مجلة الاقتصاد الإسلامي العالمية

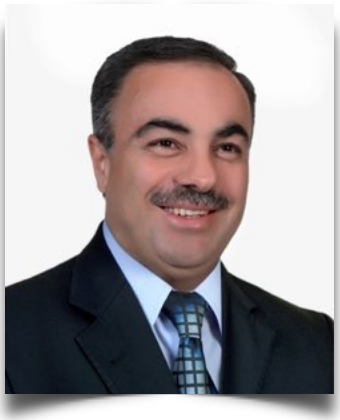
GLOBAL ISLAMIC ECONOMICS MAGAZINE

العدد (٤٢) صفر ١٤٣٧ هـ الموافق تشرين ثاني/نوفمبر ٢٠١٥ م

مجلة شهرية الكترونية تصدر عن المجلس العام للبنوك والمؤسسات المالية الإسلامية بالتعاون مع مركز أبحاث فقه المعاملات الإسلامية

- تَغيُّرُ قِيمَةِ العُمْلَةِ وأثرُها على سِدادِ الدُّيونِ
- الدِّينارُ الذَّهَبيُّ مَورُوثٌ حَضارِيٌّ ومُرساةُ استقرارٍ في النظامِ النَّقديِّ الدّولي
- النُّقودُ تعريفُها وحُكْمُ وَقْفِها
- خيار النَّقد وتطبيقاته الاقتصاديَّة المعاصرة
- المالُ في الإسلامِ : مَفهومُه، أقسَامُه، عَوائِدُه

كلمة رئيس التحرير



الدكتور سامر مظهر قنطقجي
رئيس التحرير

تهديدُ خدماتِ المؤسَّساتِ الماليَّةِ الالكترونيَّة
- هجَماتُ DD4BC -

تُعتبَرُ المؤسَّساتُ الماليةُ أكبرَ المستفيدينَ من تكنولوجيا المعلوماتِ في العالَم؛ لأنّها مستثمِرةٌ لها، وبها توسَّعَت أعمالُها، وزادَت خدماتُها، وانعكسَ ذلك رضاءً لزبائنها، وكذلك مزيداً من الإيرادات لخزينتها.

لكن بما أنّ المخاطرَ هي سِمَةُ تلك المؤسسات؛ فالمخاطرُ الالكترونيةُ هي صنفٌ جديدٌ أُضيفَ لما يكتنفُها من مخاطرَعديدة، وتُعتبَرُ هجماتُ حرمانها من الخدمات، أو هجوم حَجْبِ الخدمة Denial of Service Attacks أو DoS من أكثرِ تلك المخاطرِ انتشاراً وتكراراً. وهي عبارةٌ عن هجماتٍ تتمُّ بهدف إغراقِ مواقعِ المؤسسات المالية بسَيلٍ من البيانات غير اللازمة لإرباكها، وإرباكِ مستخدميها؛ حيث تُرسلُ إليها إشاراتٍ وطلباتٍ من أجهزةٍ مُصابةٍ ببرامجَ تُسمّى DDos Attacks يتحكَّمُ بها قراصنةٌ وعابثينَ إلكترونيينَ عبرَ شبكة الإنترنت؛ ممّا يُسبِّبُ بُطءَ خدماتها؛ بسببِ ازدحامِ مواقعِ تلك المؤسسات؛ فيصبحُ وصولُ عملاءها صَعباً.

وحتى اليوم لا يُوجَدُ علاجٌ لهجومٍ كهذا؛ لأنّه يتمُّ دونَ كسرِ جدرانِ الحماية، أو ملفاتِ كلماتِ السرِّ، أو سرقةِ البيانات؛ بل يكتفي قراصنتُها بحجبِ الخدمة من خلالِ إطلاقِ برنامجٍ يعملُ على إيجادِ ازدحامٍ مروريٍّ للموقعِ فيضعفُ حزمةً بياناته لمنعِ أيِّ مُستخدَمٍ من الوصولِ لخدماتِ الموقع، وينعكسُ ذلك على مبيعاتِ خدماتِ المؤسسةِ المالية المتعرِّضةِ للهجومِ فيسيءُ لسُمعَتِها، وقد ازدادَت شدَّةُ هذه الهجمات، وباتتْ تستهدفُ أهدافاً مُحدَّدة.

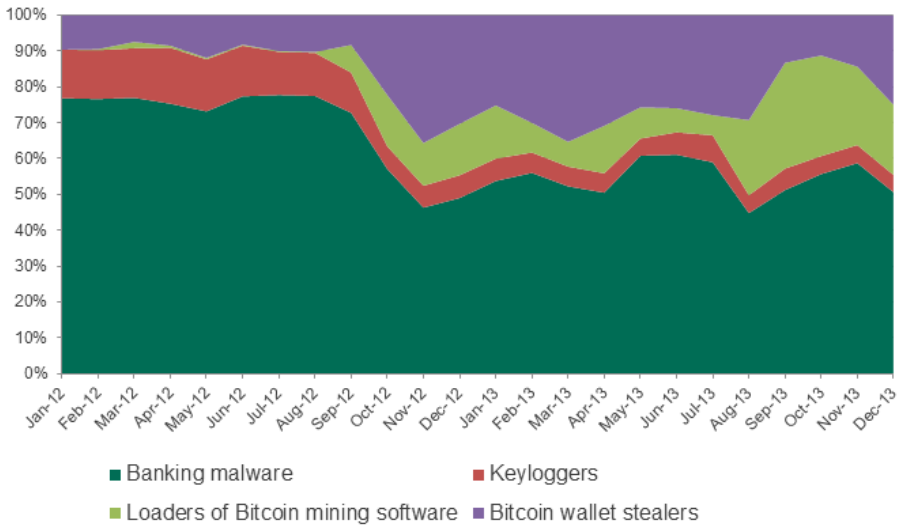
وقد حذَّرَتْ شركةُ (سيمانتك) المُتخصِّصة في الأمن الرقْميِّ عام ٢٠٠٤ من تلك الهجمات، وأوضحتْ أنّ متوسِّطَ عددِ هجماتِ الحرمانِ من الخدمةِ قد وصلَ إلى ٩٢٧ هجمةً في النصفِ الثاني من عام ٢٠٠٤ بزيادةٍ قدْرُها ٦٧٩٪ عنها في النصفِ الأوَّلِ من العامِ نفسه.

وبعدَ عشرَةِ أعوامٍ أطلقتْ شركةُ (كاسبرسكاي) المتخصِّصةُ في الأمنِ الرقْميِّ على موقعها تحذيراً بأنّ المؤسساتِ المالية هي أهمُّ أهدافِ هجومِ DDoS خلالَ الرُّبعِ الثالثِ من عام ٢٠١٤، ويُظهرُ الشكلُ التالي بعضَ إحصائيات أعوام (٢٠١٢ و٢٠١٣) ويبدو فيه ضخامةُ حجمِ هجماتِ وقفِ الخدمة. وقد جاءتِ المؤسَّساتُ الماليةُ في استراليا ونيوزيلندا في المرتبةِ الأُولى من حيث تعرُّضُها لهجماتِ وقفِ الخدمةِ DDoS. ووجَّهتِ الشركةُ اتِّهامَها إلى المجموعةِ الإجراميّةِ (السيبرانية)

المعروفة باسم DD4BC، التي تشنُّ هجماتِها في سبيلِ الحصولِ على عُملةِ (بيتكوين). ويُقصَدُ بلاحقةِ (سايبر) Cyber الكمبيوتر أو شبكته Online.

وانضمَّت سويسرا إلى قائمةِ الضحايا كاستراليا ونيوزيلندا لهجماتِ وقفِ الخدمةِ، وذكر كُلٌّ من بنك الصينِ وبنك شرق آسية إلى أنّه: قد تمَّ استهدافُهم عن طريقِ نشاطاتٍ غيرِ مشروعة.

وقالت (كاسبرسكاي): إنَّ العديدَ من المؤسساتِ الماليةِ الروسيةِ قد حصلَت على تنبيهاتٍ من مُجرمي الإنترنت يُطالِبونَ بالحصولِ على مبالغَ مُعيَّنةٍ عن طريقِ عملةِ بيتكوين لإنهاءِ هُجومِهم.



The percentage of users attacked by different types of malware each month

وعليه فقد توزَّعَت الهجماتُ على أنحاءِ العالَمِ كافّةً؛ فحصلت الصينُ على نسبة ٣٥٪ من مُجمَلِ هجماتِ حَجْبِ الخدمةِ DDoS حول العالَم؛ بينما حصلَت الولاياتُ المتحدةُ على نسبة ٢١٪، وحلَّت كوريةُ الجنوبيةُ في المرتبةِ الثالثةِ بنسبة ١٨٪، بارتفاعٍ بمعدَّلِ ٧.٩٪ في الهجمات التي تستهدفُ كوريةَ الجنوبيةَ مقارنةً بالرُّبعِ السابق.

وسجَّلَت (كاسبرسكاي) خلالَ الرُّبعِ الثالثِ أطولَ وقتٍ مستمرٍّ لهجومِ حَجبِ الخدمةِ، استمرَّ لمدّة (٣٢٠) ساعةً متواصلةً – أي أسبوعينِ مُتواصِلَين –.

واستهدفَ هذا التهديدُ المؤسساتِ الإعلاميةَ وشركاتِ الألعاب، وهدَّدَت بإيقافِ مواقعِها وخدماتِها في حالِ لم تدفعِ الفديةَ، وتقومُ مجموعاتُ القرصنةِ بالطلبِ من أصحابِ الأجهزةِ التي تمَّ تعطيلُها، وشنِّ هجماتٍ عليها دفعَ مبالغَ تتراوحُ بين ٢٥ و٢٠٠ بيتكوين، ويُعادل البيتكوين ٢٣٠ دولاراً أمريكياً.

وقد ذكرت فاينانشيال ريفيو الاسترالية في مقالٍ على موقعِها الالكترونيِّ بتاريخ ٢٠١٥/٩/٢٧ ارتفاعَ الهجماتِ ضدّ المؤسساتِ الماليةِ من مُجرمي الانترنيت (بيتكوين) DD4BC. ويُتوقَّعُ شنُّ هجماتٍ (سايبرية) أكثرَ خُطورةً على بعضِ المؤسساتِ الماليةِ الاستراليةِ بما في ذلك (ست) و(بنك ماكواري)؛ ولأجل ذلك شكَّلَت الحكومةُ الاستراليةُ ما يُسمَّى (مركز الأمن السيبراني الأسترالي) بهدفِ وقفِ حملاتِ الابتزازِ التي يقومُ بها مُجرِمُو الإنترنت سيئو السُّمْعَة، والذين زادتْ هجماتُهم خلال الأشهرِ القليلةِ الماضية، وحوَّلوا اهتمامَهم إلى القطاعِ الماليِّ؛ كالمصارف، والسماسرَة، ومراكزِ تبادُلِ المعلوماتِ في أستراليا.

وما يجبُ أن نعلَمَهُ أنه طالما أنّ الأسواق ومؤسساتها متّصلَةٌ بالانترنيت فهي مُعرَّضَةٌ لهجمات (مُتطوِّرة) على نحوٍ مُتزايدٍ على الشبكات والنظم؛ لذلك فإنّ الأسواقَ الماليةَ، وأسواقَ الأوراقِ الماليةِ ليستا في مأمَنٍ من هذا الخَطر. وإنّ إعدادَ شنِّ هجومِ حجبِ الخدمةِ لا يتطلَّبُ أيَّةَ معرفةٍ تقنيةٍ خاصَّةٍ، بل يُمكِن لأيِّ شخصٍ أو مجموعةٍ إجراميةٍ شنُّ هجومٍ قويٍّ بسهولةٍ إلى حدٍّ ما.

إنّ رَمزَ DD4BC يُشيرُ إلى (دوس بيتكوين) وهو بمثابةِ هجومٍ (سايبري) يهدفُ إلى إسقاطِ المواقعِ، وإضعافِ مُلقّماتِ شبكة (الويب) من خلالِ الاعتداءِ على UDP أيِّ بروتوكول بيانات المستخدمِ User Datagram Protocol وهو أحدُ بروتوكولات الإنترنت Internet Protocol التي تُستخْدَمُ لنقلِ الرسائلِ إلى أجهزةٍ أُخرى على شبكةٍ تعملُ ببروتوكول الإنترنت دونَ الحاجة لإجراء أيَّةِ اتصالاتٍ أوَّليَّةٍ لإنشاءِ قنواتِ اتصالٍ قبلَ بَدءِ إرسالِ البيانات، وهذا ما يُسمّى بروتوكول البياناتِ العالَميّ Universal Datagram Protocol.

أما أشكالُ الابتزازِ فهي بإرسالِ رسائلَ للمُلقِّمات مفادُها:

- أنتَ تحت هجومِ (دوس)؛ إلاّ إنْ دَفعت ٢٥ بيتكوين؛ ممّا جعلَ أكبرَ المصارفِ الاسترالية يَسحَبُ دعمَه للبيتكوين.
- ليس سهلاً التخفيفُ من أعمالِنا الهجومية؛ فلدينا قوَّةُ UDP تُقدَّرُ بـ ٤٠٠ إلى ٥٠٠ جيجا بايت في الثانية، وهذا فقط لنُثْبِتَ أنَّنا جادُّونَ.
- إذا كان بإمكانِك تجاهُلنا ولم تدفَع في غُضونِ ٢٤ ساعة؛ فسوف يبدأُ الهجومُ، وسيزدادُ السعرُ مقابلَ كلِّ ساعةِ تأخير.
- إذا كنتَ تُفكِّرُ في إبلاغِ السلطات، فلا تتردَّد. ولكن ذلك لن يُساعِدَك فنحنْ لسنا هُواة. نحنُ نفعلُ أشياءَ سيِّئةً؛ ولكنَّنا نُحافظ على كلمتِنا.

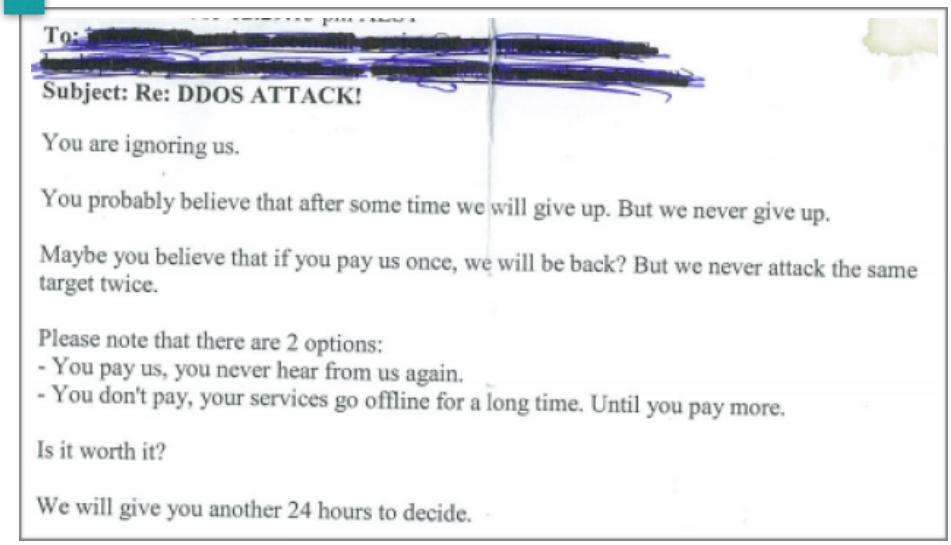
ونعرض أدناه أنموذجين عن تلك الرسائل.

تمتلكُ الروبوتاتِ العاملةُ على أنظمةِ لينكس سِمةَ استخدامِ تشفيرِ XoR في البرامجِ الضارَّة، وفي التواصُلِ مع خوادمِ C&C الخاصَّةِ بالسيطرةِ والعمليات؛ حيث تقومُ بإصدارِ الأوامرِ للروبوتات، وتتلقّى التقاريرَ من الأجهزةِ التي تمت السيطرةُ عليها، كما تقومُ تلك الروبوتات – في الوقتِ نفسِه – بمُهاجَمةِ الدليلِ الجذرِ في أنظمةِ لينكس المستَهدفةِ مُحاولةَ الحصولِ على كلماتِ سرِّها لنشرِ نفسِها بشكلٍ أكبرَ.

وقالت (كاسبرسكاي): إنّ نسبةَ الهجماتِ التي تتمُّ عبرَ روبوتاتٍ تعتمدُ على أنظمةِ لينكس قد ازدادَت من نسبة ٣٧.٦٪ في الرُّبعِ الثاني إلى نسبة ٤٥.٦٪ في الرُّبعِ الثالث، وأضافتِ الشركةُ أنّ مُعظَمَ الضحايا هي مواقعُ آسيويةٌ تنتمي إلى مؤسساتٍ تعليميةٍ أو مجتمعاتِ ألعاب.

طُرُقُ الحماية:

أظهرَ استطلاعٌ أجرتْه شركةُ (كاسبرسكاي) أنّ الكثيرَ من المستخدمينَ لا يُدرِكُونَ القواعدَ الأمنيةَ الأساسيةَ عند القيامِ بسدادِ دُفعاتٍ، أو استخدامِ الأنظمةِ المصرفيةِ عبرَ الإنترنت؛ فعلى سبيلِ المثالِ: فإنّ نصفَ المستخدمينَ يقومونَ بالتأكُّدِ فيما إذا كان موقعُ


To: [redacted]

Subject: Re: DDOS ATTACK!

You are ignoring us.

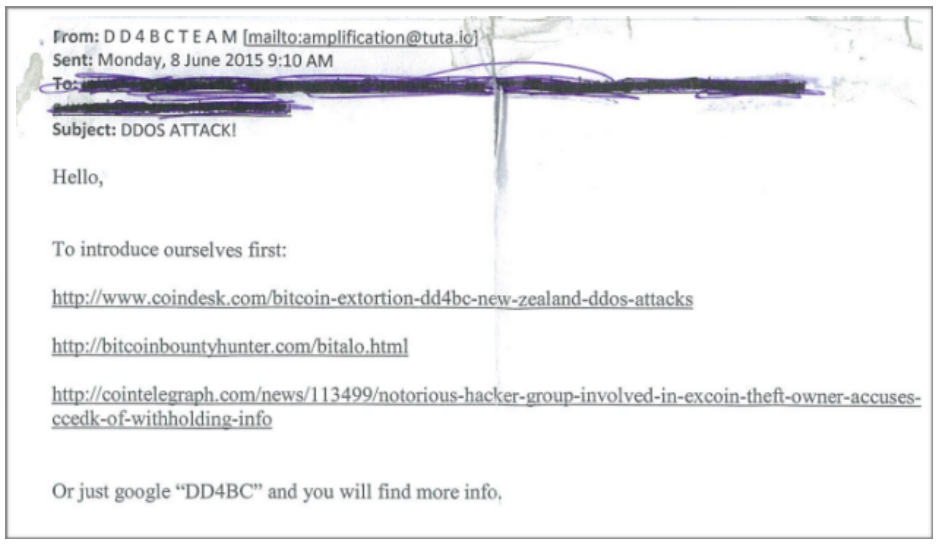
You probably believe that after some time we will give up. But we never give up.

Maybe you believe that if you pay us once, we will be back? But we never attack the same target twice.

Please note that there are 2 options:
- You pay us, you never hear from us again.
- You don't pay, your services go offline for a long time. Until you pay more.

Is it worth it?

We will give you another 24 hours to decide.


From: D D 4 B C T E A M [mailto:amplification@tuta.io]
Sent: Monday, 8 June 2015 9:10 AM
To: [redacted]
Subject: DDOS ATTACK!

Hello,

To introduce ourselves first:

http://www.coindesk.com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks

http://bitcoinbountyhunter.com/bitalo.html

http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info

Or just google "DD4BC" and you will find more info.

الانترنت حقيقيٌّ، أو مُزيَّف قبل إدخال بياناتهم المالية في حين أنّ الثُّلُثَ تقريباً يعتقدونَ بألاّ ضرورةَ لاتخاذ أيِّ إجراءات لحماية تعاملاتهم المالية عبر الانترنت. (رابط الموقع)

ومِمَّا يُذكرُ من طُرقِ الحماية:

- قليلٌ من المستخدمينَ يتعرَّفونَ على الموقعِ الإلكترونيِّ الآمنِ غيرُ محدَّدِ الاسم، والذي له بادئة https للإشارة بأنّه رابطٌ مشفَّرٌ. وقلَّةٌ همْ مَن يستخدمُونَ لوحةَ المفاتيح الافتراضية لحماية كلمات المرور الخاصَّة بهم من هجمات البرمجيات الخبيثة.
- إنَّ أكثرَ المستخدمينَ ليس لديهم نيّةٌ لاتخاذ إجراءات حمائية لاعتقادهم أنّ المواقعَ الإلكترونيةَ الخاصَّةَ بالشركات الكبيرة والمعروفة محميَّةٌ بما فيه الكفايةُ. مع العلم أنّه حتى المواقعَ الإلكترونيةَ المحميَّةَ لا يُمكنُها أن تضمنَ عدمَ قيامِ مُجرمي الإنترنت باختراق عملية الدفع، أو أنّ الجهازَ المستخدَمَ خالٍ من أيِّ برمجيةٍ خبيثةٍ مُصمَّمةٍ خصِّيصاً للسطوِ على الأموال.
- استخدامُ وضعِ (التخفِّي Incognito) لحمايةِ عمليةِ الدفع.
- استخدامُ برامجِ إخفاءَ هُويةِ المستخدمِ أو عنوانِ بروتوكول الإنترنت الخاصِّ بالمستخدَمِ (مثل Anonymizer).
- إدخالُ ومسحُ البياناتِ مِراراً وتكراراً من أجلِ (التشويشِ على الفيروسات).

علماً أنّ هذه الإجراءات كلَّها لا تُجدي نفعاً من حيث حمايةُ معلوماتِ المستخدمِ المالية؛ وذلك لأنّ هناك أناساً يتساهلونَ في حمايةِ بياناتِ الدفعِ الخاصَّةِ تماماً كما يفعلونَ في عالَمِهم الحقيقيِّ؛ فهناك أكثرُ من ٢٠٪ لا يرونَ مشكلةً في أن تغيبَ بطاقةُ الدفعِ المصرفية الخاصَّةِ بهم عن أعينهم عند استخدامِها للدفعِ في أحدِ المطاعم؛ ممّا يمنحُ المُحتالينَ فرصةً ذهبيةً لأخذِ نُسخةٍ عنها؛ لذلكَ يعتقدُ (روس هوغان، الرئيس العالَميّ لإدارةِ مكافحة الاحتيال في شركة كاسبرسكاي) أنّ ذلك لا يُعرِّضُ المستخدمينَ أنفسَهم وأموالَهم فقط للمخاطر؛ بل أيضاً قنواتِ وأنظمةِ الدفعِ المصرفيةِ التي يستخدمونَها. وعليه فقد صارَ استخدامُ حلولِ الأمنِ المتخصِّصةِ لمكافحةِ السرقةِ عبر الإنترنت ضرورةً مُلحَّةً وماسَّةً.

لقد قدمتْ شركاتُ الأمنِ الالكترونيِّ منصَّاتِ حمايةٍ للبنوكِ؛ لحمايةِ البياناتِ الماليةِ، ومكافحةِ الاحتيالِ؛ حتى فيما لو أبدى المستخدمونَ إهمالاً عند قيامِهم بإجراءِ معاملاتِهم الماليةِ عبر الإنترنت. ويُمكِنُ للبنوكِ تثبيتُ حلِّ الحمايةِ مباشرةً على أجهزةِ العملاءِ– بما في ذلك الأجهزةُ المتنقِّلةُ، أو استخدامُ مكوِّناتِ هذه المِنصَّةِ التي تستطيعُ أن تستكشِفَ عن بُعدٍ فيما لو كان الجهازُ مُصاباً بالبرمجياتِ الخبيثةِ المصمَّمةِ للسطوِ على الأموالِ.

وهذا ما أتاحَ لشركاتِ الأمنِ الالكترونيِّ أعمالاً جديدةً ومبتكرةً تنشئ بيئةً آمنةً لإنجازِ العملياتِ الماليةِ المحصَّنَةِ كافّةً ضدَّ الاختراقِ، ومنعِ وصولِ المحتالين.

لكن ماذا عن مُساهَمةِ المجلس العام للبنوك والمؤسسات المالية الإسلامية CIBAFI في تطويقِ هذا الخطرِ؟ وما مدى تعرُّضِ المصارفِ الإسلاميةِ له؟ وهل سنشهدُ تشكيلَ (مركزِ الأمنِ السيبراني للمؤسَّساتِ الماليةِ الإسلامية)؟

حماة (حماها الله) بتاريخ ٠٩-١١-٢٠١٥ م