الخليج

اقتصاد, تقنية وسيارات

22 مارس 2023 23:50 مساء

توجهات لعمليات الابتزاز الإلكتروني حول العالم 6

«دبي: «الخليج

رصدت شركة بالو ألتو نتوركس، أبرز التوجهات التي تشهدها عملية الابتزاز الإلكتروني عبر الإنترنت؛ وذلك اعتماداً على تقرير الاستجابة للحوادث الأمنية إلى جانب تقييم مشهد التهديدات الواسع من قبل خبراء ومحللي الشركة.

وتتجه جماعات الجريمة الإلكترونية بشكل متزايد نحو توظيف أساليب متنوعة في الابتزاز من أجل ممارسة الضغوط على المؤسسات المستهدفة وتحقيق مآربها. وفي حين توجهت الأضواء في السنوات الأخيرة على هجمات برمجيات الفدية إلا أن جماعات الجريمة الإلكترونية الحديثة أصبحت تتبع أساليب إضافية في الابتزاز من أجل إخضاع المؤسسات المستهدفة وإجبارها على الدفع، وقد تذهب أحياناً إلى الاستغناء عن برمجيات الفدية بالمجمل والاستعاضة عنها بممارسة الابتزاز بحد ذاته.

وتحتاج المؤسسات بدورها إلى تطوير دفاعاتها من أجل مواجهة الأساليب المتنوعة التي تسلكها جماعات الجريمة

الإلكترونية لممارسة الضغوط؛ لذلك يجب ألا تكون خطط الاستجابة للحوادث محصورة بالاعتبارات التقنية فحسب؛ بل يجب أن تشمل تدابير وقائية تحمي سمعة المؤسسات إلى جانب اعتبارات تهتم بكيفية حماية الموظفين أو العملاء الذين قد يتعرضون للاستهداف بأساليب ابتزاز أكثر شراسة من جانب تلك الجماعات.

وتمثلت أبرز توجهات الابتزاز الإلكتروني في:

1. استخدام تكتيكات الابتزاز المتعدد بوتيرة متزايدة؛ حيث لوحظ لدى مراجعة هجمات برمجيات الفدية التي رصدتها شركة بالو ألتو نتوركس اعتباراً من أواخر 2022، قيام جماعات الجريمة الإلكترونية بشن عمليات لسرقة البيانات في نحو 70 في المئة من الحالات بالمتوسط. ومقارنة مع منتصف 2021، نلاحظ أن عمليات سرقة البيانات قد وقعت فقط في نحو 40 في المئة من الحالات بالمتوسط.

وفي الأغلب تهدد الجماعات بتسريب البيانات المسروقة على مواقع التسريب في شبكة الويب المظلمة والتي أصبحت أحد المكونات الرئيسية التي ترفد جهودها بشكل متزايد لابتزاز المؤسسات. والتحرش بدوره أسلوب آخر في الابتزاز، نراه يستخدم في المزيد من حالات الهجمات ببرمجيات طلب الفدية. وأصبحت جماعات الجريمة الإلكترونية تستهدف أفراداً بعينهم، في الأغلب من موظفي الإدارة التنفيذية العليا، عن طريق إطلاق تهديدات، وإجراء اتصالات غير مرغوب فيها. وبحلول نهاية 2022، كان التحرش من أحد العوامل الداخلية في نحو 20 في المئة من حالات الهجمات ببرمجيات الفدية. ومقارنة مع منتصف 2021، نرى بأن التحرش كان أحد العوامل الداخلية في أقل من 1 في المئة من هجمات برمجيات الفدية التي رصدتها شركة بالو ألتو نتوركس.

2. عصابات الابتزاز تتسم بالانتهازية إلا أن هناك أنماطاً تتعقبها في المؤسسات المستهدفة. استناداً إلى تحليلنا لمواقع التسريب في شبكة الويب المظلمة، كان قطاع التصنيع أحد أكثر القطاعات المستهدفة خلال 2022؛ حيث تم التشهير علناً بـ 447 مؤسسة صناعية مخترقة على مواقع التسريب تلك. وتعتقد شركة بالو ألتو نتوركس أن ذلك يعزى إلى انتشار أنظمة برمجية متقادمة في القطاع الصناعي، لا يتم تحديثها أو تصحيحها بشكل سهل أو منتظم، ناهيك عن مسألة التراخي السائدة في هذا القطاع بشأن فترات التعطل عن العمل. وكانت المؤسسات الصناعية الواقعة في الولايات المتحدة الأكثر تضرراً وفقاً لبيانات مواقع التسريب؛ حيث شكلت 42 في المئة من التسريبات التي تم رصدها في 2022.

3. الشركات متعددة الجنسيات تعد أهدافاً مربحة جداً لجماعات الجريمة الإلكترونية؛ حيث تشكل الهجمات ضد أكبر الشركات في العالم نسبة ضئيلة، لكنها ملحوظة من حوادث الابتزاز العلني. في 2022، خضعت 30 شركة مدرجة على قائمة فوربس لأكبر 2000 شركة عالمية بشكل علني لمحاولات ابتزاز. ومنذ 2019، تعرض ما لا يقل عن 96 من هذه الشركات إلى تسريب ملفاتها السرية وكشفها بدرجة معينة كجزء من محاولات الابتزاز التي تعرضت لها.

4. الجماعات المتطورة قد تستخدم الابتزاز وبرمجيات الفدية من أجل تمويل أنشطة أخرى ـ أو لإخفائها. لوحظ أن الجماعات في الدول الخاضعة لحظر أو عقوبات اقتصادية تقوم باستخدام برمجيات الفدية والابتزاز من أجل تمويل عملياتها. ويظهر أن جماعات أخرى، بما فيها بعض المجموعات من إيران أو الصين، تسعى إلى تحقيق أهداف مغايرة من وراء استخدامها لبرمجيات الفدية؛ حيث يمكن لجماعات التهديدات الإلكترونية أن تحقق مكاسب أكبر من المال عند نشر برمجيات الفدية، وتحديداً اكتساب قدرات محتملة على التدمير والتجسس.

:هناك مجموعة من التحركات من جانب جماعات الابتزاز التي قد نشهدها العام المقبل، وهي .5

.سيشهد عام 2023 أكبر عمليات اختراق في البيئات السحابية باستخدام برمجيات الفدية ·

.تصاعد عمليات الابتزاز المرتبطة بتهديدات ناشئة من داخل المؤسسات ·

.تصاعد محاولات الابتزاز المدفوعة بأهداف سياسية ·

استخدام برمجيات الفدية والابتزاز لصرف الانتباه عن الهجمات التي ترمي إلى إصابة سلاسل التوريد أو التعليمات · .المصدرية للبرمجيات