الخليج

اقتصاد, تقنية وسيارات

21 سبتمبر 2023 15:02 مساء

بوزيتف تكنولوجيز»: الهجمات السيبرانية تستهدف الأفراد ببرمجيات تجسس»

دبي: «الخليج»

قامت شركة «بوزيتف تكنولوجيز» بتحليل الهجمات السيبرانية التي تعرض لها الأفراد في دول الشرق الأوسط خلال الفترة ما بين عامي 2022 و2023، وخلصت الشركة إلى أنه جرى استخدام البرمجيات الضارة في 70% من الهجمات الناجحة، وقد تضمنت أكثر من نصف هذه الهجمات برمجيات تجسس.

وقد وجدت الشركة أن غالبية هذه الهجمات قد استخدمت تقنيات الهندسة الاجتماعية، حيث اتخذت 20% من هجمات التصيد الاحتيالي شكل الهجمات متعددة الجوانب التي استهدف خلالها المهاجمون قنوات هندسة اجتماعية متعددة في نفس الوقت.

ووفقاً للبيانات الصادرة عن «بوزيتف تكنولوجيز»؛ فقد استخدم مجرمو الإنترنت البرمجيات الضارة التي استهدفت الأفراد في منطقة الشرق الأوسط بمعدل 7 من أصل 10 هجمات ناجحة. وغالباً ما نجح المهاجمون باستهداف أجهزة المستخدمين وإصابتها ببرامج تجسس (3 برمجيات ضارة من أصل 5)، حيث يستهدف هذا النوع من البرمجيات الضارة جمع المعلومات من الجهاز المصاب ثم إيصالها إلى المهاجم. واستناداً إلى الغرض الذي جرى تصميمها لتحقيقه، فإن برمجيات التجسس لها القدرة على سرقة أنواع مختلفة من المعلومات الحساسة، بما في ذلك البيانات

.الشخصية والمالية، وبيانات اعتماد المستخدم، والملفات المخزنة في ذاكرة الجهاز

برمجيات التجسس •

وفي هذا الصدد، قال رومان ريزنيكوف، محلل أبحاث أمن المعلومات لدى شركة «بوزيتف تكنولوجيز»: «يُمكن للمهاجمين استخدام برمجيات التجسس ليس فقط لاختراق المعلومات الشخصية ومعلومات الدفع/ التسديد المالي والحسابات الشخصية؛ بل أيضاً لسرقة بيانات اعتماد الشركات ومعلومات اتصال الشبكة وغيرها من البيانات الحساسة الأخرى. يتم بعد ذلك عرض البيانات المسروقة للبيع في منتديات شبكة الإنترنت المظلمة. ونتيجة لذلك، يُمكن للمهاجم المحترف الوصول إلى المؤسسة أو الشركة وتنفيذ هجوم ناجح، ما يؤدي إلى عواقب غير مقبولة؛ مثل تعطيل العمليات التكنولوجية والتجارية، وسرقة الأموال، وتسرب المعلومات السرية، وشن الهجمات السيبرانية على العملاء والشركاء».

وشهدت غالبية الهجمات الناجحة التي استهدفت الأفراد في دول الشرق الأوسط، والتي بلغت نسبتها 96%، استخدام تقنيات الهندسة الاجتماعية. وقد كانت هذه الهجمات في معظم الأحيان هجمات جماعية يهدف فيها المجرمون الوصول إلى أكبر عدد ممكن من الضحايا. ولتحقيق ذلك، استغل المجرمون الأخبار المرتبطة بالأحداث والفعاليات الإقليمية والعالمية المهمة، بما في ذلك كأس العالم FIFA 2022 قطر.

التصيد الاحتيالي •

شهد 20% من حملات التصيد الاحتيالي استخدام استراتيجية هجوم متعددة الأوجه، والتي تمت باستغلال قنوات الهندسة الاجتماعية المختلفة في نفس الوقت، حيث قام مجرمو الإنترنت بتوجيه الضحايا بشكل ممنهج من خلال سلسلة من الإجراءات التي أدت في نهاية المطاف إلى إصابة الجهاز وسرقة البيانات. مثلاً، يمكن للمجرمين إغراء الضحايا من خلال حسابات التواصل الاجتماعي التي تحتوي على روابط تؤدي إلى منصة أو قناة مراسلة تغري المستخدمين لتثبيت تطبيق ضار بشكل غير مقصود.

وأحد أسباب نجاح عمليات الهندسة الاجتماعية هي تسرب البيانات للعديد من المؤسسات والشركات المختلفة. وتشير الدراسة التي أجرتها «بوزيتف تكنولوجيز» حول مشهد التهديدات السيبرانية في الشرق الأوسط إلى أن 63% من الهجمات الناجحة على الأفراد قد نجمت عن حالات تسرب للمعلومات السرية. وتألفت غالبية المعلومات المسروقة من بيانات شخصية بنسبة 30%، وبيانات اعتماد الحسابات بنسبة 30%. كان مجرمو الإنترنت مهتمون أيضاً بسرقة بيانات بطاقات الدفع المالي بنسبة 10%، وسرقة مراسلات المستخدمين بنسبة 8%.

وتقوم الجهات الخبيثة ببيع معلومات المستخدمين على شبكة الإنترنت المظلمة، وتقوم أيضاً بتوفير أرشيفات البيانات المسروقة مجاناً. يستخدم المجرمون المعلومات المسروقة في الهجمات اللاحقة على المستخدمين، حيث يمكن على سبيل المثال أن يسفر الهجوم الناجح على أحد البنوك عن إجراءات احتيالية ضد عملائه.

ويوصي خبراء الأمن السيبراني المستخدمين باتباع قواعد النظافة والسلامة السيبرانية. وتحتاج الشركات، أيضاً، إلى ضمان أمن بيانات الموظفين والعملاء؛ إذ يمكن أن تتسبب خروق بياناتهم بأضرار مالية كبيرة، وأن يتعرّض المستخدمون الذين تم اختراق معلوماتهم للخطر. وللحفاظ على المرونة والسلامة السيبرانية، من الضروري إجراء التقييم المنتظم لاختبار فاعلية التدابير الأمنية وإيلاء اهتمام خاص للتحقق من الأحداث غير المقبولة والتي لا يمكن تحمل عواقبها.