أساليب لصوص البنوك الجدد والتهديد الذي يمثلونه

ترجمة وتحرير نون بوست

تحدث إلى المصرفيين وسيخبرك بعضهم أنه عندما يتعلق الأمر بالجرائم الإلكترونية، فإن البنوك تحتل المرتبة الثانية بعد الجيش من حيث قوة دفاعاتها. ومع ذلك، فإن البحث في شبكة الإنترنت المظلمة، كما فعلت شركة "إنتل 471" الاستخباراتية نيابةً عن صحيفة "الإيكونوميست" في شهر أيار/ مايو، يُظهر أنه من الواضح أن محاولات اختراق تلك الأسوار المنيعة شائعة.

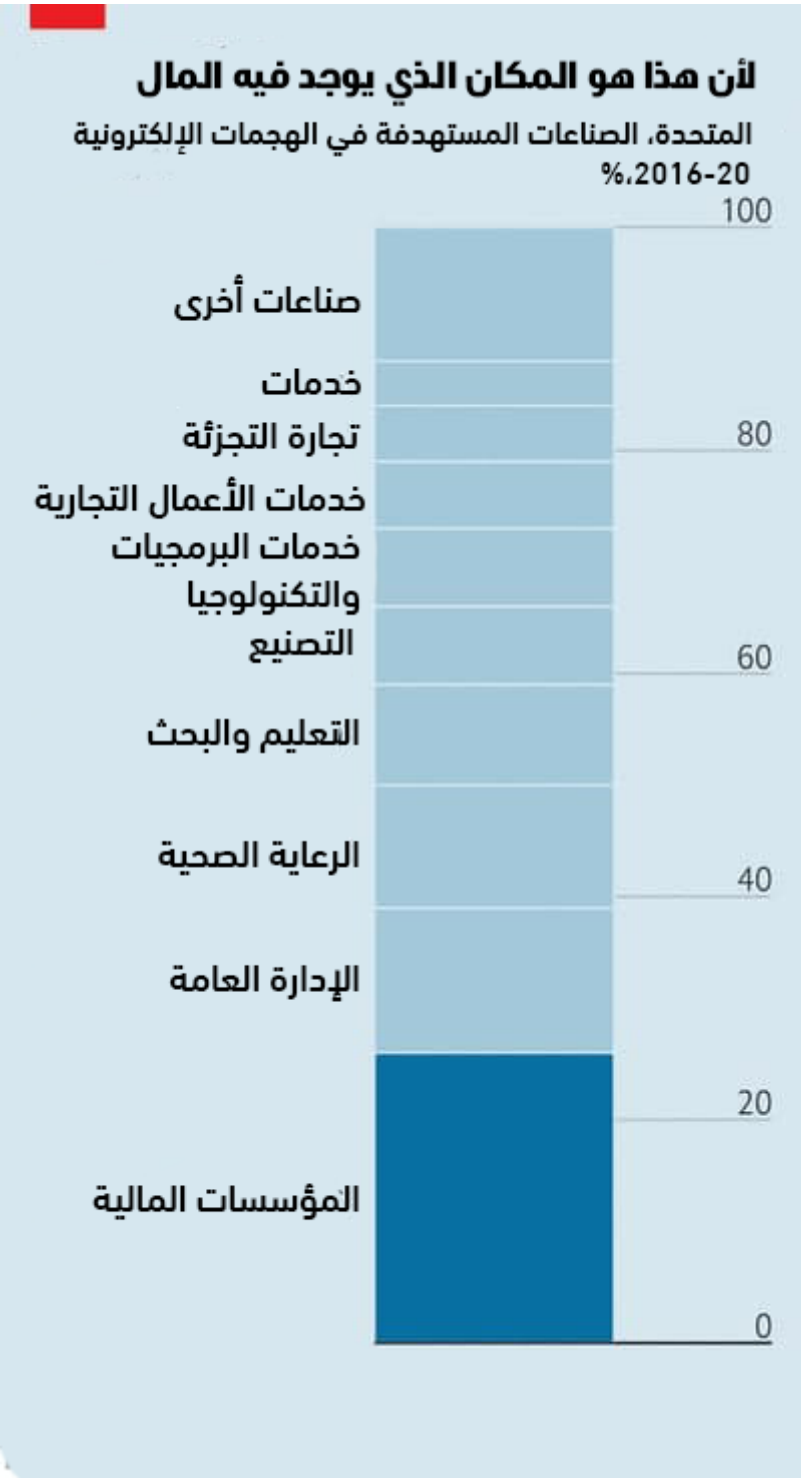
كشف أمر أحد المجرمين وهو يحاول تجنيد موظفين من البنك داخل أكبر ثلاثة بنوك في الولايات المتحدة، بنك "جي بي مورغان تشيس" و"بنك أمريكا" و"ويلز فارغو"، حيث كان يُقدم دفعة أسبوعية من "سبعة إلى ثمانية أرقام" للسماح بالتحويلات البنكية الاحتيالية. وكان لص آخر يبيع بالمزاد بيانات 30 مليون حساب في بنك "ملت" في إيران (التي يبلغ تعداد سكانها 83 مليونا).

يمارس هذا النشاط المُبتذل نوع جديد من لصوص البنوك. وبصرف النظر عن معوقات الماضي، فمن المرجح أن أذكى المخترقين يتلقون الدعم اليوم من الدول المارقة مثل كوريا الشمالية – وبدرجة أقل – إيران، أو تتسامح معهم دول مثل روسيا والصين؛ كما أنهم يستفيدون من موارد غير مسبوقة وحماية من وكالات إنفاذ القانون. وإلى جانب محاولة سرقة الحسابات، فإنهم يستهدفون أيضًا البيانات المتعلقة بالتجارة الداخلية.

باعتبارها واحدة من أولى الصناعات التي تقدم المعاملات عبر الإنترنت، تقاوم البنوك المخترقين منذ ظهور الإنترنت. وتُنفق المؤسسات المصرفية على الأمن السيبراني أكثر من أي نوع آخر من الشركات – 2691 دولارا لكل موظف – كما تمكنت من إحباط الكثير من محاولات السرقة. مع ذلك، منذ سنة 2016، لم تتعرض أي صناعة أخرى للهجمات أكثر من البنوك (انظر الرسم البياني).

في حديثها إلى الكونغرس في شهر أيار/ مايو، وصفت جاين فريزر التي تدير بنك "سيتي غروب"، وهو أحد أكبر البنوك في وول ستريت، عمليات الاختراق باعتبارها أكبر تهديد للنظام المالي الأمريكي. بينما قال

جيمي ديمون، رئيس مجلس إدارة بنك "جي بي مورغان تشيس" إنها يمكن أن تصبح "من أعمال الحرب".



نتيجة لذلك، تتعرض البنوك لضغوط مستمرة للاستعداد للأسوأ. وحسب رئيس الأمن السيبراني في أحد البنوك المركزية فإن "الأمر لا يتعلق باحتمال وقوع عمليات اختراق، وإنما بتوقيت حدوث هذه الهجمات". بعبارة أخرى، يحتاج المصرفيون إلى معرفة أساليب ودوافع أعدائهم، وما الذي تعلموه، وما إذا كان يمكنهم أن يسبقوهم بخطوة للأمام؟

كما هو الحال في الصناعات الأخرى، تبدأ محاولات سرقة البنوك عبر الإنترنت عمومًا باستراتيجية "الخداع

الإلكتروني" أو خداع الموظف لتنزيل برنامج حميد المظهر يُعرف باسم "حصان طروادة"، والذي ينشئ بابا خلفيا للفيروسات الأخرى بمجرد تثبيته من أجل اختراق أنظمة الشركة. ويمكن أن تكون الخدع مدروسة.

في سنة 2019، عندما تسلل المخترقون إلى "ريد بانك"، وهي شبكة مشتركة بين البنوك تربط نظام الصراف الآلي في تشيلي، قاموا بتزييف عملية توظيف مطولة واستكملوا عملية الاحتيال بجولات من مقابلات الفيديو لخداع ضحية واحدة لتنزيل برنامج "حصان طروادة" وتشغيله.

بمجرد تثبيت هذا البرنامج الخبيث، يكون لدى المخترقين العديد من أساليب الاختراق، وقد تطورت أساليبهم مع مرور الوقت. في مطلع سنة 2010 وحتى منتصفه، وتتمثل الاستراتيجية الشائعة في تغيير قواعد بيانات البنوك لتضخيم الأرصدة في الحسابات الحالية من أجل استنزافها بالتحويلات الاحتيالية عبر الإنترنت.

وتتمثل الاستراتيجية الأخرى في سرقة أسماء وكلمات مرور الموظفين المصرح لهم بالوصول إلى "سويفت"، وهو نظام المراسلة المشترك بين البنوك المستخدم في التحويلات الدولية، من أجل إجراء تحويلات احتيالية إلى الحسابات المصرفية الخاصة باللصوص.

في سنة 2016، وفي أكبر عملية سرقة إلكترونية في العالم، قام اللصوص بتحويل الأموال من حساب البنك المركزي البنغلاديشي في البنك الاحتياطي الفيدرالي في نيويورك إلى بنوك في الفلبين وسريلانكا وأجزاء أخرى من آسيا، وسرقوا ما يُقدّر بـ 81 مليون دولار.

تتزايد هجمات برامج الفدية، مثل الهجمات الشائعة في قطاعات أخرى من الأعمال التجارية. ولكن البنوك بشكل خاص مهددة بطرق أخرى أيضًا، وأحد الأمثلة على ذلك هو عملية "الفوز بالجائزة الكبرى"، حيث تخترق البرامج الضارة أجهزة الصراف الآلي وتتلاعب بها لتسهيل الوصول إلى الكثير من الأموال النقدية التي يمكن الوصول إليها عن طريق البطاقات المزيفة، حتى في حالة عدم وجود أموال.

غالبا ما تتعاون الدول المارقة في مشاريع مشتركة مع عصابات خاصة، من بينها فريق يتحدث الروسية ويدير برنامجًا خبيثا سيئ السمعة يسمى "تريكبوت" يوفر إمكانيّة الوصول إلى العديد من أجهزة الكمبيوتر المخترقة

بعد ذلك، يستأجر اللصوص مجموعات من الأشخاص لنقل المال، يكونون عادة من المافيا المحلية، لإجراء عمليات سحب متعددة في وقت واحد. وباستخدام مثل هذه الأساليب، تمكن المجرمون في سنة 2018 من تجميع 13.5 مليون دولار من بنك كوزموس الهندي من خلال إجراء 15 ألف عملية سحب نقدي في غضون ساعتين فقط.

يتمثل التكتيك الآخر في تحويل المواقع الإلكترونية التي تزورها البنوك بانتظام إلى "منطقة استدراج" خطيرة. وقد حصلت أشهر سرقة من هذا النوع في سنة 2017 عندما استهدف المجرمون بنجاح 104 شركة مالية تواجد معظمها في 31 دولة، بما في ذلك سبعة بنوك في بريطانيا و15 بنكا في الولايات المتحدة.

في هذه الحادثة، تم استهداف المواقع الإلكترونية للبنوك المركزية في بولندا والمكسيك وغيرها بطريقة تدفعها لتنزيل ملفات ضارة وإصابة نفسها ببرامج ضارة يمكن استخدامها للتجسس عليها وسرقة بياناتها وإجراء عمليات تحويل احتيالية في نهاية المطاف. وفي بعض الأحيان، تكون البيانات هي ما يسعى اللصوص وراءه وليس المال.

تتمثل الحيلة الأخيرة في سرقة بيانات السوق المالية من داخل البنوك من أجل تسهيل التداول من الداخل. وقد أظهر استطلاع أجرته شركة "في إم وير" للأمن السيبراني على 126 شركة مالية في جميع

أنحاء العالم أن 51 بالمئة من المؤسسات المصرفية شهدت ارتفاعًا في أعداد هذه الهجمات خلال السنة الماضية. وحسب توم كيليرمان، مدير استراتيجية الشركة، فإن مديري المحافظ الماليّة في الولايات المتحدة وبريطانيا الذين تعرّضوا للإختراق مؤخرا كانوا يلاحظوا وجود نشاط مشبوه كلما كانوا على وشك التداول.

تتفاقم وتيرة هذه الأساليب بسبب حقد المتورطين، إذ تُنفذ عمليات السرقة في الواقع من قبل لصوص مأجورين من دول الاتحاد السوفيتي سابقًا. ومن بين هؤلاء "كاربناك"، وهي عصابة سيئة السمعة سرقت أكثر من مليار دولار من 100 بنك بعد سنة 2013 (ألقي القبض على العقول المدبرة للعصابة في سنة 2018). ذكر مايكل دامبروسيو، أحد كبار المحققين في الاستخبارات السريّة الأمريكيّة، أنه منذ أن قامت الولايات المتحدة بإخراج كوريا الشمالية من نظامها المالي في سنة 2017، ضاعفت الدولة المنبوذة علاقتها مع العصابات الإجرامية كوسيلة "لجني الأرباح والتهرب من العقوبات".

تُعرف هذه الكيانات، التي ترعاها الدولة ويُطلق عليها اسم "لازاروس" أو "بلونرأوف" أو "بيغلبويز"، بقدرتها على الوصول إلى الموارد والموظفين أكثر بكثير من المجرمين. ويقول مارك أرينا من شركة "إنتل 471" إنه غالبا ما يعيش أعضاء هذه المجموعات في الخفاء في روسيا والصين. اتهمت وزارة العدل الأمريكية، في لائحة اتهام نشرتها في كانون الثاني/ يناير، شخصين مرتبطين بوكالة استخبارات عسكرية من كوريا الشمالية بمحاولة سرقة أكثر من 1.3 مليار دولار من البنوك عبر الإنترنت ومداهمات أجهزة الصراف الآلي فضلا عن ابتزاز شركات العملة المشفرة.

يمكن لأحد قضايا المحكمة العليا في بريطانيا التي عُقدت هذا الصيف أن تسهل سير الدعاوى القضائية الجماعية المرفوعة من قبل العملاء المتضررين من الانتهاكات الإلكترونية

غالبا ما تتعاون الدول المارقة في مشاريع مشتركة مع عصابات خاصة، من بينها فريق يتحدث الروسية ويدير برنامجًا خبيثا سيئ السمعة يسمى "تريكبوت" يوفر إمكانيّة الوصول إلى العديد من أجهزة الكمبيوتر المخترقة. ومؤخرًا، صُدم بعض خبراء الإنترنت عندما اكتشفوا أن هذا البرنامج استُخدم مع برامج كوريا الشماليّة الضارة التي تسبّبت في الهجمات الأخيرة.

لا يمكن تحديد حجم الأموال التي تُستنزف في الخفاء. تشير الأرقام التي تم تحليلها من قبل شركة "أدفايزن" الاستشارية إلى أن البنوك قد خسرت حوالي 12 مليار دولار بسبب جرائم الإنترنت منذ سنة 2000، حوالي ثلاثة أرباع هذه المبالغ كانت نتيجة انتهاكات البيانات. وتشير الدراسات إلى أن توقف سير العمل لمدّة ساعة يكلف البنك 300 ألف دولار بمعدّل متوسط، بينما يؤدي خرق البيانات إلى خسائر قدرها 6 ملايين دولار.

عادة ما تمنع البنوك موظفيها من مناقشة مثل هذه الهجمات، كما أن الأرقام المُبلغ عنها تقلل من الحجم الحقيقي للمشكلة. مع أن العديد من المؤسسات ملزمة بإبلاغ المنظمين والعملاء أيضًا في بعض الأحيان عن هذه الحوادث، إلا أن القواعد تتغير بشكل متكرر وتختلف عبر الولايات القضائية مما يجعل عملية الإفصاح عن المعلومات عشوائية.

يمكن أن تتضاءل الخسائر الأولية بتأثيرات من الدرجة الثانية. ويشير جون ماير من شركة "كورنرستون إدفايزر" الاستشارية إلى أن الحادث العادي يعرّض 27 بالمئة من العملاء لخطر كبير يتمثل في إغلاق حساباتهم في الشركة المستهدفة وخفض أسعار أسهم الشركات بنسبة 5 أو 7 بالمئة بمعدّل متوسط.

ويمكن لأحد قضايا المحكمة العليا في بريطانيا التي عُقدت هذا الصيف أن تسهل سير الدعاوى القضائية الجماعية المرفوعة من قبل العملاء المتضررين من الانتهاكات الإلكترونية، مما يعرّض البنوك لاحتمال دفع تعويضات بمئات الملايين من الجنيهات الإسترلينية.

لكن الأمور لا تجري لصالح المجرمين على الدوام. تبلي شركات التحليل الجنائي الرقمي بلاءً حسنا في تتبع الهجمات وتحديد مرتكبيها، وتعمل وكالات الاستخبارات على ربط أسماء المستخدمين بأشخاص حقيقيين. على هذا النحو، يتم إيقاف بعض العصابات أو القبض عليها.

في أيلول/ سبتمبر، شنّ الجيش الأمريكي هجومًا إلكترونيًا أضعف عمل "ترك بوت"، وهو أحد أحصنة طروادة المدعومة من كوريا الشمالية. وفي كانون الثاني/ يناير، نجحت الشرطة الأوكرانية في إطار عملية مشتركة مع نظرائها الأوروبيين والأمريكيين في إلقاء القبض على اللصوص الذين يديرون برامج "إيموتيت"، وهي شبكة "بوت نت" أخرى يُزعم أنها مسؤولة عما لا يقل عن سرقة 2.5 مليار دولار منذ سنة 2014.

تسعى البنوك جاهدة لإرساء أنظمة دفاعية أكثر فاعلية وتوظيف قراصنة من "أصحاب القُبّعات البيضاء" للتأكد من كفاءة دفاعاتها. وفي هذا الصدد، ينفق أكبر البنوك مبالغ طائلة حيث أعلن "بنك أمريكا" في حزيران/ يونيو عن قراره استثمار مليار دولار سنويًا للتصدي للتهديدات المتزايدة.

وجدت دراسة استقصائية أجرتها شركة "ديلوات" أن المؤسسات المالية قد أنفقت 0.48 بالمئة في المتوسط من إيراداتها على الأمن السيبراني في السنة المنقضية، مسجلة زيادة عن نسبة 0.34 بالمئة المسجلة في سنة 2019. وبتطبيق ذلك على إجمالي إيرادات القطاع في سنة 2020، فإن الإنفاق قد يصل إلى 23 مليار دولار في أمريكا لوحدها.

مع ذلك، قد تزداد الأمور سوءًا ويعود ذلك لسببين: أولهما أن تأمين شبكات البنوك قد أصبح أكثر تكلفة. ويقول المسؤول عن الشؤون السيبرانية لأحد البنوك الأمريكية الكبرى: "نحن ندرك أننا لن نتصدى لكل شيء، لذلك ينبغي أن يكون لدينا دفاعات متعددة الطبقات توضع على افتراض أن كثيرا من الدفاعات ستبوء بالفشل". والآن، في ظل تضاعف عدد الأجهزة المتصلة بالإنترنت، ورقمنة الخدمات المصرفية، والعمل عن بُعد، زادت الثغرات التي يمكن للجهات المعتدية استغلالها.

تزداد العصابات الإلكترونية ثراءً، حيث أعلنت عصابة "ميز" عن "التقاعد" في تشرين الثاني/ نوفمبر بعد أن حصلت على ما يزيد عن مئة مليون دولار من الفديات في سنة واحدة

تعرضت شركة "أكامي"، وهي شركة أمنية تستفيد من خدماتها ثمانية من أكبر عشرة بنوك في العالم، ما وصل إلى 736 مليون هجوما استهدف تطبيقات الشركات المالية القائمة على الويب في السنة الماضية فقط، بزيادة تعادل الثلثين مقارنة بسنة 2019. لقد أدى التوسع في شركات التكنولوجيا المالية دون مصاحبته بلوائح متسقة إلى خلق نقاط مبهمة. كما أن انتقال البنوك إلى السحابة، التي تعتبر أكثر أمانًا نظريًا، يمكن أن يأتي بنتائج عكسية إذا انتهى الأمر بتركيز المخاطر على عدد قليل من المنصات، وذلك حسب ما أفاد به سمسار التأمين جانو بيرموديز من شركة "مارش آند ماكلينان".

ثانيًا، بات لدى المجرمين قدر أكبر من الموارد – سواء تكنولوجية أو مالية – تحت تصرفهم. ووفقًا لخبراء أمنيين، يكون التركيز بشكل أساسي على طرد المتسللين قبل أن تتسنى لهم فرصة السرقة. ويتوقع أحد الخبراء أنه من المرجح أن يبدأ المتسللون باستخدام الذكاء الاصطناعي قريبا لتسريع عملية الهجوم من البداية وحتى النهاية – فيما يسمى بـ "سلسلة القتل السيبراني" في المصطلحات التخصصية.

تزداد العصابات الإلكترونية ثراءً، حيث أعلنت عصابة "ميز" عن "التقاعد" في تشرين الثاني/ نوفمبر بعد أن حصلت على ما يزيد عن مئة مليون دولار من الفديات في سنة واحدة. ويحاول المجرمون الصاعدون النسج على منوالهم.

في الخريف الماضي، قام بعض القراصنة بانتحال صفة مجموعتي "لازاروس" و"فانسي بير" (مجموعة روسية سيئة السمعة)، وهددوا أكثر من مئة هيئة مالية بهجمات الحرمان من الخدمة الموزعة "دوس"،

التي يقوم "سادة البوت" بصددها بحشد شبكات واسعة من الأجهزة المصابة بالفيروسات لإغراق أهدافهم بحركة إنترنت غير اعتيادية في حالة رفضهم دفع الفديات.

يمكن لمثل هؤلاء القراصنة الاعتماد على الأسواق الثانوية المزدهرة لتحقيق الدخل من غنائم جرائمهم. ومؤخرا، زارت صحيفة "ذي إيكونوميست" موقع "تور ريز" المشابه لموقع "إي باي" عبر متصفح لا يمكن تعقبه، ووجدت فيه أن تفاصيل بطاقة ائتمان واحدة تباع بمبلغ 25 دولارًا – أو الأربعة بسعر ثلاثة. ومقابل 4.99 دولارات، يقدم برنامج تعليمي المساعدة في بناء مواقع تصيد احتيالية تحاكي مواقع بنك "باركليز" البريطاني.

تُجرى المشتريات في "تور ريز" بالعملات المشفرة التي يمكن صرفها في الحسابات المصرفية المفتوحة باستخدام معرّفات مزيفة (على سبيل المثال، تبلغ تكلفة رخصة القيادة من ولاية تينيسي 150 دولارًا). على هذا النحو، مازال لصوص البنوك الجدد رواد أعمال محنكين كأسلافهم تماما.

المصدر: الإيكونوميست

رابط المقال: https://www.noonpost.com/40988/