

**البنك الفيدرالي لأتلانتس، محدود**

أبراج البنك الفيدرالي لأتلانتس

أتلانتس 123456

الهاتف: +1123.456.789

الفاكس: +1123.456.987

التاريخ: 2 أكتوبر 2017

أتلانتس

**قسم تكنولوجيا المعلومات**

**تصريح السيد "نيو ماتركس"**

أشتغل في البنك الفيدرالي لأتلانتس كرئيس قسم تكنولوجيا المعلومات.

في يوم 29 سبتمبر، بعد الظهر على ما أظن، أُخبرت أن شيئا ما لم يتم كما يجب بشأن تحويل مبلغ مالي من شركتنا إلى شركة "البنك المتحد للطباعة" (UBP). وتحديدا، يبدو أن شخصا تمكن من النفاذ إلى المراسلات المتبادلة بين الأشخاص المعنيين بهذه المعاملة.

بدأتُ على الفور بتحليل التسجيلات في الفترة ما بين 20 سبتمبر و1 أكتوبر، خاصة بالنسبة للأجهزة ذات عناوين بروتوكول الإنترنت التابعة ل"نيكوس نيكولاكيس"، "جورجس أتلانتس"، "يورغوس يورغوس" و"أرتميدا أولمبياكوس".

لكن ما بدا غريبا على الفور هو أن جميع حواسيبهم كانت متصلة بكمبيوتر خاص في قسم اللوجستيك والعمليات على نوافذ غير معتادة بالنسبة للتواصل المنتظم. بالإضافة إلى أن نوع البيانات التي تم تحويلها كان في صيغة غريبة لا نعرفها.

بعد فحص ذلك الجهاز المعين، أصبح الأمر أكثر غرابة، لأنه بعد كل تواصل بين تلك الحواسيب، كان خادوم البريد يسجل إرسال الرسائل القصيرة كمبيوتر "الحصاد" والكمبيوتر المرسل أو أجهزة الكمبيوتر المرسِلة، بما في ذلك كمبيوتر على منافذ وبروتوكولات تشبه إلى حد كبير خوادم SMTP المفتوحة.

عندما فحصنا بعمق الكمبيوتر المعني، وجدنا آثارًا لواجهة تحكم وسجلات برنامج التجسس مشابهة جدًا لبرمجية FlexiSpy أو Spytech. وتم تحديد كمبيوتر الحصاد الذي يستخدمه موظف جديد بقسم اللوجستيك والعمليات (DLO) يدعى "هرمس نوفاس".

قمنا باستخراج سجلات الحركة وخوادم البريد وبإجراء نسخة عن صندوق البريد الخاص بكمبيوتر "هرمس نوفاس". كما ختمنا جميع الحواسيب المذكورة أعلاه وحافظنا على البيانات في حاسوبنا المركزي بعد إخبار مجلس الإدارة الذي أذن لنا بذلك في انتظار تولي السلطات المعنية زمام الأمور.

رئيس قسم تكنولوجيا المعلومات

لدى البنك الفيدرالي لأتلانتس

"نيو ماتركس"