آندي غرينبرغ | نشر في ١٧ أبريل ٢٠١٧,

تقارير مسربة تكشف تغلغل وكالة الأمن القومي بالنظام المصرفي في الشرق الأوسط

ترجمة وتحرير: نون بوست

على امتداد ثمانية أشهر، قامت مجموعة من القراصنة التي تُعرف باسم "وسطاء الظل" بكشف النقاب شيئا فشيئا عن بيانات بالغة السرية تمتلكها وكالة الأمن القومي الأمريكية. مؤخرا، وفي الوقت الذي بدى فيه أن خزينة الأسرار قد نفذت، قام "وسطاء الظل" بتقديم دفعة جديدة منها أظهرت أن وكالة الأمن القومي نجحت في التوغل عميقا داخل البنية التحتية المالية في الشرق الأوسط. ونتيجة لذلك، قد يساهم هذا التطور في الكشف عن فضائح جديدة في حق وكالة التجسس التي تمتلك أفضل الموارد في العالم.

في صبيحة يوم الجمعة الماضي، نشر "وسطاء الظل" وثائق، في انتظار إثبات صحّتها، تبيّن مساعي المخابرات الأمريكية إلى إضعاف عناصر من النظام المصرفي العالمي. كما يشمل التسريب الجديد أدلة مفادها أن وكالة الأمن القومي اخترقت شركة "إيستنيتس" العالمية، التي يقع مقرها في مدينة دبي. والجدير بالذكر أن هذه الشركة تشرف على المبادلات المالية لعشرات البنوك العميلة لديها وغيرها من الشركات، خاصة في منطقة الشرق الأوسط، وذلك ضمن نظام المعاملات "سويفت" العالمي.

يتضمن التسريب قوائم مفصلة تحتوي على أجهزة الكمبيوتر التي تمت قرصنتها أو التي من المحتمل استهدافها، بما في ذلك تلك التي تتبع شركات في كل من قطر، ودبي، وأبو ظبي، وسوريا، واليمن والأراضي الفلسطينية

فضلا عن ذلك، يتضمن التسريب قوائم مفصلة تحتوي على أجهزة الكمبيوتر التي تمت قرصنتها أو التي من المحتمل استهدافها، بما في ذلك تلك التي تتبع شركات في كل من قطر، ودبي، وأبو ظبي، وسوريا، واليمن والأراضي الفلسطينية. بالإضافة إلى تضمّنت قائمة البيانات، كما هو الحال في الإصدارات السابقة "لوسطاء الظل"، مجموعة من أدوات القرصنة الجديدة، التي تستهدف هذه المرة نطاقا واسعا من إصدارات نظام "ويندوز" للحواسيب.

في هذا الصدد، أرفقت مجموعة القراصنة التسريبات التي أصدرتها بيانا كتبت فيه: "هل كنتم تعتقدون أن تلك كانت النهاية؟". علاوة على ذلك، كانت هناك تكهنات قبيل نشر "وسطاء الظل" في ذلك الصباح حول كشف القراصنة بالفعل عن مجموعة كاملة من الوثائق المسروقة، وذلك في أعقاب محاولة فاشلة لاستردادها مقابل مبالغ بعملة "بيتكوين". وقد علّق القراصنة حول هذه المسألة قائلين "من المؤسف أن يقرر أحد ما أن يدفع مبالغ مالية لوسطاء الظل حتى يلتزموا الصمت".

عملية "السويفت"

في الواقع، يتعرّض بروتوكول المعاملات "سويفت" إلى استهداف مكثف من قبل القراصنة الذين يسعون لإعادة توجيه ملايين الدولارات من البنوك في جميع أنحاء العالم. وقد تركزت هذه العمليات مؤخرا في كل من الهند، والإكوادور، وبنغلاديش. كما أن الباحثين الأمنيين كانوا قد سلّطوا الضوء على أدلة تفيد بأن سرقة مبلغ بقيمة 81 مليون دولار من مصرف بنغلاديش عبر نظام "سويفت" قد يكون من عمل الحكومة الكورية الشمالية.

في المقابل، احتوت أحدث تسريبات "وسطاء الظل" على دليل جديد يوضح أن وكالة الأمن القومي قد أضرت هي الأخرى بنظام "سويفت"، حتى وإن ارتبط ذلك بعمليات التجسس الصامت دون القيام بالسرقة الفعلية. من جهتها، نفت شركة "إيستنيتس" أنه قد تمت قرصنتها، حيث أكدت على حسابها في موقع "التويتر" أن "إدعاء السيطرة على معلومات عملاء "إيستنيتس" المتداول على شبكة الإنترنت والمتعلقة بمكتب الشركة لخدمات "سويفت"، لا أساس له من الصحة".

تضمنت اللائحة بورصة دبي للذهب والسلع، وبنك التضامن الإسلامي الدولي، علاوة على بنك نور الإسلامي، ومؤسسة البترول الكويتية، وشركة اتصالات قطر وغيرها من الشركات الأخرى

خلافا لذلك، أشار "وسطاء الظل" من خلال تسريباتهم إلى عكس ما صرّحت به الشركة. فعلى سبيل المثال، جاء في إحدى جداول البيانات المسربة قوائم أجهزة كمبيوتر عن طريق عناوين "آي بي" التابعة لشركات في قطاع التمويل، على غرار بنك قطر الأول للاستثمار، والمؤسسة العربية للاستثمارات البترولية. كما تضمنت اللائحة بورصة دبي للذهب والسلع، وبنك التضامن الإسلامي الدولي، علاوة على بنك نور الإسلامي، ومؤسسة البترول الكويتية، وشركة اتصالات قطر وغيرها من الشركات الأخرى.

من ناحية أخرى، يشير الوصف الموجود في أعلى جدول البيانات الذي تمت سرقته إلى أن 16 عنوان بروتوكول الإنترنت "أي بي"، قد "تمت قرصنته وبدأت عملية جمع المعلومات منها". وتعني هذه العبارة أن جهاز الكمبيوتر قد تمت قرصنته بنجاح بالاعتماد على برامج تجسس الوكالة. ومن هذا المنطلق، قال الباحث الأمني، مات سويش، الذي يعمل في دبي، إن عناوين "آي بي" الآنف ذكرها ليست مرتبطة فعليا بأجهزة الكمبيوتر الخاصة بالعميل، بل تتوافق مع أجهزة الكمبيوتر التي تخدم هؤلاء العملاء في شركة "إيستنيتس".

وأضاف سويش أنها هذه الأجهزة تمثل واحدة من أصل 120 "مكتب" يشكل جزءا من شبكة "سويفت" ويُعنى بتقديم الخدمات المالية وإجراء المعاملات نيابة عن العملاء. وأورد سويش، مؤسس شركة "كوماي تكنولوجيز"، التي تتخذ من دولة الإمارات العربية المتحدة مقرا لها، أن "الأمر يعادل

قرصنة جميع البنوك في المنطقة من دون اللجوء إلى قرصنتها كل على حدى، مما يمكنك من الولوج إلى جميع معاملاتهم".

الانتكاسة

على الرغم من أن تسريبات "وسطاء الظل" السابقة تضمّنت البرامج الخبيثة التي تستخدمها وكالة الأمن القومي، إلا أن التسريب الأخير يحمل أول مؤشر على استهداف القرصنة المتطورة للنظام المصرفي العالمي. وعلى عكس عمليات قرصنة الشبكة المالية "سويفت" السابقة والمعروفة، تخلو الوثائق المسربة الجديدة من أية إشارة إلى أن وكالة الأمن القومي استخدمت ولوجها إلى أنظمة "سويفت" التابعة لشركة "إيستنيتس" بهدف تغيير فعلي للمعاملات أو سرقة الأموال.

في المقابل، قد يمكّن التتبع الخفي للمعاملات داخل تلك الشبكة وكالة الأمن القومي من اكتساب رؤية واضحة لتدفقات الأموال في المنطقة، بما في ذلك تلك المُوجّهة للجماعات الإرهابية، أو المتطرفة، أو المتمردة المحتملة. وفي حال ارتبط هدف الوكالة الفعلي بالتجسس على هذا النوع من التمويل، فذلك يعني أنها لم تنحرف عن مهمتها الأساسية.

التأكيد على خوض الوكالة لهذه العملية سيؤدي إلى انتكاسة على مستوى وكالة الأمن القومي والحكومة الأمريكية، خاصة وأن العديد من الأهداف المدرجة تُعدّ بمثابة دول صديقة للولايات المتحدة على غرار دبي وقطر

وعلى الرغم من ذلك، بيّن مات سويش أن التأكيد على خوض الوكالة لهذه العملية سيؤدي إلى انتكاسة على مستوى وكالة الأمن القومي والحكومة الأمريكية، خاصة وأن العديد من الأهداف المدرجة تُعدّ بمثابة دول صديقة للولايات المتحدة على غرار دبي وقطر. وأضاف سويش أن "عاصفة كبيرة تلوح في الأفق، كما أنه من المتوقع أن يثير ذلك الأمر غضب قيادات المنظمات الرئيسية الشديد على غرار البنوك والحكومات، وأنها لن تتوان عن إبداء ردّ الفعل".

وخلافا لشركة "إيستنيتس"، أشار مات سويش إلى المراجع في الملفات التي سلطت الضوء على استهداف "مجموعة بيزنس كومبيوتر" الواقعة في باناما، على الرغم من أنه ليس من الواضح ما إذا كانت الشركة قد تعرضت بالفعل للقرصنة. وبصرف النظر عن بيانها على موقع "تويتر"، لم تستجب شركة "إيستنيتس" لطلب موقع "وايرد" لإدلاء بأي تعليق. كما أن الموقع لم ينجح في الحصول على رد من طرف "مجموعة بزنس كومبيوتر"، ووكالة الأمن القومي".

نوافذ على العالم

فضلا عن نظام "سويفت"، تحتوي التسريبات أيضا على وفرة من الأدوات أو "البرامج الخبيثة" التي تستخدمها وكالة الأمن القومي للقرصنة، ويشمل ذلك ما كان يُعتبر سابقا تقنيات سرية لقرصنة أجهزة الكمبيوتر والخوادم التي تعمل بنظام التشغيل "ويندوز". وفي هذا الصدد، قام مؤسس شركة "هاكر هاوس" الأمنية، ماثيو هيكي، بتحليل مجموعة الأدوات حيث يعتقد أن هناك أكثر من 20 برنامجا خبيثا داخل التسريب، كما تم تضمين حوالي 15 منها داخل برمجة قرصنة آلية تُدعى "فوزبانش".

من جهة أخرى، يبدو أن الهجمات التي تستهدف أحدث إصدارات أنظمة "ويندوز" باستثناء "ويندوز 10"، تسمح للقراصنة باكتساب القدرة الكاملة لتشغيل التعليمات البرمجية الخاصة بهم على الجهاز المستهدف. وفي هذا السياق، أوضح ماثيو هيكي أن "التسريبات تحتوي على برامج خبيثة من المرجح أن تتيح لك في زمن قياسي اختراق أي عدد من الخوادم على شبكة الإنترنت، وبشكل كبير".

لمّح "وسطاء الظل" من خلال المعلومات المسربة إلى أنهم لم ينتهوا بعد من افتعال المشاكل لوكالة الأمن القومي. وفي هذا السياق، وجه هؤلاء القراصنة رسالة جاء فيها أننا "سنواصل عملياتنا حتى في

حال اندلاع حرب عالمية ثالثة"

وفي بيان وجّهه المتحدث باسم شركة "مايكروسوفت" لموقع "وايرد"، قال فيه إن "الشركة قد سبق لها تصحيح جميع نقاط الضعف في أنظمة "ويندوز" والتي تقوم أدوات القرصنة باستغلالها". وأضاف المتحدث الذي لم يتم الإفصاح عن هويته قائلا: "لقد تحققنا وأكدنا أن البرامج الخبيثة التي كشف عنها "وسطاء الظل" قد تم تناولها بالفعل من خلال التحديثات السابقة لمنتجاتنا المدعومة".

ومن خلال مدونتها، أوضحت الشركة أن العديد من البرامج الخبيثة لا تزال تعمل، ولكن فقط على إصدارات "ويندوز" التي تسبق "ويندوز 7". في المقابل، لمّح "وسطاء الظل" من خلال المعلومات المسربة إلى أنهم لم ينتهوا بعد من افتعال المشاكل لوكالة الأمن القومي. وفي هذا السياق، وجه هؤلاء القراصنة رسالة جاء فيها أننا "سنواصل عملياتنا حتى في حال اندلاع حرب عالمية ثالثة".

المصدر: وايرد

رابط المقال: https://www.noonpost.com/17591/