تقرير تزداد القرصنة الإلكترونية في ظل انتشار استخدام الإنترنت في جميع المجالات، وتحديداً التعاملات المصرفية. الغنائم الناجمة عن عمليات الاختراق والقرصنة هذه تزداد بوتيرة متسارعة، إذ بلغ عدد العمليات المبلّغ عنها، التي تعرضت لها المصارف في لبنان، نحو 233 عملية إلكترونية، ووصلت قيمة الأموال المقرصنة عبرها إلى نحو 26 مليوناً ونصف مليون دولار

«القراصنة» في لبنان: الاستيلاء على 26,5 مليون دولار

تعرّضت المصارف في لبنان لـ 7 أنواع من الهجمات الإلكترونية

إيفا الشوفي

بلغ عدد عمليات القرصنة الإلكترونية التي تعرضت لها المصارف حصراً منذ عام 2011 حتى الفصل الثالث من السنة الحالية، وفق أرقام هيئة التحقيق الخاصة لدى مصرف لبنان، 233 عملية، وصلت فيها قيمة الأموال التي تعرضت للقرصنة إلى نحو 26 مليوناً ونصف مليون دولار، من ضمنها 15 مليون دولار بين عامي 2015 و2016 طاولت القطاع المصرفي بشكل مباشر، وفق رئيسة مكتب مكافحة الجرائم المعلوماتية وحماية الملكية الفكرية، المقدم سوزان الحاج. تعكس هذه الأرقام الحد الأدنى، إذ إن القيمة الفعلية للغنائم وعدد العمليات الإلكترونية، باعتراف هيئة التحقيق ومكتب مكافحة الجرائم المعلوماتية، أكبر بالتأكيد، لأن هناك حالات لم يتم الإبلاغ عنها إما بدافع الحفاظ على السمعة أو يقيناً باستحالة استعادة تلك الأموال.

تطور العمليات المسجلة

منذ عام 2014، ارتفعت معدلات ما يُطلق عليه قانوناً اسم الجريمة الإلكترونية في لبنان، ما وضع المعنيين في المصارف والمؤسسات المالية والأجهزة الأمنية أمام سباق مع القراصنة القادرين على تطوير أدواتهم وتكتيكاتهم بموازاة تطور وسائل المكافحة. في إطار هذا السباق المثير، نُظّم أول من أمس "ملتقى مكافحة الجريمة الإلكترونية الثاني"، حيث تم الكشف عن حجم الأموال المختلسة الضخمة، بلسان الجهتين الأكثر اطلاعاً عليها: مكتب مكافحة الجرائم المعلوماتية في قوى الأمن الداخلي وهيئة التحقيق الخاصة لدى مصرف لبنان.

عام 2011، تلقت هيئة التحقيق الخاصة لدى مصرف لبنان تقريراً واحداً بمعاملة "مشبوهة" بقيمة 5500 دولار. في العام التالي، لم تصل أي شكوى إلى الهيئة، أما في عام 2013 فقد سجّلت الهيئة 8 تقارير بمعاملات بلغت قيمتها 895 ألف دولار. في عام 2014، ازدادت التقارير بشكل حاد ليبلغ عددها 51 شكوى توزعت بين طلبات مساعدة وتقارير بمعاملات "مشبوهة"، وبلغت قيمتها 5 ملايين دولار. التطوّر الأبرز حصل في عام 2015 عندما وصلت قيمة الأموال التي تعرضت للقرصنة إلى 12 مليون دولار في عام واحد عبر 84 عملية. عدد الشكاوى والقضايا الواردة إلى الهيئة ازداد سنوياً ليصل هذه السنة في فصلها الثالث إلى 89 قضية بلغت قيمة الأموال فيها 8 ملايين ونصف مليون دولار.

يشرح أنطوان مندور، نائب مدير مساعد في هيئة التحقيق الخاصة لدى مصرف لبنان، وضع التقارير الواردة إلى الهيئة بشكل مفصّل منذ بداية السنة حتى الفصل الثالث منها. يتبيّن أن الهيئة تلقت هذه السنة 139 قضية من المصارف، منها 119 قضية عبارة عن تقارير بمعاملات "مشبوهة" و20 طلب مساعدة. بلغت قيمة العمليات المنفذة نحو 3 ملايين و700 ألف دولار، لم تتمكن الهيئة من استرجاع سوى 833 ألف دولار منها، أي ما نسبته 28,50%.

تصنيف العمليات وأنواعها

تعرض الهيئة تصنيف القضايا الواردة إليها ليظهر أن العدد الأكبر من العمليات المنفذة وغير المنفذة يندرج ضمن فئتين أساسيتين:

> **تم استرداد 833 ألف دولار فقط من أصل 3 ملايين و700 ألف دولار**

الفئة الأولى هي BEC1، أي عمليات إلكترونية تتم عبر اختراق البريد الإلكتروني للمصرف أو العميل، إذ يقوم المقرصن بالدخول إلى البريد الإلكتروني للعميل أو ينشئ بريداً إلكترونياً مشابهاً له ويراسل المصرف لطلب إجراء عملية تحويل من حسابه إلى حساب آخر، ليتبين لاحقاً أن العميل الأساسي لم يطلب إجراء أي عملية تحويل. بلغ عدد العمليات المنفذة 29 عملية مقابل 46 عملية غير منفذة، وعليه، تستغرب الهيئة حصول عمليات منفذة ضمن هذه الفئة التي يمكن كشفها بسهولة، إذ إنه تم إلزام المصارف بالاتصال هاتفياً بالعميل قبل إجراء عملية تحويل للتأكد من صحة العملية والحساب المرسل إليه.

أمّا الفئة الثانية وهي CEC1، أي انتهاك البريد الإلكتروني للشركة المورّدة، إذ يقوم المقرصن باختراق البريد الإلكتروني للمورّد الذي يتعامل معه العميل ويطلب إجراء تحويل إلى حسابه ليتبيّن لاحقاً أن الحساب مخترق. المستغرب في هذه الفئة هو أن عدد العمليات المنفذة يفوق بنسبة 95% عدد العمليات غير المنفذة، إذ بلغ عدد العمليات المنفذة حتى الفصل الثالث من هذه السنة 36 مقابل عمليتين فقط غير منفذتين. باتباع وجهة الأموال المقرصنة، يظهر أمر مشترك وهو أن النسبة الأكبر من التحويلات تتم إلى مصارف في بريطانيا، التي تلقت 38 عملية تحويل بقيمة 1,3 مليون دولار، تليها هونغ كونغ بـ 12 عملية تحويل بمجموع 1,6 مليون دولار.

أبرز الهجمات الإلكترونية على المصارف

تعرّضت المصارف في لبنان خلال فترة 2015 - 2016 لـ 7 أنواع من الهجمات الإلكترونية، وفق مكتب مكافحة الجرائم المعلوماتية. النوع الأول من الهجمات هو الـ DDoS attack، أي هجمات الحرمان من الخدمة، وهي عبارة عن إغراق خادم المصرف بعدد كبير من الطلبات الوهمية حتى يقف عن العمل. مصرفان اثنان كانا عرضة لهذا الهجوم، وفي إحدى الهجمات تبيّن أنّ الهجوم الإلكتروني تم من خلال مشاركة محلية مع مجموعة "أنونيموس" العالمية، وتم توقيف الشخص المقرصن الذي أعاد تمثيل عملية القرصنة.

النوع الثاني من الهجمات استهدف قرصنة التطبيقات الهاتفية للمصارف، وتقول الحاج إنّ غالبية تطبيقات المصارف تعرضت للقرصنة. جراء هذه الهجمات، توقفت 3 تطبيقات عائدة لثلاثة مصارف عن العمل، ما أدى إلى خسائر بقيمة 15 ألف دولار ناتجة من سرقة الأموال من هذه الهجمات. تحصل هذه الهجمات جراء نجاح المقرصن بتجاوز مسار الدفع والاحتيال على النظام وسرقة الأموال بسبب ضعف في الـ source code العائد للتطبيق، وقد قام مكتب مكافحة الجرائم المعلوماتية بتوقيف جميع المقرصنين.

4 مصارف تعرّضت لسرقة الـ ATM عبر الاحتيال على النظام وخرق المعلومات الخاصة بالزبائن وسحب الأموال من الـ ATM ثم تطورت إلى هجمات على خوادم الـ ATM بحيث يُعطى أمر بإفراغ الأموال الموجودة داخلها مثلما حصل في دول عديدة مثل روسيا وهولندا وأرمينيا... لا يعلن مكتب مكافحة الجرائم المعلوماتية عن حجم الخسائر الناتجة من هذه العمليات. وتقول الحاج فقط إنّ "قيمة الخسارة تمتلكها المصارف".

كذلك تعرضت 5 مصارف لهجوم يقوم على استنساخ الموقع الإلكتروني للمصرف (cloning of banks and forex websites) وتعديل برمجته بحيث يدخل العملاء جميع معلوماتهم على الموقع الوهمي، وبالتالي يسلمون القراصنة كلمات مرورهم. الخسائر الناجمة عن هذه العمليات بلغت 50 ألف دولار، ويتوقع المكتب أن تزداد هذه العمليات، علماً بأنه تم إغلاق المواقع الوهمية.

20 عملية متعلقة باستخدام بطاقات مقرصنة للشراء على الإنترنت تعرضت لها المصارف، ووصلت الخسائر الناجمة عنها إلى مليوني دولار تمت بغالبيتها شراء بطاقات سفر. أمّا الهجوم السادس فهو نشر برمجيات خبيثة (MALWARE) هدفها سرقة قاعدة المعلومات العائدة لزبائن المصرف، وقد أصابت هذه الفيروسات 100 شركة عبر سرقة المعلومات الشخصية لها. إضافة إلى الـ RANSOMWARE أو برنامج الفدية بحيث يقوم المقرصن بتشفير خوادم المصارف والشركات ويطالب بفدية مقابل فك التشفير. وقد بلغ عدد هذه الجرائم 45 جريمة نتج منها خسائر بقيمة مليون دولار. تتوقع الحاج أن يزداد هذا النمط، لافتةً إلى أن مكافحة ظاهرة نشر الفيروسات تحتاج إلى أعتدة وتدريبات خاصة.

أمّا الهجوم الأخير فهو الاحتيال عبر اختراق البريد الإلكتروني للمصرف وللشركات الموردة والعملاء، وقد كبّد المصارف خسائر بقيمة 10 ملايين دولار! ورغم جميع الجهود المبذولة، لا يزال هذا النوع من القرصنة يزداد لأن المقرصن لا يحتاج إلى خبرات تقنية متقدمة جداً لتنفيذه.