تحقيق: ملاحقة الصين لمسلميها أطول وأوسع بكثير مما نعرف

ترجمة وتحرير: نون بوست

قال باحثون إنه قبل تثبيت الشرطة الصينية كاميرات مراقبة عالية الدقة ومحاصرة مئات الآلاف من الأقليات العرقية في إقليم شينجيانغ غرب الصين، سعى القراصنة الصينيون لتصميم برامج ضارة.

يوم الأربعاء، قال باحثون من شركة "لوك أوت" – وهي شركة متخصصة في أمن تكنولوجيا المعلومات مقرها سان فرانسيسكو – إن حملة القرصنة الصينية التي بدأت بالعمل بشكل جدي منذ سنة 2013 وتستمر في العمل حتى يومنا هذا، كانت جزءًا من جهد واسع النطاق ولكنه غير مرئي في كثير من الأحيان لسحب البيانات من الأجهزة التي تعرف الأشخاص بشكل أفضل: هواتفهم الذكية.

عثرت شركة "لوك أوت" على روابط بين ثمانية أنواع من البرامج الضارة – بعضها معروف سابقًا والبعض الآخر غير معروف – تُظهر كيفية اختراق المجموعات المرتبطة بحكومة الصين لهواتف أندرويد التي يستخدمها سكان إقليم شينجيانغ ذوي الأغلبية المسلمة على نطاق أكبر بكثير مما تم إدراكه.

يشير الجدول الزمني إلى أن حملة القرصنة مثلت حجر الزاوية في جهود مراقبة الأويغور في الصين التي امتدت لاحقًا إلى جمع عينات الدم والبصمة الصوتية ومسح الوجه والبيانات الشخصية الأخرى لتحويل شينجيانغ إلى دولة بوليسية افتراضية. كما يُظهر الجدول الزمني أيضًا طول المدة التي قرر فيها الصينيون اتباع الأويغور أثناء فرارهم من الصين لما يصل إلى 15 دولة أخرى.

تتخفى الأدوات التي جمّعها المتسللون في لوحات مفاتيح خاصة استخدمها الأويغور حيث وقع إيهامهم بأنها تطبيقات شائعة الاستخدام في مواقع الويب التابعة لجهات خارجية. يمكن لبعض هذه البرمجيات تشغيل ميكروفون الهاتف عن بعد أو تسجيل المكالمات أو إرسال الصور ومواقع الهاتف والمحادثات

على تطبيقات الدردشة. تم تضمين البعض الآخر في التطبيقات التي توفر الأخبار باللغة الأويغورية، ونصائح التجميل التي تستهدف الأويغور، والنصوص الدينية مثل القرآن وتفاصيل أحدث اعتقالات رجال الدين المسلمين.

حسب أبورفا كومار، وهي مهندسة في التهديد الاستخباراتي في "لوك أوت"، التي ساعدت في الكشف عن الحملة، فإنه "أينما ذهب الأويغور الصينيون، ومهما ابتعدوا، سواء كانوا في تركيا أو إندونيسيا أو سوريا، فإن البرامج الضارة تتبعهم هناك. كان الأمر أشبه بمشاهدة مفترس يطارد فريسته في جميع أنحاء العالم".

قبل عقد من الزمان، لم يكن قراصنة جيش التحرير الشعبي ملحوظين بفضل درجة تعقيد برمجياتهم بقدر ما كانوا معروفين بحجم هجماتهم. لكن تحت التهديد بالعقوبات الأمريكية، أبرم الرئيس الصيني شي جين بينغ اتفاقية مع الرئيس السابق باراك أوباما سنة 2015 لوقف اختراق الأهداف الأمريكية لتحقيق مكاسب تجارية. في المقابل، وقع تعليق الاتفاقية لبعض الوقت مع انخفاض كبير في هجمات الاختراق الصيني في الولايات المتحدة.

في الخريف الماضي، توصل باحثون من القطاع الخاص إلى أنه – خلال نفس الفترة – قامت الصين بتحويل أدوات القرصنة الأكثر تقدمًا نحو شعبها. في الاكتشافات المتداخلة، كشف الباحثون في غوغل وشركة الأمن فيلوكزيتي ومختبر سيتيزن لاب في كلية مدرسة مونك للشؤون العالمية بشكل منفصل ما يرقى إلى اختراق صيني متقدم ضد أجهزة أيفون وأندرويد التابعة للأويغور الصينيين والتبت في جميع أنحاء العالم.

نقطة تفتيش أمنية مزودة بتقنية التعرف على الوجه عند مدخل حديقة في شينجيانغ.

اكتشف باحثو غوغل أن القراصنة أصابوا مواقع ويب يرتادها الأويغور، داخل الصين وبلدان أخرى، بأدوات

يمكنها اختراق أجهزة الأيفون الخاصة بهم وسرقة بياناتهم. يشير أحدث تحليل لشركة "لوك أوت" إلى أن حملة القرصنة التي شملت الهواتف في الصين كانت أوسع نطاقا وأكثر عدوانية مما أدركه خبراء الأمن ونشطاء حقوق الإنسان وضحايا برامج التجسس. لكن الخبراء في المراقبة الصينية يقولون إنه لا ينبغي أن يكون الأمر مفاجئًا، نظرًا للجهود التي بذلتها بكين لمراقبة شينجيانغ.

حيال هذا الشأن، يقول دارين بايلر، الذي يدرس مراقبة الأقليات السكانية في جامعة كولورادو بولدر، إنه "يجب أن نفكر في حقيقة أن مراقبة الهواتف الذكية باتت وسيلة لتتبع الحياة الشخصية للناس، وسلوكهم اليومي، ومدى وفائهم". وأضاف بايلر أنه في سنة 2015، ومع سعي بكين للقضاء على العنف العرقي المتفرق في شينجيانغ، أصبحت السلطات "يائسة" لتتبع اتصالات الأويغور سريعة النمو عبر الإنترنت. بدأ الأويغور يخافون من أن محادثاتهم عبر الإنترنت التي تناقش الإسلام أو السياسة كانت محفوفة بالمخاطر. ويقول بايلر، الذي عاش في شينجيانغ سنة 2015، إنهم كانوا يحملون معهم "هاتفًا نظيفًا" ثانيًا.

في شوارع شينجيانغ، بدأت الشرطة بمصادرة هواتف الأويغور. في بعض الأحيان، أعادوها الى أصحابها بعد أشهر لكن مع تثبيت برامج تجسس جديدة عليها. وفي أوقات أخرى، أعيدت لهم هواتف مختلفة تمامًا. كان المسؤولون الذين يزورون قرى الأويغور يسجلون بانتظام الأرقام التسلسلية المستخدمة لتحديد الهواتف الذكية. كما ثبّتوا في الشوارع أجهزة جديدة تتعقب هواتف الأشخاص أثناء سيرهم.

اعتقلت السلطات الأويغور في معسكرات إعادة التأهيل إما بسبب وجود هاتفين أو هاتف قديم أو إتلاف الهاتف أو عدم امتلاك هاتف على الإطلاق، وذلك وفقًا للشهادات والوثائق الحكومية.

خلال الفترة نفسها، قالت شركة "لوك أوت" إن جهود قرصنة الهواتف في الصين تسارعت. في وقت مبكر من سنة 2011، استُخدم نوع واحد من البرامج الضارة الصينية، المعروف باسم "غولدن إيغل" وهي كلمات المتسللين المنتشرة في رمزهم – وهي إشارة واضحة إلى النسور المستخدمة للصيد في شينجيانغ. لكن استخدامه ارتفع ما بين 2015 و2016. وكشفت "لوك أوت" عن أكثر من 650 إصدارًا من برامج "غولدن إيغل" الضارة وعدد كبير من تطبيقات الأويغور المزيفة التي تعمل مثل حصان طروادة للتجسس على اتصالات المستخدمين.

تحاكي التطبيقات الخبيثة ما يسمى بالشبكات الخاصة الافتراضية، التي تستخدم لإجراء اتصالات ويب آمنة وعرض المحتوى المحظور داخل الصين. كما استهدفت التطبيقات التي يكثر استخدامها من قبل الأويغور للتسوق وألعاب الفيديو وبث الموسيقى ووسائط البالغين وحجز الرحلات، بالإضافة إلى تطبيقات لوحة مفاتيح الأويغور المتخصصة. قدم بعضها نصائح للجمال والطب التقليدي موجهة للأويغور. تنتحل برمجيات أخرى اسم تطبيقات معروفة مثل تويتر وفيسبوك وخدمة المراسلة الفورية الصينية كيو كي ومحرك البحث بايدو.

كشفت لوك أوت عن برامج ضارة صينية متخفية في تطبيق يسمى أخبار سورية

بمجرد تنزيلها، تظهر التطبيقات للمتسللين الصينيين نافذة يتابعون من خلالها نشاط هاتف الشخص المستهدف. كما مُنح المبرمجون في الصين القدرة على تدمير برامج التجسس الخاصة بهم، خاصة عندما تستنزف البطارية. في بعض الحالات، اكتشفت "لوك أوت" أن جميع المتسللين الصينيين الذين كانوا يسرقون البيانات من هاتف الهدف كانوا يرسلون للمستخدم رسالة نصية غير مرئية. حينها تلتقط البرامج الضارة بيانات الضحية وتعيدها إلى هاتف المهاجم عبر رد نصي، ثم تحذف أي أثر للتبادل.

في حزيران/ يونيو 2019، كشفت "لوك أوت" عن برامج ضارة صينية متخفية في تطبيق يسمى أخبار سورية. كان المحتوى يركز على الأويغور، مما يشير إلى أن الصين كانت تحاول إغراء الأويغور داخل سوريا

لتنزيل برامجها الضارة. إن قيام قراصنة بكين بتعقب الأويغور في سوريا أعطى الباحثين في "لوك أوت" فكرة عن مدى قلق الصين من تورط الأويغور في الحرب السورية. وقد وجد باحثو "لوك أوت" تطبيقات خبيثة مشابهة مصممة خصيصًا للأويغور في الكويت وتركيا وإندونيسيا وماليزيا وأفغانستان وباكستان.

كان باحثون في مجموعات بحثية أمنية أخرى، مثل سيتيزن لاب، قد اكتشفوا سابقًا أجزاء مختلفة من حملة قرصنة الهواتف في الصين وربطوها مرة أخرى مع قراصنة الدولة الصينيين. ومع ذلك، يبدو أن تقرير "لوك أوت" الجديد كان المرة الأولى التي يتمكن فيها الباحثون من ربط هذه الحملات القديمة ببرامج ضارة جديدة تستهدف الهواتف وربطها بنفس المجموعات.

في هذا الصدد، قال كريستوف هيبسين، مدير المخابرات الأمنية في لوك أوت: "إن السؤال المفتوح المطروح دائما هو إلى أي مدى لا علاقة للدولة بهذه العمليات؟ قد يكون هؤلاء قراصنة وطنيين، مثل النوع الذي رأيناه في روسيا. لكن استهداف الأويغور والتبتيين والشتات وحتى تنظيم الدولة في إحدى الحالات يوحي بغير ذلك".

جاءت إحدى الإشارات إلى هويات المهاجمين عندما اكتشف باحثو "لوك أوت" ما بدا أنه نسخ تجريبية من البرامج الضارة الصينية على العديد من الهواتف الذكية التي تم تجميعها داخل وحول مقر المقاول الدفاعي الصيني شيان تيانهي لتكنولوجيا الدفاع.

أرسلت شركة تيانهي، وهي مورد كبير لتكنولوجيا الدفاع، موظفين إلى مؤتمر دفاعي كبير في شينجيانغ سنة 2015 لتسويق المنتجات التي يمكن أن تراقب الحشود. مع سيطرة حمى الذهب على المنطقة، تضاعفت حجم تيانهي، حيث أسست شركة تابعة في شينجيانغ سنة 2018. لم ترد الشركة على رسائل البريد الإلكتروني التي تطلب التعليق. وفي هذا الشأن قال هبيسين: "قد تكون هذه مصادفة مثيرة للاهتمام، أو قد تكون دليلا قاطعا".

المصدر: نيويورك تايمز

رابط المقال: https://www.noonpost.com/37523/