



المقاطعة الجنوبية أرض خصبة لأنشطة العصابات (Getty)

## انتقلت العصابات الإجرامية الصينية إلى دول جنوب شرق آسيا، لتمارس أنشطتها غير المشروعة، في الاحتياك الإلكتروني بشتى أنواعه، عبر استخدام أنظمة الذكاء الاصطناعي، في ظل سهولة جمع بيانات الضحايا وانتهاك خصوصيتهم

المبرمج جين إلى أن هذه البيانات يتم شراؤها بأسعار منخفضة، وغالبا ما يتم جمعها من تطبيقات إلكترونية، وكلما كانت البيانات أكثر تفصيلاً وتحديداً، ارتفع سعرها على سبيل المثال، ويمكن تسعير البيانات الشاملة التي قد تتضمن الراتب السنوي للمفرد وموقعه الوظيفي بحوالي 70 يوان للشخص الواحد، أي ما يعادل 10 دولارات. وعن كيفية عمل مثل هذه التقنيات، يشرح جين أن المحتالين يستخدمون معدات يمكنها مقاطعة إشارات الاتصالات والتلاعب بها، بحيث يعتقد الضحايا أنهم يتلقون رسائل مكالمات من أرقام رسمية. ويستخدمون برامج المراسلة الجماعية لإرسال رسائل نصية مقنعة كإشعارات من مشغلي الاتصالات والبنوك والمؤسسات الأخرى إلى آلاف المستخدمين. وأضاف: «تستخدم هذه المجموعات تطبيقات مصممة خصيصاً لجعل الأشخاص يعتقدون أنهم يقومون بتسجيل الدخول إلى منصات استثمار مشروعة ومرخصة، أو التقدم إلى وظائف تجذبهم لكونها بروتات ممتازة. بالإضافة إلى استخدام الفيروسات للوصول إلى أجهزة المستخدمين، ومن ثم سرقة معلوماتهم الشخصية، بعد تصميم نصوص مستهدفة بناء على المعلومات الشخصية، مما يسهل من تضليل الضحية».

### ضعف فعالية السلطات

يشير مصطلح «الاحتياك عبر شبكات الاتصالات» إلى فعل السطو على الممتلكات العامة والخاصة باستخدام تكنولوجيا شبكات الاتصالات بغرض الحيازة غير المشروعة عن طريق الاتصال من بعد وغيرها من الوسائل غير المشروعة، حسب المادة الثانية من قانون مكافحة الاتصالات والاحتياك عبر الإنترنت. ويؤكد المحامي وي أن السلاسل الإجرامية المتشعبة حسب طبيعة هذه الجرائم تصعب من عملية القضاء عليها، فإذا تم تفكيك حلقة واحدة في السلسلة، لا يعتبر ذلك كافياً لمحكمة بعض المشتبه فيهم الذين يعملون في أعلى السلسلة كشركاء، وبالتالي يستمر وقوع الضحايا، ومن بينهم وانغ شين، والذي حصل على دمية مجانية لابنه عبر مسح باركود باستخدام جواله وقام بتعبئة استثمار قصيرة تشمل اسمه ورقم هاتفه بعدما اقنعه شابة تقف في الشارع بالامر، وفي ذات اليوم، تلقى اتصالاً من رقم مجهول أخبره بأن شركة الدمى تقدر مشاركته، وأنها ستكافئ كل عشرة تعليقات يومية على صفحتها بمنحه مبلغاً مالياً قيمته 100 يوان صيني (ما يعادل 15 دولاراً)، وعليه أن يسجل حسابه البنكي لتحويل المبلغ إليه. وبالفعل استلم أول مائة يوان في حسابه وكرر ذلك على مدار أسبوع كامل، وبعدها لم يستلم أي أموال فاتصل بالرقم للاستفسار وكان الرد أن هناك مشكلة في البرمجة وعليه مسح باركود سيصل إليه عبر تطبيق ويتشأت الصيني (مرتبطة بالحساب البنكي للمستخدم) من أجل حل المشكلة، لكن بدلاً من تلقي المال فوجئ باستلام إشعار من البنك يفيد بأنه تم اقتطاع مبلغ 10 آلاف يوان من رصيده، أي 1500 دولار.

دولار)، وجرى التوصل إلى حلول في ثلث القضايا، فضلاً عن اعتقال 361 ألف متورط في هذه الجرائم، ونتيجة لجهود الوقاية تم منع 8,7 ملايين شخص من تحويل 272 مليار يوان إلى المحتالين (37,3 مليار دولار) كما يقول وي، معيداً سبب ارتفاع نسبة الجرائم في ذلك العام إلى جائحة كورونا التي رافقتها إغلاقات متكررة على مستوى المدن والمقاطعات والحدود.

ويبلغ متوسط الخسارة لكل ضحية احتياك إلكتروني في الصين 48 ألف يوان صيني (6592 دولاراً)، ويشكل الضحايا الذكور نسبة أعلى وصلت إلى 70,3 في المائة، بينما شكلت النساء نسبة 29,7 في المائة، حسب تقرير صدر في أغسطس الماضي، عن شركة 360 لأمن الإنترنت (خاصة) والتي تقدم خدماتها لـ 1,03 مليار مستخدم في الصين. ويمثل ضحايا الاحتياك عبر الهاتف المحمول المولودين في التسعينيات 36,4 في المائة من جميع الضحايا (لكونهم الأكثر استخداماً للتكنولوجيا)، يليهم من ولدوا في الثمانينيات بنسبة 35,3 في المائة، ثم جيل الألفية الثانية بنسبة 18,2 في المائة، ومن بين جميع أنواع الاحتياك، استحوذت المواعد على النسبة العظمى (تطبيقات للتعرف بين الجنسين يتم من خلالها استهداف الضحايا عبر حسابات وهمية تدفعهم لفتح رابط محدد أو استخدام الماسح الضوئي لمتابعة بعض المجموعات التي توفر فتيات بمواصفات معينة، ولاحقاً يجري سحب أموال من أرصدهم البنكية)، إذ بلغت 41,3 في المائة، ويكشف التقرير أنه من حيث التوزيع الجغرافي، كانت مقاطعة قوانغدونغ الجنوبية المنطقة الأكثر تضرراً من الاحتياك، بنسبة بلغت 9,7 في المائة، تليها مقاطعة خبي شمال البلاد بنسبة 7,4 في المائة، ثم مقاطعة شانغونغ الشرقية بنسبة 7,1 في المائة. وتوصل التقرير إلى أن بكين لديها أكثر المستخدمين تعرضاً للاحتياك، ويوضح المحامي وي أن سبب ارتفاع جرائم الاحتياك الإلكتروني في الجنوب، وتحديداً في مقاطعة قوانغدونغ، يعود إلى اعتبار أن المقاطعة الجنوبية تعد المركز التجاري في البلاد وتضم أكبر الحواضر المالية، مثل كوانزو وشينزن وشانتو وفوشان، لذلك تعتبر أرضاً خصبة لأنشطة العصابات.

### تبدأ الجريمة عبر انتهاك خصوصية الضحايا

يوضح تشاو جين، المبرمج في شركة شو جوانغ لنظم المعلومات والحاسوب (خاصة)، أن عصابات الاحتياك تستخدم أنظمة الذكاء الاصطناعي المتقدمة للاتصال والتلقائي بالآلاف العملاء المحتملين يومياً، باستخدام بياناتهم الشخصية التي يتم شراؤها من سماسرة وشركات متواطئة. ويحث قانون مكافحة الاتصالات والاحتياك عبر الإنترنت الذي تم إقراره في الثاني من سبتمبر/ أيلول العام الماضي ودخل حيز التنفيذ في الأول من ديسمبر/ كانون الأول من نفس العام، المؤسسات على حماية خصوصية المستخدمين لكنه لا يلزمهم، بحسب المادة 29 من الفصل الخامس الذي يحمل عنوان تدابير شاملة، وبالتالي يلفت



## انتقلت العصابات الإجرامية الصينية إلى دول جنوب شرق آسيا

464 الف حالة احتياك عبر الاتصالات والإنترنت في 2022

في كلية العدالة الجنائية بجامعة الصين للعلوم السياسية والقانون، لو فنغ، أن ضعف القوانين في دول جنوب شرق آسيا جعلها بيئة خصبة لنشاط العصابات المتخصصة في الاحتياك الإلكتروني، فضلاً عن الاضطرابات الأمنية والسياسية في تلك المناطق. وينشط في شمال وشرق ميانمار حوالي مائة ألف شخص يرتكبون جرائم الاحتيال الإلكتروني كل عام، وفق ما يؤكد لو الذي يتابع الملف، مضيفاً أن السلطات الصينية تعمل على التعاون مع سلطات هذه الدول لضبط المتورطين الذين يحملون الجنسية الصينية وجلبهم إلى البر الرئيسي، خصوصاً أن جل الضحايا من المواطنين الصينيين. وأضاف أن عمليات الاحتياك لا تنطوي فقط على خداع الأشخاص السذج لسرقة أموالهم، بل تتضمن أيضاً تزوير مستندات رسمية، بالإضافة إلى سلوكيات إجرامية أخرى تشمل الاتجار بالبشر وتهريب المخدرات عبر الحدود. وتبرز خطورة الظاهرة في إعلان وزارة الأمن العام الصينية في الثامن من سبتمبر/ أيلول الماضي، عبر موقعها الإلكتروني بأنها تسلمت 1207 مشتبه بهم في عمليات احتياك من شمال ميانمار، بما في ذلك 41 مطلوباً، بالإضافة إلى عدد كبير من أدوات الجريمة، مثل أجهزة الكمبيوتر والهواتف المحمولة وبطاقات الهاتف المحمول والبطاقات المصرفية. وقالت إن السلطات الصينية نجحت خلال أغسطس/ آب الماضي في مدهمة بالتعاون مع شرطة ميانمار أدت إلى تدمير 11 وكراً لشبكات الاحتيال في في شمال ميانمار والقبض على 269 متورطاً في عمليات الاحتيال، من بينهم 186 صينياً، و66 بورمياً، و15 فيننامياً، و2 ماليزيين.

### كيف تفاقم الظاهرة؟

أعلنت وكالات الأمن العام الصينية، في التاسع والعشرين من أغسطس من عام 2022، عن كشف 464 ألف حالة احتياك عبر الاتصالات والإنترنت في جميع أنحاء البلاد. ويوضح المحامي وي أن عام 2020 شهد أعلى نسبة احتياك عن بعد في البلاد، إذ تم رفع 927 ألف قضية، وبلغ حجم الخسائر 35 مليار يوان (4,8 مليارات

### يكين. علي ابو مريحيلا

خسر التاجر الأردني محمد عبد الفتاح نصف مليون يوان صيني (70 ألف دولار)، بعدما استقبلت موظفة تعمل في شركته مكالمات هاتفية ادعى المتصل خلالها أنه موظف في مؤسسة مالية تتعامل معها الشركة وأبلغها بتجميد الحساب البنكي مؤقتاً بسبب تنبؤ برنامج تدقيق جديد على الحسابات الأجنبية، وفي حال كانت ترغب في تدارك الأمر عليها الذهاب إلى البنك للمراجعة، أو إرسال رمز التحقق الذي سيصل إليها على رقم الهاتف عبر رسالة نصية. اختارت الموظفة الخيار الثاني، لكن سرعان ما وصلها إشعار بنكي بتحويل مبلغ مالي من حساب الشركة لصالح حساب آخر، ليتضح لاحقاً أنها وقعت في شرك عصابات الاحتيال الإلكتروني. وقدم عبد الفتاح، الذي يعمل في مجال الشحن بالصين منذ 11 عاماً، بلاغاً إلى قسم شرطة كوانزو في التاسع من يناير/ كانون الثاني الماضي، وبعد مضي أسبوعين من التحقيق أُبلغ بأن المبلغ المقتطع تم تحويله إلى خارج الصين، وأن ذلك يندرج ضمن عمليات الاحتيال العابرة للحدود، وهو ما يعني إغلاق الملف، على اعتبار أن المجرم مجهول الهوية، وفي هذه الحالة يتم الاحتفاظ بالمعلومات الخاصة بالضحية للعودة إليه في حال ظهور أي مستجدات ذات صلة، كما يقول عبد الفتاح، والذي يعد واحداً من بين نصف مليون ضحية سنوياً في الصين، كما يوضح المحامي جو وي (يدير مكتب محاماة في بكين) المتخصص في تتبع الجرائم الإلكترونية.

### جريمة عابرة للحدود

انتقلت العصابات الإجرامية الصينية إلى دول جنوب شرق آسيا، بما في ذلك ميانمار ولاوس وتايلاند، إذ تجنّد مواطني بلادها وأبناء تلك الدول عن طريق إعلانات ووظائف وهمية ووعود بروتات عالية، وبعد استدراجهم يتم احتجازهم بشكل غير قانوني، بحسب ما رصدته وزارة الأمن العام الصينية، ويوضح الأستاذ السابق