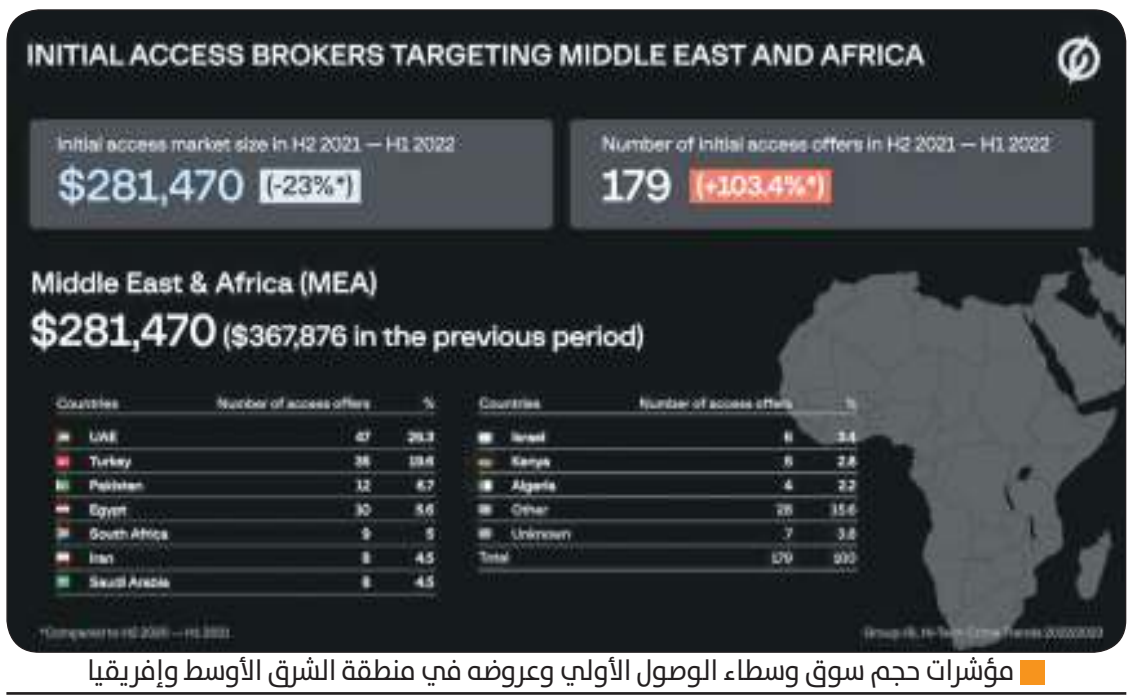
العدد الفعلي أعلى بكثير نظراً لاختيار العديد من الضحايا القبول بالمساومة

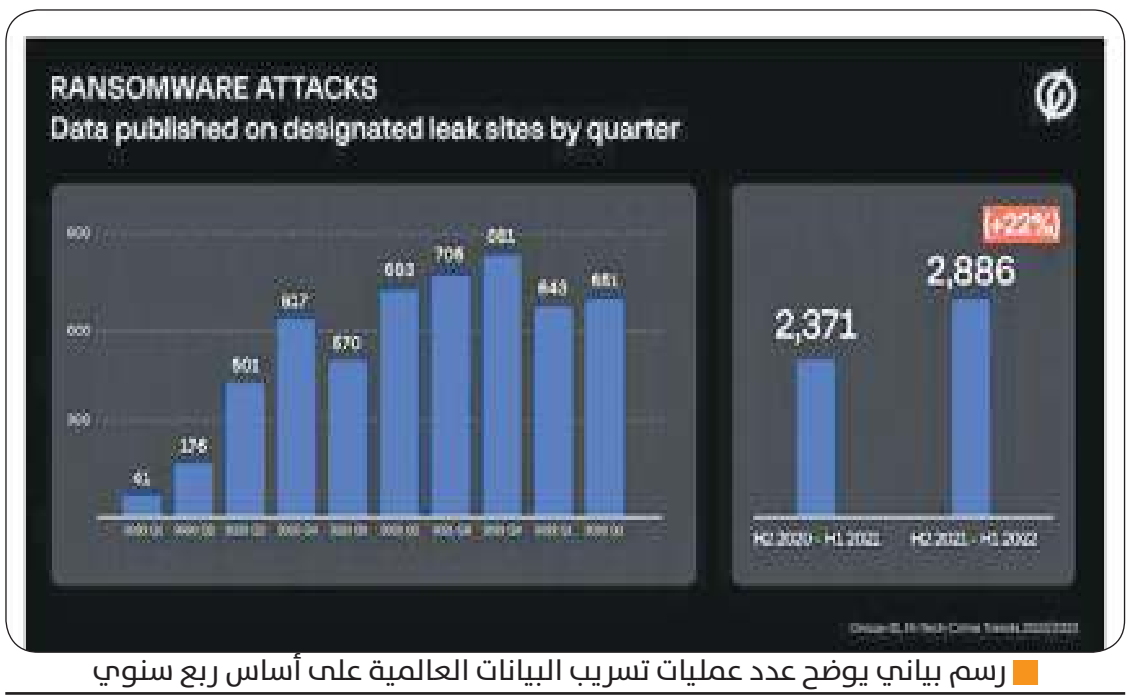
"جروب-آي بي": 21 في المئة من هجمات برامج الفدية موجعة لشركات الكويت

فولكوف: عدد الضحايا عالميا خلال الفترة بين النصف الثاني 2020 والنصف الأول من 2021 ارتفع 935 في المئة

منطقة الشرق الأوسط وإفريقيا ثاني أقل المناطق تأثرا بتسريبات البيانات والدولة الأكثر تضررا هي الكيان الصهيوني



مؤشرات حجم سوق وسطاء الوصول الأولي وعروضه في منطقة الشرق الأوسط وإفريقيا



رسم بياني يوضح عدد عمليات تسريب البيانات العالمية على أساس ربع سنوي

العديد من عصابات الفدية البارزة تحولت إلى شركات إجرامية ناشئة تمتلك تسلسلا هرميا قويا

نشرت «جروب-آي بي»، الشركة الرائدة عالمياً في مجال الأمن السيبراني والمتخصصة في التحقيق بالجرائم الإلكترونية والوقاية منها، تقريرها الجديد اتجاهات الجرائم ذات التقنية العالية للعام 2022 / 2023، والذي يعد الإصدار الأحدث من تقرير الشركة السنوي حول التهديدات السيبرانية العالمية. وكشف محللو وخبراء استقصاء التهديدات لدى «جروب-آي بي» في التقرير كيف أن برامج الفدية لا تزال تمثل التهديد السيبراني الأكبر للشركات والمؤسسات في جميع أنحاء العالم بين النصف الثاني من عام 2021 والنصف الأول من عام 2022، لا سيما في الشرق الأوسط وأفريقيا. وفقا للدراسة التي أجرتها «جروب-آي بي»، فقد ارتفع عدد الشركات التي تم تحميل معلوماتها الخاصة بها على المواقع الإلكترونية المتخصصة بتسريب البيانات بين النصف الثاني من عام 2021 والنصف الأول من عام 2022 بنسبة سنوية بلغت 22 % ليبلغ عددها 2886 شركة، وهو ما يعادل تسريب بيانات 8 شركات على الإنترنت يوميا. وعلى صعيد منطقة الشرق الأوسط وأفريقيا، فقد تم تسريب معلومات 150 شركة على مواقع تسريب البيانات خلال الفترة المشمولة بالتقرير.

في منطقة دول مجلس التعاون الخليجي على وجه الخصوص 42 من الشركات نشرت بياناتها أو ملفاتها أو معلوماتها حول DLS بعد هجمات برامج الفدية. من بينها، شهدت منظمات في الإمارات العربية المتحدة (33٪) والمملكة العربية السعودية (29٪) غالبية الهجمات، تليها دول الخليج الأخرى: الكويت (21٪) وقطر (10٪) وعمان (5٪) والبحرين (2٪). من ناحية الصناعات، كانت قطاعات الطاقة والاتصالات وتكنولوجيا المعلومات والتصنيع مستهدفة بشكل متكرر.

وللسنة الثانية على التوالي، لاحظ خبراء «جروب-آي بي» التأثير المتزايد لوسطاء الوصول الأولي (IAB) على سوق برامج الفدية في منطقة الشرق الأوسط وأفريقيا وخارجها. واكتشف الباحثون لدى الشركة ما يصل إلى 2348 حالة من حالات الوصول إلى بيانات الشركات التي يتم بيعها في منتديات على شبكة الإنترنت المظلمة أو بشكل خاص من قبل وسطاء الوصول الأولي، وهو ضعف ما تم تسجيله خلال الفترة السابقة. كما ارتفع عدد الوسطاء من 262 إلى 380 وسيط، الأمر الذي أدى إلى انخفاض الأسعار وسهل من استخدام عصابات برامج الفدية والجهات الفاعلة الخبيثة لشن الهجمات. وعلى مستوى منطقة الشرق الأوسط وأفريقيا، فقد تضاعف عدد عروض الوصول إلى الشبكة لتصل إلى 179 عرضاً خلال الفترة ما بين النصف الثاني من عام 2021 والنصف الأول من عام 2022، مما أدى إلى انخفاض في إجمالي سعر العروض بنسبة 23 %.

وللسنة الحادية عشرة على التوالي، يقوم تقرير "اتجاهات الجرائم ذات التقنية العالية" بتحليل الجوانب المختلفة لعمليات صناعة الجريمة الإلكترونية، ويفحص الهجمات، ويقدم التوقعات الخاصة بمشهد التهديدات لقطاعات رئيسية مختلفة مثل القطاع المالية، وقطاع الاتصالات السلكية واللاسلكية، وقطاع التصنيع وقطاع الطاقة. وتقدر «جروب-آي بي» سنوياً نظرة عامة شاملة لمشهد التهديدات العالمية، ويشارك باحثو وخبراء الشركة توقعاتهم لما ينتظرنا في المستقبل. وتلعب الخبرة العملية التي تتمتع بها «جروب-آي بي» في التحقيق في الجرائم الإلكترونية، إلى جانب مجموعتها المبتكرة من المنتجات والخدمات دوراً هاماً في وصف جميع الاتجاهات والأنشطة السرية التي تستحق المتابعة، وتوفير توقعات طويلة الأجل تساعد مسؤولي الأمن السيبراني في جميع أنحاء العالم على تخصيص أساليب الحماية الإلكترونية لديها للتصدي للهجمات المختلفة.

ارتفاع وتيرة هجمات برامج الفدية

على الصعيد العالمي، تم نشر معلومات وملفات وبيانات تخص 2886 شركة على مواقع تسريب البيانات خلال الفترة ما بين النصف الثاني من عام 2021 والنصف الأول من عام 2022، بارتفاع بلغ 22 % مقارنة مع 2371 شركة تأثرت خلال الفترة السابقة (النصف الثاني من 2020 حتى النصف الأول من عام 2021). وكما هو الحال مع العام السابق، بلغ عدد تسريبات البيانات المتعلقة ببرامج الفدية ذروته خلال الربع الأخير من عام 2021، حيث تمت مشاركة بيانات 881 شركة على مواقع تسريب البيانات. ويُعتقد أن العدد الفعلي لهجمات برامج الفدية أعلى بكثير، نظرا لاختيار العديد من الضحايا دفع الفدية، كما أن بعض عصابات برامج الفدية لا تستخدم المواقع الإلكترونية المتخصصة بتسريب البيانات.

وفي هذا الصدد، قال ديمتري فولكوف، الرئيس التنفيذي لدى «جروب-آي بي»: "من الهام جداً ملاحظة أن عدد الضحايا الذين تم نشر بياناتهم في أعقاب هجمات الفدية خلال الفترة ما بين النصف الثاني 2020 والنصف الأول من عام 2021 قد ارتفع بنسبة 935 % مقارنة بالعام السابق. ونتيجة لذلك، يشير النمو السنوي البالغ نسبته 22 % والذي تم تسجيله خلال فترة التقرير إلى أن سوق برمجيات الفدية المقدمة كخدمة قد اجتاز مرحلة النمو السريع ليصل الآن إلى مرحلة الاستقرار".

اكتشفت «جروب-آي بي» أن الشركات التي تتخذ من أمريكا الشمالية مقراً لها (50 % من الشركات التي تم تسريب بياناتها من قبل عصابات برامج الفدية) هي الأكثر تضرراً من تسريب البيانات جراء الهجمات التي تستخدم برامج الفدية. وبالمقارنة، كانت منطقة الشرق الأوسط وإفريقيا ثاني أقل المناطق تأثراً بتسريبات البيانات الناجمة عن هجمات برامج الفدية، حيث تم نشر بيانات 150 شركة من المنطقة على الإنترنت.

ويذكر أن 5.3 % فقط من التسريبات التي تمت على مواقع تسريب البيانات تحتوي على معلومات من دول من هذه المنطقة. وكانت الدول الأكثر تضرراً هي إسرائيل بواقع 23 شركة، وجنوب إفريقيا بواقع 21 شركة، وتركيا بواقع 14 شركة، ودولة الإمارات العربية المتحدة بواقع 14 شركة، والمملكة العربية السعودية بواقع 12 شركة. وكانت أكثر عصابات برامج الفدية نشاطًا في منطقة الشرق الأوسط وإفريقيا هي عصابة Lockbit التي قامت بنشر 37 % من بيانات الضحايا من المنطقة على مواقع تسريب البيانات. واحتلت عصابة Conti المرتبة الثانية في هذه القائمة وهي عصابة الفدية التي تتحدث اللغة الروسية والمسؤولة عن إطلاق حملة ARMa-tack المدمرة في نهاية عام 2021، والتي كانت مسؤولة عن 12 % من نسبة التسريبات، واحتلت عصابة Hive المرتبة الثالثة بنسبة تسريبات بلغت 4 %.

وكشف تقرير «جروب-آي بي» أن أكبر عدد من ضحايا تسريب البيانات الناتجة عن هجمات الفدية قد تم تسجيله في القطاعات العالمية التالية: قطاع التصنيع بواقع 295 شركة، وقطاع العقارات بواقع 291 شركة، وقطاع الخدمات المهنية بواقع 226 شركة، وصناعات النقل بواقع 224. وعلى صعيد منطقة الشرق الأوسط وأفريقيا، فقد نشرت الجهات الإجرامية الفاعلة بيانات عدد من الشركات على مواقع تسريب البيانات بواقع 18 شركة متخصصة بالخدمات المالية، و12 شركة تصنيع، و7 شركات عاملة في مجال طاقة، و3 شركات عاملة في قطاع اتصالات، و3 شركات تكنولوجيا معلومات.

وخلال الفترة المشمولة بالتقرير، ارتفع عدد هجمات برامج الفدية التي استهدفت الشركات العاملة في قطاع التصنيع على مستوى العالم بنسبة 19 % مقارنة بالفترة السابقة (النصف الأول من عام 2020 والنصف الأول من عام 2021) لتصل إلى 295 هجمة. وتم أيضاً تسجيل زيادة مماثلة في هجمات الفدية التي استهدفت قطاع الطاقة بزيادة بنسبة 43 % لتبلغ 80 هجمة، والمؤسسات المالية بزيادة بنسبة 43 % لتبلغ 181 هجمة، وقطاع تكنولوجيا المعلومات بزيادة بنسبة 18 % لتبلغ 120 هجمة. ومن الجدير بالاهتمام ملاحظة أن الهجمات على شركات الاتصالات قد انخفضت بواقع 15 % على أساس سنوي لتبلغ 29 هجمة.

وتابع ديمتري فولكوف، الرئيس التنفيذي لدى مجموعة «جروب-آي بي» حديثه قائلا: "من المتوقع أن تبقى برامج الفدية تمثل تهديداً رئيسياً للشركات والحكومات في جميع أنحاء العالم خلال عام 2023. وقد تمكنت عصابات برامج الفدية من تأسيس سوق مستقرة لمؤسساتها الإجرامية، كما أن مبالغ الفدية التي يتم طلبها من الشركات التي تتعرض للهجوم تواصل ارتفاعها بشكل سريع. لقد تحول العديد من عصابات الفدية البارزة إلى شركات إجرامية ناشئة تمتلك تسلسل هرمي قوي وتقدم حوافز ومكافآت للإنجازات والأداء المتميز. وبالرغم من التوقعات التي تشير إلى تباطؤ سوق برامج الفدية، إلا أنه من المرجح أن تشهد سوق برامج الفدية تماسكا أكبر، وأن يتواصل الاتجاه الذي سجلته خلال الفترة ما بين النصف الثاني من عام 2021 والنصف الأول من عام 2022".

شهية مفتوحة للوصول الأولي إلى بيانات الشركات

خلال الفترة ما بين النصف الثاني من عام 2021 والنصف الأول من عام 2022، قامت وحدة استقصاء التهديدات التابعة لمجموعة «جروب-آي بي» بتحليل الإعلانات السرية التي تصف الشبكات المخترقة، واكتشفت 2348 حالة وصول للشركات المعروضة للبيع، أي ضعف العدد الذي سجل خلال الفترة السابقة (1099 حالة وصول). من بين هذه الحالات، قدمت 2111 حالة معلومات حول الدولة، في حين قامت 1532 حالة بتحديد القطاع الصناعي الذي تعمل به الشركات.

قام وسطاء الوصول الأولي بتعزيز حضورهم بشكل كبير في مختلف أنحاء العالم. وارتفع عدد الدول التي تم فيها اختراق شبكات الشركات بنسبة 41 %، بارتفاع من 68 إلى 96 دولة خلال الفترة من النصف الثاني من عام 2021 إلى النصف الأول من عام 2022. وكما هو الحال في العام الماضي، كانت الشركات العاملة في الولايات المتحدة هي الأكثر شعبية بين وسطاء الوصول الأولي، حيث أن ما يصل إلى ربع عروض الوصول المكتشفة كانت لشركات أمريكية بواقع 558 شركة. وعلى غرار العام الماضي، كانت القطاعات الأكثر تضررًا من هجمات وسطاء الوصول الأولي هي قطاع التصنيع بواقع 5.8 % من جميع الشركات وقطاع الخدمات المالية بواقع 5.1 %، وقطاع العقارات بواقع 4.6 %، وقطاع التعليم بواقع 4.2 %.

وتابع ديمتري فولكوف قائلا: "يلعب وسطاء الوصول الأولي دور الممول الرئيسي للاقتصاد السري بأكمله، فهم يعملون على تغذية وتسهيل عمليات المجرمين الآخرين، مثل برامج الفدية والعصابات الاجرامية التي تعمل لأهداف ولدول قومية. ومع استمرار نمو مبيعات حالات الوصول الأولي وتنويعها، تعد هجمات وسطاء الوصول الأولي من أبرز التهديدات التي يجب مراقبتها خلال العام 2023. ويجب على الشركات الخاصة والعامة في منطقة الشرق الأوسط وأفريقيا التفكير في إعداد برامج قوية لاستقصاء التهديدات لمراقبة بيانات الاعتماد المخترقة للقوى العاملة لديها".

على مستوى منطقة الشرق الأوسط وإفريقيا، بقيت الشركات الإماراتية الأكثر استهدافا والتي استحوذت على 26.3 % من جميع عروض حالات الوصول إلى شبكات الشركات في المنطقة التي تم اكتشافها بين النصف الثاني من عام 2021 والنصف الأول من عام 2022، تلتها تركيا بواقع 19.6 %، ثم باكستان بواقع 6.7 %، ومصر بواقع 5.6 %، وجنوب إفريقيا بواقع 5 %، وإيران بواقع 4.5 %، والمملكة العربية السعودية بواقع 4.5 %، وكينيا بواقع 2.8 % والجزائر بواقع 2.2 %.

تماشيا مع التوجهات العالمية، انخفضت التكلفة الإجمالية لعروض الوصول الأولي إلى شبكات الشركات في منطقة الشرق الأوسط وأفريقيا المتداولة في الأسواق السرية بنسبة 23 % لتصل إلى 281،470 دولارًا أمريكيًا. ويرجع هذا الانخفاض إلى الزيادة الكبيرة في العروض، فقد تضاعف عدد عروض الوصول إلى شبكات الشركات العاملة في منطقة الشرق الأوسط وإفريقيا بأكثر من الضعف من 88 عرضاً خلال الفترة من النصف الثاني من 2020 إلى النصف الأول من عام 2021، إلى 179 عرضاً خلال العام الماضي، وهو ما يفسر ارتفاع الهجمات باستخدام برامج الفدية في المنطقة. وشددت «جروب-آي بي» على أنه لايتعين على الشركات أن تفكر في اعتماد الأنظمة العالمية للحماية، بل يجب عليها أن تعرف من يقف وراء الهجوم، وأن تستخدم التقنيات القائمة على التحقيقات السيبرانية والبحوث وعمليات الاستجابة للحوادث في المنطقة التي تعمل فيها.

ارتفاع شعبية سجلات البيانات المسروقة

من أبرز التغييرات التي طرأت على مشهد التهديدات العالمية هو الشعبية المتزايدة للسجلات التي تم الحصول عليها باستخدام سرقة المعلومات، وهي برامج ضارة تجمع التفاصيل الشخصية من البيانات الوصفية لمتصفح الإنترنت الخاصة بالمستخدم. ويمكن لهؤلاء المخترقين الحصول على بيانات الاعتماد والبطاقات المصرفية وملفات تعريف الارتباط وبصمات المتصفح وما إلى ذلك. وجدت «جروب-آي بي» أنه خلال الفترة من 1 يوليو 2021 حتى 30 يونيو 2022، تم عرض أكثر من 96 مليون سجل للبيع، ووجدت أن معظم البيانات المخترقة تعود لمستخدمين من الولايات المتحدة بنسبة 80 %، تلاها المملكة المتحدة بنسبة 5.4 %، والهند بنسبة 4.6 %، وإندونيسيا بنسبة 2.4 %، والبرازيل بنسبة 2.0 %.

ومن بين هذه السجلات البالغ عددها 96 مليون سجل، اكتشف خبراء «جروب-آي بي» أكثر من 400 ألف سجل للدخول الأحادي، ويعد سجل الدخول الأحادي من آليات المصادقة المؤسسية المعروفة والتي تستخدم زوجًا واحدًا فقط من بيانات الاعتماد للوصول إلى خدمات وتطبيقات متعددة، مما يجعلها من الآليات الهامة التي يحرص مجرمو الإنترنت على استهدافها لأنها تسمح لهم بالدخول إلى عدة أنظمة في وقت واحد وبجهد ضئيل. كما اكتشف خبراء «جروب-آي بي» أن عامل التهديد الذي يقف وراء الهجوم الأخير على شركة أوبر قد اشترى سجلات مسروقة من أحد الأسواق السرية مقابل 20 دولارًا، واحتوت هذه السجلات على بيانات اعتماد الدخول الموحّد لاثنين على الأقل من موظفي شركة أوبر.

واختتم ديمتري فولكوف، الرئيس التنفيذي لدى «جروب-آي بي» حديثه قائلاً: "إنه لأمر مقلق بشكل كبير أن نرى ما يستطيع مجرم إلكتروني يمتلك 20 دولارًا ومهارات تقنية متواضعة القيام به هذه الأيام. فمع انتشار نماذج العمل عن بُعد وخدمات الدخول الموحّد (SSO)، فقد بتنا نرى في كثير من الأحيان حالات الوصول إلى شبكات الشركات ضمن سجلات البيانات المسروقة. إن الاستفادة من بيانات موظف واحد لشن الهجمات على الشركات ستصبح واحدة من مصادر القلق الكبيرة، ولا يوجد حل سحري للتصدي لمثل هذه الهجمات، الأمر الذي يسلط الضوء على حاجة الشركات إلى تطوير قدرات الأمن السيبراني على جميع المستويات لديها، بما في ذلك تدريب الموظفين على الاستجابة والتعامل مع الهندسة الاجتماعية، وتعزيز قدرات الكشف والاستجابة، بالإضافة إلى مراقبة المجرمين الإلكترونيين تحت الأرض بحثا عن سجلات الموظفين المخترقة والعروض المتعلقة ببيع بيانات الوصول إلى شبكاتهم".