علوم وتكنولوجيا

4 طرق لربح المال من الإنترنت

يبحث كل منا عن وظيفة مناسبة لقدرات تساعده على تحقيق ذاته وجمع بعض الأموال، ولكن طبيعة الوظائف والاستيقاظ مبكراً والالتزام بمواعيد محددة والتعامل مع شخصيات من خلفيات مختلفة أمر قد يجعلك تفكر أكثر من مرة في البحث عن عمل حر، أو عن طرق للاستفادة من قدراتك في الربح من الإنترنت، وفيما يلي بعض الأمور التي يمكن أن تنجزها من منزلك.

مواقع PTC

إذا قررت تحقيق بعض الربح من الإنترنت، فعليك البحث عن مواقع PTC والتي تجعلك تملأ بعض الوثائق التي تستغرق من 5 إلى 30 دقيقة وفقاً لما تطلبه الشركة صاحبة تلك المسوح، وهناك وظيفة أخرى وهي الحصول على أموال مقابل البحث ونشر التعليقات المرتبطة بالتسويق على مواقع الويب مختلفة.

استضافة الإعلانات على مدونتك

القنوات التلفزيونية تجمع معظم أموالها من خلال الإعلانات، وإذا كان لديك موقع أو مدونة فيمكنك أيضا كسب مبلغ جيد من المال عن طريق استضافة الإعلانات، ولكن يجب أن تلتزم بمعايير المعلنين، وعندما يشاهد أحد الزائرين إعلاناً أو ينقر عليه عبر موقعك ستحصل تلقائياً على المال.

الريفيو

هناك العديد من الشركات التي تبحث عن طرق مختلفة لجعل منتجاتها أكثر شعبية، مثل الدفع لأشخاص لكتابة مراجعة جيدة عن تطبيق أو منتج ما على الإنترنت، ولكن هذا الأمر لا يحقق أموالاً جيدة في أغلب الأوقات، كما يُعتبر غير أخلاقي.

بيع الصور والفيديوهات

هناك طريقة أخرى لتحقيق الدخل من وقتك على الإنترنت عن طريق بيع أشياء مثل الصور والفيديوهات، فإذا كانت خاصة بأحداث هامة أو بجودة عالية فيمكن بيعها للوكالات التي توزعها بعد ذلك.

المصدر: (اليوم السابع)

باحثون أمنيون لبنانيون يكتشفون ثغرات في فيسبوك وخدماتها ويدرجون على لائحة الشرف

اكتشف ثلاثة شبان لبنانيون مختصون في مجال الأمن الإلكتروني ثغرات أمنية خطيرة في خدمات فيسبوك، الأمر الذي استحقوا لأجله تكريم الشركة التي سارعت إلى إصلاح الثغرات المكتشفة.

وقال فياض عطوي، وقاسم بزون، وحمزة بزون، في حوار إن الثغرات التي أبلغوا عنها تمت معالجتها وسُمح لهم بنشر تفاصيلها بعد الحصول على مكافأة مالية وإدراج اسم الفريق في لائحة شرف الموقع للعام2017.

وذكر الباحثون الأمنيون الثلاثة أن هناك المزيد من الثغرات الأمنية التي اكتشفوها ويجري العمل على إصلاحها في الوقت الراهن، لذا فليسوا مخولين بالإفصاح عنها قبل انتهاء عملية المعالجة.

أما فيما يتعلق بالثغرات، فأوضح الباحثون الذين يديرون شركة للبرمجة والحماية الإلكترونية باسم Semicolon Programming and Security أن الثغرة الأولى اكتشفت في تطبيق التراسل الفوري التابع لفيسبوك، مسنجر، وهي تستهدف كافة مستخدمي الخدمة، وتطبيقها على كافة المنصات، بما في ذلك نسخة الويب وتطبيقات الهواتف المحمولة.

وأضاف الباحثون أن خطورة هذه الثغرة تكمن في أنها تؤدي إلى إيقاف خدمة مسنجر ورسائل فيسبوك، وتمنع المستخدم من دخول تطبيق مسنجر أو موقعه الإلكتروني، إضافة إلى قسم الرسائل على الشبكة الاجتماعية، نهائيًا عبر تعطيل عمل الخادم المسؤول عن عرض الرسائل.

وبالنسبة للثغرة الثانية، فقد كانت في تطبيق مشاركة الصور المملوك لفيسبوك، إنستغرام، وهي تستهدف المستخدمين الذين يربطون حساباتهم مع موقع فيسبوك، وتؤدي الثغرة إلى الاستيلاء على حساب إنستغرام تمامًا وتغيير كافة إعداداته.

وأوضح الفريق أن هذه الثغرة موجودة تحديدًا في خاصية وصل صفحات فيسبوك بحساب إنستغرام التابع للصفحة، والتي لا يحق لأي مدير من مدراء الصفحة الدخول إليه أو تعديل إعداداته (ما عدا صاحب الحساب الأساسي).

ويرى الباحثون الأمنيون أن خطورة هذه الثغرة تكمن في إمكانية تطبيقها على الشخصيات العالمية ووسائل الإعلام وغيرها من الحسابات المؤثرة، واستحالة استرجاع الحساب دون تقديم طلب رسمي إلى إدارة فيسبوك.

واكتشف الباحثون ثغرة ثالثة في نظام المنشورات الخاص بمتابعي صفحات فيسبوك، وتكمن خطورتها في تجاوز بعض صلاحيات مدير الصفحة واستخدامها.

وأوضح الفريق أن هذه الثغرة تسمح لمن يريد نشر منشور مسيء على إحدى الصفحات فعل ذلك دون تحكم من مديرها، مع الإشارة إلى أن مديري الصفحات يقومون عادةً بحجب مثل تلك المنشورات عن باقي متابعي الصفحة أو تفعيل ميزة مراجعة المنشورات والموافقة على نشرها أو رفضه، ولكن هذه الثغرة تحول دون ذلك.

كاسبرسكي لاب تكتشف برمجية خبيثة تسرق أجهزة الصراف الآلي

بقلم: أحمد عبدالقادر

اكتشف باحثون خبراء لدى كاسبرسكي لاب برمجية خبيثة تستهدف أجهزة الصراف الآلي. وقالت الشركة إن البرمجية المسمّاة Cutlet Maker والتي تباع علناً في أسواق الشبكة المظلمة Dark-Net تتألف من ثلاثة مكونات وتمكّن القراصنة من إفراغ أجهزة الصراف الآلي من النقد من خلال القدرة على التحكم بآلية إخراج النقد من الجهاز، أو ما يُعرف بـ jackpotting، إذا استطاعوا الوصول شخصياً إلى تلك الأجهزة. وتباع المجموعة البرمجية هذه التي يمكن للقراصنة استخدامها لسرقة ما يصل إلى الملايين، مقابل 5,000 دولار فقط، بل إنها تأتي مزوّدة بدليل إرشادي يُبيّن طريقة الاستخدام خطوة بخطوة.

ولا تزال أجهزة الصراف الآلي أهدافاً مجدية للمحتالين واللصوص الذين يستخدمون أساليب مختلفة لاستخلاص أقصى قدر من الأرباح من عملياتهم التخريبية. وبالرغم من أن البعض يعتمد على أساليب تخريبية مادية كاستخدام أدوات قطع المعادن، يختار آخرون الإصابات التخريبية البرمجية التي تمكّنهم من التحكّم بأجهزة الصراف الآلي من الداخل. ويُظهر هذا الاكتشاف أن واضعي البرمجيات الخبيثة يستثمرون مزيداً من الموارد لجعل منتجاتهم متاحة حتى لمن هم ليسوا على دراية كافية بعلوم الحاسوب، وذلك على الرغم من أن الأدوات البرمجية الخبيثة المخصصة لاختراق أجهزة الصراف الآلي معروفة منذ سنوات عديدة.

وفي التفاصيل، قدّم أحد شركاء كاسبرسكي لاب لأحد الباحثين في الشركة، في وقت سابق من هذا العام، عيّنة لبرمجية خبيثة غير معروفة سابقاً من المفترض أنها تصيب أجهزة الحاسوب التي تعمل داخل أجهزة الصراف الآلي. واعترى الباحثين الفضول لمعرفة ما إذا كانت هذه البرمجيات الضارة، أو أية متعلقات بها، متاحة للشراء عبر منصات سريّة. وأسفر البحث عن القطع الفريدة الخاصة بالبرمجية الخبيثة عن العثور على إعلان يعرض بالوصف سلالة من البرمجيات الضارة بأجهزة الصراف الآلي على موقع ذي شعبية على الشبكة المظلمة، اسمهAlphaBay، وهو ما أفضى إلى كشف أن العينة الأولية تنتمي إلى مجموعة البرامج الخبيثة التجارية التي تم إنشاؤها بالكامل لمهاجمة أجهزة الصراف الآلي وسرقتها. كذلك وجد الباحثون إعلاناً عاماً نشره بائع برمجيات خبيثة، لا يقتصر محتواه على وصف البرامج الخبيثة والتعليمات بشأن كيفية الحصول عليها، وإنما يشمل تقديم دليل مفصل خطوة بخطوة حول كيفية استخدامها في شنّ الهجمات، مع تعليمات ودروس بالفيديو.

ووفقاً للبحث، تتكون مجموعة الأدوات البرمجية الخبيثة من ثلاثة عناصر:

برمجية Cutlet Maker، التي تُعد الوحدة الرئيسية المسؤولة عن التواصل مع جهاز إخراج النقود داخل أجهزة الصراف الآلي.

برمجية c0decalc، المصمم لتوليد كلمة مرور من أجل تشغيل تطبيق Cutlet Maker وحمايته من الاستخدام غير المصرح به.

تطبيق محفز، يوفر الوقت للمجرمين من خلال تحديد حالة العبوات الخاصة بحفظ النقد داخل الصراف الآلي. ويتلقى المهاجم، عن طريق تثبيت هذا التطبيق، معلومات دقيقة عن العملة والقيمة وعدد الأوراق النقدية في كل عبوة، ما يتيح له اختيار واحدة تحتوي على أكبر مبلغ، بدلاً من سحب العبوات بطريقة عمياء واحدة تلو الأخرى.

ويلزم القراصنة لبدء السرقة الوصول المباشر إلى داخل أجهزة الصراف الآلي من أجل الوصول إلى منفذ USB، الذي يُستخدم لتحميل البرمجيات الخبيثة عبر ربط قطعة ذاكرة عليها مجموعة الأدوات البرمجية الخبيثة. ويقوم المجرمون، كخطوة أولى، بتثبيت برمجية Cutlet Maker، ويستخدمون برمجية c0decalc المثبتة على جهاز آخر مثل حاسوب محمول أو جهاز لوحي في توليد كلمة مرور لحماية Cutlet Maker نظرا لأنها محمية بكلمة مرور، وذلك كنوع من الحماية لـ "حقوق التأليف" يتم تثبيتها من قبل مؤلفي Cutlet Maker لمنع المجرمين الآخرين من استخدامه مجاناً. وبعد إنشاء الشفرة البرمجية، يدخل المجرمون إلى واجهة استخدام Cutlet Maker للشروع في إفراغ الصراف الآلي من النقد.

ويُعتبر Cutlet Maker معروضاً للبيع منذ 27 مارس من العام الجاري، لكن حسبما اكتشف الباحثون، فإن أول عينة معروفة من هذه البرمجية الخبيثة كانت قد ظهرت لمراقبين من الأوساط الأمنية في شهر يونيو من العام الماضي 2016. في ذلك الوقت تمّ تقديمها إلى خدمة عامة متعدّدة الماسحات من أوكرانيا، ولكنها قدمت أيضاً في أوقات لاحقة من بلدان أخرى. وليس من الواضح ما إذا كان قد تم استخدام البرمجيات الخبيثة في هجمات واقعية، ولكن الإرشادات التوجيهية التي تضمنتها المجموعة البرمجية الخبيثة تحتوي على مقاطع فيديو قدّمها المؤلفون كدليل واقعي على كفاءة عملها.

ولا يُعرف من يقف وراء هذا النشاط الإجرامي، لكن تحليلاً للغة المستخدمة من الباعة المحتملين والأخطاء الإملائية والنحوية والأسلوبية التي ارتكبوها، يشير إلى كون الإنجليزية ليست لغتهم الأم.

ولا يتطلب تشغيل Cutlet Maker أية معرفة أو مهارات متقدمة في استخدام الحاسوب تقريباً، وفق ما قال كونستانتين زايكوف الباحث في الأمن الإلكتروني لدى كاسبرسكي لاب، الذي اعتبر أن هذه المجموعة البرمجية "استطاعت أن تحوّل قرصنة أجهزة الصراف الآلي من عملية هجومية معقدة إلى وسيلة غير قانونية لكسب المال متاحة عملياً أمام أي شخص يملك بضعة آلاف من الدولارات لشراء البرمجيات الخبيثة"، وأضاف: "قد يشكل هذا التحوّل تهديداً خطراً للمؤسسات المصرفية، ولكن ما هو أكثر لإثارة للقلق هو تفاعل البرمجية الخبيثة مع البرمجيات والأجهزة الخاصة بأجهزة الصراف الآلي من دون أن تواجه تقريباً أية دفاعات أمنية على الإطلاق، وهو ما ينبغي تغييره من أجل تعزيز حماية أجهزة الصراف الآلي".

التتمة في الصفحة 8

أمازون تطلق خدمة جديدة لتوصيل الطرود الى داخل منازل العملاء أثناء وجودهم في الخارج

أعلنت شركة أمازون عن إطلاق خدمة جديدة باسم "أمازون كي" Amazon Key تهدف من خلالها إلى تمكين عملائها من استلام طرودهم داخل منازلهم، خاصةً أثناء وجودهم خارجها.

وتقوم خدمة "أمازون كي" الجديدة على نظام يجمع بين الأقفال الذكية وكاميرات المراقبة المنزلية؛ يمكن للمستخدمين التحكم به عن بعد لمنح أشخاص الإذن لهم بدخول منازلهم. ويسمح النظام للعملاء بإنشاء أرقام مرور مؤقتة للأصدقاء وموظفي الخدمات الأخرى لدخول المنزل أيضًا.

ويُعتقد أن الخدمة الجديدة، التي بدأت عملاق التجارة الإلكترونية الأميركية العمل عليها منذ أكثر من سنة، سوف تساعد أمازون على الاستحواذ على مبيعات المتسوقين الذين لا يستطيعون استلام طرودهم داخل المنزل شخصيًا، أو الذين لا يريدون أن تُسرق الطرود من عتبات منازلهم. كما يُعتقد أنها تعطي إشارة لطموحات أمازون في دخول السوق النامي لأجهزة الحماية المنزلية، الذي سوف تتنافس فيه مع شركة نست، الشقيقة لشركة جوجل.

وقال بيتر لارسن، نائب رئيس شركة أمازون لتقنيات التوصيل، في مقابلة: "هذه ليست تجربة بالنسبة لنا. هذا جزء أساسي من تجربة التسوق لأمازون اعتبارًا من هذه النقطة".

ويمكن لأعضاء خدمة التسوق الخاصة بأمازون، أمازون برايم، الحصول على الخدمة الجديدة مقابل 249.99 دولارًا أميركيًا لقاء الحصول على كاميرا يُتحكم بها عبر الإنترنت وجهاز قفل ذكي تثبتهم الشركة نفسها.

ويُطلب من موظفي التوصيل المأذون لهم أن يرنوا جرس الباب أو يطرقوا الباب حين يصلون إلى المنزل، فإذا لم يكن هناك أحد موجود في المنزل، فيمكنهم الضغط على زر "افتح" في تطبيق محمول، لتقوم أمازون بدورها بالتحقق في أنظمتها من كونه الشخص المسموح له بالدخول مع طرد خاص بالمستخدم.

وبعد ذلك تقوم الكاميرا المثبتة في المنزل والمتصلة بالإنترنت ببث فيديو لصاحب المنزل تُظهر موظف التوصيل حين وضع الطرد. ووفقًا للارسن، فإن السرقة مع الخدمة الجديدة غير ممكنة، وذلك بالنظر إلى الاختبارات الأولية لها.

يُشار إلى أن متاجر "وول-مارت" Wal-Mart الأميركية، والتي تعد أحد أبرز منافسي أمازون في مجال تجارة التجزئة، تملك خططًا مشابهة، إذ أعلنت في أيلول الماضي أنها سوف تختبر خدمة لتوصيل الخضار إلى ثلاجات العملاء مباشرة.

يُذكر أن خدمة "أمازون كي" الجديدة سوف تكون قيد التطبيق اعتبارًا من يوم 8 تشرين الثاني/نوفمبر الحالي في 27 موقعًا في الولايات المتحدة.

ابتكار جهاز يرفع من قدرات الدماغ

اخترع العلماء في جامعة "ماكجيل" ومختبر "HRL" الكنديْن جهازاً لتطوير القدرات المعرفية للدماغ. وقامت إدارة المشاريع والبحوث العلمية الواعدة في وزارة الدفاع الأميركية بتمويل مشروع تصميم محفز كهربائي للدماغ.

ويستخدم الجهاز التيار الكهربائي المؤثر على الفص الجبهي لقشرة الدماغ الذي يتولى المسؤولية عن وظائف معرفية مثل حفظ المعلومات والانتباه واتخاذ القرارات. وقد زاد استخدام هذا الجهاز من الترابط بين مختلف مناطق الدماغ، ما ساعد بدوره في التعلم السريع. ويتم تركيب أقطاب الجهاز على الرأس دون أي تدخل جراحي. وتمّت تجربة الجهاز على القرود، حيث طلب منها تحديد مكان يحتوي على الغذاء بواسطة علامات ضوئية. وقامت الحيوانات بـ22 محاولة قبل أن تكون علاقة تربط بين العلامات والغذاء. وبعد تعريضها لتأثير المحفز الكهربائي، استطاعت تعلم ذلك بعد 12 محاولة فقط.

ويأمل الباحثون في استخدام أسلوبهم على نطاق أوسع، بما في ذلك في القوات المسلحة.