كيف يعمل برنامج التجسس الذي اشترته السعودية من إسرائيل؟

الاثنين 26 نوفمبر 2018 10:11 م

كشف تحقيق صحفي لصحيفة "هآرتس" العبرية في عددها الصادر الأحد أن مجموعة "أن أس أو" الإسرائيلية المتخصصة بتطوير برامج التجسس أبرمت صفحة مع مسؤولين سعوديين لبيعهم برنامج لاختراق الهواتف الخلوية يدعى "بيغاسوس 3" مقابل مبلغ 55 مليون دولار

كما قد تكون هناك صلة بين مقتل الصحفي السعودي جمال خاشقجي في قنصلية بلاده في إسطنبول الشهر الماضي واستخدام السعودية لبرناج بيغاسوس، وفقا لمسرب البيانات الشهير إدوارد سنودن الذي تساءل في اتصال فيديو مع صحفيين إسرائيليين من موسكو في وقت سابق هذا الشهر "كيف عرفوا ما كانت نواياه؟ وكيف قرروا أنه كان شخصا يحتاجون اتخاذ إجراء ضده وأنه يستحق المخاطرة؟".
فما هذا البرنامج؟ وما مدى خطورته؟

مجموعة أن أس أو
"أن أس أو" هي شركة إسرائيلية متخصصة في تطوير أدوات التجسس السيبراني، تأسست عام 2010 ويعمل فيها نحو 500 شخص وتقع قرب تل أبيب

وقد كانت الشركة محل جدل كبير في السنوات الأخيرة، حيث يقول مختبر سيتزن لاب الكندي لمراقبة الإنترنت، إن "بيغاسوس"، الذي تسوقه الشركة، تستخدمه دول تتميز "بسجلات مشبوهة في حقوق الإنسان وتواريخ من السلوك التعسفي لأجهزة أمن الدولة".

وبيغاسوس من برامج التجسس باهظة التكلفة، فوفقا لقائمة أسعار 2016 –بحسب موقع فاست كومباني- فإن شركة "أن أس أو" تطلب 650 ألف دولار من العملاء مقابل اختراق عشرة أجهزة إضافة إلى نصف مليون دولار رسوم تثبيت البرنامج

اكتشافه
ويعتبر بيغاسوس من أخطر برامج التجسس "وأكثرها تعقيدا" وهو يستهدف بشكل خاص الأجهزة الذكية التي تعمل بنظام التشغيل آي أو أس لشركة آبل، لكن توجد منه نسخة لأجهزة أندرويد تختلف بعض الشيء عن نسخة آي أو أس

وقد اكتشف باحثون هذا البرنامج أول مرة في أغسطس/آب 2016 بعد محاولة فاشلة لتنصيبه على هاتف آيفون لناشط في حقوق الإنسان في الإمارات العربية يدعى أحمد منصور، من خلال رابط مشبوه في رسالة نصية، حيث كشف التحقيق تفاصيل عن البرنامج وإمكانياته، والثغرات الأمنية التي يستغلها

الرابط المشبوه في الرسالة النصية التي جاءت إلى هاتف أحمد منصور ويؤدي النقر عليه إلى تثبيت فايروس بيغاسوس (سيتيزن لاب)

مدى خطورته
توضح شركة كاسبرسكي المتخصصة في برامج الحماية من الفيروسات أن بيغاسوس من نوع (modular malware) أي أنه مؤلف من وحدات حيث يقوم أولا بمسح الجهاز المستهدف، ثم يثبت الوحدة الضرورية لقراءة رسائل المستخدم وبريده الإلكتروني، والاستماع إلى المكالمات، والتقاط صور للشاشة، وتسجيل نقرات المفاتيح، وسحب سجل متصفح الإنترنت، وجهات الاتصال

كما أن بإمكانه الاستماع إلى ملفات الصوت المشفرة، وقراءة الرسائل المشفرة، بفضل قدراته في تسجيل نقرات المفاتيح وتسجيل الصوت، حيث يسرق الرسائل قبل تشفيرها، (والرسائل الواردة بعد فك تشفيرها).

ويقول الباحث في سيتزن لاب جون سكوت رايتون، إن بإمكان البرنامج فعل أي شيء يمكن للمستخدمين القيام به، بما في ذلك قراءة الرسائل النصية، وتشغيل الكاميرا والميكروفون، وإضافة وإزالة الملفات، ومعالجة البيانات.

كيف يعمل؟

تعتبر طريقة "التصيد" أكثر الوسائل شيوعا لإصابة الجهاز ببرنامج التجسس هذا، حيث يتم إرسال رسالة بريد إلكتروني إلى الضحية تضم رابطا مشبوها، وعند النقر عليه يتم تثبيت الفيروس في الجهاز.

وعندما اكتشف الفيروس أول مرة كان المستهدف هاتف آيفون يعمل بنسخة غير مكسورة من آي أو أس (non-jailbroken iOS) ولذلك وصفه الباحثون بأنه الهجوم الأكثر تعقيدا الذي شاهدوه.

ويعتمد البرنامج على ثلاث ثغرات لم تكن معروفة في نظام آي أو أس بدءا من الإصدار 7 وحتى الإصدار 9.3.4، تدعى "زيرو-داي" تتيح للفيروس اختراق نظام التشغيل بصمت وتثبيت برامج تجسس.

المستهدفون

لأن بيغاسوس من برامج التجسس الموجهة والمكلفة جدا فإن الجهات الفاعلة تستخدمه لمهاجمة أفراد "ذوي قيمة عالية" من الناشطين السياسيين أو غيرهم ممن بإمكانهم الوصول إلى معلومات مهمة وحساسة وسرية.

ولكن من المحتمل أيضا استخدامه للهجوم على أهداف محددة لأغراض متعددة، بما في ذلك التجسس على الشركات الكبرى، وكثيرا ما يكون الرؤساء التنفيذيون والمديرون الماليون والمسؤولون التنفيذيون والفرق المالية في مرمى الهجوم، لأنهم عادة يملكون وصولا إلى البيانات السرية، خاصة عبر أجهزتهم المحمولة.

آي أو أس وأندرويد

لا تختلف نسخة أندرويد –التي اكتشفت في 2017- كثيرا عن نسخة آي أو أس، لكنها لا تعتمد على ثغرات "زيرو-داي" لاختراق الجهاز وإنما تعتمد على أسلوب معروف جدا لكسر حماية الجهاز يدعى "فراماروت" (Framaroot).

كما يوجد اختلاف آخر هو أنه في حال فشل نسخة آي أو أس في كسر حماية الجهاز فإن الهجوم بأكمله يفشل، لكن في حالة نسخة أندرويد فإنه حتى لو فشل الفيروس في الوصول إلى جذر الهاتف لتثبيت برامج التجسس فإنه سيظل يحاول الطلب من المستخدم الحصول على الأذونات اللازمة لاستجلاب بعض البيانات على الأقل.

الحماية

في العادة عندما تصدر نسخة جديدة من برنامج بيغاسوس لنظام آي أو أس، فإن آبل تتحرك بسرعة لمواجهة ذلك، وقد أصدرت الشركة تحديثا أمنيا سد جميع الثغرات المذكورة. أما غوغل فتلجأ إلى طريقة أخرى وهي تنبيه المستهدفين بهذا الفيروس مباشرة.

فإذا كنت حدثت نظام التشغيل آي أو أس إلى آخر إصدار، ولم تتلق رسالة تحذير من غوغل، فعلى الأرجح أنك بأمان من بيغاسوس، وفقا لكاسبرسكي، وعليك دائما تحديث جهازك بآخر الرقع الأمنية وتثبيت حلول أمنية جيدة.

حجم الانتشار

على مدى العامين الماضيين مسح مختبر سيتيزن لاب الإنترنت بحثا عن خوادم مرتبطة ببيغاسوس، ووجد آثاره في 45 دولة من بينها 17 دولة عربية هي: الجزائر والبحرين ومصر والعراق والأردن والكويت ولبنان وليبيا والمغرب وعمان وفلسطين وقطر والسعودية وتونس والإمارات واليمن. إلى جانب دول مثل الولايات المتحدة والمملكة المتحدة وكندا وفرنسا وإسرائيل وتركيا.

ويقول المعهد في التقرير المنشور على موقعه في سبتمبر/أيول الماضي إنه حدد ما يبدو أنه توسع كبير في استخدام بيغاسوس في دول مجلس التعاون الخليجي. وأنه في الإجمال تم تحديد ستة مشغلين على الأقل بعمليات مهمة في دول مجلس التعاون الخليجي منها اثنتان يبدو أنهما تركزان في الغالب على دولة الإمارات العربية، وواحد يركز في الغالب على البحرين، وآخر يركز على السعودية.