هاكرز يسطون على ٣٠ مصرفًا أوروبيًا والحصيلة ٣٦ مليون يورو

سرق لصوص من "الهاكرز" أكثر من ٣٦ مليون يورو من ٣٠ بنكا عبر أوروبا، باستخدام فيروس من الطراز الطروادي ذي المرحلتين، ينتشر من حاسب الضحية الشخصي إلى هاتفه الجوال .

وطال الفيروس أكثر من ٣٠ ألفا من عملاء المصارف في ألمانيا، وإيطاليا، وإسبانيا، وهولندا، وأطلقت عليه شركات الحماية اسم يوروجرابر (مُنتزع اليورو) .

ويعد هذا ثاني أهم اختراق مصرفي هذا العام. كان الأول بواسطة فيروس يدعى هاي رولر، أمكن بواسطته تحويل ٦٠ مليون دولار من الأوراق المالية المزوره إلى ٦٠ مؤسسة مالية، وفقا لـ "جارديان أنالاتيك"، وهي شركة أمن مصرفي عبر الإنترنت .

ومثل هاي رولر، بدأ يوروجرابير في إيطاليا قبل أن ينتشر في أنحاء أوروبا ، وكلا الهجومين استخدم بديلا لزيتمو، أو لزيوس في الجوال. والفيروس الطروادي هو نوع من الفيروسات ليس له تأثير مرئي، وهو يبقى في حالة كمون حتى تجيء الخطة المؤاتية .

ومع ذلك، يعتبر يوروجرابر أول فيروس طروادي ينتقل من حاسب المستخدم إلى هاتفه الجوال، كما أنه يستهدف الخدمات المصرفية عبر الإنترنت على وجه التحديد. ومع إصابة كل من الحاسب والجوال يمكن تسجيل رموز التحقق التي تم إرسالها نصيا إلى العملاء، لتستخدم لإنشاء دورة مصرفية ثانية في وقت قصير، ثم يحول المال من هذه الحسابات بقيم تراوح من ٥٠٠ يورو إلى ٢٥٠ ألف يورو .

وقال داريل بركي، مدير منتجات منع التسلل لدى شيك بوينت، وهي شركة تبيع منتجات لحماية الحاسب والشبكات: "دون تمجيد للمهاجمين، هذا عمل مصمم باحتراف". وأضاف: "الهواتف الجوالة التي استُهدفت شائعة جداً، كما أنهم استهدفوا مصارف ناجحة جداً ."

التصديق يكون من خطوتين، حيث يُدخل العميل رمزا يُرسل له بواسطة البنك، إضافة إلى كلمة المرور العادية، وهو أمر شائع في الخدمات المصرفية عبر الإنترنت، ويتم استخدامه أيضا من قبل شركات، مثل جوجل، لجعل خدمات الحوسبة السحابية أكثر أمنا.وقال إيال جرنير، مهندس الحماية الذي تعقب الفيروس لدى فيرسايف، وهي شركة أمن على الإنترنت: "أكثر من ٣٠ في المائة من بنوك الاتحاد الأوروبي والولايات المتحدة تستخدم شيئا مشابها لهذه الآلية". وتم الكشف عن الهجوم الذي وقع في آب (أغسطس) عندما أصاب الفيروس عملاء من شركتي شيك بوينت وفيرسايف. وتقول كلتا الشركتين إن هناك دلائل تشير إلى أنه كان مفعلا منذ أوائل عام ٢٠١٢ .

ولم تقل الشركتان مَن مِن العملاء أو البنوك هو المتضرر، لكنها قالت إنها على علم بالمتضررين. واستهدف الفيروس هواتف أندرويد وبلاك بيري .

ويوروجرابر هو أحدث مثال على الهجوم المخطط اجتماعيا، حيث يتم استخدام المعلومات من مواقع الإنترنت والشبكات الاجتماعية لتصميم بريد إلكتروني يغري الشخص لينقر على رابط، أو مستند يحمل الفيروس الأولي .

وقال بركي وجرنير إن بإمكان الناس تجنب مثل هذه الهجمات إذا أبقوا على ترقية برامج حواسبهم وهواتفهم، وابتعدوا عن الضغط على روابط ورسائل إلكترونية مجهولة المصدر.