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

المملكة العربية السعودية

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 2021.

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 ٢٠ بالمائة في خلال نفس الفترة في عام 2020. 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

٢٦

نواقل الهجمات المستخدمة

١. تضخيم Chargen
٢. تضخيم Citrix-ICA
٣. تضخيم CLDAP
٤. DNS
٥. تضخيم DNS
٦. ICMP
٧. تضخيم IPMI
٨. بروتوكول IPv4 0
٩. ISAKMP
١٠. تضخيم L2TP
١١. تضخيم mDNS
١٢. تضخيم Memcached
١٣. تضخيم MSSQLRS
١٤. تضخيم NetBIOS
١٥. تضخيم NTP
١٦. تضخيم OpenVPN
١٧. تضخيم RIPv1
١٨. تضخيم rpcbind
١٩. تضخيم SNMP
٢٠. تضخيم SSDP
٢١. تضخيم TCP ACK
٢٢. تضخيم TCP NULL
٢٣. تضخيم TCP RST
٢٤. تضخيم TCP SYN
٢٥. تضخيم TCP SYN/ACK
٢٦. تضخيم Ubiquiti

أعلى ٥ نواقل هجومية

Ta	Np	Dn	Im	Ts
TCP ACK	تضخيم NTP	تضخيم DNS	ICMP	TCP SYN
عدد الهجمات	عدد الهجمات	عدد الهجمات	عدد الهجمات	عدد الهجمات
٧٣,٤٠٠	١٤,٠٢٦	١٠,٧٨٧	١٠,٦٢١	٩,٩٩٣

احصاءات DDoS

معدل تكرار الهجمات	+٢٥٠%
الإنتاجية القصوى	+١%
متوسط المدة	+٩٢%
الحد الأقصى لحجم الهجمة	+١٣%

أكبر هجوم

الحجم	٣٥٢,٧٤ غيغابت/ثانية
السرعة	٣١,٠٦ مليون حزمة في الثانية
المدة	٣٥٣ ثانية

الحد الأقصى لذروة الإنتاجية

التاريخ	٢٠٢١٠١١٠٤
الإنتاجية القصوى	٩٦ مليون حزمة في الثانية

الحد الأقصى لذروة عرض النطاق

التاريخ	٢٠٢١٠١١٠٤
الحد الأقصى لعرض النطاق	٤٧٩ غيغابت/ثانية

NETSCOUT

أهم صناعات السوق العمودية المعرضة للهجوم

يبين الرسم البياني التالي عينة من القطاعات الأكثر استهدافًا خلال النصف الأول من عام ٢٠٢١ حسب عدد الهجمات.

الطبقة	عمودي	التردد	أقصى هجمة	أشد أثر	متوسط المدة
١	شركات الاتصالات السلكية	٤,٢٣٦	٩٣,١١ غيغابت/ثانية	١٩,٧٨ مليون حزمة في الثانية	٨٦,٣ دقيقة
٢	معالجة البيانات, الاستضافة + الخدمات ذات الصلة	١٥٠	١٦,٥٠ غيغابت/ثانية	٤,٠٣ مليون حزمة في الثانية	٣٦.٠ دقيقة
٣	كل وسائل الاتصالات الأخرى	٧١	١٤,٣٤ غيغابت/ثانية	٣,٨٠ مليون حزمة في الثانية	٨٨.٠ دقيقة
٤	تصنيع أجهزة كمبيوتر التخزين	٥	١,٩٧ غيغابت/ثانية	٠,٢٣ مليون حزمة في الثانية	٥٦,٨ دقيقة
٥	مكاتب الأطباء (باستثناء أخصائيي الصحة العقلية)	٢	٠,٠٣ غيغابت/ثانية	٠.٠٠ مليون حزمة في الثانية	١٤,٥ دقيقة
٦	النقل الجوي للركاب المخطط له	١	٠.٠٤ غيغابت/ثانية	٠.٠٠ مليون حزمة في الثانية	٤٢.٠ دقيقة
٧	ناشرو البرمجيات	١	٠.١١ غيغابت/ثانية	٠.٠١ مليون حزمة في الثانية	١٢.٠ دقيقة

الصورة الكبيرة

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

إستعراض التقرير التفاعلي

NETSCOUT

SECR_036_AR-2102 09/2021