الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

السلامة الرقمية

العدد الرابع
الخميس 7 من ربيع الآخر 1446هـ
الموافق 10 أكتوبر 2024م

تغريم موقع نووي بريطاني
بسبب ثغرات في الأمن السيبراني

هجوم سيبراني
يؤدّي إلى تعطيل MoneyGram لمدة خمسة أيام

ثغرة خطيرة في Zimbra
تُستغل لتنفيذ تعليمات برمجية عن بُعْد

برمجيات خبيثة
تُنشَر عبر تحديثات مزيَّفة للمتصفح

خرق بيانات FBCS
يُؤثّر على Comcast وTruist Bank

> **دلال العقيدي**
> المبادرة الوطنية للسلامة الرقمية تواكب التطورات السيبرانية الدولية

المحتويات

المبادرة الوطنية للسلامة الرقمية

تواكب التطورات السيبرانية الدولية

يشـــهد الفضاء الســـيبراني تطورات متســـارِعة، وتترافـــق بزيادة هائلة في التهديدات الســـيبرانية التي تُواجه الدُّوَل والمؤسسات والمجتمعـــات والأفراد. وفي ظل هذه التطورات المتســـارِعة، لا بدَّ من تحصين المجتمع من خلال تبنّي مبادرات وأنشـــطة وبرامج توعوية في الأمن الســـيبراني والسلامة الرقمية، وهذا ما ترجمته الوكالـــة الوطنية للأمن الســـيبراني من خلال المبـــادرة الوطنية للسلامة الرقمية.

إنّ معـــدل التطـــور الســـريع في الفضـــاء الســـيبراني يفرض على المؤسســـات الرســـمية المعنيَّة بتعزيز الأمن الســـيبراني مواكبة هـــذه التطورات؛ علـــى اعتبار أن المعارف الســـيبرانية الفعَّالة في الوقـــت الراهن قد لا تكون ذات الفاعلية في المســـتقبل القريب، وهـــذا ما توليـــه الوكالة أهميةً كافيةً، وتحـــرص على تطبيقه في مختلف أنشطة وفعاليات المبادرة، وذلك من خلال مواكبة تطوُّر التهديدات الســـيبرانية، وتحقيق هـــذا الأمر من خلال الحرص على تقديم محتوى توعوي بالغ الحداثة.

كما حرصت المبادرة الوطنية للسلامة الرقمية على تقديم محتوى توعوي حديـــث من خلال عدَّة تقنيات، منها إعداد عدَّة دراســـات علميـــة، منها ما اهتم بتحليل أنشـــطة المراكز البحثية الدولية في مجال السلامة الرقمية، ودراسات أخرى حلَّلت أبرز التجارب الدولية فـــي مجال السلامة الرقمية. ومن خلال هذه الدراســـات اطَّلعت الوكالة وبدقَّة على الاتجاهات الدولية الحديثة في مجال السلامة الرقمية، وحدَّدت بشكل دقيق ومُمَنهج طبيعة المحتوى التوعوي المطلوب، والذي بالفعـــل يُقدّم قيمةً مضافةً توعوية للمجتمع، ويســـهم بشـــكل فعَّال في تحقيق أهداف المبادرة وبلوغ رؤيتها ورسالتها.

دلال العقيدي

مدير إدارة التميز السيبراني الوطني

ثغرة خطيرة في Zimbra تُستغل لتنفيذ تعليمات برمجية عن بُعْد

في أوائل أكتوبر 2024، تمَّ الكشف عن ثغرة خطيرة في برنامج Zimbra للبريد الإلكتروني، وهي ثغرة تسمح للمهاجمين بتنفيذ تعليمات برمجية عن بُعْد (RCE) على الخوادم المستهدَفة. وتُعدّ Zimbra واحدة من أكثر الحلول شيوعاً لإدارة البريد الإلكتروني، خاصةً للشركات الصغيرة والمتوسطة. استغلال هذه الثغرة يُمثّل خطراً كبيراً؛ حيث يُتيح للمهاجمين إمكانية الوصول إلى خوادم البريد الإلكتروني دون الحاجة إلى بيانات اعتماد.

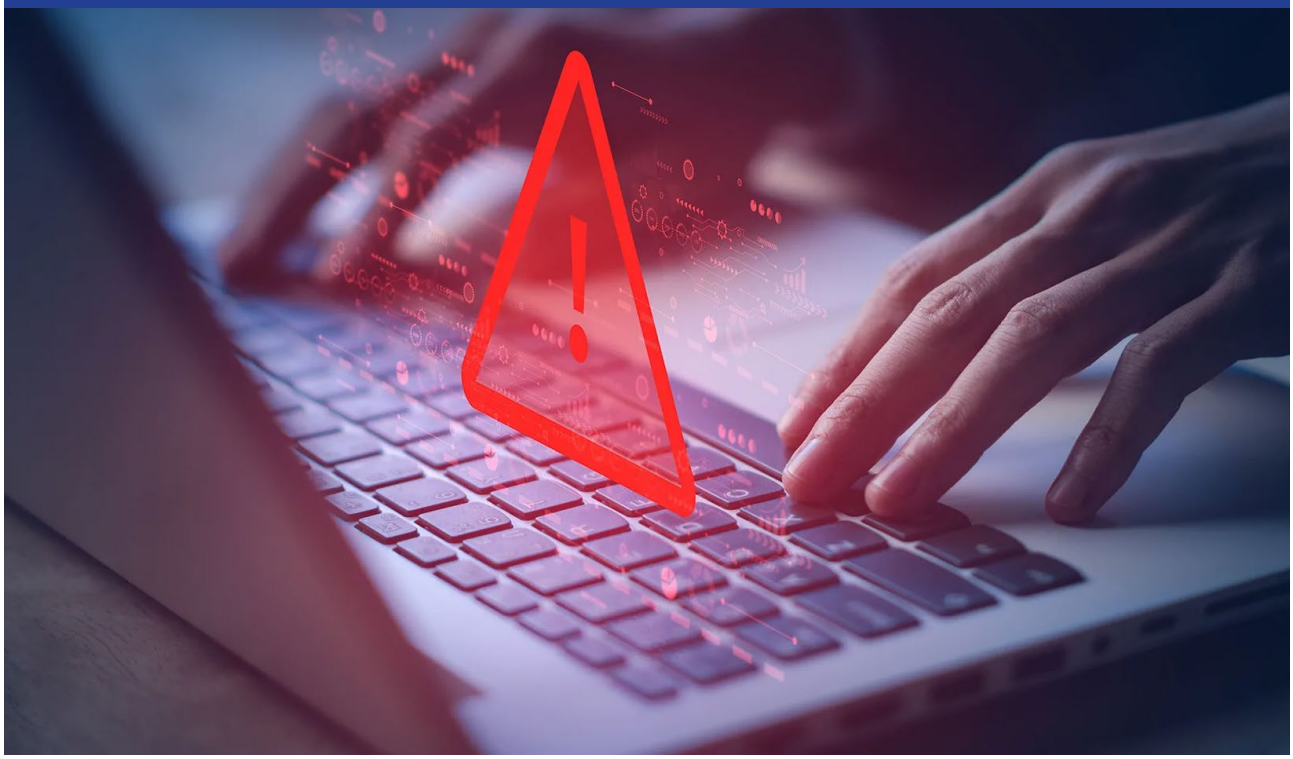
ثغرة خطيرة في Zimbra تهدّد آلاف الشركات باستغلال تعليمات برمجية عن بُعْد

تُمكّن الثغرة المهاجمين من إرسال طلبات HTTP مُعدَّة بشكل خاص إلى خوادم Zimbra، مما يسمح بتنفيذ تعليمات برمجية على النظام المتضرّر. هذه التعليمات البرمجية يمكن أن تشمل تحميل ملفات ضارَّة، الوصول إلى بيانات المستخدمين، أو حتى التحكم الكامل بالخادم. وتعتبر هذه الهجمات ذات طابع خطير، لا سيما أن البريد الإلكتروني يُمثّل وسيلة اتصال حيوية للشركات، وأي استغلال لثغرات في هذه الأنظمة يمكن أن يؤدي إلى سرقة معلومات حسّاسة أو تعريض أعمال الشركات للشلل[1].

وفقاً للتقارير، بدأت بعض المجموعات السيبرانية بالفعل في استغلال هذه الثغرة، ما أدَّى إلى تسريع الجهود لتطوير تحديثات أمنية وإطلاقها. المستخدمون الذين لم يقوموا بتحديث أنظمتهم في الوقت المناسب مُعرَّضون بشكلٍ كبيرٍ لمخاطر الاستغلال. في بعض الحالات، كانت الهجمات تَستهدف بالأساس المؤسسات الحكومية والمالية؛ حيث يتم توجيه المهاجمين إلى خرق خوادم البريد الإلكتروني بهدف التجسس أو تعطيل الخدمات.

1. Jones, Connor. Zimbra mail servers under siege through RCE vuln, The Register, October 2024, on site: https://www.theregister.com/2024/10/02/mass_exploitation_of_zimbra_rce/

مهاجمون يستغلّون ثغرة في Zimbra للوصول إلى خوادم البريد الإلكتروني



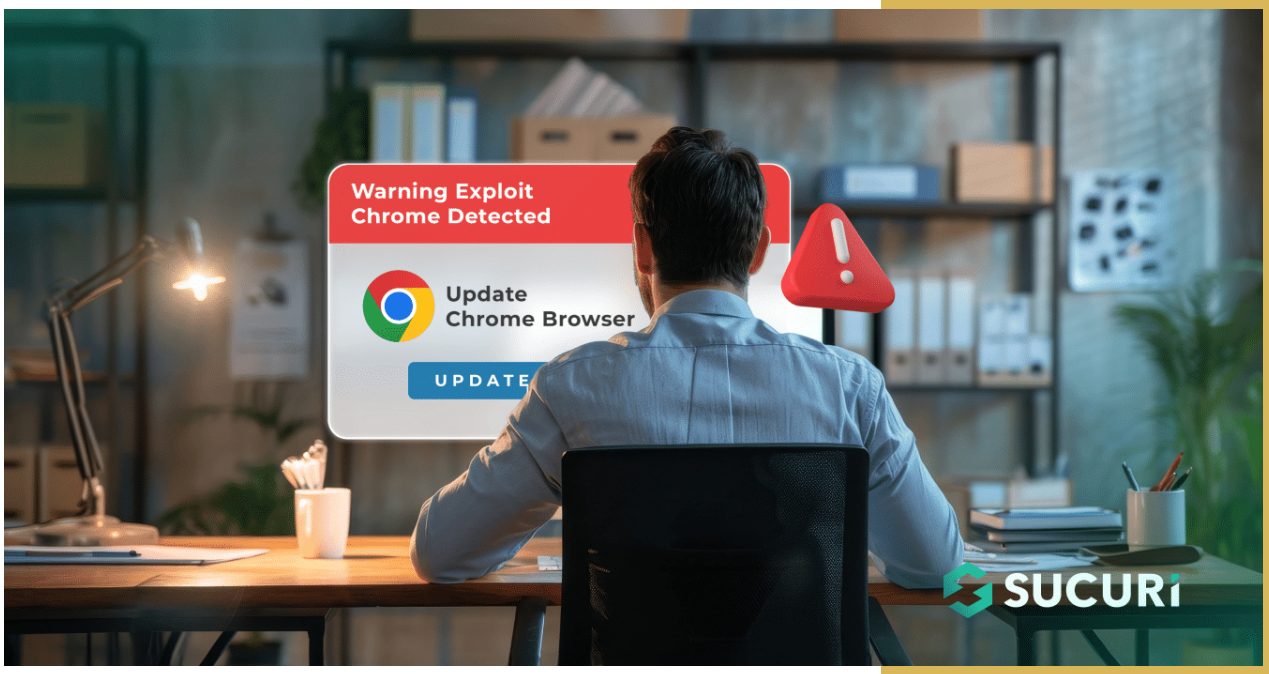
هذه الثغرة الأمنية أثارت القلق الكبير نظراً لانتشار استخدام Zimbra في مختلف القطاعات. وتعتمد الشركات الصغيرة والمتوسطة بشكل كبير على هذا البرنامج بسبب كُلفته المنخفضة وفعاليته، ولكن مع ذلك فإن ثغرات من هذا النوع تكشف عن نقاط الضعف في البرامج ذات الاستخدام الواسع، والتي تتعرَّض بشكل دائم لهجمات سيبرانية. بالإضافة إلى ذلك، من المعروف أن مهاجمي الفدية يستغلّون مثل هذه الثغرات لطلب فدية مقابل استعادة البيانات المسروقة، أو عدم نشرها على الإنترنت[1].

وقد أصدرت شركة Zimbra تحديثاً أمنياً عاجلاً لسدّ هذه الثغرة، وحثَّت جميع المستخدمين على تحديث أنظمتهم فوراً. وأكدت الشركة أن تجاهل هذا التحديث قد يُعرّض خوادم البريد الإلكتروني لمخاطر جسيمة، بما في ذلك سرقة البيانات أو حتى الاستخدام الخبيث للأنظمة المخترقة.

في الختام، يُمثّل اكتشاف هذه الثغرة في Zimbra تحذيراً آخر للشركات بضرورة الاهتمام بتأمين أنظمتها التكنولوجية. ويتعين على الشركات أن تتعامل مع التهديدات السيبرانية بجدية تامة، وأن تكون مستعدَّة دائماً للتعامل مع أيّ تهديدات جديدة، خاصةً في ظل ازدياد تعقيد وتنوع الهجمات السيبرانية.

1. Toulas, Bill. Critical Zimbra RCE flaw exploited to backdoor servers using emails, Bleeping Computer, October 2024, on site: https://www.bleepingcomputer.com/news/security/critical-zimbra-rce-flaw-exploited-to-backdoor-servers-using-emails/

برمجيات خبيثة
تُنشَر عبر تحديثات مزيَّفة للمتصفح



احــذر! تحديثــات متصفّح مزيَّفة تنشــر برمجيات خبيثة تسرق بياناتك الحساسة

مؤخراً تم اكتشاف حملة سيبرانية واسعة النطاق تستخدم تحديثات مزيفة للمتصفح لنشــر برمجيات خبيثة على أجهزة المستخدمين. هذه الحملة تعتمد على خداع المستخدمين برسائل منبثقة تدَّعي أن متصفحهم يحتاج إلى تحديث أمني عاجل. وعندما يقوم الضحية بالنقر على هذه الرســائل وتثبيت التحديث "المزعوم"، يتم تحميل برمجيات خبيثة في الخلفية دون عِلْم المستخدم.

تستغل هذه البرمجيات الخبيثة ثقة المستخدمين في المتصفحات الشــهيرة مثــل Chrome وFirefox وEdge؛ حيــث يتــم تقديم التحديث بشــكل يبدو شــرعياً تماماً من الناحية البصرية. لكن في الواقع، التحديث ليس إلا واجهة زائفة تم تصميمها خصيصاً لخداع المستخدمين، وإقناعهم بتنزيل برمجيات خبيثة.

تحديثات زائفة على Chrome وFirefox: كيف تستغل البرمجيات الخبيثة ثقة المستخدمين؟

فـور التثبيـت، يقـوم البرنامـج الخبيث بسـرقة بيانات حسّاسـة مثـل: كلمات المـرور، معلومات البطاقـات البنكيـة، وتفاصيـل الحسـابات الشـخصية. في بعـض الحـالات، يتم اسـتخدام البرمجيـات الخبيثـة أيضـاً لتنفيذ هجمـات أخرى مثل: هجمات الفديـة (Ransomware) ، أو توفير بـاب خلفـي للمهاجميـن للوصول إلى الشـبكات المستهدَفة[1].

يُعتقَـد أن هذه الحملة تسـتهدف المسـتخدمين فـي مناطـق جغرافية متعـدّدة، مع تركيـزٍ خاصّ على الشـركات الصغيرة والأفراد الذين لا يملكون أنظمة حماية متقدّمة. وتعتمد الحملة على تقنيات الهندسـة الاجتماعيـة (Social Engineering)؛ حيث يتم تضليل المستخدمين بالاعتماد على حاجة المتصفحـات للتحديثـات الدورية بهدف تحسـين الأداء وزيـادة الأمـان. المهاجمـون يعرفـون أن المسـتخدمين يميلون إلى قبول التحديثات بشكل آلي دون تدقيق في المصدر أو التأكد من مصداقية الرسائل التي تظهر على شاشاتهم[2].

تشير التقارير إلى أن هذه الحملة الخبيثة أصبحت أكثر شيوعاً بفضل استخدام المهاجمين لشبكات إعلانية مشروعة لعرض رسائل التحديث المزيفة على مواقع الويب الشـهيرة. كما تم اكتشاف أن بعض الرسائل المنبثقـة ظهرت على مواقع مشـهورة، مما يزيد من إحسـاس المسـتخدمين بالثقة في التحديثات المزيفة. كما أن بعض المهاجمين قد يسـتهدفون صفحـات ويب معينة تحظـى بتقييم عالٍ من حيث الأمان؛ لتقليل الشكوك لدى المستخدمين.

شـركة Google وMozillag، الشـركات المسؤولة عن تطوير متصفحـات Chrome وFirefox، قامتا بإصدار تحذيرات رسـمية لمستخدميهم حول هذه التحديثـات المزيفـة، وحثّتهـم على توخّـي الحذر والتأكُّـد من مصـدر التحديثـات قبل القيـام بأيّ تثبيت. كما قامت شركات الأمن السيبراني بإطلاق تحذيرات مماثلة، مع تزويد المستخدمين بإرشادات حول كيفية التعامل مع رسائل التحديث المشبوهة.

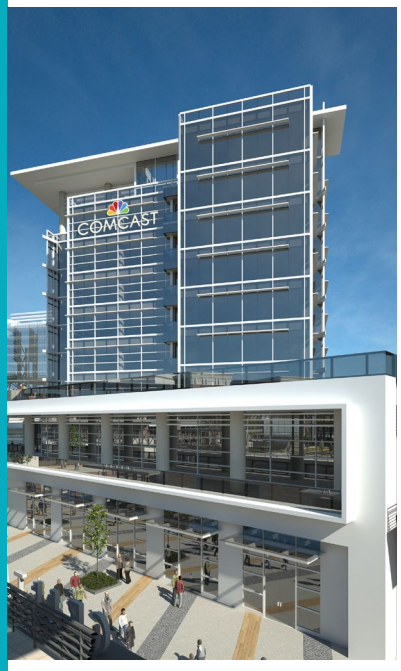
فـي النهاية، أبـرزت هذه الهجمـات أهمية الوعي السـيبراني؛ حيث إن المهاجمين يعتمدون بشـكل كبير علـى التلاعب النفسـي والإغـراءات التقنية لخداع المستخدمين. لذلك أصبح التعليم المستمر للمسـتخدمين حول المخاطر السـيبرانية وكيفية تجنُّبهـا ضرورة فـي ظل تزايـد وتنـوع الهجمات السيبرانية.

1. Toulas, Bill. Fake browser updates spread updated WarmCookie malware, , Bleeping Computer, October 2024, on site: https://www.bleepingcomputer.com/news/security/fake-browser-updates-spread-updated-warmcookie-malware/
2. Fake browser updates spread updated WarmCookie malware, Community.Riskiq, October 2024, on site: https://community.riskiq.com/article/a850b55a

خرق بيانات FBCS

يؤثّر على Truist Bankg Comcast

في شـــهر أكتوبر الجاري، وقع خرق بيانات ضخم في شركة FBCS، وهي شـــركة خدمات تحصيل الديون، مما أثّر بشـــكل مباشـــر على شـــركات كبيـــرة مثـــل Comcast Truist Bankg؛ حيـــث تمكّـــن المهاجمـــون من الوصول إلى بيانات حساســـة تشـــمل معلومات شخصية للعملاء مثل الأسماء، العناوين، أرقام الضمان الاجتماعي، وتفاصيل الحســـابات البنكيـــة. ويُعدّ هذا الخرق جزءاً من سلســـلة هجمات اســـتهدفت شـــركات تعمل في مجال الخدمات المالية؛ حيث يُستخدم نوع من البرمجيات الخبيثة للتسلل إلى أنظمة FBCS والتمكن من الوصول إلى هذه البيانات.



خـــرق ضخـــم: بيانـــات Truistg Comcast Bank في خطر بعد هجوم ســـيبراني على شركة FBCS

تأثر كلّ من Comcast Truist Bankg بالخرق؛ لأنهما كانا يتعاملان مع FBCS لتحصيـــل الديون من العملاء. وهذا جعـــل معلومات عملائهما عُرْضة للخرق، مما أثار مخاوف بشـــأن الأمن السيبراني لشركات الطرف الثالث، وكيفية تأثيره على مؤسســـات كبيرة. ويُعدّ هذا الهجوم واحداً من سلسلة من الهجمات التي تُركّز على الوصول إلى شركات الخدمات المالية، والتي تُعتبر مســـتودعات ضخمة للمعلومات الحساســـة التي يمكن استغلالها لعمليات احتيال أو سرقة الهوية[1].

1. Roth, Emma. Data breach leaks SSNs of over 230,000 Comcast customers, The Verge, , October 2024, on site: https://www.theverge.com/2024/10/7/24264283/comcast-fcbs-data-breach-ssn-names

خرق معلومات حساسة عبر FBCS يهدّد الأمن السيبراني لعملاء Truist Bankو Comcast

بمجرد اكتشـاف الخرق، قامت الشركات المتضرّرة بإخطار العـملاء، وحثّتهم على مراقبة حسـاباتهم البنكية، والتأكد من عدم وجود أيّ أنشطة مشبوهة. كما قدّموا خدمات مراقبة الائتمان بشـكل مجاني لمتضرّري الخرق؛ لضمان أن المعلومات المسروقة لا تُستخدَم في أنشـطة غير قانونية. في المقابل، أطلقـت FBCS تحقيقاً داخلياً، وبـدأت العمل مع شـركات الأمن السـيبراني لتحديـد كيفية حدوث الخرق، واتخاذ تدابير لمنع وقوع حوادث مشـابهة في المستقبل.

التحليـل الأولي يُشـير إلى أن الهجوم قـد تم عبر استغلال ثغرة في النظام الأمني للشركة، ما سمح للمهاجمين بالدخول إلى الشـبكة الداخلية، والبدء في سـرقة البيانات. مثل هذه الهجمات تكشـف عن مدى أهمية تأمين شـبكات الشركات الصغيرة والمتوسـطة، خاصة تلك التي تتعامل مع شركات أكبر وتحتفظ ببيانات حسّاسة لعملائها[1].

الهجمات السيبرانية على مثل هذه الشركات تؤكد أن الأمن السـيبراني ليس مجرد مسـؤولية شركة واحدة، بل هو سلسلة متصلة تحتاج كلّ حلقة فيها إلى تعزيز وسائل الأمان؛ لضمان حماية البيانات في العصر السيبراني.

1. FBCS Breach Exposes Millions, Comcast and Truist Bank Affected, Soc Radar, October 2024, on site: https://socradar.io/fbcs-breach-exposes-millions-comcast-and-truist-bank/

هجوم سيبراني يؤدّي إلى
تعطيل MoneyGram لمدة خمسة أيام

تعرَّضت شـركة MoneyGram لهجوم سيبراني أدَّى إلى تعطيل خدماتها لمدة خمسـة أيـام، ممَّا أثَّر علـى قدرتها على إجراء التحـويلات المالية. ويُعتقَد أن الهجوم كان مُدبَّراً باستخدام برمجيات خبيثة تستهدف أنظمة الشركة الأساسية، مما أدَّى إلى توقُّف العمليات التجارية في العديد من فروع الشركة حول العالم.

الهجوم تسبَّب في توقُّف مؤقَّت لقدرة المستخدمين على إرسال الأموال أو استلامها، مما أحدَث فوضى بين العملاء الذين يعتمدون على خدمات MoneyGram بشكل يومي.

خرق سـيبراني ضخم: توقُّف تام لخدمات MoneyGram وسـط تحقيقات مستمرة حول هجوم فدية

التحقيقات الأولية أشارت إلى أن الهجوم استهدف النظام الرئيسـي للشـركة من خلال ثغرة أمنية غير معروفـة حتـى الآن؛ حيث تمكَّـن المهاجمون من الوصول إلى الشبكة، وتعطيل الخوادم المسؤولة عـن معالجة التحـويلات المالية. لم يتم الكشـف عن الجهة المسـؤولة عن الهجوم، ولكن يُعتقَد أن الجريمة السـيبرانية تهدف إلى الابتزاز المالي؛ حيث طالب المهاجمـون بفدية كبيرة مقابل اسـتعادة النظام إلى وضعه الطبيعي. هذا النوع من الهجمات، المعروف بهجمات الفدية (Ransomware)، أصبح شـائعاً بشكل متزايد، ويُعتبر تهديداً كبيراً للشركات التي تعتمد على العمليات الرقمية[1].

هجـوم سـيبراني يشـلّ خدمـات MoneyGram ويُوقف التحويلات المالية لمدة خمسة أيام!

على مدى خمسة أيام، كانت MoneyGram تعمل على استعادة النظام وتأمين البنية التحتية الخاصة بهـا. وأصدرت الشـركة تصريحات دوريـة للعملاء؛ حيث اعتذرت عن الإزعاج، وأكدت أنها تبذل قصارى جهدها لاستعادة الخدمة. ومع ذلك، فقد أثَّر بشدة على العديد من المسـتخدمين، خاصةً في البلدان النامية؛ حيـث يعتمد الناس على تحويلات الأموال لدعم أسرهم وتلبية احتياجاتهم اليومية.

بالإضافـة إلى التعطيل، أثـار الهجوم أيضاً مخاوف بشـأن أمـن المعلومات فـي شـركات الخدمات المالية الكبرى مثل MoneyGram تُواجه الشركات التي تُدير عمليات تحويل الأموال مسؤوليات كبيرة في حمايـة بيانات العـملاء والحفاظ على سـرية التحـويلات. الهجمات من هذا النـوع لا تُؤثّر فقط على العمليات اليومية، بل تضع أيضاً سمعة الشركة وثقة العملاء في خطر[2].

الهجوم علـى MoneyGram يُسـلّط الضوء على التحديـات الكبيرة التي تواجهها الشـركات المالية في العصر السـيبراني؛ حيث تصبح البيانات والنظم الإلكترونية أهدافاً رئيسـية للهجمات السـيبرانية. كما يُظهـر أهمية تطوير إسـتراتيجيات اسـتجابة سـريعة وفعّالة لضمان عدم تأثير الهجمات بشكل كبير على العملاء والعمليات التجارية.

1. Schappert, Stefanie. MoneyGram cyberattack leads to days-long outage, unprocessed payments, cyber news, September 2024, on site: https://cybernews.com/news/moneygram-cyberattack-outage-unprocessed-payments/
2. Fadilpašić , Sead. MoneyGram says no evidence ransomware is behind recent cyberattack, Tech Radar, October 2024, on site: https://www.techradar.com/pro/security/moneygram-says-no-evidence-ransomware-is-behind-recent-cyberattack

مدارس Highline

تُغلق أبوابها بسبب هجوم فدية

هجوم ســـيبراني يُعطِّل النظام المدرســـي في واشـــنطن ويفرض إغلاقاً غير مسبوق!

تعرَّضت مدارس Highline في واشـــنطن لهجوم فدية ســـيبراني تسبَّب في إغلاق المدارس لعدة أيام. المهاجمون استهدفوا الأنظمة التكنولوجية الخاصة بالمقاطعة التعليمية، مما أدَّى إلى تعطيل الوصول إلى الشـــبكات الحيوية المستخدَمة لتشغيل العمليات المدرسية اليومية، مثل الجدولة، حضور الطلاب، وأنظمة الاتصال بين المدارس والأهل. كما تم تعطيل الفصول الدراســـية تماماً؛ بسبب عدم القدرة على تشغيل البرامج التعليمية الرقمية، والتي تعتمد عليها المدارس بشكل كبير في عمليات التعليم والتقييم.

الجهة المسؤولة عن الهجوم طلبت فدية كبيرة مقابل استعادة الأنظمة وإعادة تشغيلها، وهو ما أثار قلقاً كبيراً بين الأهل والطلبة والإدارة. وأدّى الإغلاق إلى تعطيل التعليم وتوجيه ضربة قوية للمجتمع التعليمي؛ حيث تعتمد هذه المدارس بشكل كبير على التكنولوجيا لإدارة اليوم الدراسي في ظل اعتماد متزايد على التعلم الرقمي. وتمثل الهجمات السيبرانية مثل هذه تهديداً حقيقياً للمؤسسات التعليمية التي قد لا تمتلك دائماً بنية تحتية قوية للأمن السيبراني مثل المؤسسات المالية أو الشركات الكبيرة[1].

كردّ فِعْل سريع، قامت إدارة المدارس بالتواصل مع خبراء الأمن السيبراني والشركات المختصة لاستعادة السيطرة على الأنظمة. ومع ذلك، استغرق الأمر عدة أيام لإعادة الأنظمة إلى وضعها الطبيعي، وخلال هذه الفترة تم تعليق الحصص الدراسية والتقييمات؛ مما أدّى إلى حالة من الفوضى والتأخير في البرنامج التعليمي. كما قامت المقاطعة بإصدار بيانات للأهل والطلبة، موضِّحةً فيها الوضع وداعيةً إلى التحلّي بالصبر حتى تتم استعادة الأنظمة بالكامل.

هذا الهجوم يعكس التحديات المتزايدة التي تواجهها المؤسسات التعليمية في مواجهة تهديدات هجمات الفدية. على الرغم من التقدم التكنولوجي الهائل الذي تم إدخاله إلى القطاع التعليمي، إلا أن هذا التقدُّم يصاحبه تهديدات جديدة تجعل المدارس عُرْضة للهجمات. وتزداد الحاجة إلى تعزيز الأنظمة الأمنية للمؤسسات

هجوم فدية سيبراني يُغلق مدارس Highline ويُعطِّل التعليم الرقمي بالكامل!

التعليمية، وتوفير موارد أكبر للحماية من الهجمات السيبرانية التي تُهدّد العملية التعليمية بأكملها.

وتُعدّ حادثة مدارس Highline تذكيراً مهماً بضرورة التحصين ضد هذه الهجمات؛ من خلال الاستثمار في الدفاعات السيبرانية، والتدريب المستمر للموظفين، واتباع إستراتيجيات استجابة سريعة للأزمات السيبرانية. ومن المهم أن تظل المؤسسات التعليمية متأهبة ومستعدَّة لتفادي هذه الهجمات، أو الحد من تأثيرها على أكبر عدد ممكن من المستويات.

1. Bazzaz, Dahlia. Hackers target Seattle-area school district for ransomware attack, The Seattle Times, October 2024, on site: https://www.seattletimes.com/education-lab/hackers-target-seattle-area-school-district-for-ransomware-attack/

تغريم موقع نووي بريطاني

بسبب ثغرات في الأمن السيبراني

تــم تغريم موقع نووي بريطاني مبلغاً كبيراً نتيجة لثغرات خطيرة في أنظمته للأمن الســيبراني، مما أثار القلق بشأن حماية البنية التحتية الحساسة في البلاد. ووفقاً للتحقيقات، فشلت الشركة المسؤولة عن الموقع في تأمين بياناتها بشــكلٍ كافٍ، مما جعل الأنظمة عُرضة للاختراقات السيبرانية. هذا الضعف أثار قلق الســلطات البريطانية، لا ســيما في ظل زيادة التهديدات الســيبرانية التي تستهدف البنية التحتية الحيوية مثل المنشآت النووية.

ضعف الأمن السيبراني في منشــأة نووية بريطانية يُؤدّي إلى غرامة ثقيلة وتحذيرات صارمة!

تم اكتشــاف الثغرات خلال عملية تفتيش روتينيــة أجرتها هيئة تنظيم الطاقــة النووية في المملكة المتحدة؛ حيــث تبين أن الأنظمة لم تكن محدَّثــة بشــكلٍ كافٍ، ولم تتبع أفضل الممارســات فــي الحماية من الهجمات الســيبرانية. إضافةً إلى ذلك، أشار التقرير إلى وجود قصور في تدريب الموظفين على التعامل مع التهديدات الســيبرانية، مما زاد من خطورة الموقف[1].

1. Martin, Alexander. Sellafield, UK's largest nuclear site, fined £330,000 for cybersecurity failings, The Record, October 2024, on site: https://therecord.media/sellafield-nuclear-site-cybersecurity-failings-fine

ثغرات سيبرانية خطيرة في موقع نووي بريطاني تُثير القلق!

الهجمـات السـيبرانية على البنيـة التحتية النووية تُشـكّل تهديداً خطيراً، ليس فقط على المسـتوى الأمنـي، ولكـن أيضاً من حيـث العواقـب البيئية والاقتصادية التي قد تحدث إذا تم اسـتغلال هذه الثغرات. بينما لم يتم الكشف عن أيّ محاولة ناجحة لخرق الموقع النووي؛ إلا أن الفشل في حماية هذه المنشآت يُمثّل خطراً جسـيماً قد يؤدي إلى وقوع كوارث محتملة في المستقبل.

الهيئـات المعنية بالأمن السـيبراني في المملكة المتحدة شدّدت على أهمية تعزيز تدابير الحماية في المواقع الحساسة، خاصةً في ظل التزايد المستمر للتهديدات السيبرانية التي تستهدف البنية التحتية الحيوية. وقد أصدرت توصيات بضرورة تنفيذ برامج تدريبية مكثّفة للعاملين، فضلاً عن تحديث الأنظمة الأمنية بانتظام لضمان عدم اسـتغلال أيّ ثغرة قد تؤدي إلى أضرار كارثية[1].

الشركة التي تدير الموقع النووي استجابت بسرعة لهذه التحذيرات، وأعلنت عن تنفيذ مراجعات شاملة لأنظمـة الأمن السـيبراني، مع التركيـز على تعزيز الحماية من التهديدات المحتملة. كما أوضحت أنها ستتعاون بشـكل كامل مع السلطات لضمان تلبية جميع معايير الأمان المطلوبة.

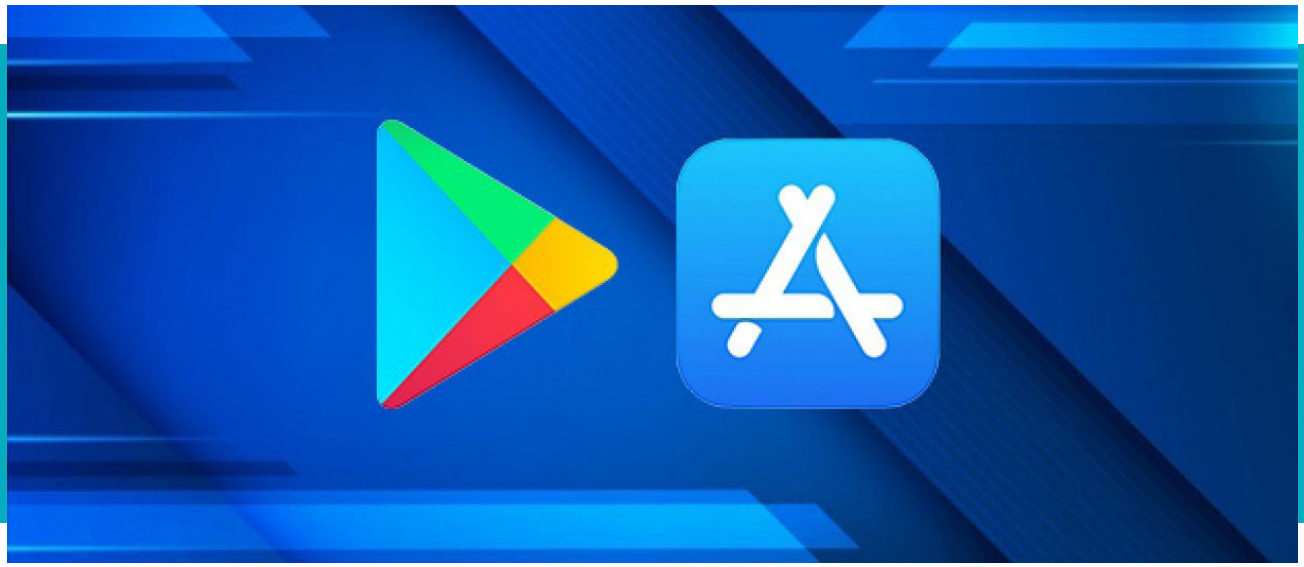
الخطوة المتّخذة بتغريم الموقع النووي البريطاني تعكس مدى التزام المملكة المتحدة بالحفاظ على مسـتوى عالٍ من الأمان السـيبراني في المواقع الحساسة، والتصدي بصرامة لأيّ تقصير قد يُعرّض الـبلاد للخطر. ومـع تزايـد الهجمات السـيبرانية العالميـة، أصبحت هذه الإجـراءات ضرورية لضمان حمايـة الأصول الوطنية والقدرة على التصدي لأيّ تهديدات مستقبلية.

1. UK's nuclear waste unit Sellafield fined for cybersecurity failings, Reuters, October 2024, on site: https://www.reuters.com/technology/cybersecurity/uks-nuclear-waste-unit-sellafield-fined-cyber-security-failings-2024-10-02/

تطبيقات احتيال Pig Butchering

تظهر على App Storeو Google Play

مؤخراً تم اكتشاف عدد متزايد من تطبيقات احتيال تحت اسم Pig Butchering تظهر على Google Play وApp Store. تعتمد هذه التطبيقات على تقنيات الاحتيال الاجتماعي لإقناع المستخدمين بالاستثمار في مشاريع وهمية، أو شراء منتجات غير موجودة.



في هذه الحِيَل، يتظاهر المحتالون بأنهم مرشدون ماليون أو شركاء عمل، ويستخدمون التطبيقات المزيَّفة لبناء ثقة طويلة الأمد مع الضحايا. بمجرد أن يثق المستخدِم، يتم حثّه على استثمار مبالغ مالية ضخمة في مشاريع استثمارية أو خدمات احتيالية.

تطبيقات Pig Butchering مستوحاة من تكتيك قديم في الاحتيال المالي؛ حيث يقوم المحتالون "بتسمين" الضحية بإغراقها بالوعود والمعلومات المغرية قبل أن يطلبوا منها مبلغاً كبيراً من المال. الضحايا غالباً ما يعتقدون أنهم يقومون باستثمارات مربحة، ولكن في الواقع، أموالهم يتم سرقتها. ما يزيد الأمر سوءاً أن هذه التطبيقات تبدو قانونية تماماً؛ لأنها متوفرة في متاجر التطبيقات الرسمية مثل Google Play وApp Store، مما يجعلها تبدو أكثر مصداقية للمستخدمين[1].

1. Google Play Store and Apple App Store hit by fraudulent trading apps in 'pig butchering' scheme, Indian Express, October 2024, on site: https://indianexpress.com/article/technology/tech-news-technology/google-app-app-store-fake-trading-apps-pig-butchering-9604982/

تحذير من تطبيقــات احتيال "Pig Butchering": اســتثمارك قد يكون فخّاً!

الســلطات الأمنية وشــركات التكنولوجيا تحاول مكافحة هذه التطبيقات بشكل سريع؛ حيث تقوم Google وApple بمراجعــة التطبيقــات على منصاتها، والتأكد من مصداقيتها، بالإضافة إلى تعزيز سياســات الأمان لمنع ظهور تطبيقات احتيالية جديدة. ورغم الجهود المتزايدة، لا يزال الكثير من المســتخدمين يقعون ضحايا لهذه الهجمات المتقدّمة؛ حيث يستخدم المحتالون أساليب جديدة ومعقَّدة لتجنُّب الاكتشاف.

تطبيقــات مزيَّفــة علــى App Store وGoogle Play تســتنزف أموالــك بخطط احتيالية!

واحدة من الطــرق التي يلجأ إليهــا المحتالون هي تصميــم تطبيقات متخصصة تبدو قانونية بشــكل كامل، وتقدم خدمات شائعة مثل إدارة الأموال أو تداول العملات الرقمية. بعد جذب المســتخدمين، يتــم تحويل الأمــوال إلى حســابات خارجية يصعب تعقُّبهــا، ويصبــح اســترداد الأمــوال أمــراً شــبه مستحيل[1].

يجب على المســتخدمين توخّي الحذر الشديد عند تحميــل أيّ تطبيقات مالية، خصوصاً إذا كانت تقدم وعوداً غيــر واقعية أو تطلب معلومات شــخصية حساســة. الخبراء ينصحــون بالتأكُّد مــن موثوقية المطوّريــن وقــراءة المراجعات بدقــة قبل تثبيت التطبيقــات. كما يجب عدم الوثوق بشــكلٍ كامل فــي التطبيقات الموجودة علــى متاجر التطبيقات الرسمية فقط؛ لأن وجودها هناك لا يعني بالضرورة أنها آمِنَة.

الحــملات التوعوية حــول هذا النوع مــن الاحتيال أصبحــت ضرورية مــع تزايــد اعتماد الأفــراد على التطبيقــات الإلكترونيــة لإدارة حياتهــم الماليــة. ويجب على المســتخدمين أن يكونــوا أكثر يقظةً، وأن يفكّروا بشــكلٍ نقديّ قبل القيام بأيّ اســتثمار عبر التطبيقات؛ خاصــةً تلك التي تبدو حديثة أو غير معروفة.

1. Lakshmanan, Ravie. Fake Trading Apps Target Victims Globally via Apple App Store and Google Play, The Hacker News, October 2024, on site: https://thehackernews.com/2024/10/fake-trading-apps-target-victims.html

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

للتواصل مع إدارة التميُّز السيبراني الوطني

00974 404 663 79
00974 404 663 62
www.ncsa.gov.qa/
cyberexcellence@ncsa.gov.qa