تفاصيل التحقيق بقرصنة بن سلمان لهاتف جيف بيزوس

كتبه كيم زاتر | 23 يناير ,2020

ترجمة وتحرير: نون بوست

تمكن موقع فايس الإخباري الأمريكي من الحصول على التقرير التقني الجنائي، الذي أعدته مؤسسة أف تي أي كونسلتينغ للاستشارات التي يقع مقرها في واشنطن العاصمة، حول كيفية ضلوع ولي العهد محمد بن سلمان في الاختراق المفترض لهاتف جيف بيزوس المدير التنفيذي لموقع أمازون.

هذا التقرير الذي يبحث في فرضية اختراق هاتف جيف بيزوس، يشير إلى أن محققي الفحص التقني عثروا على ملف مثير للريبة، ولكن لم يجدوا أي أدلة على وجود برمجية خبيثة في الجهاز. كما يشير تقرير المؤسسة إلى أن المحققين اضطروا لإعادة تعيين كلمة سر جديدة لحساب بيزوس في تطبيق آي تيونز لتنظيم وتشغيل الموسيقى والفيديو، لأنهم لم يعثروا عليها من أجل الدخول إلى خدمة الدعم في هاتفه. وهذه النقطة تشير إلى أن بيزوس على الأرجح نسي كلمة السر الخاصة به.

هذا التقرير الذي حصل عليه موقع فايس، جاء فيه أن المحققين قاموا بإنشاء مختبر رقمي آمن لفحص الهاتف والأكسسوارات التابعة له، وقد قضوا يومين في تفريغ الجهاز من محتوياته، ولكن لم يعثروا على أية برمجية خبيثة. وعوضا عن ذلك، وجدوا فقط ملف فيديو مثير للريبة، تم إرساله إلى بيزوس في 1 مايو/ آيار 2018، يبدو أنه فيلم ترويجي باللغة العربية حول مجال الاتصالات.

هذا الملف تظهر فيه صورة العلمين السعودي والسويدي، وقد وصل مصحوبا ببرمجية تنزيل مشفرة. ولأن هذه البرمجية كانت مشفرة فإن هذا أخر أو عطل فحص رموز التشفير التي وصلت مع الفيديو.

وقد اعتبر المحققون أن الفيديو أو برمجية التنزيل المرافقة له مثيران للاشتباه، لأن هاتف بيزوس بعد ذلك بدأ في إرسال كميات كبيرة من البيانات، حيث يقول التقرير: "خلال ساعات من تلقيه هذه البرمجية، بدأ هاتف جيف بيزوس في عملية إرسال للبيانات ضخمة وغير مصرح بها، وقد تصاعدت وتيرتها خلال الأشهر الموالية."

On May 1, 2018, Bezos received a text from the WhatsApp account used by MBS. This WhatsApp message contained a large video attachment that arrived unexpectedly and without explanation, meaning it was not discussed by the parties in advance of being sent.

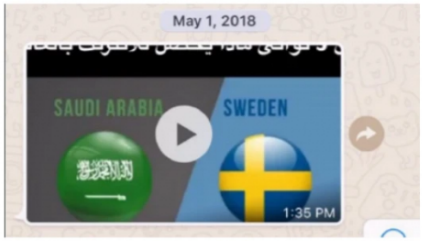

Figure 3: The text containing video file sent to Bezos from MBS account.

Source: Bezos' iPhone, WhatsApp application

"إن كمية البيانات التي يتم إرسالها من هاتف بيزوس تغيرت بشكل دراماتيكي بعد وصول ملف الفيديو عبر تطبيق واتساب، ولم يعد أبدا كما كان في السابق. وعلى إثر تفعيل ملف التنزيل المشفر المرسل من حساب محمد بن سلمان، ارتفع حجم البيانات الصادرة من الجهاز مباشرة بحوالي 29 ألف بالمائة."

وتظهر عمليات الفحص التقني أنه خلال الأشهر الستة قبل وصول الفيديو عبر الواتساب، كان هاتف بيزوس يرسل في المعدل 430 كيلو بايت من البيانات يوميا، وهو أمر طبيعي في أجهزة الآي فون. ولكن بعد ساعات من وصول مقطع الفيديو عبر واتساب، ارتفعت كمية هذه البيانات اليومية إلى 126 ميجا بايت. كما حافظ الجهاز على مستوى مرتفع من البيانات المرسلة، بمعدل 101 ميجا بايت يوميا خلال الأشهر الموالية، من بينها ارتفاعات ضخمة وغير طبيعية في كمية البيانات الصادرة.

وبالاعتماد على نتائج الفحص الرقمي، إلى جانب عملية تحقيق واسعة النطاق، واستجوابات وأبحاث ومعلومات استخباراتية، خلص المحققون إلى تقييم مفاده أن هاتف بيزوس تعرض للاختراق عبر أدوات اشتراها سعود القحطاني.

ويشار إلى أن سعود القحطاني هو صديق ومستشار مقرب من ولي العهد محمد بن سلمان. كما أنه كان رئيس ورئيس مجلس إدارة للاتحاد السعودي للأمن السيبراني والبرمجة والطائرات المسيرة، وقد كان معروفا بشرائه لبرمجيات هجومية للاختراق، نيابة عن النظام الحاكم السعودي، من بينها

أدوات من إنتاج الشركة الإيطالية هاكينغ تيم.

وقد نشرت صحيفة الغارديان البريطانية البعض من هذه النتائج التي توصل إليها المحققون، إلا أنها تعرضت للانتقاد من خبراء في أمن المعلومات، لأن تقريرها أشار إلى أن الأداة المستخدمة ربما تكون قد طورتها الشركة الإسرائيلية أن أس أو جروب، التي تقوم بصنع أدوات مهاجمة واختراق الهواتف. إلا أن تقرير الفحص التقني لا يشير إلى أن أدوات أس أن أو جروب تم استخدامها، بل يشير فقط إلى أن منتجات هذه الشركة لديها القدرة على القيام بعمليات اختراق مماثلة لتلك التي يبدو أن هاتف بيزوس تعرض لها.

> بسبب تقنية "التشفير بين الطرفيات" المستخدم في واتساب، فإنه من غير الممكن فك شفرات برمجية التنزيل من أجل تحديد ما إذا كانت تحتوي على رموز تشفير خبيثة مع الفيديو المرسل

ويقول التقرير: "فقط البرمجيات الخبيثة المتطورة، مثل بيغاسوس من شركة أن أس أو غروب، وغاليليو من شركة هاكينغ تيم، هي القادرة على الاندساس في البرمجيات العادية، واختراق الهاتف بطريقة تمكنها من التخفي والتمويه والتشويش على أنشطتها، وذلك بهدف اعتراض البيانات وسرقتها. ونجاح مثل هذه التقنيات هو على الأرجح أفضل تفسير للارتفاعات الغريبة في كمية البيانات المسحوبة من جهاز بيزوس."

وإلى جانب الكمية الكبيرة من البيانات التي قاموا باستخراجها من هاتف بيزوس أثناء الفحص، فإن المحققين أشاروا أيضا إلى الطبيعة الغريبة لاثنين من الرسائل النصية الموجهة إليه من حساب واتساب مرتبط بولي العهد السعودي. وأولى الرسالتين كانت بتاريخ 8 نوفمبر/ تشرين الثاني 2018، وهي تتضمن صورة امرأة تشبه لورين سانشيز، المرأة التي كان بيزوس متورطا معها في علاقة غرامية سرية في ذلك الوقت. وحين تلقي بيزوس لتلك الرسالة والصورة لم تكن أخبار هذه العلاقة قد افتضحت بعد.

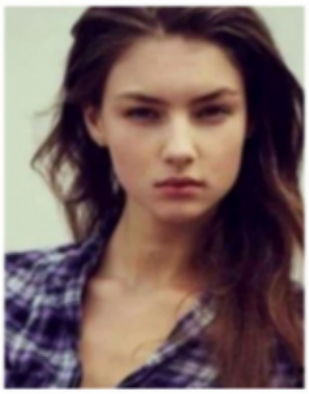

Figure 4: Photo sent to Bezos.
Source: Bezos' iPhone, WhatsApp application

Figure 5: Lauren Sanchez.
Source: The Mega Agency

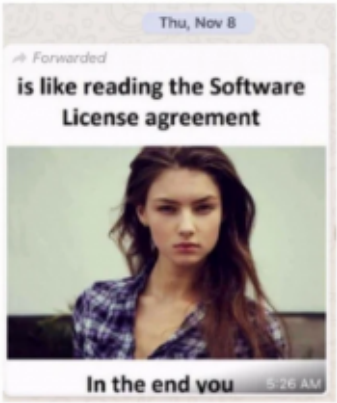

Figure 6: Text sent to Bezos from MBS account.
Source: Bezos' iPhone, WhatsApp application

أما الرسالة الثانية فهي بتاريخ 16 فبراير/ شباط، بعد أن حصل بيزوس على تقرير عبر هاتفه يحذره من وجود حملة عبر شبكة الإنترنت تشنها ضده جهات سعودية. وقد بدا أن رسالة الواتساب تشير إلى هذا الموضوع، وتدعو بيزوس إلى عدم تصديق كل ما يسمعه أو يقال له.

وقد واجه المحققون اثنين من الصعوبات على الأقل، أثناء عملية فحص واختبار جهاز الهاتف. وتعلقت الصعوبة الأولى ببرمجية التنزيل المشفرة. إذ أن الفريق فحص أولا الملف المرفق بمفرده، قبل أن يقرر أنه يحتاج إلى القيام بعملية فحص وتحليل تقني شامل لكل محتويات الجهاز والبيانات الواردة والمرسلة. واستخدموا بهذا الغرض أداة من شركة سيلبرايت، من أجل استخراج صور التحليل من الجهاز، وقاموا بإنشاء مختبر رقمي آمن ومؤقت للقيام بالفحوصات على مدى يومين. ورغم أنهم لم يعثروا على أي رموز تشفير خبيثة مرفقة مع ملف الفيديو، فإنهم اكتشفوا أن الفيديو تم إيصاله عبر برمجية تنزيل مشفرة تتم استضافتها في خوادم شركة واتساب.

وتوصل الباحثون إلى أنه بسبب تقنية "التشفير بين الطرفيات" المستخدم في واتساب، فإنه من غير الممكن فك شفرات برمجية التنزيل من أجل تحديد ما إذا كانت تحتوي على رموز تشفير خبيثة مع

الفيديو المرسل.

أما الصعوبة الثانية فهي تتعلق بكلمة السر لدعم تطبيق آي تيونز. إذ أنه خلال المحاولات الأولى لجمع صور تحليلة من جهاز الآي فون، توصلت شركة أف تي آي المشرفة على هذه العملية إلى أن الجهاز يحتوي على تشفير لحساب الآي تيونز، وأن التحليل الكامل للمحتويات يستوجب فك هذه الشفرة.

ويبدو أن هذا الفريق لم يتوصل أبدا إلى تحديد كلمة السر، لأن التقرير جاء فيه أنه في 20 مايو/ آيار 2019، قام الباحثون بتجربة بعض الخيارات من أجل تجاوز كلمة السر المستخدمة في دعم حساب آي تيونز، واضطروا في النهاية إلى إعادة تعيين كل الإعدادات في جهاز آي فون أكس، لارجاع إعدادات الجهاز إلى حالة المصنع، وبهذه الطريقة تم التخلص من كلمة السر مع الحفاظ على نظام الملفات وكل البيانات المتعلقة به. وقد حصلت مؤسسة آف تي آي على تصريح للقيام بعملية إرجاع إعدادات المصنع، ثم بعد ذلك شرعت في القيام بالفحص التقني.

المصدر: فايس

رابط المقال : https://www.noonpost.com/35687/