المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

السلامة الرقمية

العدد الخامس/ الخميس 14 ربيع الآخر 1446هـ - 17 أكتوبر 2024م

تصاعُد خطر البرمجيات الخبيثة على الهواتف المحمولة

دلال العقيدي
البحث العلمي في المبادرة الوطنية للسلامة الرقمية

هجمات CosmicSting
تخترق أكثر من 4000 متجر Magento

Google تُؤكّد
إرسال إشعارات خاطئة عبر Google Pay

المحتويات

البحث العلمي في المبادرة الوطنية للسلامة الرقمية

تسعى الوكالة الوطنية للأمن السيبراني، من خلال المبادرة الوطنية للسلامة الرقمية، إلى تعزيز مؤشرات السلامة الرقمية على مستوى الدولة والمجتمع، وتحويلها لثقافة حياة وممارَسة مستدامة، وهي أهداف إستراتيجية، وتحقيقها يتطلّب الالتزام بمنهج علمي قويم، يشمل مراحل التخطيط، والتنفيذ، والرقابة، والتقييم. وهذا ما تحرص عليه الوكالة في مختلف مراحل المبادرة.

تُدرك الوكالة الوطنية للأمن السيبراني أن نجاح المبادرة الوطنية للسلامة الرقمية يرتبط بشكل مباشر بمدى الاعتماد على البحث العلمي ومخرجاته، والابتعاد التام عن التقدير الشخصي، وهذا ما تم تحقيقه من خلال إعداد عدة دراسات علمية، شملت قطاعات متعدّدة، بما فيها تحديد الاتجاهات الحالية للسلامة الرقمية في دولة قطر، ودراسة وتحليل أبرز التجارب الدولية الرائدة في مجال السلامة الرقمية، وتحليل أنشطة المراكز البحثية الدولية فيما يتعلق بالسلامة الرقمية، إضافةً لدراسة منهجية الشراكة مع المؤسسات الوطنية والدولية، وتحليل خصائص الشرائح المستهدَفة، ودراسة القدرات الحالية والمستهدَفة لأدوات التوعية بالسلامة الرقمية.

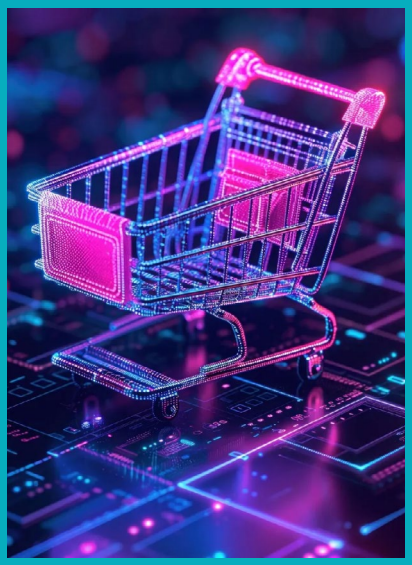
هذه الدراسات كانت بمثابة المُوجّه العام والناظم الرئيس لمختلف أنشطة المبادرة، بما يشمل تحديد طبيعة المحتوى التوعوي المطلوب، وتحديد مزيج الأدوات التوعوية اللازمة لكل شريحة من الشرائح المستهدَفة بالمبادرة. لذلك يمكن القول بأن المبادرة قائمة بالمُجمَل على البحث العلمي، وبذلك يمكن وصفها بأنها نتاج علمي مستند إلى منهجيات بحث قويمة. ومن خلال هذه المنهجيات العلمية والبحثية يمكن ضمان تحقيق أهداف المبادرة وبلوغ رؤيتها ورسالتها.

دلال العقيدي

مدير إدارة التميز السيبراني الوطني

هجمات CosmicSting

تخترق أكثر من 4000 متجر Magento



تم اكتشـاف هجمات سـيبرانية خطيرة تحت اسم CosmicSting تسـتهدف أكثر مـن 4000 متجر عبـر الإنترنت باسـتخدام منصة Magento، وهي واحدة من أشـهر منصات التجارة الإلكترونية في العالم. هذه الهجمات نجحت في اختراق المواقع وسـرقة بيانات حساسة تتعلق بعملاء تلك المتاجر، بما في ذلك معلومات الدفع مثـل أرقام بطاقات الائتمـان. الهجوم بدأ باسـتخدام ثغرات غير معروفة في برمجيات Magento، مما سمح للقراصنة بزرع شفرات خبيثة في مواقع الضحايا.

ثغـرات في منصة Magento تتسـبَّب في خرق عالمي وسـرقة معلومات الدفع من آلاف المتسوقين

المهاجمون اسـتغلوا ضعف تحديث الأنظمة الأمنية في تلك المواقع لحقن برمجيات خبيثة تجمع البيانات الشـخصية والمصرفية للمستخدمين عند إتمام عمليات الشـراء. بفضل هذه الهجمات، تمكَّن القراصنة من سـرقة معلومات حساسـة من آلاف العملاء، مما عرَّضهم لخطر الاحتيال المالـي. كانت الهجمات منظَّمة بعناية، وشملت عدة مواقع على نطاق عالمي، مما أثار القلق بشأن مدى انتشار وتأثير الهجوم[1].

Magento، رغم شـعبيتها الكبيـرة، تُمثِّل هدفاً متكـرراً للقراصنة؛ نظراً لأن العديد مـن المتاجر الإلكترونية الصغيرة ومتوسـطة الحجم لا تقوم بتحديث أنظمتها بشـكلٍ دَوري، ممّا يفتح الباب أمام استغلال الثغرات الأمنية. وعلى الرغم من توافر تحديثات الأمان؛ إلا أن بعض المواقع لم تقم بتثبيتها، مما سـمح للمهاجمين بتنفيذ هجماتهم بنجاح.

1. Kaaviya, CosmicSting Hack Hits Thousands of Adobe Commerce and Magento Stores, Cyber Press, October 2024, on site: https://cyberpress.org/thousands-of-adobe-commerce-and-magento-stores/

هجـــوم CosmicSting الإلكتروني يضـــرب 4000 متجر إلكتروني ويسرق بيانات بطاقات الائتمان

الشركات المتضررة كانت مُجبَرة على إغلاق أنظمتها مؤقتاً، والتحقيق في مدى الضرر الذي ألحقه الهجوم بعملائها، مع محاولة اســتعادة السيطرة على بيانات العملاء، والتخفيف من التأثيرات السلبية للهجمات. وبشــكلٍ عامّ، فإن الضّرر المالي وتضرُّر السُّــمعة الذي يلحق بهذه الشــركات لهما تأثير كبير على المدى الطويل[1].

الخبراء في مجال الأمن السيبراني، أكدوا أن هذا النوع من الهجمات يُعزّز الحاجة إلى تعزيز دفاعات المواقع الإلكترونية، خاصةً تلك التي تتعامل مع بيانات حساســة مثل بيانات الدفع. ويُوصي الخبراء بضرورة اعتماد بروتوكولات حماية صارمة، من بينها: التحقُّق من الهوية بشكلٍ ثنائي، وتحديث الأنظمة بانتظام، وضمان وجود أنظمة مراقبة قوية لاكتشاف أيّ نشاط مشبوه في الوقت الفعلي.

الهجمات مثل CosmicSting تُذكّرنا بالأهمية القصوى للأمن السيبراني، خاصةً مع تزايد عمليات التجارة الإلكترونية حــول العالم. ويجب أن تلتزم الشــركات والمتاجر الإلكترونية باتخاذ إجراءات أمنية اســتباقية لحمايــة بيانات العملاء؛ لأن مثــل هذه الاختراقات لا تُعــرِّض العملاء فقط للخطر، بــل يمكن أن تُلْحِق أضراراً لا تُحْصَى بسُــمْعة الشركات، وتجعلها عُرْضة للمزيد من الهجمات في المستقبل.

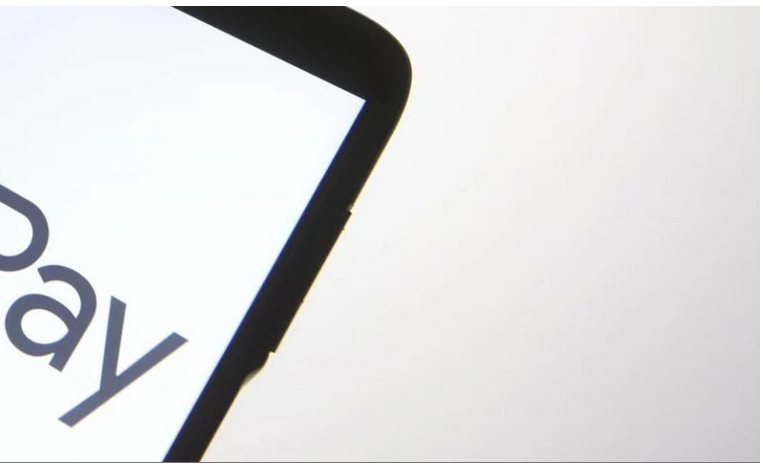
هذه الحادثة تُمثِّل تحذيراً قوياً للشركات في مختلف أنحــاء العالــم بضرورة عــدم التهاون فــي تحديث أنظمتها الأمنيــة، والاعتماد على أحــدث تقنيات الحمايــة الســيبرانية؛ لتجنُّب مثل هــذه الهجمات المدمِّرة.

1. CosmicSting Attacks Compromise Over 4,000 Adobe Commerce and Magento Stores, Vulnera, October 2024, on site: https://vulnera.com/newswire/cosmicsting-attacks-compromise-over-4000-adobe-commerce-and-magento-stores/

Google تُؤكّد
إرسال إشعارات خاطئة عبر Google Pay

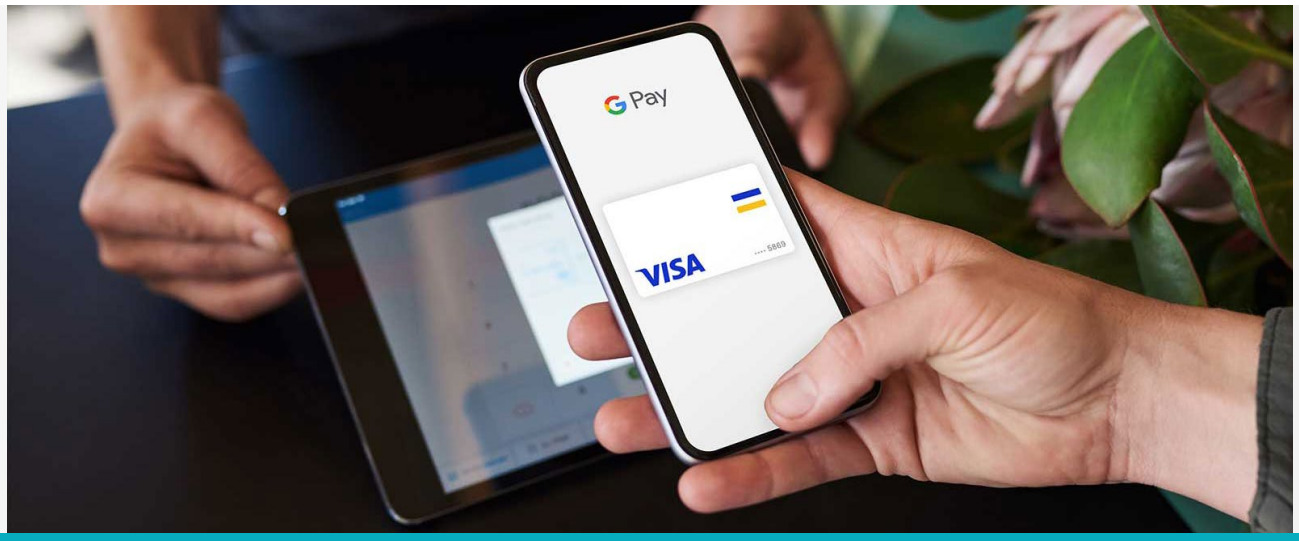
أكّدت Google أنها أرســلت إشــعارات خاطئة عبر تطبيق Google Pay إلى عدد كبير من المستخدمين حول العالم. تلقّى هؤلاء المستخدمون رسائل غير صحيحة تفيد بوجود معاملات أو تحويلات مالية لم تحدث، مما أثار القلق بين المستخدمين، ودفع البعض إلى الاعتقاد بحدوث خرق أمني أو مشكلة في حساباتهم البنكية. جاء رد Google ســريعاً؛ حيث أوضحت أن المشــكلة كانت نتيجة خطأ تقني داخلي، وليس هجوماً ســيبرانياً، مؤكدةً أن أموال المستخدمين وحساباتهم لم تتأثّر، وأن الفريق التقني يعمل على حلّ المشكلة بأسرع وقت ممكن[1].

خطأ تقني أم خرق أمني؟ جوجل تُوضّح ســبب الإشعارات المضلّلة في Google Pay!



من جانب المستخدمين، انتشرت تقارير على منصات التواصــل الاجتماعــي تُظهــر ارتباكهــم وقلقهم من الإشــعارات الواردة؛ حيث أفــاد البعض بتلقّي إشــعارات تفيد بعمليات شــراء أو تحويلات مالية لم يقومــوا بها. هذا الخلل أدّى إلى زيادة المخاوف حول موثوقية تطبيقات الدفع الإلكتروني، ومدى قدرتها على حماية معلومات المستخدمين المالية.

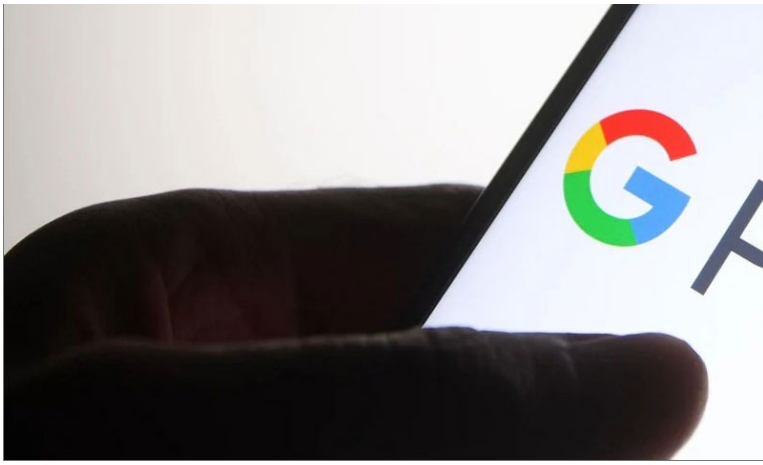
1. Li, Abner. Google Pay confirms 'You added a new card to your Google Account' email error, 9to5google, October 2024, on site: https://9to5google.com/2024/10/03/google-pay-new-card-error/



Google سارعت إلى الاعتذار عن هذا الخطأ، وأكّدت أن النظام تعرّض لخلل تقني أرسل إشعارات خاطئة تتعلّق بالمعاملات، لكنّها أكّدت أن هذه الإشعارات لم تكن مرتبطة بأيّ حركات مالية فعلية. في بيانها، أشارت الشركة إلى أنها ستقوم بتحديث النظام؛ لضمان عدم تكرار هذه المشكلة، كما نصحت المستخدمين بتجاهل الإشعارات الخاطئة، والتحقق من حساباتهم المالية عبر التطبيقات المصرفية المعتمَدة للتأكد من سلامتها[1].

فيما يتعلق بردود الفعل، أبدى المستخدمون ارتياحهم بعد التوضيحات التي قدّمتها Google، لكنّ الحادثة أثارت نقاشات حول أهمية تعزيز الشفافية، وضمان جودة تطبيقات الدفع الإلكتروني التي يعتمد عليها ملايين الأشخاص في حياتهم اليومية. ورغم الاعتذار السريع من الشركة، فقد أكّد بعض الخبراء على ضرورة أخذ هذه الحوادث بجدية؛ لأنها تثير تساؤلات حول جاهزية الأنظمة التقنية لمواجهة الأخطاء المحتملة، وكيفية التعامل معها.

هذه الحادثة تأتي في وقتٍ حسّاس؛ حيث تزداد الهجمات السيبرانية والمخاوف المتعلقة بأمان التطبيقات المالية. وفي ظل تزايد الاعتماد على تطبيقات الدفع الرقمي مثل Google Pay، من الضروري أن تبذل الشركات جهوداً أكبر لضمان أمان وسلامة بيانات المستخدمين.



1. Sharma, Ax. Google Pay alarms users with accidental 'new card' added emails, Bleeping Computer, October 2024, on site: https://www.bleepingcomputer.com/news/security/google-pay-alarms-users-with-accidental-new-card-added-emails/

الشرطة الهولندية

تحقّق في عملية اختراق مرتبطة بالدولة

بدأت الشــرطة الهولندية تحقيقاً واسع النطاق فــي هجوم ســيبراني، يُعتقد أنــه مرتبط بإحدى الدول. الهجوم اســتهدف البنية التحتية الرقمية لحكومة هولندا ومؤسســات كبــرى أخرى، مما أثار القلق بشــأن تورُّط جهات حكومية أو جماعات مدعومة مــن دُوَل أخرى. ويُعتقد أن الهجوم كان مُوجّهــاً لتعطيــل الخدمات الحكومية، وســرقة معلومات حساسة، ما دفَع السلطات إلى التحرُّك بســرعة للتحقيق فــي كيفية اختــراق الأنظمة واستهدافها[1].

تحقيــق هولندي يكشــف عن هجوم ســيبراني مُعقَّد يُهدّد البنية التحتية الحكومية

التحقيق الذي تقوده الشرطة الهولندية، يركّز على تحديد مصدر الهجوم، وتقييم مدى الضرر الذي لحق بالبنية التحتية الرقمية. وفقاً للتقارير الأولية، يُعتقد أن الهجوم قــد تم بواســطة أدوات متطورة غالباً ما تُســتخدَم في الهجمات المرتبطة بالدول، مثل البرمجيات الخبيثة التي تستغل ثغرات غير معروفة ســابقاً (Zero-days). ويشــتبه المحققون في أن الجهة الفاعلــة قد تكون دولة معادية أو مجموعة قراصنة مدعومين حكومياً، يســعَون للوصول إلى بيانات حساسة أو تعطيل الأنشطة الحكومية[2].

1. Antoniuk, Daryna. Dutch police blame 'state actor' for recent data breach, The Record, October 2024, on site: https://therecord.media/dutch-police-state-actor-breach
2. Jennings-Trace, Ellen. Dutch police say state actor likely behind recent data breach, Tech Radar, October 2024, on site: https://www.techradar.com/pro/dutch-police-say-state-actor-likely-behind-recent-data-breach

هل وراء الهجوم السيبراني في هولندا دُوَل معادية؟ الشرطة تبدأ تحقيقات موسَّعة

الهجمات السيبرانية المرتبطة بالدول تُشكّل تحدياً كبيراً للسلطات الأمنية؛ لأنها غالباً ما تكون جزءاً من حملات تجسُّس أو حملات تخريبية، تهدف إلى التأثير على السياسة الداخلية والخارجية للدول المستهدفة. في حالة هولندا، تزايدت المخاوف من أن هذا الهجوم قد يكون جزءاً من تصعيد أوسع للتهديدات السيبرانية التي تستهدف الاتحاد الأوروبي، خاصةً مع تصاعد التوترات الجيوسياسية في مناطق مثل أوروبا الشرقية والشرق الأوسط.

هذا الهجوم يُعدّ تذكيراً واضحاً بالخطر المتزايد الذي تُشكّله الهجمات السيبرانية المرتبطة بالدول على البنية التحتية الحساسة. وبينما تعمل الدول على تطوير دفاعاتها السيبرانية، يبقى التهديد الإلكتروني تحدياً مُعقَّداً يتطلب تنسيقاً دولياً مستمراً وجهوداً مشتركة للتصدّي له.

بالنسبة لهولندا، فإن التحقيق في هذا الهجوم قد يكون بدايةً لفهم أعمق للتهديدات التي تواجهها المنطقة، وكيفية التصدي لها في المستقبل القريب.

هجوم فدية يستهدف CASIO:

سرقة بيانات العملاء وإثارة مخاوف أمنية

خلال أكتوبر الجاري، تعرَّضت شركة كاسيو، المشهورة عالمياً بتصنيع الساعات والأجهزة الإلكترونية، لهجوم فدية سيبراني أدَّى إلى سرقة بيانات حساسة لعملائها. وفقاً للبيان الصادر عن الشركة، استهدف الهجوم الأنظمة الداخلية لكاسيو؛ حيث تمكّن المهاجمون من الوصول إلى معلومات شخصية تشمل الأسماء، عناوين البريد الإلكتروني، وربما تفاصيل الدفع المالي.

CASIO تعلن عن اختراق أمني بعد هجوم فدية وسرقة بيانات العملاء

هذا النوع من الهجمات أصبح شائعاً في السنوات الأخيرة؛ حيث يستغل القراصنة الثغرات الأمنية في الأنظمة القديمة وغير المُؤمَّنة بشكلٍ كافٍ لسرقة البيانات أو تشفيرها، ثم طلب فدية مالية مقابل عدم تسريبها أو إعادتها إلى أصحابها. في هذا السياق، أكَّدت كاسيو أنها لم تتَّخذ قراراً بعدُ حول دفع الفدية، لكنَّها تتعاون بشكلٍ وثيق مع الجهات المختصة وخبراء الأمن السيبراني؛ لمحاولة استعادة السيطرة على الأنظمة وحماية بيانات العملاء[1].

ما يزيد من خطورة هذا الهجوم هو أنه جزء من سلسلة هجمات سيبرانية عالمية؛ حيث تزايدت وتيرة هذه الهجمات التي تستهدف الشركات الكبرى والمؤسسات الحكومية؛ حيث أصبحت هجمات الفدية تُشكِّل تهديداً كبيراً ليس فقط للشركات، بل للاقتصادات الرقمية بشكلٍ عامّ. إن شركة مثل كاسيو تعتمد على بنيتها التحتية التكنولوجية لتقديم خدماتها، ولذلك فإن أيّ اختراق يُؤثّر بشكل مباشر على قدرتها على تقديم تلك الخدمات، فضلاً عن التأثير على سُمْعتها في السوق.

1. Toulas, Bill, Casio confirms customer data stolen in a ransomware attack, Bleeping Computer, October 2024, on site: https://www.bleepingcomputer.com/news/security/casio-confirms-customer-data-stolen-in-a-ransomware-attack/

هجوم فديــة على CASIO: مَطالِب ماليــة وهواجس حول حماية البيانات

أوضحت كاسـيو أنها تقوم بإجـراءات فورية لتعزيز أمنهـا السـيبراني، بما في ذلك تحديـث أنظمتها وتفعيـل تدابير إضافيـة للحماية مثـل المصادقة الثنائيـة، وتثقيف الموظفين حـول كيفية التَّعرُّف على الهجمات المحتملة، ونصحت الشركة العملاء بتوخّـي الحذر وتغيير كلمات المرور بشـكل دوري، وخاصـةً فـي حسـاباتهم المتعلقة بالمشـتريات الإلكترونيـة، من أجل تفـادي اسـتغلال بياناتهم المسروقة.

يُعـدّ هـذا الهجوم مثـالاً آخر علـى الضعف الذي يمكـن أن تواجهـه حتـى الشـركات الكبيـرة في مواجهة الهجمات السـيبرانية، ممـا يدفع العديد من المؤسسـات إلـى إعادة تقييم إسـتراتيجياتها في حمايـة البيانات؛ حيث تُعدّ التكنولوجيا أحد أهم العوامل التـي تعتمد عليها الشـركات في تقديم خدماتها اليوم، ولكن دون وجود حماية قوية، يمكن أن تكـون تلـك التكنولوجيا سلاحـاً ذا حدَّين، ومع تصاعد هـذه التهديدات، من المتوقع أن تسـتثمر المزيد من الشركات في تطوير وتعزيز أنظمة الأمن السيبراني لضمان حماية بيانات العملاء وتعزيز ثقة الجمهور.

هجوم سيبراني

يستهدف مؤسسة صحية غير ربحية في الولايات المتحدة

في حادثة تُبرز التهديدات المتزايدة التي تُواجه قطاع الرعاية الصحية، تعرَّضت مؤسسة صحية غير ربحية في ولاية كولورادو الأمريكية لهجوم سيبراني ضخم؛ أثَّر على خدماتها وقُدرتها على تلبية احتياجات المرضى.

ووفقاً للتقارير الأخيرة؛ فقد استهدف هذا الهجوم منظمة Colorado Access، وهي منظمة غير ربحية متخصصة في تقديم خدمات الرعاية الصحية لمجموعة كبيرة من الأفراد المحتاجين في المنطقة.

الهجمات السيبرانية تُهدّد قطاع الرعاية الصحية... أحدث ضحاياها مُؤسّسة صحية أمريكية غير ربحية!

الهجوم تمثَّل في استخدام أدوات سيبرانية مُعقَّدة تُستخدم عادةً في الهجمات التي تستهدف البيانات الحساسة مثل برمجيات الفدية، مما أدَّى إلى تعطيل كبير في عمليات المؤسسة. هذه الهجمات غالباً ما تهدف إلى تعطيل الخدمات أو سرقة المعلومات الحيوية، وطلب فدية مقابل استعادتها، وهو ما قد يكون له تأثير مدمّر على المنظمات التي تعتمد على البيانات الرقمية لتقديم الرعاية الصحية.

وفقاً للمصادر، تم اكتشاف الهجوم في وقتٍ مبكرٍ عندما لاحَظ موظفو Colorado Access تعطلاً في أنظمة الاتصال الداخلية والخدمات الإلكترونية التي تَعتمد عليها المؤسسة في تقديم خدماتها. هذا الهجوم أدَّى إلى شَلّ حركة العمل في العديد من أقسام المنظَّمة، وإلى عدم قدرتها على معالجة الطلبات، وتقديم الرعاية الصحية اللازمة للمرضى. بمرور الوقت، تبيَّن أن القراصنة تمكَّنوا من الوصول إلى بيانات حسّاسة؛ تشمل معلومات شخصية وطبية عن المرضى، مما زاد من تعقيد الأمور[1].

1. Greig, Jonathan. Cyberattack targets healthcare nonprofit overseeing 13 Colorado facilities, The Record, October 2024, on site: https: https://therecord.media/cyberattack-targets-healthcare-nonprofit-colorado

هل قطاع الرعاية الصحية في خطر؟ هجوم سـيبراني كبير على منظمة صحية غير ربحية في الولايات المتحدة

لم يتم الكشـف بشكلٍ مباشـر عن تفاصيل المدى الكامـل للأضرار، ولكن مـن المتوقع أن يكون حجم التأثيـر كبيراً، خاصةً مع تزايد الاعتماد على الأنظمة الرقميـة فـي إدارة سـجلات المرضـى وتقديـم الخدمات الصحية. الهجـوم لم يقتصر على تعطيل العمليـات اليومية فقط، بل أثار أيضاً مخاوف كبيرة حول أمن المعلومات الحسّاسـة للمؤسسة، وهي قضية حيوية في ظـل الاهتمـام المتزايد بحماية بيانات المرضى.

استجابة Colorado Access للأزمة كانت سريعة، حيـث أطلقـت المؤسسـة فـوراً تحقيقـاً داخلياً بالتعاون مع خبـراء في الأمن السـيبراني؛ لتحديد حجـم الضرر، والعمل على احتـواء الهجوم. وأكدت المؤسسـة أنها قامت بفصل الأنظمة المصابة عن الشبكة الرئيسـة؛ لمنع المزيد من الاختراقات، كما بدأت في تنفيذ خطط الطوارئ لاسـتعادة القدرة على تقديم خدماتها بسرعة.

في حيـن أن المؤسسـة لـم تُفصِح عـن مَطالب القراصنة؛ فإن التعامل مع مثل هذه الهجمات غالباً مـا يكون صعباً؛ حيث تكون الخيـارات محدودة بين دفع الفدية أو محاولة اسـتعادة الأنظمة بشـكل مسـتقل. تدابير مثل هذه تتطلَّب استثمارات كبيرة في التقنيات المتقدمة وفِرَق متخصصة في الأمن السيبراني للتعامل مع التهديدات بسرعة وفاعلية.

الهجوم السيبراني على Colorado Access يُسلِّط الضـوء على أهميـة تأمين الأنظمـة الرقمية في المؤسسـات الصحية والتهديـدات المتزايدة التي تواجهها؛ حيث بات من الضروري اتخاذ تدابير وقائية شـاملة لحماية هذه المؤسسـات الحساسة، التي تلعب دوراً رئيساً في تقديم الرعاية الصحية للأفراد.

وعلى الرغـم من أن هذا الهجـوم كان له تداعيات كبيـرة على العمليـات اليوميـة؛ إلا أن اسـتجابة المؤسسة وسرعة التعامل مع الأزمة تُظهر أهمية التخطيط الجيد والمرونـة في مواجهة التهديدات السيبرانية.

تصاعُد خطر البرمجيات الخبيثة على الهواتف المحمولة

هجمات البرمجيات الخبيثة علـــى الهواتف المحمولة في ازدياد.. هل هاتفك الذكي في خطر؟

تشـــهد البرمجيات الخبيثة الموجَّهة للأجهزة المحمولة تصاعُداً ملحوظاً، ما يُشكّل تحدياً خطيراً لمستخدمي الهواتف الذكية على مستوى العالم. في السنوات الأخيرة، انتقلت الهجمات السيبرانية من استهداف أجهزة الحاســوب والشــبكات التقليدية إلى الهواتف المحمولة، مما يزيد من التعقيدات ويطرح أسئلة كبيرة حول مــدى الأمان الذي توفّره الأجهــزة الذكية التي باتت جزءاً لا يتجزّأ من حياتنــا اليومية. وفقاً لتقرير حديث من SpyCloud، شــهدت الهجمات التي تستهدف الأجهزة المحمولة زيادة ملحوظة، ويبدو أن قراصنة الإنترنت يُطوّرون باستمرار أدواتهم وأساليبهم لاستغلال الثغرات الموجودة في أنظمة التشغيل للهواتف المحمولة وتطبيقاتها[1].

الهجمات على الهواتف المحمولة لم تعد مقتصرة على محاولات اختراق بســيطة، أو إرســال رســائل تصيدية. بدلاً من ذلك، أصبح المهاجمون يعتمدون على تقنيات متقدّمة تشــمل البرمجيــات الخبيثة المتطورة التي يمكنها ســرقة البيانات الشخصية، والتجسُّــس علــى المكالمــات والرســائل، وحتى التحكُّم الكامل بالجهاز المستهدَف.

من أبرز ســمات الهجمات الســيبرانية الأخيرة على الأجهزة المحمولة هو عدم استهدافها فئة معينة فقط من المستخدمين. سواء كنت مستخدماً فردياً تعتمد على هاتفك للتواصــل وتصفُّح الإنترنت، أو كنت جزءاً من شركة تعتمد على الهواتف المحمولة لإدارة العمليات، فإنك عُرْضة للهجمات.

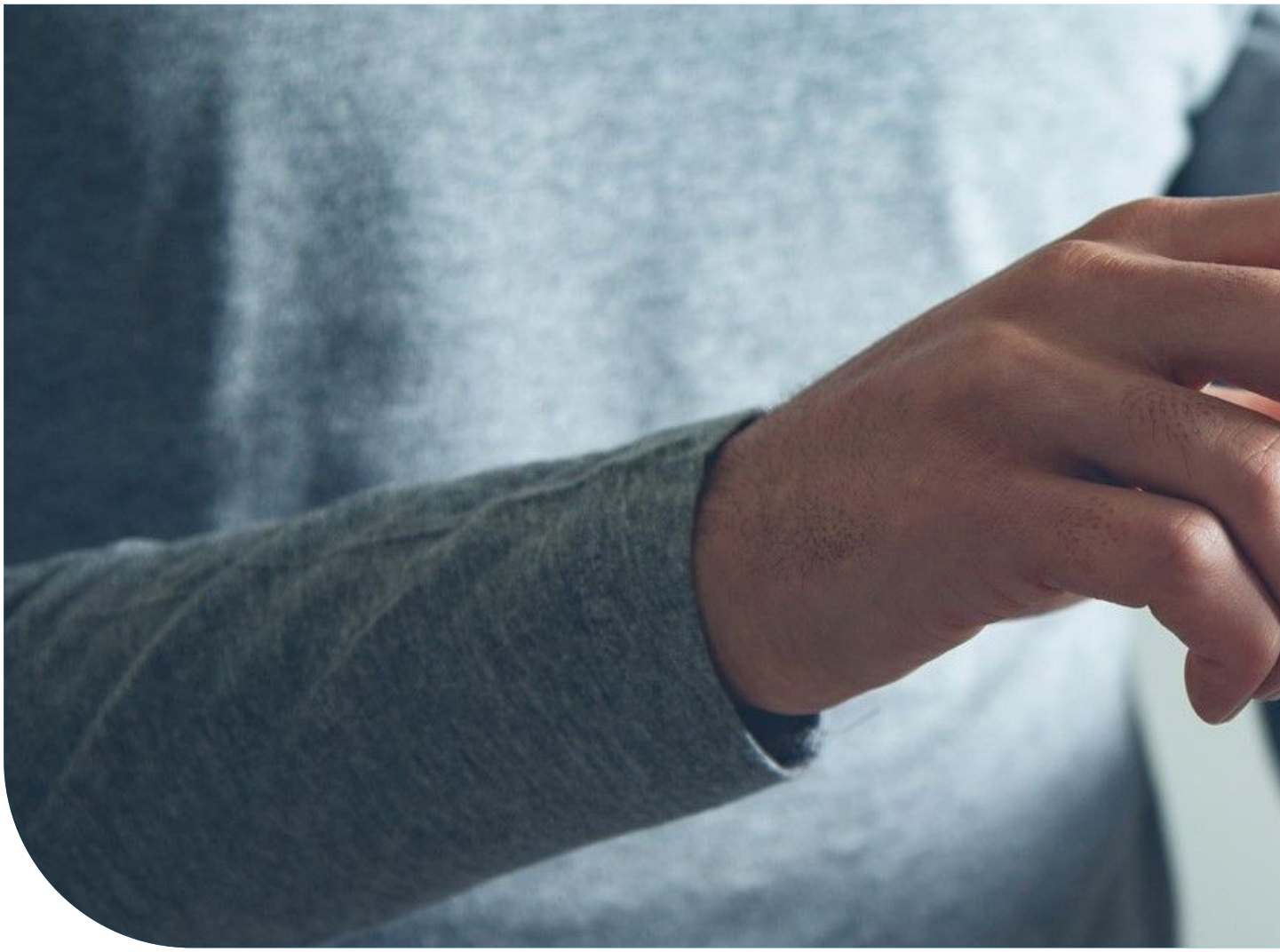
وتشــير التقارير إلــى أن قراصنــة الإنترنت يقومون باســتهداف الهواتف المحمولة بطــرق مختلفة؛ حيث يستغلون التطبيقات الشائعة لنشر البرمجيات الخبيثة.

1. Thies, Becca. The Rise of Mobile Malware, Spy Cloud, September 2024, on site: https://spycloud.com/blog/rise-of-mobile-malware/

كيف تستهدف البرمجيات الضّارّة أجهزتك المحمولة دون أن تلاحظ؟

أحد أبرز الأمثلة على ذلك هو انتشار تطبيقات مزيَّفة تبدو وكأنها أدوات أو برامج ترفيهية شرعية، ولكنّها في الواقع تحتوي على برمجيات خبيثة. بمجرد تنزيل هــذه التطبيقات، تبدأ البرمجيات الضارة في العمل دون أن يشــعر المستخدم، ممّا يُمكّن القراصنة من الوصول إلى المعلومات الحساســة مثل الحسابات البنكية، كلمات المرور، أو حتى القدرة على تسجيل المكالمات الصوتية والمرئية.

إذا تعرَّض هاتفك المحمول لهجومٍ ناجح باستخدام برمجيات خبيثة، يمكن أن تكــون النتائج كارثية. من ســرقة المعلومات الشــخصية والبيانــات المالية إلى التجسُّــس علــى كل ما تقوم بــه على جهازك، يمكن للقراصنة الاستفادة من هذه البيانات بطُرُق لا تتوقعها. في أســوأ الســيناريوهات، قد يتمكن المهاجمون من التحكم الكامل بالجهاز، مما يسمح لهم بمراقبة نشاطك، تســجيل مكالماتك، أو حتى الوصول إلى كاميرا هاتفك دون أن تدري.



الهجمات السيبرانية تنتقل إلى جيوبنا: البرمجيات الخبيثة تزداد تعقيداً على الهواتف الذكية

في ظل الاعتماد المتزايد على الهواتف المحمولة لإدارة حياتنا اليومية وأعمالنا، أصبح من الضروري حماية أجهزتنا من التهديدات السيبرانية المتزايدة.

الهجمات باستخدام البرمجيات الخبيثة على الهواتف المحمولة أصبحت أكثر تعقيداً واستهدافاً، مما يتطلّب من المستخدمين والشركات، على حدّ سواء، اتخاذ إجراءات وقائية لحماية بياناتهم وحياتهم الرقمية. ومن خلال اتباع أفضل الممارسات الأمنية وتوخّي الحذر عند تحميل التطبيقات أو التعامل مع الرسائل المشبوهة، يمكن تقليل خطر التعرُّض للهجمات السيبرانية والبرمجيات الخبيثة.

اختراق أرشيف الإنترنت:
تسريب بيانات 31 مليون مستخدِم

أرشيف الإنترنت يتعرض لهجوم سيبراني.. بيانات 31 مليون مستخدم في خطر!

تعرَّض أرشـيف الإنترنت (The Wayback Machine)، واحد من أكبر المكتبات الرقمية في العالم، لهجوم سـيبراني خطير أثّر على بيانات أكثـر من 31 مليون مسـتخدِم. هذا الخرق الأمني يُعـدّ مِن بين أكبر الهجمات التي تَسـتهدف المنصات الرقميـة العملاقة التي تحتفظ بكميـات هائلة من المعلومات الرقمية. وقـد أدى هذا الحادث إلى تسريب بيانات شخصية للمستخدمين بما في ذلك معلومات تسجيل الدخـول، مما أثار موجة من القلق حول مدى أمان هذه المنصة التي يستخدمها الملايين في جميع أنحاء العالم.

اختـــراق أرشـــيف الإنترنـــت: تفاصيـــل الهجـــوم وتأثيـــره علـــى المستخدمين حول العالم

الهجوم السيبراني الذي استهدف The Wayback Machine لـــم يكن مجرد حادثة صغيرة، بل شـــكّل صدمـــةً كبيرةً للمســـتخدمين الذين يعتمدون على هـــذه المنصـــة للوصول إلى مجموعـــة ضخمة من المحتويات الرقمية، بما في ذلك الكتب، المقالات، والأفلام.

ووفقـــاً للتقارير، فقد تمكّـــن القراصنة من الوصول إلى بيانات التســـجيل الخاصة بالمستخدمين، والتي قد تشمل عناوين البريد الإلكتروني وكلمات المرور. وما يزيد من خطورة الأمر هو أن بعض المستخدمين يمكن أن يكونوا قد استخدموا نفس بيانات تسجيل الدخول على منصات أخرى، مما يُوسّع نطاق التأثير ويُعرّض حسابات أخرى للخطر[1].

حتى الآن، لم تكشف المنصة عن التفاصيل الدقيقة لكيفية حدوث الاختراق، لكن من الواضح أن القراصنة استغلوا ثغرة أمنية تمكنوا من خلالها من الوصول إلى قاعـــدة بيانـــات المســـتخدمين. وبينما تعمل الفِرَق التقنية على تحديد أبعاد الاختراق وتصحيحه؛ فإن هذا الحـــادث يُعيد إلى الأذهـــان أهمية تأمين الأنظمة الرقمية وتحديثها بشـــكلٍ مستمرّ لتجنُّب مثل هذه الهجمات.

بالإضافـــة إلـــى تســـريب البيانات الشـــخصية، فإن الاختـــراق قـــد يؤثر على ثقـــة المســـتخدمين في منصات الأرشـــيف المفتوح، خاصة تلك التي تعتمد على التبرعات والمشاركة المجتمعية. في حال تأكيد أن البيانات المسربة تشمل معلومات حساسة، قد يضطـــر المســـتخدمون إلى تغيير كلمـــات مرورهم في حســـابات أخرى لتجنُّب المزيـــد من الأضرار. كما أن هـــذا الحادث يُعيد الجدل حـــول أهمية الاعتماد على تقنيات أمـــان متقدّمة مثل المصادقة الثنائية لحماية الحسابات الشخصية.

هذا الاختراق يُشكّل جرس إنذار جديداً للمؤسسات والأفراد على حدّ ســـواء بأهميـــة الحفاظ على أمن المعلومات، وضرورة اتخاذ التدابير الوقائية لتجنُّب الوقوع في فخاخ الهجمات السيبرانية المتكرّرة.

1. Abrams, Lawrence. Internet Archive hacked, data breach impacts 31 million users, Bleeping Computer, october 2024, on site: https://www.bleepingcomputer.com/news/security/internet-archive-hacked-data-breach-impacts-31-million-users/

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

للتواصل مع إدارة التميُّز السيبراني الوطني

00974 404 663 79

00974 404 663 62

www.ncsa.gov.qa/

cyberexcellence@ncsa.gov.qa