كاسبرسكي لاب: هجمات Botnet DDoS تستمر لمدة أطول وهي أكثر انتشارا وتكرارا

الاثنين 11 سبتمبر 2017 07:09 م

أظهر تقرير جديد من شركة أمن المعلومات الروسية كاسبرسكي لاب أن الربع الثاني من عام 2017 شهد عودة نشاط هجمات DDoS طويلة الأمد.

وقالت كاسبرسكي لاب في تقرير أعده خبراؤها عن هجمات Botnet DDoS في الربع الثاني من عام 2017 إن أطول هجوم شهده الربع الثاني من العام كان نشطًا لمدة 277 ساعة (أي أكثر من 11 يومًا متواصلة) وهو ما يمثل زيادة بنسبة 131% مقارنة بالربع الأول من العام، ويعد ذلك رقمًا قياسيًا لهذا العام حتى الآن.

وأضافت الشركة أن طول المدة لم تكن هي السمة المميزة الوحيدة لهجمات DDoS بين شهر نيسان/أبريل وشهر حزيران/يونيو، فقد شهدت جغرافية مناطق الهجمات تغيرًا جذريًا فيما يتعلق بالمؤسسات التي لديها موارد عبر الإنترنت في 86 دولة تم استهدافها في الربع الثاني من العام (مقارنة بعدد 72 دولة في الربع الأول).

وبحسب التقرير، فقد كانت الدول العشر الأكثر تضررًا هي الصين وكوريا الجنوبية والولايات المتحدة وهونج كونج والمملكة المتحدة وروسيا وإيطاليا وهولندا وكندا وفرنسا مع حلول إيطاليا وهولندا محل فيتنام والدنمارك اللتين كانتا من بين الأهداف الرئيسية في الربع الأول من العام.

وشملت أهداف هجمات DDoS واحدة من أكبر وكالات الأنباء، وهي وكالة أنباء الجزيرة، وموقعي صحيفتي Le Monde وFigaro، وأنها أصابت خوادم سكايب أيضًا. أدت زيادة أسعار العملات الإلكترونية المشفرة في الربع الثاني من عام 2017 أيضًا، إلى قيام مجرمي الإنترنت بمحاولة التلاعب بتلك الأسعار من خلال هجمات DDoS.

كما تعرضت Bitfinex، وهي أكبر بورصة لعملة البيتكوين Bitcoin الرقمية، للهجوم بالتزامن مع بدء التداول في عملة رقمية جديدة تسمى عملة IOTA، وفى وقت سابق، أعلنت بورصة BTC-E الالكترونية عن تباطؤ في عملياتها بسبب هجمات DDoS الشديدة.

وأشارت كاسبرسكي لاب إلى أن مصلحة مدبري هجمات DDoS للحصول على المال تتجاوز مجرد التلاعب في أسعار العملات الرقمية المشفرة، إذ يمكن الاستفادة من استخدام هذا النوع من الهجمات لابتزاز المال في شن هجمات الفدية RdoS. وعادة ما يرسل مجرمو الإنترنت رسالة إلى الضحية يطالبون بفدية تتراوح ما بين 5 إلى 200 عملة بيتكوين الرقمية. وفي حال رفض الشركة الضحية أن تدفع، يهدد المهاجمون بشن هجوم DDoS على أحد الموارد الهامة على الإنترنت يكون خاصا بالضحية. ويمكن أن تكون هذه الرسائل مصحوبة بهجمات DDoS قصيرة الأجل للتأكيد بأن تلك التهديدات حقيقية للغاية. ففي نهاية شهر يونيو من هذا العام، شنت عصابة تدعى Armada Collective هجمات فدية RdoS واسعة النطاق، طالبت فيها بحوالي 315,000 دولار أمريكي من سبعة مصارف كورية جنوبية.

ومع ذلك، فقد ترى كاسبرسكي لاب أن هناك دائمًا طرق أخرى للتحايل من بينها الطريقة التي أصبحت أكثر شيوعًا في الربع الأخير من العام وهي طريقة الفدية RdoS، ولكن مع عدم وجود أي نوع من هجمات DDoS على الإطلاق، إذ يرسل مجرمو الإنترنت رسائل تهديد إلى عدد كبير من الشركات على أمل أن تفضل واحدة من تلك الشركات سلامة مواقعها عن الشعور بالندم بعد شن الهجمات وفوات الأوان. وقد لا يتم شن أي هجمات أبدا بعد تلك التهديدات، ولكن إذا قررت شركة واحدة فقط أن تدفع الفدية، عندئذ يكسب مجرمو الإنترنت أرباحا وفيرة مع بذل الحد الأدنى من الجهد.

وعلق كيريل إلجانايف، رئيس كاسبرسكي للحماية من هجمات DDoS في كاسبرسكي لاب بالقول: "في الوقت الحاضر، لم يعد أمر شن

هجمات الفدية RDoS مقتصرًا على فرق معينة من مجرمي الإنترنت من ذوي الخبرة الفائقة في مجال التقنية، حيث يمكن لأي محتال لا يملك حتى المعرفة أو المهارة التقنية المطلوبة لتنظيم هجمات DDoS واسعة النطاق، يمكنه أن يشتري نموذجا توضيحيًا للهجمات بغرض استخدامها في الابتزاز في الغالب، ينتقي مثل هؤلاء المحتالين الشركات غير الحريصة التي لا تحمي مواردها من هجمات DDoS بأي شكل من الأشكال، وبالتالي، يمكن إقناعها بسهولة أن تدفع الفدية بمجرد استخدام نموذج بسيط للهجمات".

ويحذر خبراء كاسبرسكي لاب من أنه في حال قررت إحدى الشركات من الضحايا أن تدفع الفدية التي يطلبها المهاجمون، فإن ذلك قد يسبب لها أضرارًا على المدى البعيد، بالإضافة إلى الخسارة المالية الفورية، حيث ينتشر خبر الفدية التي سددتها الشركة الضحية بسرعة من خلال شبكة الإنترنت مما يحفز مجرمي الإنترنت الآخرين على شن المزيد من الهجمات على تلك الشركة

وقالت كاسبرسكي لاب إن حل Kaspersky DDoS Protection التابع لها يجمع بين خبرتها الواسعة في مكافحة التهديدات الإلكترونية وبين التطورات الداخلية الفريدة التي تقوم الشركة بتنفيذها، إذ يوفر هذا الحل الحماية ضد جميع أنواع هجمات DDoS بغض النظر عن تعقيدها، أو قوتها أو مدتها

وأشارت الشركة إلى أن نظام الكشف عن هجمات DDoS (جزء من حل Kaspersky DDoS Protection) صُمم لاعتراض وتحليل الأوامر المرسلة إلى الأجهزة المثبتة على شبكات Bots من خوادم التحكم والسيطرة، وليس من الضروري الانتظار حتى تتم إصابة أجهزة المستخدم أو يتم تنفيذ الأوامر التي يصدرها مجرمو الإنترنت من أجل جمع البيانات من المهم ملاحظة أن الإحصاءات المتعلقة بنظام الكشف عن هجمات DDoS تقتصر على تلك الشبكات التي تم الكشف عنها وتحليلها من قبل كاسبرسكي لاب