لمواجهة هجمات حجب الخدمة الموزعة بشكل أفضل

«نتسكاوت آربور»: المؤسسات ستلجأ لتوحيد عملياتها الشبكية والأمنية في 2019

الحلول الأمنية الإلكترونية ضرورة حتمية

■ توقعات بارتفاع وتيرة هجمات البوتنت التي تستهدف أجهزة إنترنت الأشياء خلال العام 2019

أوضح تقرير متخصص حديث من شركة «نتسكاوت آربور»، أنه خلال العام 2018، أصبحت تقنيات التخفيف من حدة هجمات حجب الخدمة الموزعة (DDoS) أكثر ذكاءً بفضل التطورات الحاصلة في الحلول الأمنية الإلكترونية الخاصة بهجمات حجب الخدمة الموزعة، وتقنيات ضمان الشبكات والتطبيقات. ومن المتوقع أن نشهد خلال العام 2019 حدوث أمر مشابه على مستوى المؤسسات، حيث ستقوم فرق عمليات الشبكات بمشاركة تصوراتها ورؤاها مع الفرق الأمنية. كما ستتعرف الفرق الأمنية على المزيد من الرؤى القيمة التي توفرها حالياً البنى التحتية للشركات. وستصبح بذلك أكثر ذكاءً من خلال دمج التصورات الحالية في عملياتها للتعامل مع التهديدات وتحييدها. وتشهد الهجمات الخبيثة التي تستهدف الشركات، ومزودي الخدمات، والبنية التحتية المحلية الحيوية ارتفاعاً كبيراً، فيما ستجبر المخاوف الناجمة عن هجمات حجب الخدمة الموزعة مسؤولي ومهندسي أمن المعلومات على التفكير في استراتيجيات وحلول جديدة لحماية البنية التحتية الرقمية الرئيسية. ويشمل ذلك القدرة على اكتشاف هجمات حجب الخدمة باكراً، قبل أن تلحق الضرر بالإنتاجية، وأداء الأعمال، والسمعة بشكل عام؛ فالهدف هو التمكن من تخفيف حدة الهجمات، ومنعها نهائياً.

تشكل الوقاية تحدياً لمسؤولي أمن المعلومات الأكثر خبرة، وذلك نظراً لبحث مجرمو الإنترنت الدائم عن سبل الالتفاف على أي شكل من أشكال الدفاع التي يواجهونها. ويسهم الانتقال السريع والمتنامي للشركات إلى السحابة الهجينة والبنية السحابية المتعددة في تفاقم المشكلة من خلال زيادة تعقيد شبكات تكنولوجيا المعلومات والبنية التحتية، وبالتالي توسيع سطح الهجوم وكشف نقاط ضعف جديدة. وإلى جانب ذلك، فإن الفرق الأمنية لديها ما يكفيها فعلياً، ولا ينقصها القلق بشأن اعتماد السحابة ودمج الخدمات والتطبيقات الجديدة. غير أن كل هذا سيتغير مع غياب الحدود التي تفصل بين العمليات الأمنية وعمليات الشبكات، مما سيسمح للفرق بالتعاون وتبادل المعلومات.

الرؤية المشتركة تقود إلى نجاح مشترك

لسنوات عديدة، تشاركت الفرق الشبكية والأمنية الكثير من القدرات. ويقع على عاتق كليهما مسؤولية مراقبة شبكات الشركات، وخدماتها، وتطبيقاتها، والبحث عن العيوب في النظام أو أي حالات غير اعتيادية قد تؤدي إلى فشله أو تعرضه لنشاط خبيث.

لذا، فإن التكامل ما بين مركز العمليات الشبكية ومركز العمليات الأمنية من شأنه أن يحقق فوائد ملموسة للشركات. إذ سيعمل كلا القسمين بالتوازي ويديران بنجاح شبكات الشركات وبرامجها ويدافعون عنها. وبذلك سيكون بمقدورهم التواصل والتنسيق بسلاسة، وهو ما من شأنه أن يزيد الكفاءة، ويحسن الموارد، ويخفض التكاليف.

إن جهود الضمان وأمن الحماية من هجمات حجب الخدمة الموزعة باتت تتضافر في نهاية المطاف لتزويد الفرق الشبكية والأمنية داخل الشركة بمنصة تحقق أعلى درجة ممكنة من الرؤية بشأن السوق اليوم. يعزز هذا المقترح البيانات والتحليلات الذكية التي ستوفر للفرق الأمنية والشبكية تصوراً شاملاً عما سيحدث داخل البنية التحتية لتكنولوجيا المعلومات في الزمن اللحظي، وهو ما سيمكنها من اتخاذ القرارات التي سيكون لها تأثير فوري.

الجرائم الإلكترونية

شهدنا خلال العام 2018 تضييق الحكومات والسلطات الغربية الخناق على مجرمي الإنترنت والجهات الفاعلة المشبوهة المدعومة من دول محددة. ومن المتوقع أن تزداد هذه الإجراءات ضد الجهات المشبوهة خلال العام 2019، وذلك مع اعتماد الدول الغربية على هذا التعاون لمحاربة الجرائم الإلكترونية. وتقود الحكومات الغربية الجهود جلب المجرمين الإلكترونيين للعدالة من خلال المبادرات السياسية التي ستقود إلى مزيد من الاتهامات، وربما المزيد من الاعتقالات على مدار الاثني عشر شهراً القادمة. وهو ما يشكل خطوة إيجابية من الحكومات الغربية التي لم تعد مستعدة للجلوس ومراقبة الجهات الفاعلة المشبوهة وهي تحاول القضاء على البنية التحتية المحلية الحيوية، والمؤسسات المالية، وكبرى الشركات.

وفي الأشهر القليلة الماضية، كشف البيت الأبيض عن استراتيجية جديدة للأمن الإلكتروني. ما من شأنه أن يدعم البنية التحتية المحلية ويوفر حماية أكبر للأفراد والمؤسسات، فضلاً عن تزويد الحكومات ووكالات تطبيق القانون بوسائل لمحاربة المجرمين الإلكترونيين والتعامل مع الهجمات المحتملة من الدول القومية. وفي المقابل، تشهد دولا غربية، تقودها الولايات المتحدة والمملكة المتحدة، تستدعي روسيا والصين على وجه الخصوص من أجل الأعمال العدوانية في القطاع الإلكتروني. وتشكل هذه الأعمال من جانب حكومات المملكة المتحدة والولايات المتحدة تطوراً على صعيد السياسة المحلية تجاه التهديد العالمي المتنامي للجرائم الإلكترونية.

تضامن الدول

سيستمر هذا التحول في عام 2019 حيث سنشهد تعاوناً دولياً أكبر بين الشرطة ووكالات تطبيق القانون من خلال جمع الموارد وتبادل المعلومات لتحييد التهديدات. غير أن السلطات لن تتمكن وحدها من معالجة الجرائم الإلكترونية. ولذلك سنشهد المزيد من التدخل والدعم من الشركات التي ستنضم للمحاربة والمساعدة للوصول إلى آلية دفاعية أكثر قوة ومرونة ضد الجهات المشبوهة.

ستقوم الحكومات الغربية خلال العام 2019 باستدعاء القطاع الخاص لمعالجة الجرائم الإلكترونية على نطاق محلي ودولي، ويتوقع البيت الأبيض على وجه الخصوص من الشركات التقنية الناشئة والقطاع الخاص العمل بنحو وثيق مع الوكالات الحكومية لتطوير تقنيات جديدة، مثل الذكاء الافتراضي والحوسبة الكمية، تتصدى للتهديدات الإلكترونية. وللنجاح في هذا المسعى، سيتعين على الحكومات والمجتمع التكنولوجي العمل بجدية لسد الفجوة بين هذين المجتمعين. لذلك من المتوقع أن يعرف خبراء أمن المعلومات، الذين يتم استدعاؤهم دورياً ليكونوا أول المستجيبين للمشاكل الأمنية على مستوى النظام، ما هو المطلوب منهم وكيف يمكنهم التعامل مع التهديدات الجديدة والحالية حال ظهورها.

وسنشهد أيضاً خلال العام 2019 زيادة في استخدام الوسائل الإلكترونية في الحرب للعلوماتية. وقد يشمل ذلك استخدام الرسائل الإلكترونية المخترقة لأغراض دعائية، كما في اختراقات «يوتوبي» و«دي إن سي»، فضلاً عن استخدام وسائل التواصل الاجتماعي لنشر المعلومات المضللة. كما نتوقع أن يزداد استخدام حملات حرب للعلومات ضد أهداف القطاع الخاص مع انتشار الأدوات والتقنيات. وهو ما قد يؤدي إلى تحمل الخبراء الإلكترونيين جزءاً من مسؤولية إحباط حملات التضليل، بالتوازي مع العلاقات العامة، فضلاً عن دورهم التقليدي في الأمن الإلكتروني.

لجوء المهاجمون لبيع خدماتهم

لقد ولت الأيام التي كان يقوم فيها بوت واحد بنوع بسيط من هجمات حجب الخدمة الموزعة. ففي المشهد الحالي لهجمات حجب الخدمة الموزعة، بات المهاجمون يضفون المزيد من التنويع على برامجهم، ما يسمح بتنوع كبير من الهجمات والبروتوكولات لاستهداف الشبكات. في موازاة ذلك، بات المتخصصون في هجمات حجب الخدمة الموزعة يوفرون خدمات إطلاق هجمات متعددة النواقل بأسلوب بتكلفة قليلة جداً، وبأسلوب أسهل بكثير. نعيش الآن عصر هجمات حجب الخدمة الموزعة الواسعة. وفي الوقت الذي نتوقع أن نرى فيه المزيد من التهديدات الكبيرة على مدار الأشهر الاثني عشر القادمة، إلا أننا نتوقع أيضاً حدوث المزيد من الهجمات متعددة النواقل نظراً لازدياد سهولة الوصول إليها، وبوتيرة مخيفة. ويعد الهجوم الذي استهدف خوادم الذاكرة المخبأة (memcached servers) هو الهجوم الأكبر الذي سجل لغاية الآن، وقد توفر النطاق الخاص بهذا الهجوم لدى متخصصي خدمات هجمات حجب الخدمة الموزعة في غضون أيام من ظهوره. وشكل هذا الهجوم أحد نطاقات الهجوم المتعددة المتوفرة للشراء في أسواق الإنترنت الخفية.

ونتوقع في العام 2019 بروز المزيد من المهاجمين الذين يقدمون خدماتهم لمن يدفع أكثر. وتستهدف هذه الشخصيات الشريرة الأهداف عند الطلب ويأجور زهيدة. كما يمكن أن يقوموا بتسليم الأدوات الخاصة بهجمات حجب الخدمة الموزعة إلى عملائهم لتمكينهم من القيام بعملهم القذر. وعلى الرغم من هذه الأدوات ليست غريبة عن المشهد، إلا أن سهولة الوصول إليها، والتضمين السريع لأنواع جديدة، وتوفر مجموعة أوسع من العملاء الدوليين، باتت تساعد في حصول الكثير من مجرمي الإنترنت الهواة على البرمجيات الخبيثة المدمرة. ويستخدم العديد من متخصصي هجمات حجب الخدمة الموزعة ممارسات الأعمال ونماذج البرمجيات المتاحة كخدمات لتسويق وبيع الاشتراكات الشهرية، وفرض رسوم تقل عن 50 دولار للعملاء الراغبين بالحصول على هذه الامتيازات. ويمكن القيام بعمليات الشراء باستخدام العملات الرقمية، كما يمكن القيام بها عبر مواقع شرعية لتحويل الأموال مثل باي بال ما يسمح لهم بجمع الأموال وتمويل الأنشطة المستقبلية.

اليقظة هي العامل الأهم

مع استمرار المتخصصين من مزودي خدمات هجمات حجب الخدمة الموزعة في كسب المال مقابل انشطتهم غير المشروعة، نعتقد أن يكون هؤلاء المهاجمين سيكونوا أكثر اصراراً وابتكاراً، وحرصاً على تطوير البرمجيات الخبيثة وآليات الهجوم، مع استمرارهم في الوقت ذاته في استغلال نقاط الضعف المعروفة. وشبكات البوتنت الموجودة، وتقنيات الهجوم المفهومة جيداً بالنسبة لهم. وفي تطور وثيق، بتنا نرى ظهور ما يعرف بـ «حشو بيانات الاعتماد»، وهي العملية تقوم فيها شبكات البوتنت بالعديد من محاولات تسجيل الدخول الاحتيالية في تأثير مماثل لهجمات حجب الخدمة الموزعة. وتقوم مجموعة فرعية من فئات الهجوم القوي، وعمليات «حشو بيانات الاعتماد» بإدخال أعداداً كبيرة تلقائية من بيانات الاعتماد إلى مواقع الويب إلى أن تتم مطابقتها بشكل محتمل مع أحد الحسابات الحالية، الأمر الذي يمكن المهاجم باختطاف الحساب أو الهدف لأغراضه الخاصة. وإذا وضعنا التوقعات جانباً، فإن الدرس المهم الذي تعلمناه في سنواتنا العديدة التي قضيناها في تحليل مشهد التهديد هو أنه بمجرد ظهور نوع جديد من هجمات حجب الخدمة الموزعة، فإنه سيتواصل ولن يختفي. ومع ازدياد التطور والتعقيد في أدوات المهاجمين وبروز فئات جديدة للهجمات، باتت الجهات القائمة على هذه الهجمات تجد الأمر أكثر سهولة وأقل تكلفة لإطلاق هجمات أكبر وأكثر فاعلية. ويتطلب هذا الأمر وضعاً دفاعياً هجينياً أو متعدد الطبقات للحماية من هجمات حجب الخدمة الموزعة، يجمع بين القدرات والآليات الدفاعية المادية وقدرات حماية البيانات على السحابة للتعامل مع الهجمات المتطورة من حيث الكم والنوع.

ارتفاع وتيرة هجمات البوتنت

مع التوقعات بارتفاع وتيرة تبني تقنيات إنترنت الأشياء خلال العام المقبل، فإن ذلك سيخلق عاصفة مثالية للجرائم الإلكترونية، والتسبب في عواقب وخيمة على الشركات والمستهلكين. ونظراً لنشر العديد من أجهزة إنترنت الأشياء هذه عبر القطاعات الصناعية لتشغيل المصانع الذكية وخطوط الإنتاج وشبكات النقل، فإن المخاطر المرتبطة بتأمينها ستصبح واضحة وضرورية، وهذا بغض النظر عن حقيقة تواصل انتشار تقنيات إنترنت الأشياء ضمن قطاعات حيوية وهامة جداً مثل الرعاية الصحية لدعم الإجراءات الطبية ومراقبة جودة حياة المرضى. لا تزال تقنيات إنترنت الأشياء في بداياتها نسبياً، وتمثل أرضاً خصبة لمجرمي الإنترنت في سعيهم لاستغلال الثغرات ونقاط الضعف الجديدة. وبالتالي، سيؤدي انتشار الأجهزة المتصلة بالإنترنت إلى فتح المجال أمام سلالات جديدة من الثغرات والبرامج الخبيثة التي تهدف إلى تعطيل تجهيزات إنترنت الأشياء عبر الصناعات المختلفة، والمؤسسات، وقطاع الشركات الصغيرة والمتوسطة، والمنازل الذكية. وستتفاقم حالة الأمن الإلكتروني أكثر، نظراً لتجاهل مصنعي تقنيات وأجهزة إنترنت الأشياء للبروتوكولات الأمنية في أغلب الأحيان عند تصميم هذه الأجهزة، في محاولة منها للحد من تكاليف الإنتاج. ونتيجة لذلك، يتم شحن كميات كبيرة من الأجهزة دون تخزين ميزات الأمان الأساسية في تصميمها، مما يجعلها عرضة للتهديدات.

وضع معايير أمنية جديدة

من غير المفاجئ أن يتم استهداف هذه الأجهزة بواسطة مطوري البرامج الخبيثة. في عام 2018، كان هناك ارتفاع كبير في هجمات حجب الخدمة الموزعة مدفوعة بشبكات البوتنت الخاصة بأجهزة إنترنت الأشياء، وقد شهدنا بالفعل نمواً هائلاً في عدد وحجم شبكات البوتنت التي تستهدف أجهزة إنترنت الأشياء، ونتوقع أن نشهد المزيد من الهجمات المعقدة خلال العام 2019. وكان استخدام برمجيات «ميراي» الخبيثة أمراً شائعاً لدى العديد من المجرمين من مطوري شبكات البوتنت الخاصة بإنترنت الأشياء، الذين يستخدمون الشيفرة المصدرية كإطار لتطوير برمجيات خبيثة جديدة. كذلك، وسع هؤلاء المطورين من قاعدة الشيفرة المصدرية لبرمجيات ميراي الخبيثة لتعزيزها بإمكانيات ووظائف جديدة، وقد تم اعتماد أشكال أخرى متعددة لهذه البرمجيات، وتحديداً كل من OMG، وJENX، وSatori، وتروجان إنترنت الأشياء لاستخدامها في شن هجمات حجب الخدمة الموزعة على نطاق عالمي. وقد أظهرت أبحاثنا كيف يمكن استخدام مثل هذه الأجهزة كنقاط دخول للهجمات ولتوجيه هجمات حجب الخدمة الموزعة ضد الأصول الداخلية.

ومع شيوع وازدياد استخدام تقنيات إنترنت الأشياء خلال العام 2019، سيصبح مجرمو الإنترنت أكثر انتقائية، ونتوقع أن تستهدف هجمات بشبكات البوتنت تجهيزات إنترنت الأشياء محددة، والمزودين والمطورين لهذه التجهيزات، الأمر الذي قد يؤدي إلى عواقب وخيمة. سوف تتشجع الجهات الفاعلة في مجال التهديد من خلال القدرة على استغلال نقاط الضعف في إنترنت الأشياء واستهداف أجهزة وعمليات محددة. هذه هي فقط أحدث الاتجاهات في المشهد المتغير باستمرار، حيث يقوم المهاجمون الأذكياء بموائمة وتكييف حلولهم وتسخير أدوات جديدة لتفادي دفاعات الأمن الإلكتروني الحالية، ويتعين على الشركات والمستهلكين اليقظة والتجاوب باستمرار من أجل التصدي للهجمات الخبيثة، واعتماد أفضل الممارسات الصناعية الجديدة.

«نيكون» تطرح سلسلة كاميرات «Z» في سوق الكويت

كشفت شركة نيكون الرائدة في مجال تكنولوجيا التصوير ومعدات الكاميرات النقاب عن السلسلة «Z» ذات الإطار الكامل عديمة المرآة التي ينتظرها الجميع بفارغ الصبر كونها الأولى من نوعها، حيث أطلقت حتى الآن اثنين من الكاميرات الرائعة، Z6 وZ7، ونظراً لكونها مطورة إلى درجة مثالية لالتقاط صور حادة مدهشة بوضوح رائع، فإن كاميرات نيكون Z6 و Z7 ذات التشغيل الصامت تماماً، هي متعة مطلقة للمصورين، كما شهدت سلسلة نيكون «Z»، التي تم الكشف عنها بكثير من الإثارة في النادي العلمي الكويتي، ضجة واحتفالا كبيرين احتفاء بارقى أنماط هندسة تصوير الفيديو للمناظر الطبيعية. وعلقت ناريندرا ميثون، العضو المنتدب لشركة نيكون الشرق الأوسط ش. م. ح. قائلة «لقد تم تصميم السلسلة «Z» لتجمع بين الإبداع والابتكار وسهولة التشغيل لتمنح المصورين الفوتوغرافيين ومصوري الفيديو تجربة رائعة، فنحن نريد صنع أجهزة تعمل جنباً إلى جنب مع مصوري الفيديو والمصورين الفوتوغرافيين لتكون حليفاتهم يقوم بنفس عملهم وهذا ما ندور حوله سلسلة «Z» الجديدة، وقدتم صنع السلسلة «Z» لتمنح جميع صناع المحتوى تجربة رائعة لأفضل ما تقدمه شركة نيكون في مجال التصوير وتكنولوجيا الكاميرات، كما سيحظى مشترو السلسلة «Z» بميزة إضافية مع برنامج نيكون للأعضاء المتميزين (البرنامج)، حيث سيتم مكافأتهم بفرصة استكشاف المخرجات البصرية المتازة التي تتيحها السلسلة «Z» بالكامل من خلال تجربة عملية لا مثيل لها.

وأضافت ناريندرا «من خلال هذا البرنامج، سيتمكن مقتنو كاميرات السلسلة «Z» من استكشاف أرقى تكنولوجيا تقدمها تحت إشراف المصورين الفوتوغرافيين المدربين التابعين لنيكون خلال جولات التصوير الفوتوغرافي المصممة خصيصاً التي سنأخذهم فيها».

عند الإطلاق، ذكر ماجد سلطان، مصور فوتوغرافي للطبيعة والحياة البرية، «تتميز Z7 بالجمع بين القبضة المحكمة والتصميم الكلاسيكي لنيكون مع تصميمها المضغوط وخفة وزنها، وهذا ما كنت أنتظره بالضبط، وفي حين أن جودة الصورة تنافس مثيلتها في الكاميرات الرقمية ذات العدسات الأحادية العاكسة التي أمتلكها، فإن العدسات «إس» الجديدة توفر ميزة مذهلة لجودة الصورة ووضوحها، وبالنسبة لجميع رحلاتي لتصوير المناظر الطبيعية أو الأماكن التي يكون فيها لعامل الحيز والوزن الأولوية، فبالتأكيد ستكون كاميرا Z7 في حقيبة الكاميرا الخاصة بي.»

وقال كريج كوليسكاي، مصور فوتوغرافي تابع لريد بول وسفير شركة نيكون، «تعد الإضافات الجديدة إلى تشكيلة نيكون المثيرة للإعجاب دليلاً حقيقياً على التزام الشركة تجاه المصورين الفوتوغرافيين وسعيها وراء التكنولوجيا المبتكرة ذات الصلة، وبصفتي مصور فيديو ومصور فوتوغرافي رياضي، يتحتم عليّ اقتناء كاميرا متعددة الاستخدامات وخفيفة الوزن وسهلة الحمل ومعمرة وسريعة وتدعمها الجودة، وتجمع هذه المجموعة بين جميع تلك المزايا، فماذا أريد أكثر من ذلك.»

نظرة عامة على السلسلة «Z»:

نيكون Z7

تعد الكاميرا الأولى من نوعها ذات الحساس ذو الإطار الكامل عديمة المرآة عالية الدقة 45.7 ميجابيكسل هي أحدث التقنيات، فهي تتمتع بنقطة تركيز 493 تغطي 90 بالمائة من الصورة التي تراها، كما تستفيد هذه الكاميرا من محرك معالجة الصورة الجديد EXPEED 6 للحصول على صور أكثر وضوحاً، فضلاً عن التصوير المستمر حتى 9 إطارات في الثانية في وضع اللقطات المتلاحقة. تشغيل صامت تماماً.

نيكون Z6

«Ooredoo» و«AeroMobile» شريكان في خدمة التجوال الدولي بالرحلات الجوية

الأولى من نوعها في الكويت


مجبل الأيوب

أعلنت Ooredoo الكويت عن شراكتها مع AeroMobile، وهي مزود خدمات الشبكة المعتمد عالمياً في قطاع الطيران. يتيح نظام AeroMobile للركاب خيار استخدام أجهزتهم الهاتفية المحمولة بأمان تام خلال رحلات لعمل وإجراء المكالمات وارسال الرسائل النصية خلال الرحلات الجوية، ويجري احتساب أجور المكالمات حسب تعرفة التجوال الدولية. تتوفر خدمة AeroMobile للتجوال الدولي في الرحلات الجوية من ضمن باقات التجوال Ooredoo Passport.

تتيح باقات التجوال Ooredoo Passport امكانية العميل الإختيار من باقة Ooredoo Passport الأسبوعية والتي تشمل 100 دقيقة و1GB من الإنترنت مقابل 10 د.ك. اسبوعيا و Ooredoo Passport الأسبوعية والتي تشمل انترنت غير محدود مقابل 12 د.ك. أسبوعيا وOoredoo Passport الشهرية والتي تشمل انترنت غير محدود مقابل 39د.ك. شهريا مواكبة لزيادة استخدام العملاء لشبكات التواصل الاجتماعي لمشاركة أجمل اللقطات المرئية والمسموعة مع أحبائهم عبر الإنترنت، وذلك من خلال سناب شات أو إنستغرام. سيتمكن عملاء Ooredoo الآن من الإستفادة من الإنترنت غير المحدود في رحلات الطيران لتصفح الإنترنت والإستمتاع بقنوات التواصل الإجتماعي. تتوفر خدمة AeroMobile للتجوال الدولي في أكثر من 22 شركة طيران في جميع أنحاء العالم بما في ذلك الخطوط الجوية الكويتية وLufthansa والخطوط الجوية التركية وVirgin Atlantic وCathay Pacific.

وتعليقاً على هذه الشراكة، قال مدير أول إدارة الاتصال المؤسسي في Ooredoo الكويت مجبل الأيوب «هذه الشراكة المبتكرة مع AeroMobile هي الأول من نوعها في الكويت والتي نقدم لعملائنا امكانية التواصل مع محبيهم وهم على متن الطائرة من ضمن باقات التجوال Ooredoo Passport». ومن ناحيته، قال كيفن روجرز الرئيس التنفيذي لشركة AeroMobile «نحن متحمسون للغاية على هذه الإتفاقية مع شركة Ooredoo الرائدة في الشرق الأوسط وأهمية توفير خدمة الإتصالات والإنترنت على متن الطائرات».