الصباح AL-SABAH
www.alsabahpress.com Alsabah Media
No. 4679 | الأربعاء | 5 ربيع الأول 1445 هـ | 20 سبتمبر 2023 م | السنة السادسة عشرة

المعروفة بتطويرها لبرمجيات الفدية الخبيثة

«كاسبرسكي» تكتشف نشاطاً جديداً لعصابة «Cuba» السيبرانية

اكتشفت كاسبرسكي مؤخراً نشاطاً جديداً لمجموعة عصابة الإنترنت Cuba المعروفة بتطويرها لبرمجيات الفدية الخبيثة، حيث قامت المجموعة بنشر برمجية خبيثة مقلقة. إذ تمكنت البرمجية من تجنب عمليات الاكتشاف المتقدمة، واستهدفت المؤسسات حول العالم، وتركت خلفها قائمة من الشركات المخترقة في مختلف القطاعات.

كشفت كاسبرسكي في ديسمبر 2022 عن نشاط مشبوه في نظام أحد عملائها، وعثرت على ثلاث ملفات مشبوهة. كانت هذه الملفات تشغّل سلسلة من الإجراءات التي تقوم بتحميل مكتبة k-mar65، المعروفة أيضاً باسم BUGHATCH، التي تعد باباً خلفياً متطوراً ويتم تفعيلها في ذاكرة العملية.

تقوم BUGHATCH بتنفيذ جزء مضمن من النص البرمجي لواجهة البرمجة (Shellcode) داخل مساحة الذاكرة المخصصة له باستخدام واجهة برمجة التطبيقات لنظام Windows، ويتضمن هذا النص البرمجي وظائف متعددة. وبعد ذلك، يتصل البرنامج بخادم قيادة وتحكم (C2) وينتظر تلقي المزيد من الأوامر. ويمكن أن تطلب هذه الأوامر تثبيت برامج مخصصة للاختراق مثل Cobalt Strike Be-con وMetasploit. كما يشير استخدام أداة سرقة كلمات المرور Veeamp بقوة إلى يد برمجية الفدية Cuba في الأمر.

بشكل مثير للاهتمام، يشير ملف قاعدة بيانات البرنامج إلى مجلد باسم «komar»، وهي كلمة روسية تعني «البعوضة»، مما يشير إلى احتمال وجود أعضاء ناطقين بالروسية داخل المجموعة، ما يتطابق مع أدلة سابقة متعلقة بالمجموعة. وكشف تحليل إضافي أجرته كاسبرسكي عن نشر Cuba لنماذج إضافية تحسن وظائف هذه البرمجية الخبيثة. حيث يقوم أحد هذه النماذج بجمع معلومات النظام ليتم إرسالها إلى خادم عبر طلبات HTTP POST.

واصلت كاسبرسكي تحقيقاتها، واكتشفت عينات جديدة من البرامج الخبيثة المنسوبة إلى مجموعة Cuba على موقع VirusTotal. وتمكنت بعض هذه البرمجيات من تجنب الاكتشاف من مزودي الخدمات الأمنية الآخرين. تمثل هذه العينات نسخاً جديدة لبرمجية BUR-TCIGAR الخبيثة، وتستخدم بيانات مشفرة لتجنب اكتشافها من برامج مكافحة الفيروسات.

يقول جليب إيفانوف، خبير الأمن السيبراني لدى كاسبرسكي، عن هذا الاكتشاف: «تؤكد النتائج التي توصلنا إليها أهمية الوصول إلى أحدث التقارير والمعلومات عن التهديدات. فمع مواصلة عصابات برمجيات الفدية، مثل مجموعة Cuba تطوير وتحسين تقنياتها، تعد المعرفة المسبقة إجراءً مهم للتصدي للهجمات المحتملة بشكل فعال. ففي مشهد التهديدات السيبرانية دائم التغير، تعد المعرفة وسيلة الدفاع النهائية ضد المجرمين السيبرانيين الجدد.»

تعد Cuba سلالة برمجيات فدية أحادية الملف وصعبة الاكتشاف نظراً لعملها دون مكتبات إضافية. وتشتهر المجموعة الإجرامية الناطقة بالروسية بانتشارها الواسع، وتستهدف صناعات مثل البيع بالتجزئة، والتمويل، والخدمات اللوجستية، بالإضافة إلى المصانع والمنشآت الحكومية حول أمريكا الشمالية، وأوروبا، وأوقيانوسيا، وآسيا. تستخدم المجموعة مزيجاً من الأدوات العامة والخاصة، وتحدّث مجموعة أدواتها بانتظام، كما تستخدم مناورات مثل هجمات BYOVD (أحضر برنامج التعريف المعرض للخطر الخاص بك).

ما يميز عمليات المجموعة هي تلاعبها بالطوابع الزمنية لوقت تجميع برمجياتها الخبيثة بهدف تضليل المحققين. مثلاً، في عام 2020 تم العثور على عينات كان تاريخ تجميعها 4 يونيو 2020، فيما حملت الإصدارات الأحدث طوابع زمنية تشير إلى تجميعها في 19 يونيو 1992. ولا يقتصر نهج المجموعة الفريد على تشفير البيانات فقط، بل يتضمن تخصيص الهجمات لسرقة المعلومات الحساسة مثل المستندات المالية، والسجلات المصرفية، وحسابات الشركات، والكود المصدري.

وتعد شركات تطوير البرمجيات معرضة للخطر الأكبر من هذه المجموعة. وعلى الرغم من ظهور المجموعة منذ فترة ليست بقصيرة، فهي لا تزال مرنة وتطور أساليبها باستمرار.

وتحث كاسبرسكي المنظمات بأنواعها على اتباع ما يلي من التوصيات في سبيل الوقاية من برامج الفدية:

احرصوا دائماً على تحديث البرامج على جميع الأجهزة التي تستخدمونها لمنع المخترقين من استغلال نقاط الضعف واختراق شبكتكم.

ركزوا إستراتيجياتكم الدفاعية على اكتشاف الحركات الجانبية وتسرُّب البيانات إلى الإنترنت. أولوا انتباهكم لتدفق البيانات الصادرة لاكتشاف المخترقين المتصلين بشبكتكم. ومن المهم تجهيز نسخ احتياطية غير متصلة بالإنترنت لا يمكن للمخترقين التلاعب بها، وتأكدوا من قدرتكم على الوصول إليها بسرعة عند الحاجة أو في حالات الطوارئ.احموا جميع النقاط الطرفية في شبكتكم من برامج الفدية باستخدام الحلول والأدوات مثل أداة Kaspersky Anti-Ransomware Tool for Business المجانية التي تحمي الحواسيب والخوادم من برامج الفدية وأنواع أخرى من البرمجيات الخبيثة، وتحمي من الثغرات، وتتوافق مع الحلول الأمنية المثبتة مسبقاً.

تبنّوا حلولاً لمكافحة هجمات التهديد المتقدم المستمر (APT) وبرامج الاكتشاف والاستجابة للنقاط الطرفية (EDR) التي تحتوي على إمكانات متقدمة للكشف عن المخاطر والتحقيق فيها ومعالجتها السريعة. وامنحوا فرق مركز العمليات الأمني (SOC) في شركتكم وصولاً إلى أحدث معلومات التهديدات، وحسّنوا مهاراتهم بانتظام من خلال التدريب الاحترافي. يمكنكم ضمان كل هذا مع إطار عمل Kaspersky Expert Security.

زودوا أعضاء فريقكم الأمني بأحدث المعلومات عن التهديدات السيبرانية. تعد منصة Kaspersky Threat Intelligence Portal نقطة وصول موحدة لمعلومات كاسبرسكي عن التهديدات، وتوفر معلومات وتحاليل حول الهجمات السيبرانية جمعها فريق كاسبرسكي على مدار أكثر من 20 عاماً. ولمساعدة الشركات على حماية نفسها بفعالية في هذه الأوقات المضطربة، أعلنت كاسبرسكي عن تقديم الوصول إلى معلوماتها دائمة التحديث وعالمية المصادر عن الهجمات والتهديدات السيبرانية الحالية دون أي رسوم.

kaspersky

شركة كاسبرسكي

«جاهز الكويت» تطلق برنامج الجوائز النقدية اليومي

أعلنت شركة جاهز الدولية "جاهز-الكويت"، المنصة الرائدة التي تربط العملاء بمطاعمهم المفضلة من خلال منصتها الالكترونية، عن إطلاق حملتها الجديدة التي تتيح لـ 182 عميلاً محظوظاً فرصة للفوز بجوائز نقدية يصل مجموعها إلى 20،000 دينار كويتي. تمثل هذه الحملة نهجًا فريدًا اتخذته جاهز-الكويت لمكافأة عملائها المخلصين بجوائز نقدية استنادًا إلى ترتيب طلباتهم من خلال تطبيق التوصيل.

تنطلق الحملة بدءًا من 10 سبتمبر وتستمر حتى 30 سبتمبر، حيث سيحصل العملاء الذين يقومون بالطلب باستخدام تطبيق جاهز-الكويت على فرصة واحدة للمشاركة في السحب مقابل كل طلب ناجح يتم إكماله. وكلما زادت طلبات العملاء باستخدام التطبيق، زادت فرصهم للفوز بواحدة من 10 جوائز نقدية يومية بقيمة 100 دينار كويتي، أو الجائزة الكبرى بقيمة 1000 دينار كويتي التي سيتم السحب عليها في اليوم الأخير من الحملة. سيتم الإعلان عن الفائزين في السحب الذي يتم باشراف وزارة التجارة والصناعة خلال 24 ساعة من تاريخ السحب، حيث سيتلقى الفائزون الجوائز النقدية في مقر جاهز-الكويت. بمجرد فوز العملاء بإحدى الجوائز النقدية، سيتم إبلاغهم عبر التطبيق ومن خلال واتساب على رقمهم المسجل.

أكدت جاهز-الكويت أن برنامج السحوبات يهدف إلى مكافأة العملاء على ولائهم والثقة التي يضعونها في جاهز-الكويت كخدمة توصيل الطعام المفضلة لديهم. وتعتبر هذه المبادرة أيضًا مبادرة اضافية تسعى من خلالها جاهز-الكويت لمكافئة لعملائها المخلصين. وقد نظمت جاهز مؤخرًا برنامجًا للاسترداد النقدي، وقدمت توصيلًا مجانيًا لفترة محدودة، ونظمت مبادرات أخرى لتعزيز تجربة المستخدم لعملائها في الكويت. تتماشى هذه البرامج مع الإطار والنهج الاستراتيجي الذي تعتمده جاهز-الكويت لتوسيع قاعدة عملائها وجذب عملاء جدد يمكنهم الاستفادة من الفرص المميزة. "إن إطلاق برنامج الجوائز النقدية لعملائنا يشكل مصدراً لفخر واعتزاز جاهز-الكويت، والذي يشكل استمراراً للمبادرات التي قدمناها لتعزيز تجربة المستخدم لقاعدتنا المتنامية من العملاء"، صرح فيصل الساعي، مدير التسويق في جاهز-الكويت. "الهدف الرئيسي لدينا من خلال هذه المبادرة هو التفاعل مع عملائنا وتقديم فرصة مثيرة لهم للفوز بإحدى الجوائز النقدية ببساطة من خلال طلب الطعام من مطاعمهم المفضلة من خلال تطبيق جاهز-الكويت."

وأضاف قائلاً، "تعتبر جاهز-الكويت أن كل مطعم نضمه إلى منصتنا ليس مجرد إضافة إلى عدية، بل شراكة قيمة، تثري قائمة الخيارات التي نقدمها لعملائنا. استراتيجية توسعنا لا تقتصر على الأرقام فقط، بل تتعلق بشكل أساسي بربط واحتضان التنوع الغني في المأكولات في الكويت. وتحمل تطلعات وأهداف عملنا التزامًا حقيقاً بالمجتمع المحلي. حيث نهدف من خلال مجموعة واسعة من الحملات والأنشطة، إلى رفع ودعم المطاعم المحلية في رحلتها نحو النجاح".من الجدير بالذكر أن جاهز-الكويت دخلت سوق توصيل الطعام عالي التنافسية بنهج مبتكر يركز على العملاء. من خلال السماح للعملاء ببساطة بتحديد موقع للتوصيل دون الحاجة إلى إدخال عنوان، توفر جاهز-الكويت تجربة سلسة ترفع من سهولة الاستخدام إلى مستوى جديد. وتتيح المنصة للمستخدمين من خيارات دفع مرنة، مما يتيح لهم الحرية في الدفع في أي وقت، سواء قبل أو بعد التوصيل، مما يضع التحكم بالتجربة في أيدي العملاء. بالإضافة إلى ذلك، بالتعاون مع شركاء مختارين، تقدم جاهز خصومات تصل إلى 50% في بعض المطاعم، مما يوفر قيمة لا تضاهى ويجعلها خيارًا جاذبًا لخدمة توصيل الطعام في الكويت.

فيصل الساعي

249.2 مليار دولار..استثمارات 4 دول عربية بالسندات الأمريكية

ارتفعت استثمارات أكبر 4 دول عربية في أذون وسندات الخزانة الأمريكية بنسبة 0.9%، بما يعادل قيمته 2.3 مليار دولار، بنهاية يوليو الماضي مقارنة بنهاية شهر يونيو 2023.

وأظهرت بيانات وزارة الخزانة الأمريكية الصادرة، أمس الثلاثاء، أن قيمة استثمارات أكبر 4 دول عربية بسندات وأذون الخزانة ارتفعت إلى 249.2 مليار دولار في نهاية يوليو الماضي.

وكانت استثمارات دول مجلس التعاون في أذون وسندات الخزانة الأمريكية، قد بلغت 246.9 مليار دولار حتى يونيو 2023.

السعودية والإمارات تتصدران عربياً

أظهرت البيانات أن السعودية، أكبر حائزي الدول العربية للسندات الأمريكية، رفعت استثماراتها شهرياً بنسبة 1.01% إلى 109.2 مليار دولار حتى نهاية يوليو 2023، مقابل 108.1 مليار دولار حتى نهاية يونيو الماضي.

وجاءت الإمارات في المرتبة الثانية، بإجمالي استثمارات 64.9 مليار دولار بنهاية شهر يوليو الماضي، مقارنة بـ65.2 مليار دولار في الشهر السابق له، مسجلة تراجعاً بنسبة 0.46%.

وحلّت الكويت ثالثاً، حيث ارتفعت قيمة استثماراتها بالسندات الأمريكية بنهاية شهر يوليو الماضي بنسبة 4.7% إلى مستوى 42.5 مليار دولار من مستوى 40.6 مليار دولار بنهاية يونيو 2023.

فيما خفضت العراق من حيازاتها في السندات الأمريكية بنسبة 1.2% إلى قيمة 32.6 مليار دولار بنهاية يوليو الماضي مقارنة بـ33 مليار دولار في نهاية يونيو 2023.

اليابان الأولى عالمياً

وارتفع إجمالي قيمة الاستثمارات العالمية في أذونات وسندات الخزانة الأمريكية حتى نهاية يوليو الماضي، بنسبة 1.2% إلى 7.655 تريليون دولار، مقابل 7.563 تريليون في نهاية شهر يونيو 2023.

وبحسب مسح بيانات وزارة الخزانة الأمريكية الصادرة اليوم الثلاثاء، تصدرت اليابان حائزي السندات الأمريكية بـ 1.112 تريليون دولار في نهاية يوليو الماضي مقابل 1.105 تريليون دولار في نهاية يونيو 2023.

وفي المرتبة الثانية حلت الصين بعد أن تراجعت استثماراتها بالسندات الأمريكية في تلك الفترة من العام الجاري إلى 821.8 مليار دولار مقارنة بـ835.4 مليار دولار.

وفي المركز الثالث جاءت المملكة المتحدة باستثمارات 662.4 مليار دولار مقابل 672.3 مليار دولار، ثم لوكسمبورج بـ349.9 مليار دولار، مقابل 331.8 مليار دولار.

يشار إلى أن ما تفصح عنه الخزانة الأمريكية في بياناتها الشهرية هي استثمارات دول الخليج بأذون وسندات الخزانة الأمريكية فقط، ولا تشمل تلك الاستثمارات الأخرى بالولايات المتحدة، سواء كانت حكومية أو خاصة.

وتعد سندات الخزانة الأمريكية وسيلة لجمع الأموال والديون من الدول والمؤسسات، وتسددها الحكومة عند حلول ميعاد استحقاقها الذي يختلف حسب أجل السند.

وتتمتع السندات الأمريكية بالجاذبية لانخفاض مستوى مخاطرة عدم السداد؛ وهو ما يفسر انخفاض العائد عليها، الفائدة، وإن كان الاحتياطي الفيدرالي الأمريكي "البنك المركزي"، ينفذ منذ فترة خطة لرفع أسعار الفائدة.

قبل قرار «الفيدرالي»

الذهب يقفز إلى أعلى مستوياته في أسبوعين

سجلت أسعار الذهب أعلى مستوياتها في أسبوعين، أمس الثلاثاء، إثر تراجع الدولار من أعلى مستوياته في ستة أشهر قبل بدء اجتماع السياسة النقدية لمجلس الاحتياطي الفيدرالي، مع استعداد الأسواق لمجموعة جديدة من التوقعات الاقتصادية من البنك المركزي.

وسجل السعر الفوري للذهب 1،933.31 دولار للأوقية بعد وصوله لأعلى مستوياته منذ الخامس من سبتمبر. كما صعدت العقود الآجلة للذهب بنسبة 0.1 % إلى 1،955 دولار.

وقال إدوارد جاردنر، اقتصادي السلع لدى "كابيتال إيكونوميكس"، إن أي ارتفاع في توقعات أسعار الفائدة من جانب الفيدرالي عما كان متوقعاً في السابق، سيدفع أسعار الذهب للتراجع.

ارتفاع أسعار الذهب

وأوضحت "رويترز" أن النمو الأسرع وتراجع التضخم ومرونة سوق العمل تمهد الطريق لتحديث مسؤولي الفيدرالي التوقعات لتعكس ثقتهم المتنامية في تحقيق هبوط سلس للاقتصاد، مع الإبقاء على احتمالية رفع الفائدة مرة أخرى مطروحاً على الطاولة.

وتراجع الدولار دون أعلى مستوى سجله الأسبوع الماضي في ستة أشهر، ما يجعل الدولار أقل تكلفة بالنسبة للمشترين في الخارج.

وتترقب الأسواق، أيضاً، قرارات السياسة النقدية للبنوك المركزية في بريطانيا واليابان الأسبوع الجاري.

وقال مايكل لانجفورد، رئيس قسم الاستثمار لدى "سكوربيون مينرالز"، إن خطاب جيروم باول، رئيس الفيدرالي، سيسلط الضوء على أن مخاطر التضخم لم تنته بعد، ولكنهم يتبنون نهج الترقب والانتظار إزاء التضخم.وقد يشهد الذهب الذي لا يحمل فائدة تراجعاً في جاذبيته حال إشارة الفيدرالي إلى مواصلة رفع الفائدة للسيطرة على التضخم.

وأضاف جاردنر أن هناك مجالاً أمام المزيد من تراجع الذهب العام الجاري مع انخفاض طلب المستثمرين على الذهب كأداة للتحوط ضد عدم اليقين الاقتصادي وبيئة التضخم المرتفعة.

وأشارت "رويترز" إلى انخفاض حيازات صندوق "إس بي دي آر ترست جولد"، وهو أكبر صندوق مؤشرات مدعوم بالذهب في العالم، بالقرب من أدنى مستوياتها في ثمانية أشهر الأسبوع الماضي.

وارتفع السعر الفوري للفضة بنسبة 0.3 % إلى 23.31 دولار للأوقية، والبلاتين بنسبة 0.6 % إلى 938.97 دولار للأوقية.

الإسترليني يقارب أدنى مستوياته في ثلاثة أشهر

اقترب الجنيه الإسترليني من أدنى مستوياته، أمس الثلاثاء، قبل مجموعة من قرارات البنوك المركزية، بما في ذلك بنك إنكلترا، نهاية الأسبوع الجاري، ما يُتوقع أن يسفر عن رفع أخير للفائدة في دورة التشديد الحالية.

واستقر الإسترليني خلال تداولات أمس أمام الدولار عند 1.2382، أي أعلى طفيفاً من أدنى مستوى سجله خلال جلسة، أمس الأول الإثنين، عند 1.2371 دولار، وهو أدنى مستوياته منذ أوائل يونيو ، فيما استقر أمام اليورو عند 86.36 بنس.

ويجتمع البنك المركزي البريطاني، بعد غد الخميس، وأظهرت أسواق النقد أن المتداولين يتوقعون على نطاق واسع رفع أخير للفائدة بمقدار ربع نقطة إلى 5.50 % ولكن مع استبعاد أي خفض للفائدة حتى الصيف المقبل.

وتراجع التضخم إلى 6.8 % من أعلى مستوياته في 41 عاماً عند 11.1 % في أكتوبر الماضي، ولكنه لايزال الأعلى بين الاقتصادات المتقدمة، ومساعي خفضه كانت أبطأ بكثير.بينما انخفض التضخم في الولايات المتحدة إلى 3.7 % من 9.1 % في يونيو ، أما في منطقة اليورو، سجل التضخم 5.3 %، أي أنه انخفض ينحو النصف من قراءة أكتوبر عند 10.7 %.في الوقت نفسه، تباطأ النمو في المملكة المتحدة على نحو تجاوز توقعات غالبية الاقتصاديين، بعد أن أثرت الإضرابات في المستشفيات والمدارس والطقس الرطب سلباً على الإنتاج في يوليو.

وعلى هذا النحو، أظهر استطلاع أجرته "رويتر لآراء الاقتصاديين، الأسبوع الماضي، أن عدد كبير يستبعد رفع بنك إنكلترا أسعار الفائدة مرة أخرى على الأقل العام الجاري بعد سبتمبر.