القياسات الرئيسية النابعة من تقرير استخبارات التهديد NETSCOUT في النصف الأول من عام ٢٠٢١

مصر

أدى التحول الكبير إلى الحياة عبر الإنترنت بسبب جائحة كورونا COVID-19 إلى تحقيق مستويات قياسية من الابتكار من جانب الجهات الفاعلة في مجال التهديد، ويتوقع فريق ATLAS لهندسة الأمن والاستجابة (ASERT) التابع لشركة نتسكاوت أن تستمر هذه السلسلة الطويلة من ابتكارات المهاجمين حتى عام ٢٠٢١.

أطلق الفاعلون الفاسدون ما يقرب من ٥.٤ مليون هجومًا من نوعية رفض الخدمة الموزعة (DDoS) في النصف الأول من عام ٢٠٢١—وهو رقم قياسي آخر. وقد أطلق المهاجمون، على وجه الخصوص أعدادًا غير مسبوقة من هجمات رفض الخدمة الموزعة (DDoS) في الربع الأول من العام، الأمر الذي زاد من وتيرة الهجمات بنسبة 20 بالمائة في خلال نفس الفترة في عام ٢٠٢٠. واكتشف الخصوم، في نفس الوقت، أو استخدموا سلاحًا من سبعة نواقل لهجمات رفض الخدمة الموزعة (DDoS) تعكس/تضخم بروتوكول UDP، كما طوروا هجمات تكيفية متعددة النواقل مصممة خصيصًا لاستغلال نقاط الضعف في أهدافهم. وتعرضت المكونات الحيوية لسلسلة إمداد الاتصال لهجمات متزايدة، في الوقت الذي أضافت فيه عصابات برامج الفدية تكتيكات ابتزاز ثلاثية لهجمات رفض الخدمة الموزعة (DDoS) إلى مخزون ذخيرتها، وأطلق ممثل التهديد فانسي لازاروس حملة إبتزاز جديدة من هجمات رفض الخدمة الموزعة (DDoS).

أقصى عدد للهجمات متعددة النواقل

أكبر عدد نواقل شوهد في هجوم واحد

٢٠

نواقل الهجمات المستخدمة

١. تضخيم BitTorrent
٢. تضخيم Citrix-ICA
3. تضخيم CLDAP
٤. نظام أسماء النطاقات
٥. ICMP
٦. تضخيم L2TP
٧. نظام أسماء النطاقات
٨. تضخيم Memcached
٩. تضخيم MSSQLRS
١٠. تضخيم NetBIOS
١١. تضخيم NTP
١٢. تضخيم RIPv1
١٣. تضخيم SNMP
١٤. تضخيم SSDP
١٥. تضخيم STUN
١٦. TCP ACK
١٧. TCP NULL
١٨. TCP RST
١٩. TCP SYN
٢٠. تضخيم TCP SYN/ACK

أعلى ٥ نواقل هجومية

Ta	Ts	Im	Tr	Dn
TCP ACK	TCP SYN	ICMP	TCP RST	تضخيم DNS
عدد الهجمات	عدد الهجمات	عدد الهجمات	عدد الهجمات	عدد الهجمات
٢٣,١١٣	٤,١٤١	٤,١٣٧	٣,٨٠٤	٣,٥٦٢

احصاءات DDoS

معدل تكرار الهجمات	-٦٩%
الإنتاجية القصوى	-٣%
متوسط المدة	+١٠%
الحد الأقصى لحجم الهجمة	-٦٥%

أكبر هجوم

الحجم	٦٤,٠٢ جيجابت/ثانية
السرعة	5,00 مليون حزمة في الثانية
المدة	٨,٩٤١ ثانية

الحد الأقصى لذروة الإنتاجية

التاريخ	٢٠٢١\٠١\٠١
الإنتاجية القصوى	٧٩ مليون حزمة في الثانية

الحد الأقصى لذروة عرض النطاق

التاريخ	٢٠٢١\٠١\٠٣
الحد الأقصى لعرض النطاق	٩٠ جيجابت/ثانية

NETSCOUT

أهم صناعات السوق العمودية المعرضة للهجوم

يبين الرسم البياني التالي عينة من القطاعات الأكثر استهدافًا خلال النصف الأول من عام٢٠٢١حسب عدد الهجمات.

الطبقة	عمودي	التردد	أقصى هجمة	أشد أثر	متوسط المدة
١	شركات الاتصالات السلكية	١,٣٥٨	٧٣,٥٤ جيجابت/ثانية	١٥,٨٨ مليون حزمة في الثانية	٦٥,٦ دقيقة
٢	شركات الاتصالات السلكية واللاسلكية (باستثناء القمر الصناعي)	١,١٨٥	١٥,٦٤ جيجابت/ثانية	٣٣,٣٠ مليون حزمة في الثانية	٢٩ دقيقة
٣	معالجة البيانات, الاستضافة + الخدمات ذات الصلة	٨٩	١,١٠ جيجابت/ثانية	١,٢٦ مليون حزمة في الثانية	٢٣٦,٧ دقيقة
٤	النشر والبث عبر الإنترنت + بوابات البحث على شبكة ويب	١٤	٠.٠٢ جيجابت/ثانية	٠.٠٠ مليون حزمة في الثانية	٤٨,٥ دقيقة
٥	كل وسائل الاتصالات الأخرى	٣	٠.٠١ جيجابت/ثانية	٠.٠٠ مليون حزمة في الثانية	٩٣,٧ دقيقة
٦	ناشرو البرمجيات	٢	٠.٠٢ جيجابت/ثانية	٠.٠٠ مليون حزمة في الثانية	٢٩,٥ دقيقة
٧	الكليات, الجامعات + المدارس المتخصصة	١	٠.٠٧ جيجابت/ثانية	٠.٠١ مليون حزمة في الثانية	١١.٠ دقيقة
٨	الأوراق المالية + بورصات السلع	١	٠.٠١ جيجابت/ثانية	٠.٠٠ مليون حزمة في الثانية	٧٠ دقيقة

الصورة الكبيرة

اكتشف تقرير نتسكاوت الكامل عن استخبارات التهديد NETSCOUT Threat Intelligence في النصف الأول من عام ٢٠٢١ بحثًا عن آخر الأبحاث في التوجهات والأنشطة عبر مشهد التهديد العالمي برفض الخدمة الموزعة (DDoS).

عرض التقرير التفاعلي

NETSCOUT

SECR_031_AR-2102 09/2021