص لها. إحدى الأفكار التي تمت مناقشتها كانت توحيد الجهود والتغلب على العقبة التنظيمية: إذا لم تسمح إسرائيل ببيع منتج من هذا النوع كنظام مستقل، فربما تسمح بتجميع القدرات مع برامج التجسس التي تمت الموافقة عليها بالفعل للتصدير. وأجريت محادثات في هذا السياق مع "كانديرو" و"باراغون" و"نيمسيس"، وتم تقديم طلب ملموس إلى وزارة الدفاع يتضمن منتجًا متكاملًا. هذه هي خلفية ظهور "شيرلوك" في وثيقة "كانديرو" التسويقية، لكن هذه التحركات فشلت أيضًا في الحصول على موافقة الدولة.

لكن، ومع مرور الوقت، أدركت المؤسسة الأمنية بشكل متزايد أنه لم يعد من الممكن إبقاء القطة في

الحقيبة. لقد فقدت الدولة – التي سمحت لصناعة "الذكاء الإعلاني" المتقدمة بشكل متزايد بالعمل بناءً على بيانات الملكية المفتوحة فقط – القدرة على كبح جماح السوق الهجومية التي حاولت الركوب على ظهرها.

وبناءً على ذلك؛ وبمجرد تقديم الأمر إلى "إنساينت" لتجنب مزاعم المحسوبية، قررت وزارة الدفاع هذا العام منح ترخيص لشركة "رايزون" أيضًا لبيع منتج قرصنة نشط.

وتوضح حالة "رايزون" مدى عدوانية سباق التسلح الذي كان يجري في هذا المجال؛ فلسنوات امتنعت شركة "رايزون" عن إنشاء أي منتج ضار واقتصرت على المعلومات الاستخبارية القائمة على التتبع الجغرافي عبر الشبكة الخلوية ومراقبة الاتصالات غير المشفرة. بمعنى آخر؛ حتى لو كان من المستحيل تتبع شخص ما وربما الاستماع إلى محادثة أو رؤية الرسائل، فمن الممكن معرفة من يتحدث مع من وأين ومتى، وهي قدرات تخضع للرقابة وتعتمد على جمع البيانات التي تعتبر حساسة وغير مفتوحة.



ومع ذلك، واستجابة لظهور السوق وطلب العملاء المتعطشين للقدرات الجديدة، طورت الشركة، بالإضافة إلى منتج المراقبة الجغرافية "إيكو"، أداة هجومية تمكن من الإصابة ببرامج التجسس القائمة على الإعلانات. وعلى الرغم من أنها كانت من أوائل الشركات التي قدمت الطلب، إلا أن وزارة الدفاع منحت الإذن من حيث المبدأ ببيع المنتج هذا العام فقط.

ويفكر البعض في إسرائيل الآن في إمكانية وضع مجال المعلومات الاستخبارية مفتوحة المصدر والقائمة على الإعلانات بالكامل تحت إشراف وزارة الدفاع. وفي الأشهر الأخيرة، جرت محادثات حول مراجعة الأنظمة التي تحكم هذا المجال.

سبب آخر للتغيير المحتمل في السياسة في هذا المجال المحدد ينبع من الاستجابة لتغيير أكثر شمولًا من قبل وزارة الدفاع. فبعد سنوات من الترويج لهذه الصناعة كجزء مما يسمى بالدبلوماسية السيبرانية لرئيس الوزراء بنيامين نتنياهو، أصبحت الآن على خلاف مع الدولة.

قبل أقل من سنتين بقليل؛ قررت إسرائيل الإذعان للضغوط الأمريكية لكبح جماح الصناعة السيبرانية الهجومية. ومن قائمة تضم أكثر من 100 دولة عميلة محتملة، أصبح من المسموح الآن تصدير الأسلحة السيبرانية إلى ما يقل قليلا عن 40 دولة، معظمها في الغرب. ونتيجة لذلك، عدد من الشركات الإسرائيلية التي تستمد رزقها من عملاء في أجزاء أخرى أقل ديمقراطية من العالم أغلقت أبوابها.

نجحت هذه الخطوة جزئيًا في تهدئة المجال، ولكن كان لها آثار إشكالية على صناعة الأسلحة السيبرانية المحلية، فقد تم إغلاق الشركات وتم تحفيز العشرات من الإسرائيليين للانتقال إلى أوروبا والولايات المتحدة؛ حيث بدأت صناعة السيبرانية الهجومية المزدهرة في الظهور لحساب إسرائيل، وقد حاول الباحثون عن الكفاءات اصطياد أفضل المتسللين الإسرائيليين، ولكن أيضًا إلى آسيا، بعيدًا عن الهيئات التنظيمية الإسرائيلية. إحدى هذه الشركات هي شركة "ديفينس برايم"، التي يوجد مقرها في الولايات المتحدة ولكنها مملوكة لإسرائيليين؛ فقد جندت هذه الشركة موظفين إلكترونيين إسرائيليين هذا العام، بما في ذلك من مؤسسة الدفاع نفسها.

ومن الآثار الأخرى غير المقصودة الناجمة عن الأزمة التنظيمية على الإنترنت أن الشركات الأخرى بدأت في تغيير نموذج أعمالها وتحولت إلى المتاجرة ليس في برامج التجسس، بل في "برامج الاستغلال" (الحيل الفعلية المستخدمة لاختراق الأجهزة) ونقاط الضعف. فلديهم بنوك بها العديد من الخروقات جاهزة للبيع لشركات مثل "إن إس أو" وغيرها، والتي تحتاجها برامج التجسس من أجل الاستمرار في إصابة الأجهزة، حتى بعد أن تم حظر الخروقات السابقة بواسطة "أبل" أو "غوغل". وهناك عدد من الشركات تقدم مثل هذه المنتجات وتعمل من سنغافورة وإيطاليا وإسبانيا والولايات المتحدة، وتوظف كبار الإسرائيليين في مناصب عليا في هذا المجال.

وتشعر المؤسسة الأمنية بقلق حقيقي من أن هذه القدرات التكنولوجية سيتم بيعها أيضًا من قبل شركات أجنبية لا تخضع للرقابة على الإطلاق. وبناءً على ذلك، وعلى أمل إبقاء المجال الجديد في إسرائيل، وتحت الإشراف، تقرر هذا العام محاولة تنظيم الصناعة، وذلك أيضًا بهدف محاولة

استرضاء شركات الإنترنت المحلية الغاضبة من الأزمة التي شهدها مجالها المربح على مدى أكثر من عام؛ وتحديدًا الـ 20 شهرًا الماضية.

ومن المعروف منذ زمن طويل أن الدول لديها قدرات مراقبة ويمكنها استخدامها ضد مواطنيها، حتى في عصر الهواتف الذكية المشفرة. وفي السنوات الأخيرة، أدرك عامة الناس أن البلدان غير الغربية ـ في أفريقيا وآسيا وأميركا الوسطى والعالم العربي ـ تمتلك أيضًا هذه القدرات، ليس لأنها كانت قادرة على تطويرها بشكل مستقل، بل لأنها اكتسبتها في القطاع الخاص الدولي، سوق الأسلحة الرقمية.

وهذه القدرات، التي أنشأتها شركات إسرائيلية إلى حد كبير، كان المقصود منها في الأصل منع الإرهاب والجرائم الخطيرة، ويجري إساءة استخدامها أيضًا، خاصة من قبل الدول غير الليبرالية وغير الديمقراطية التي ليس لديها خبرة كبيرة في التعامل مع مثل هذه التقنيات المتقدمة. وكما هي الحال مع الأسلحة، فإلى جانب السوق القانونية المنظمة، تتشكل أيضًا أسواق أكثر قتامة وأقل خضوعًا للإشراف، والتي من خلالها تباع التكنولوجيات – سواء كانت أسلحة أو أسلحة رقمية – إلى دول مشبوهة تحظر حتى إسرائيل البيع لها، وربما حتى إلى هيئات خاصة. وتحذر مصادر في الصناعة من أنه هذه المرة أيضًا، كما حدث مع الهجمات السيبرانية، من المحتمل أن تكون هناك عواقب مماثلة.

تلقت صحيفة "هآرتس" الردود التالية من الشركات المذكورة في هذا المقال، والتي طلب منها جميعها التعليق:

ذكرت شركة "إنساينت": "إن "إنساينت" هي شركة إسرائيلية تعمل مع الالتزام الكامل والمطلق بالقانون الإسرائيلي وتوجيهاته التنظيمية الصارمة".

صرحت "رايزون": "في السنوات الأخيرة، تركز الجزء الأكبر من نشاط "رايزون" على مجالين رئيسيين، وهما: تحليل البيانات الضخمة والحلول الواسعة في مجال الدفاع السيبراني لمجموعة من العملاء في إسرائيل وعلى المستوى الدولي، من بينهم الحكومات والعملاء التجاريون. وباعتبارها شركة خاصة، تلتزم "مجموعة رايزون" بالسرية ولا تشير إلى منتجاتها أو عملائها بشكل فردي".

صرحت شركة "كوب.ويبس": "تفخر الشركة بدعم عملائنا في مجال إنفاذ القانون الذين يتصدون ليلًا ونهارًا لحمايتنا من مجموعة واسعة من التهديدات العالمية: تمويل الإرهاب، والهجمات الإلكترونية، واستغلال الأطفال، وجرائم العنف، وتهريب الأسلحة، والاتجار بالبشر. وتستفيد هذه التهديدات من أساليب الاتصال المحلية والدولية التي تقوض القدرة على التعرف عليها والتعامل معها، وتتطلب تكنولوجيا متقدمة للتعامل مع قضايا مثل الذكاء المفتوح وتحليل البيانات الضخمة. لا تعلق شركة "كوب.ويبس" على العلاقات التجارية مع العملاء. ومن ناحية الخصوصية، نود أن نشير إلى أننا نعمل فقط وفقًا للقانون ونحرص بشدة على الالتزام باللوائح الصارمة مثل اللائحة العامة لحماية البيانات في الاتحاد الأوروبي".

اختارت وزارة الدفاع و "إن إس أو" و"كانديرو" و"باراغون" و"إيه دي هوك" و"بي سايتفول" و"كوغنايت"، عدم الرد على هذا التقرير.

المصدر: هآرتس

رابط المقال : https://www.noonpost.com/168681/