/ پاییز ۱۴۰۳

گزارش تحلیلی و آماری

از حملات منع خدمت توزیع شده / DDoS / علیه زیرساخت های کشور

سامانه مقابله با حملات
منع خدمت توزیع شده سیوان

وخرد [illegible] در [illegible] سیاست

فهرست

مقدمه

با گسترش روزافزون فناوری‌های دیجیتال و وابستگی بیشتر صنایع و زیرساخت‌های حیاتی به خدمات آنلاین، امنیت سایبری به یکی از اساسی‌ترین نیازهای کشورها تبدیل شده است. در این میان، حملات منع سرویس توزیع‌شده (DDoS) به‌عنوان یکی از ابزارهای مخرب سایبری، توانسته است چالش‌های بزرگی را در مسیر پایداری و عملکرد زیرساخت‌های دیجیتال ایجاد کند. شرکت ارتباطات زیرساخت، با بهره‌گیری از تجهیزات و سامانه‌های بومی پیشرفته، گام‌های مهمی در مسیر شناسایی و مقابله با این تهدیدات برداشته است. این تلاش‌ها به ما امکان می‌دهد تا درک عمیق‌تری از ماهیت و الگوهای این حملات داشته باشیم و اقدامات پیشگیرانه مؤثرتری را طراحی کنیم. گزارش پیش‌رو، مروری جامع بر وضعیت حملات DDoS در فصل پاییز ۱۴۰۳ است و اطلاعات دقیقی از حجم حملات،

منابع اصلی آن‌ها، صنایع هدف و میزان تأثیرگذاری این تهدیدات ارائه می‌دهد. هدف از این تحلیل، کمک به ارتقای سطح آگاهی و آمادگی در میان فعالان اکوسیستم دیجیتال کشور و حمایت از توسعه زیرساخت‌های مقاوم در برابر تهدیدات سایبری است. با ارائه این گزارش، تلاش داریم بستری برای شفافیت، همکاری و تقویت توانمندی‌های ملی در حوزه امنیت سایبری فراهم نموده و گامی مؤثر در جهت حفاظت از زیرساخت‌های حیاتی و رشد پایدار فضای دیجیتال کشور برداریم.

فرضیات

/ ۰۱ / این گزارش بر اساس تحلیل‌های صورت پذیرفته بر **داده‌های آماری متقن** تدوین گردیده است و بیانگر عملکرد این شرکت در کیفیت مقابله با حملات مذکور می‌باشد.

/ ۰۲ / در این گزارش سعی شده است که با **شفافیت** نسبت به ارائه تحلیل و آمارهای موجود از وضعیت **حملات منع خدمت توزیع شده** سخن گفته شود. با این حال با توجه به سطح **محرمانگی اطلاعات** و عدم قابلیت انتشار عمومی آن، در بخش‌هایی از گزارش از ارائه دقیق معیارها به شکل مستقیم جلوگیری گردیده است.

/۰۳/ تمامی آمارهای این گزارش بر اساس تحلیل حملات منع خدمت توزیع شده صورت پذیرفته از تاریخ **۱ مهرماه سال ۱۴۰۳** الی **۳۰ آذر ماه سال ۱۴۰۳** به مدت زمان **۳ ماه** می‌باشد.

/۰۴/ بزرگترین اهداف ارائه این گزارش آگاهی رسانی عمومی و تخصصی، امید بخشی به متخصصان صنعت فناوری اطلاعات و ارائه گزارش عملکرد بخش کوچکی از اقدامات وزارت ارتباطات و فناوری اطلاعات به **آحاد مردم عزیز** می‌باشد.

تعاریف اصلی

حمله منع خدمت توزیع شده

DDoS / Distributed Denial of Service /

حمله منع خدمت توزیع شده نوعی از حملات سایبری است که در آن مهاجمان نسبت به **ارسال ترافیک کاذب** به سمت زیرساخت‌ها و سرویس‌های حیاتی اقدام نموده و بدین ترتیب سبب بروز اختلال و یا قطعی کامل خدمات‌رسانی زیرساخت و یا سرویس مربوطه به کاربران حقیقی می شود.

حمله پیشرفته و مستمر منع خدمت توزیع شده / Advance Persistent Distributed Denial of Service / APDDoS

حمله پیشرفته و مستمر منع خدمت توزیع شده گروهی از حملات سایبری می‌باشد که در آن مهاجمان ابتدا نسبت به آلوده‌سازی تعداد زیادی از **تجهیزات حوزه IT و IOT** اقدام نموده و سپس **با استفاده از شبکه آلوده ایجاد گردیده** /Botnet/ با بیشترین میزان تشابه به **رفتار کاربران** و بدون استفاده از **آدرس کاذب**، حملات منع خدمت توزیع شده خود را پی‌ریزی می‌نمایند.

حمله منع خدمت توزیع شده حجمی

VA / Volumetric Attack /

نوعی از حملات منع خدمت توزیع شده می‌باشد که در آن مهاجمان نسبت به **ارسال حجم بالایی از ترافیک** اقدام نموده و به علت سرریز کردن ظرفیت **اتصالات** و **تجهیزات میانی و پایانی** شبکه مورد حمله و از دست رفتن ترافیک حقیقی کاربران سبب اختلال گسترده در زیرساخت‌ها و سرویس‌های نهایی می‌گردند.

حمله منع خدمت توزیع شده مبتنی بر ضعف پروتکل‌های ارتباطی شبکه

Protocol Attack / PA /

نوعی از حملات منع خدمت توزیع شده می‌باشد که در آن مهاجمان با استفاده از **ضعف‌های ساختاری پروتکل‌های ارتباطی** مورد استفاده در شبکه نسبت به پی ریزی حملات اقدام می‌نمایند.

04

حملات سایبری سازمان یافته به زیرساخت‌های حیاتی کشور

در سال‌های اخیر، با توجه به شرایط سیاسی و اقتصادی، کشور عزیزمان همواره هدف تهدیدات و حملات دشمنان این مرز و بوم قرار گرفته است. دشمنان با به‌کارگیری تمامی ابزارها و ظرفیت‌های خود، تلاش دارند تا از طریق ایجاد فشارهای روانی و اقتصادی بر مردم عزیز کشورمان، امنیت و آرامش عمومی را مختل کنند. در این میان، راهبردهای تروریسم سایبری به یکی از محورهای اصلی اقدامات مخرب آن‌ها تبدیل شده است. ایجاد اختلال گسترده در زیرساخت‌های حیاتی و عمومی کشور، از جمله شبکه‌های ارتباطی، انرژی و خدمات دیجیتال بخشی از برنامه‌های هدفمند آنان برای ایجاد بی‌ثباتی و افزایش تنش‌های اجتماعی و اقتصادی بوده است.

در ادامه به بررسی نتایج و تحلیل برخی از حملات صورت پذیرفته به مقاصد سرویس‌های حیاتی و مورد نیاز جامعه خواهیم پرداخت.

میزان حملات مقابله گردیده به مقاصد سرویس‌های حیاتی و موردنیاز جامعه

بیش از ۸۹/۴۸%

از حملات در راستای محروم سازی مردم عزیز از دریافت خدمات مورد نیازشان بوده است که با تلاش متخصصین کشور حملات مذکور **تماما** با **موفقیت کامل** دفع گردیده اند.

۱,۳۸۶ ساعت

موفقیت درمقابله با حملات به شبکه مخابراتی و زیرساخت شرکت‌های ارائه‌دهنده خدمات اینترنتی

۷۳۳ ساعت

موفقیت در مقابله با حملات به کسب و کارهای اینترنتی

۵۴۰ ساعت

موفقیت در مقابله با حملات به سرویس‌های بر خط خدمات عمومی

۴۹۸ ساعت

موفقیت در مقابله با حملات به شبکه بانکی و صنعت مالی کشور

۳۲۰ ساعت

موفقیت در مقابله با حملات به درگاه‌های ارائه‌دهنده خدمات دولتی

۳۰۹ ساعت

موفقیت در مقابله با حملات به پیام‌رسان‌ها و سکوهای بومی

۰۵/ کلیات آماری

در این بخش به بررسی اجمالی معیارهای حملات منع خدمت توزیع شده خواهیم پرداخت.

یادآور می‌گردد در این گزارش مقادیر لحظه‌ای بر مبنای بیت بر ثانیه و مقادیر تجمعی بر مبنای بایت می‌باشد.

۵۷,۲۱۸ حمله

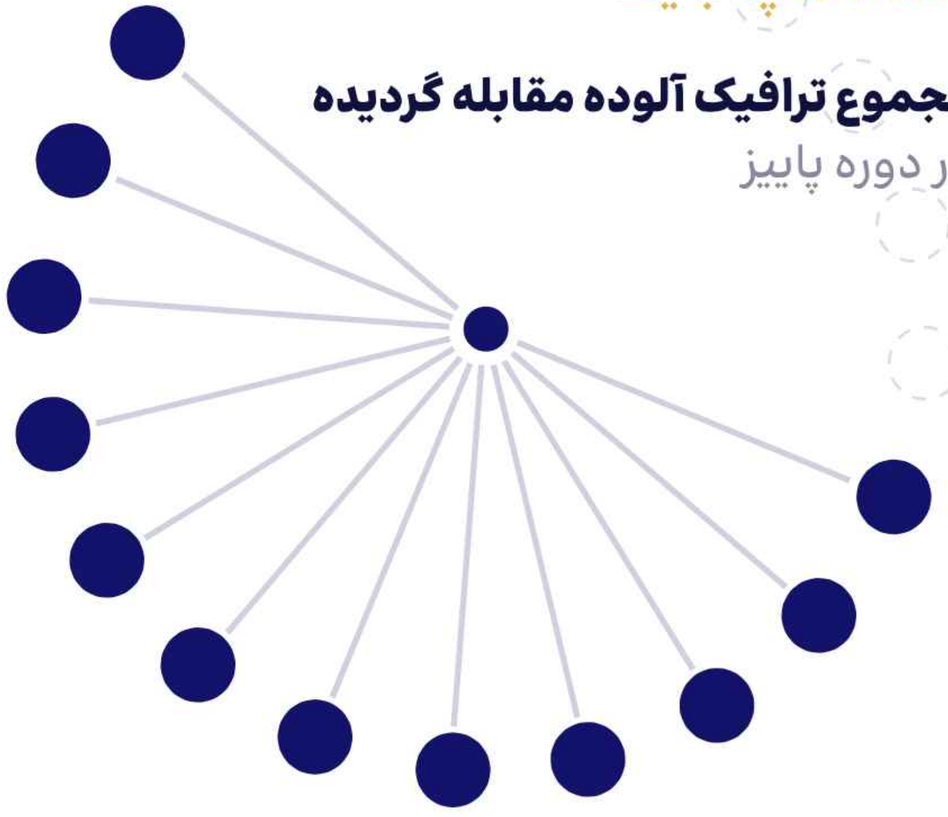
مجموع حملات مقابله گردیده

در دوره پاییز

۱۲/۵۸ پتابایت

مجموع ترافیک آلوده مقابله گردیده

در دوره پاییز



۳۶/۴۳ گیگابیت بر ثانیه

میانگین حجم حملات

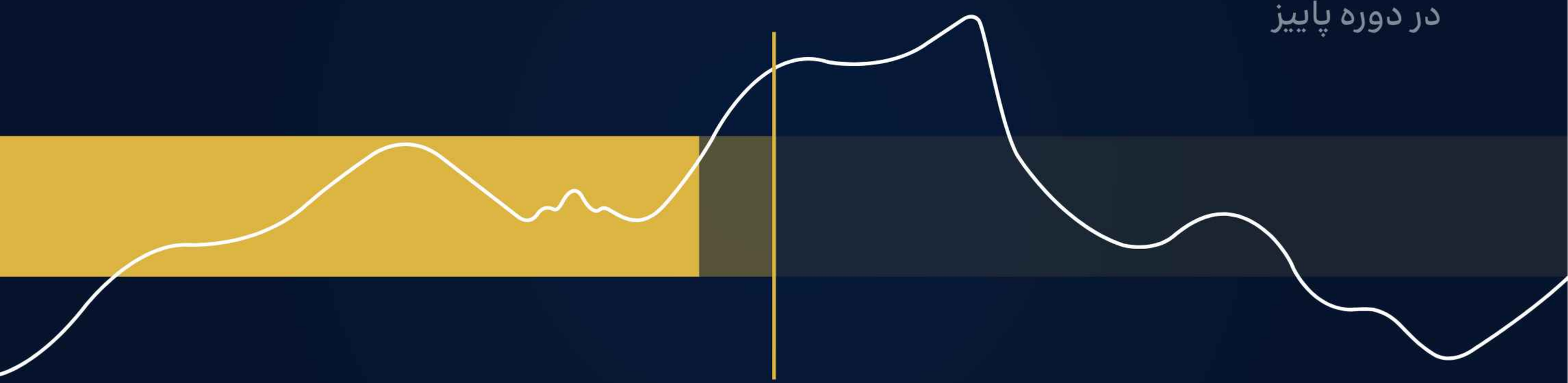
در دوره پاییز


۶۳۵ حمله
میانگین حملات روزانه
در دوره پاییز

۴ دقیقه ۳۷ ثانیه

میانگین مدت زمان حملات

در دوره پاییز



۱۴۸+ حمله

بیشینه تعداد حمله همزمان
در دوره پاییز

۷۰۷/۱۴
گیگابیت بر ثانیه

بیشینه ترافیک مقابله گردیده
در دوره پاییز

۱۷۱/۶
میلیون بسته بر ثانیه

بیشینه تعداد بسته مقابل گردیده
در دوره پاییز


۴ روز ۹ ساعت ۵۰ دقیقه
بالاترین مدت زمان حمله
در دوره پاییز

۰۶/ آگاهی رسانی آماری

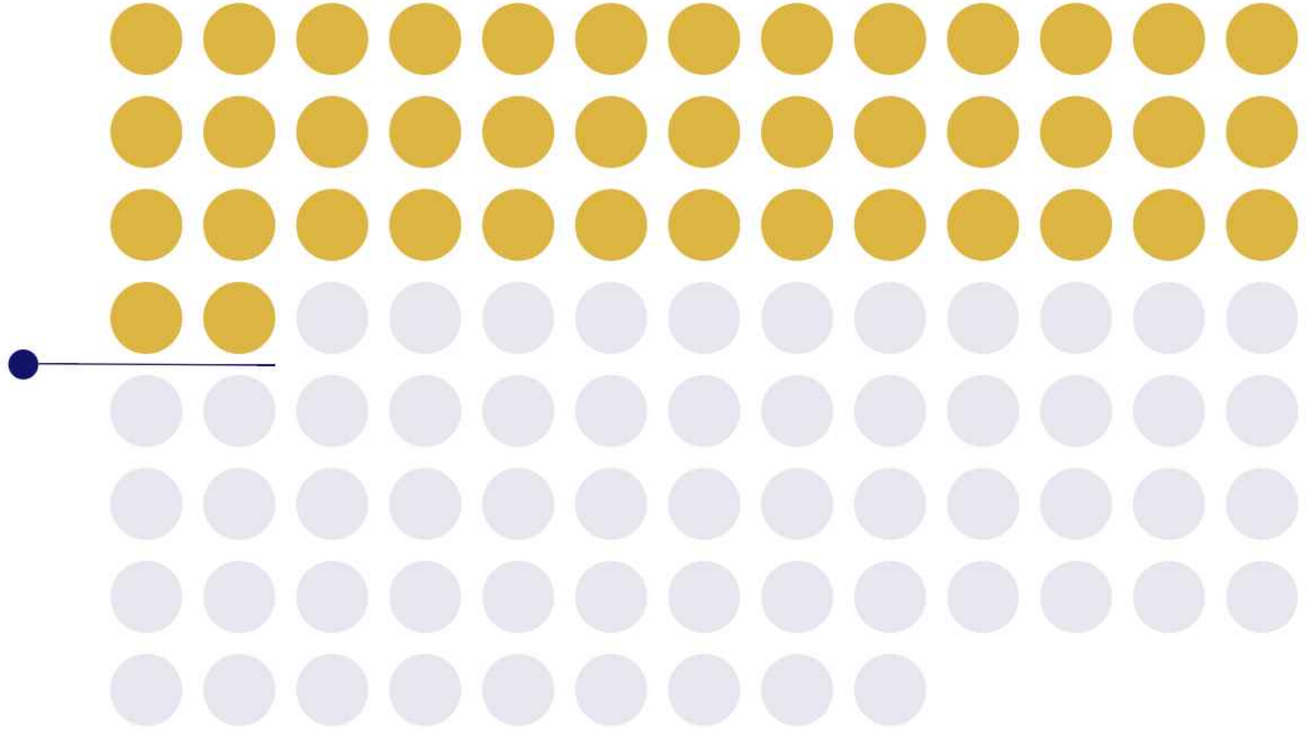
آگاهی‌رسانی آماری به معنای تطبیق صحیح داده‌های تحلیلی و تخصصی به معیارهای عمومی و همگانی می‌باشد که در راستای افزایش ضریب آگاهی مخاطبان این گزارش از **وضعیت رخدادهای منع خدمت توزیع شده** گردآوری شده است.

از هر ۱۰۰ حمله **۳۵ حمله**

از طریق شبکه دستگاه‌های آلوده /Bot Pool/

از هر ۱۰۰ حمله **۲۰ حمله**

با ظرفیتی بیش از ۱۰ گیگابیت بر ثانیه



از هر

۱۰۰ حمله

۵ حمله

با مدت زمانی

بیش از ۱۰ دقیقه

۲۱حمله

با ظرفیتی بیش از

۱ میلیون بسته بر ثانیه

۲۸ حمله

مجموع ترافیک مقابله شده

بیش از ۱۰۰ گیگابایت

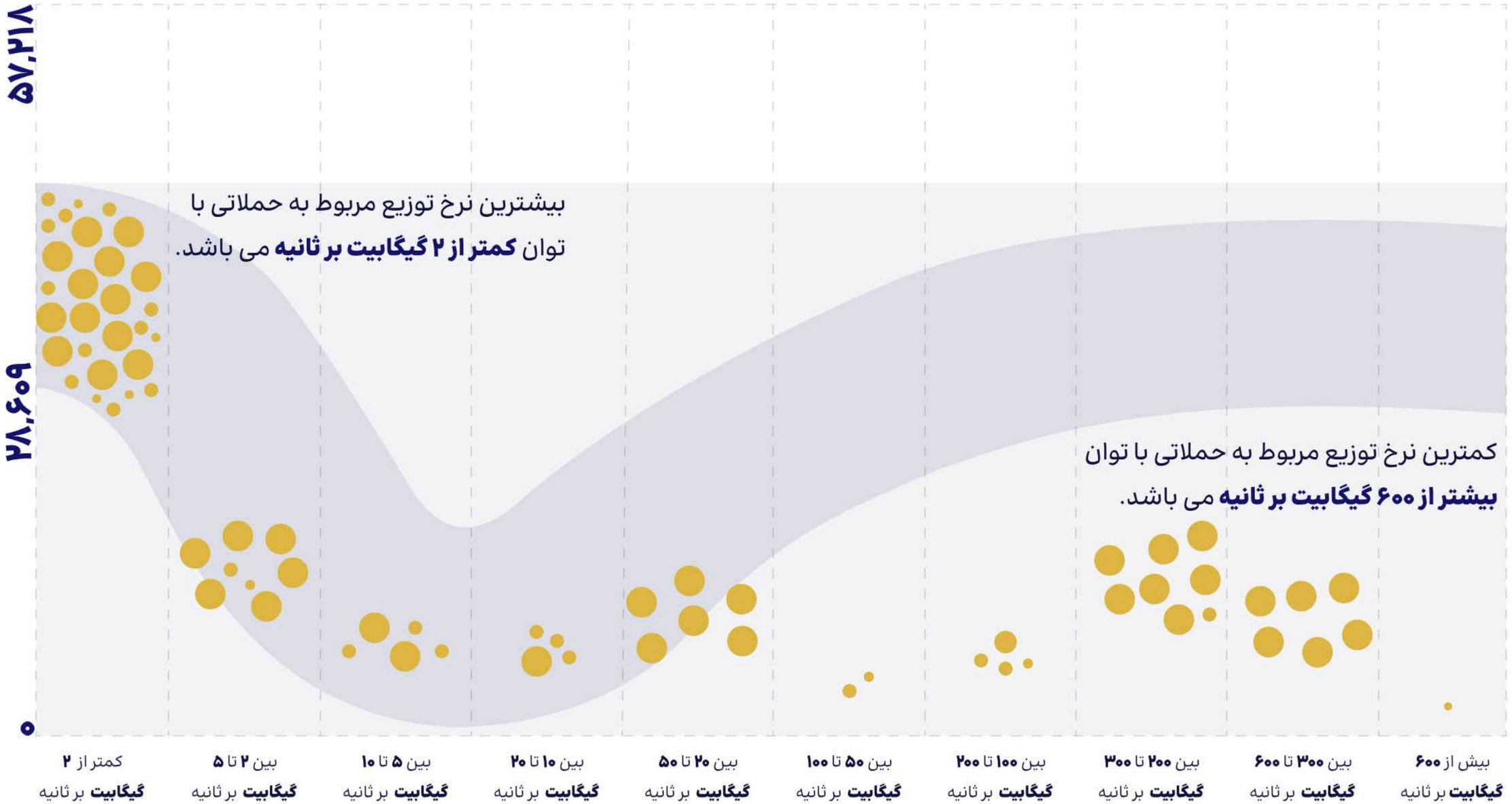
۰۷ آمار تحلیلی حملات منع خدمت توزیع شده

در این بخش به **بررسی و طبقه‌بندی حملات مقابله گردیده** توسط شرکت ارتباطات زیرساخت از منظر مفاهیم تخصصی و مقادیر قابل اندازه‌گیری خواهیم پرداخت.

حجم حملات /بر مبنای بیت بر ثانیه/

این نمودار بیانگر **تعداد وقوع حملات** در هر یک از گروه‌های طبقه‌بندی گردیده بر مبنای حجم ترافیک مقابله گردیده در ثانیه می‌باشد.

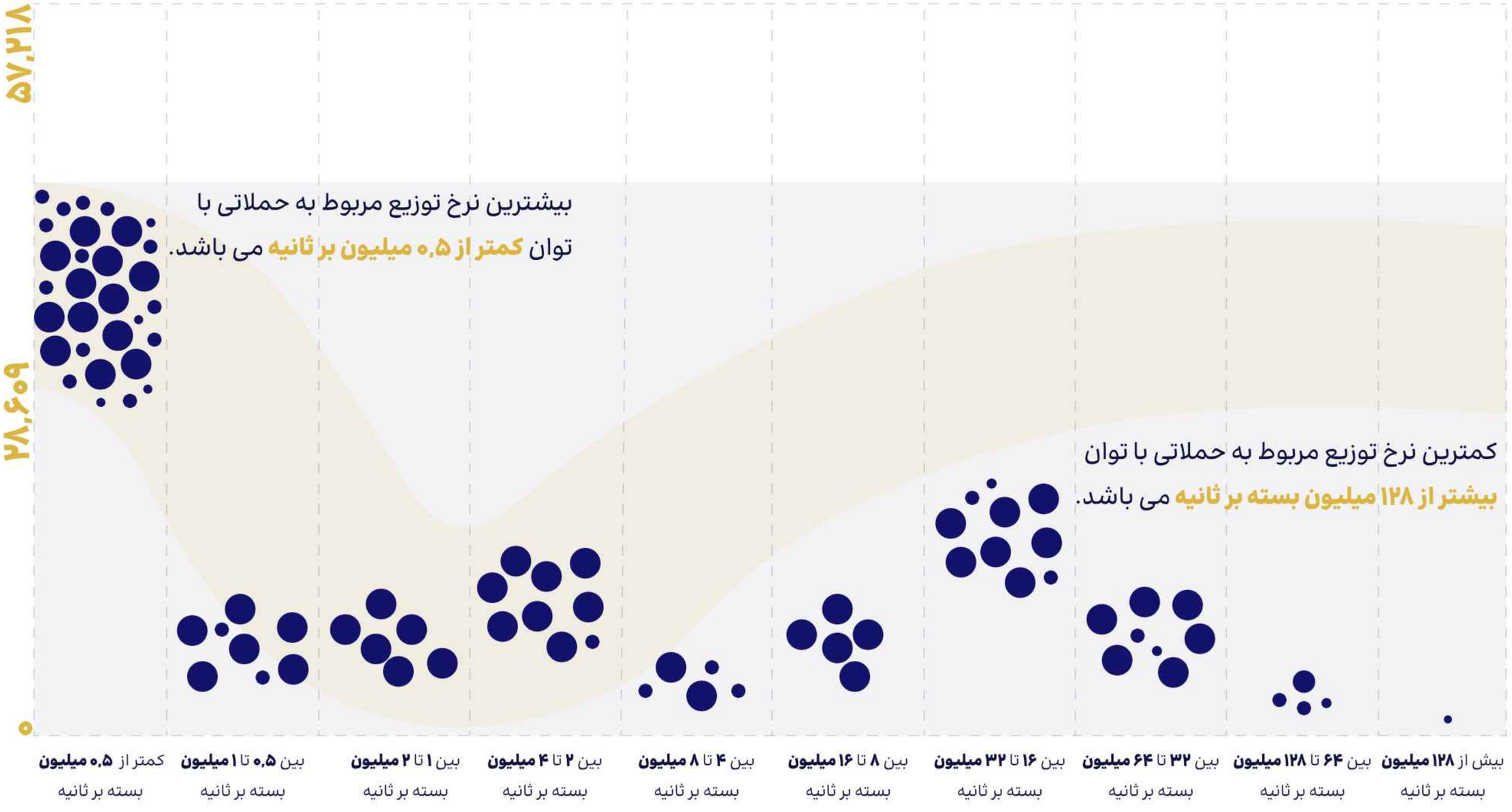
نرخ توزیع حملات به تفکیک حجم حمله / بر مبنای بیت بر ثانیه /



حجم حملات /بر مبنای تعداد بسته بر ثانیه/

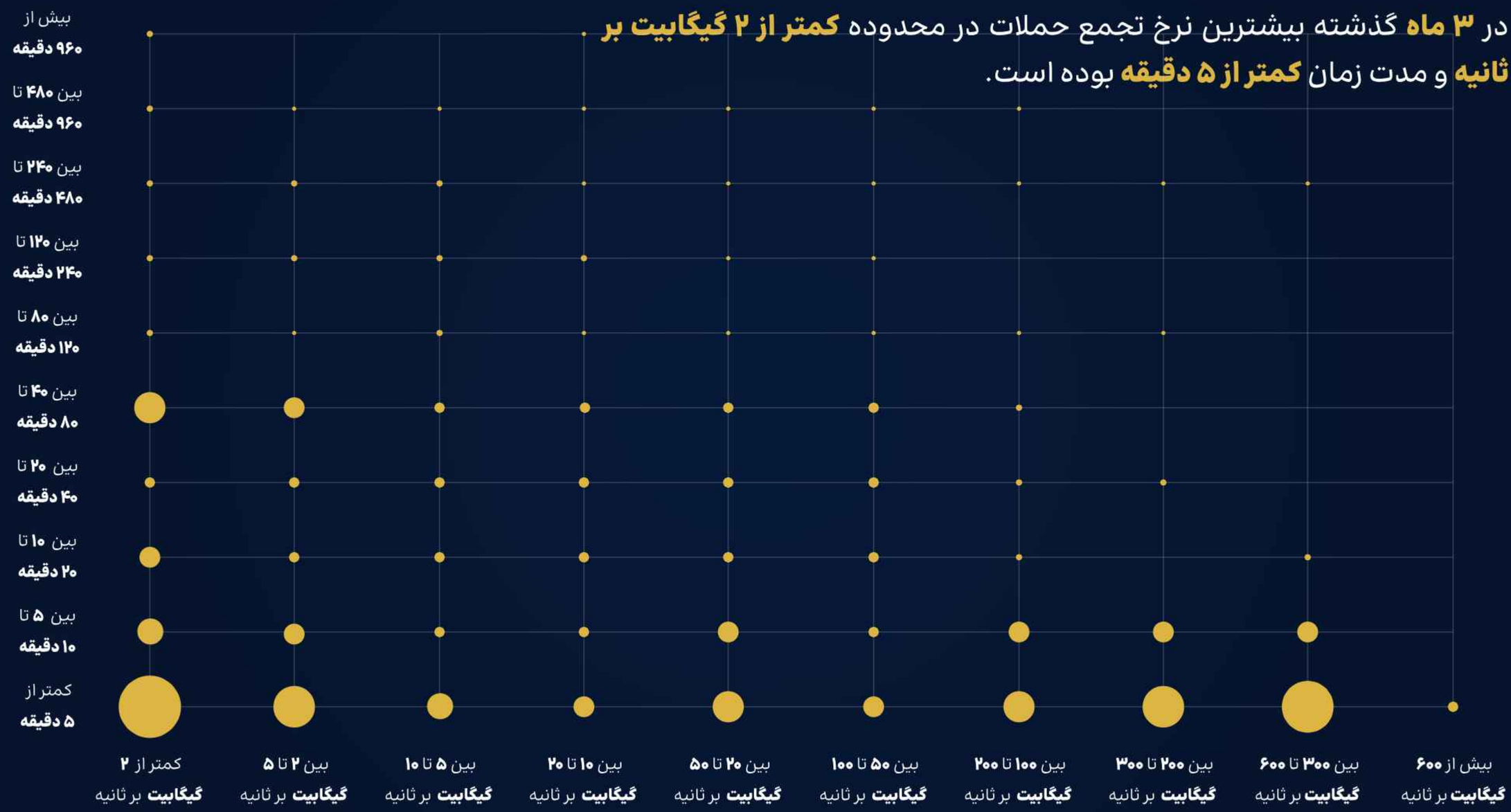
این نمودار بیانگر **تعداد وقوع حملات** در هر یک از گروه‌های طبقه‌بندی گردیده بر مبنای تعداد بسته مقابله گردیده در ثانیه می‌باشد.

نرخ توزیع حملات به تفکیک تعداد بسته / بر مبنای ثانیه /



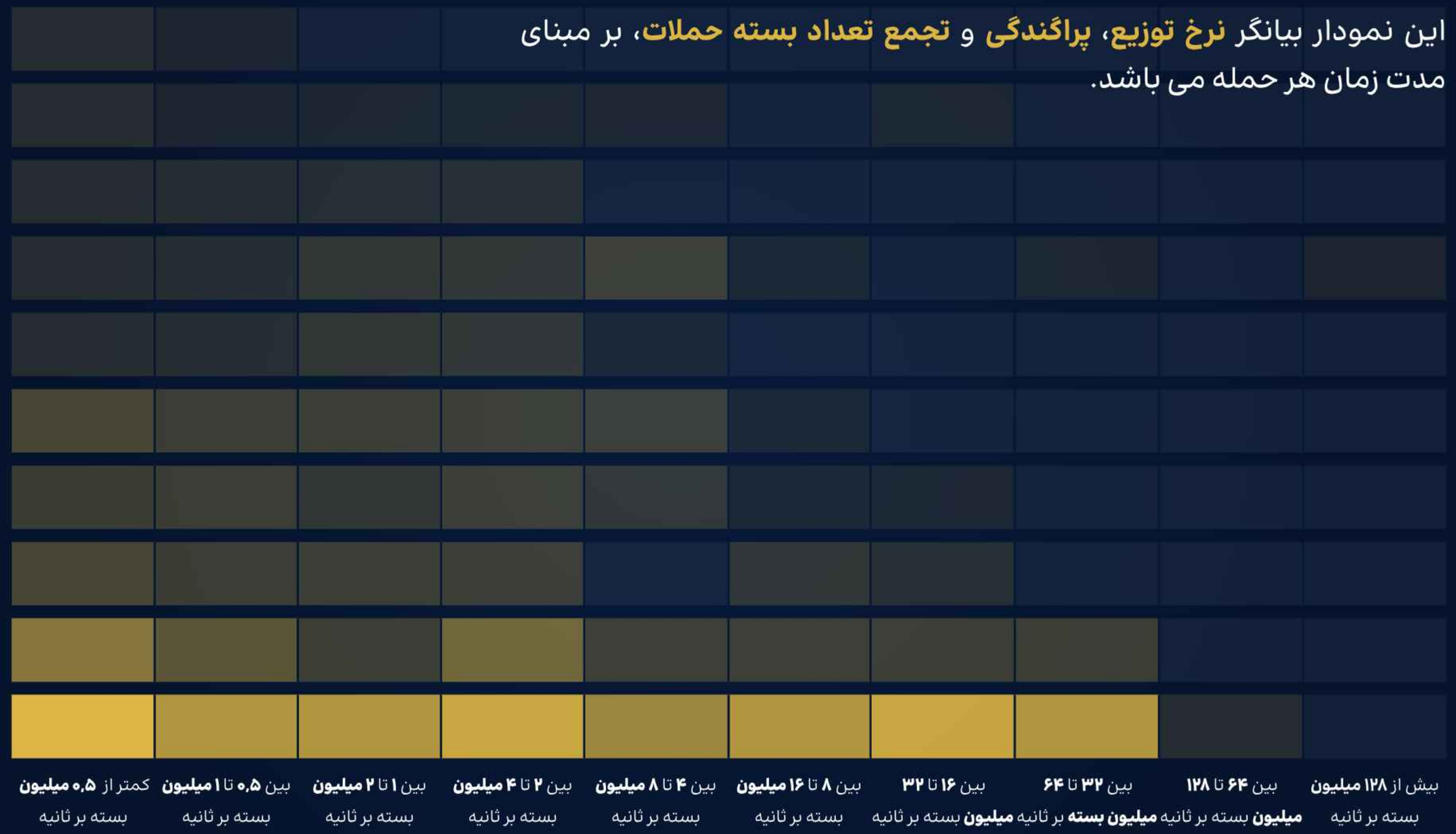
نرخ توزیع و پراکندگی حجم حملات (بیت بر ثانیه) /بر مبنای مدت زمان/

در **۳ ماه** گذشته بیشترین نرخ تجمع حملات در محدوده **کمتر از ۲ گیگابیت بر ثانیه** و مدت زمان **کمتر از ۵ دقیقه** بوده است.



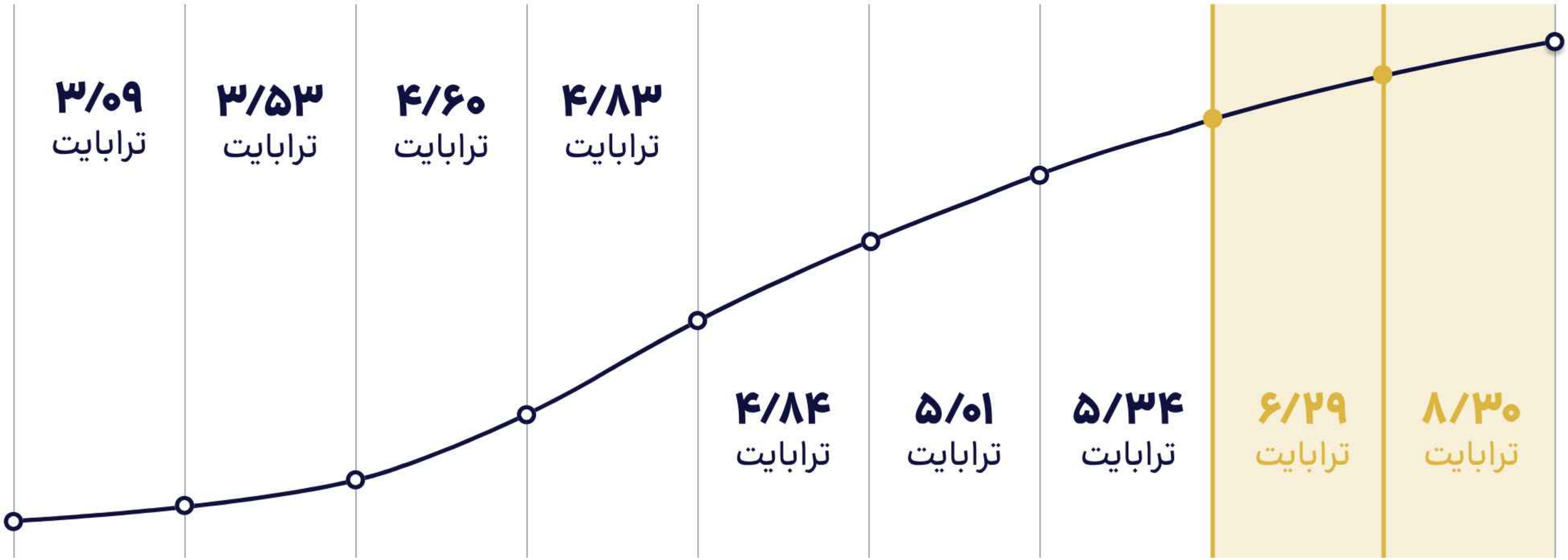
نرخ توزیع و پراکندگی حجم حملات (تعداد بسته بر ثانیه) /بر مبنای مدت زمان/

این نمودار بیانگر **نرخ توزیع**، **پراگندگی** و **تجمع تعداد بسته حملات**، بر مبنای مدت زمان هر حمله می باشد.

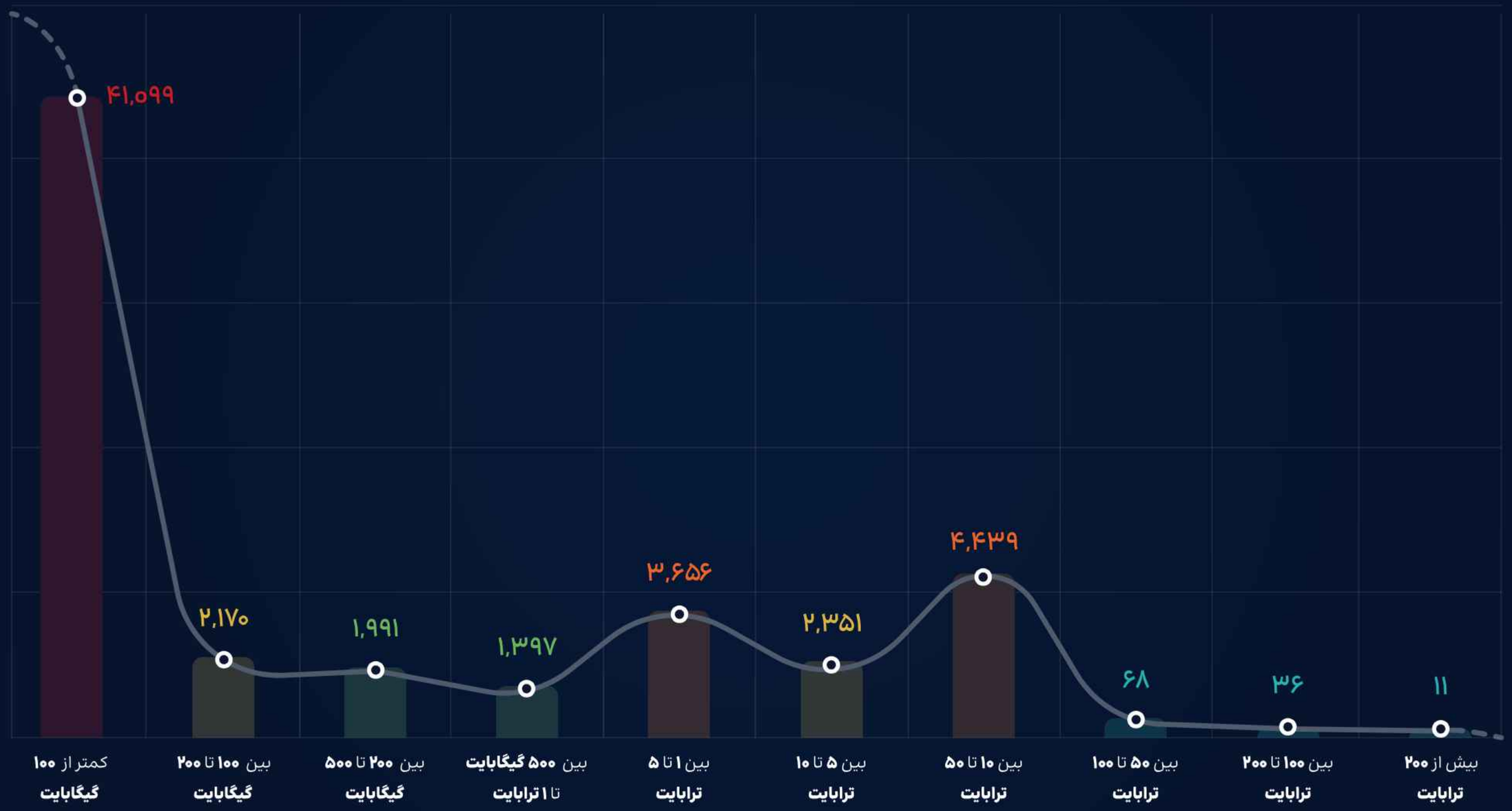


۱۰ حمله برتر / بر مبنای واحد بایت /

از منظر بیشترین حجم ترافیک مقابله گردیده به صورت جمع انباشته



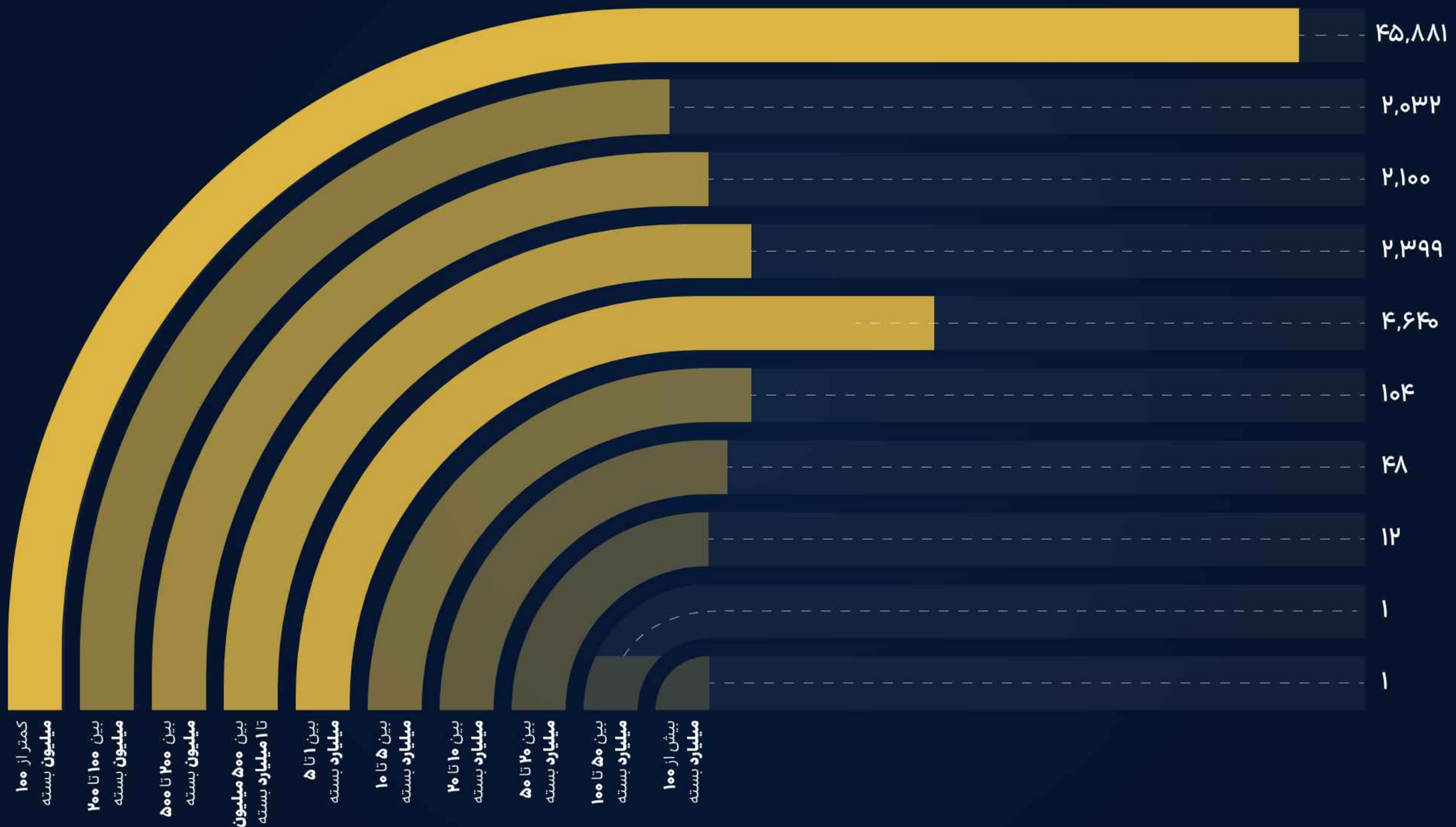
نرخ پراکندگی و تجمع حملات / بر مبنای حجم ترافیک مقابله‌گردیده به صورت جمع‌انباشته /



۱۰ حمله برتر

از منظر بیشترین تعداد بسته مقابله‌گردیده به صورت جمع‌انباشته

نرخ پراکندگی و تجمع حملات / بر مبنای تعداد بسته‌های مقابله‌گردیده به صورت جمع‌انباشته /



نرخ پراکندگی و تجمع حملات / بر مبنای پروتکل /

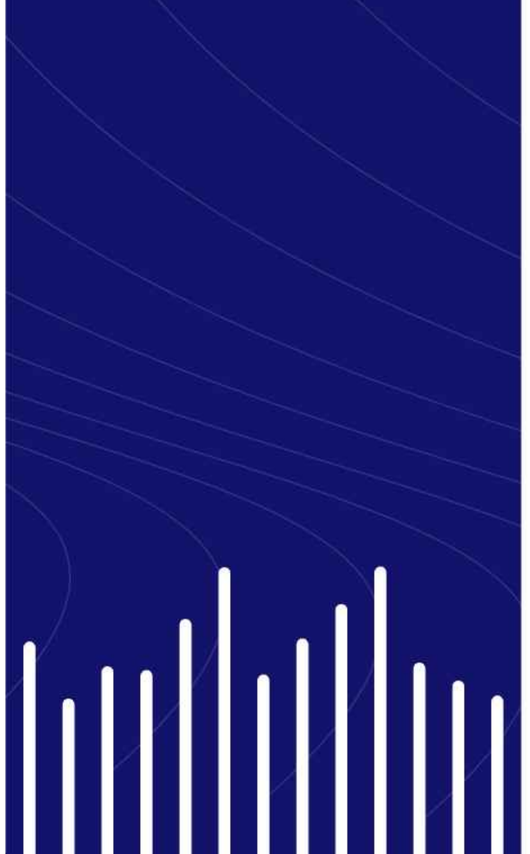
گستره پراکندگی و تجمع حملات منع خدمت توزیع شده به تفکیک پروتکل مورد استفاده در حمله

UDP
%۸۸/۷۳
بیشترین حملات منع خدمت توزیع شده در دوره پاییز

TCP
%۹/۳۳

ICMP & MALFORMED IP
%۱/۹۳

OTHERS
%۰/۰۱



نرخ پراکندگی و تجمع حملات / به تفکیک نوع حمله /

UDP NULL **۳۵,۲۰۲** / %۶۱/۵۲

DNS Amplification **۱۲,۹۵۷** / %۲۲/۶۴

TCP Malformed **۳,۹۹۶** / %۶/۹۸

UDP Flood **۱,۸۲۱** / %۳/۱۸

ICMP Flood & IP Fragmentation **۱,۱۰۵** / %۱/۹۳

ACK Flood **۶۱۰** / %۱/۰۷

NTP Amplification **۵۴۵** / %۰/۹۹

SYN Flood **۵۰۰** / %۰/۸۷

Hybrid Attack **۱۶۱** / %۰/۲۸

SYN | ACK Flood **۱۰۸** / %۰/۱۸

نرخ پراکندگی و تجمع حملات بالای ۱۰۰ گیگابیت بر ثانیه /به تفکیک نوع حمله/

تعداد حملات بر روی مقاصد یکتا

این اعداد بیانگر ۱۰ مقصد برتر از منظر تعداد حملات مقابله گردیده می‌باشد.

این مقاصد به تنهایی سهمی برابر با **۱۵/۰۶%** از کل حملات را در بر گرفته اند.

۰۸/ آمار تطبیقی حملات منع خدمت توزیع شده

در این بخش از گزارش به تجزیه و تحلیل داده های به دست آمده از سامانه تشخیص و مقابله با حملات منع خدمت توزیع شده شرکت ارتباطات زیرساخت در راستای ارائه گزارش تطبیقی از وضعیت حملات مذکور در **دوره پاییز** خواهیم پرداخت.

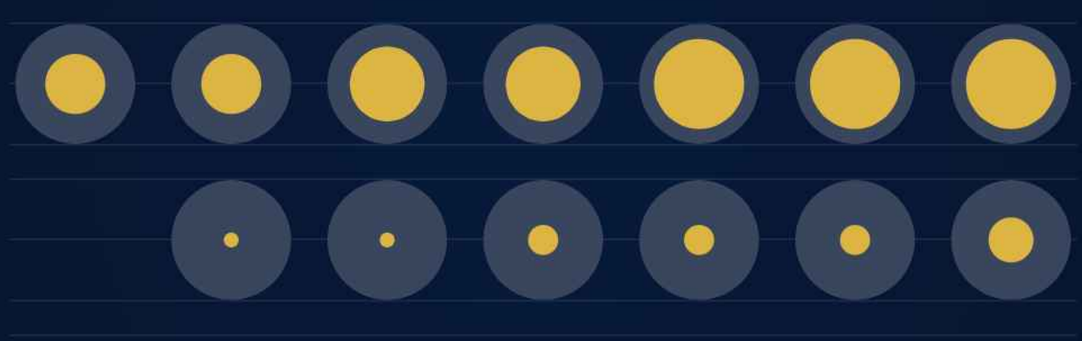
۵۰۰ مقصد بیش از **۲۵۰**

مرتبه مورد حمله قرار گرفته‌اند.

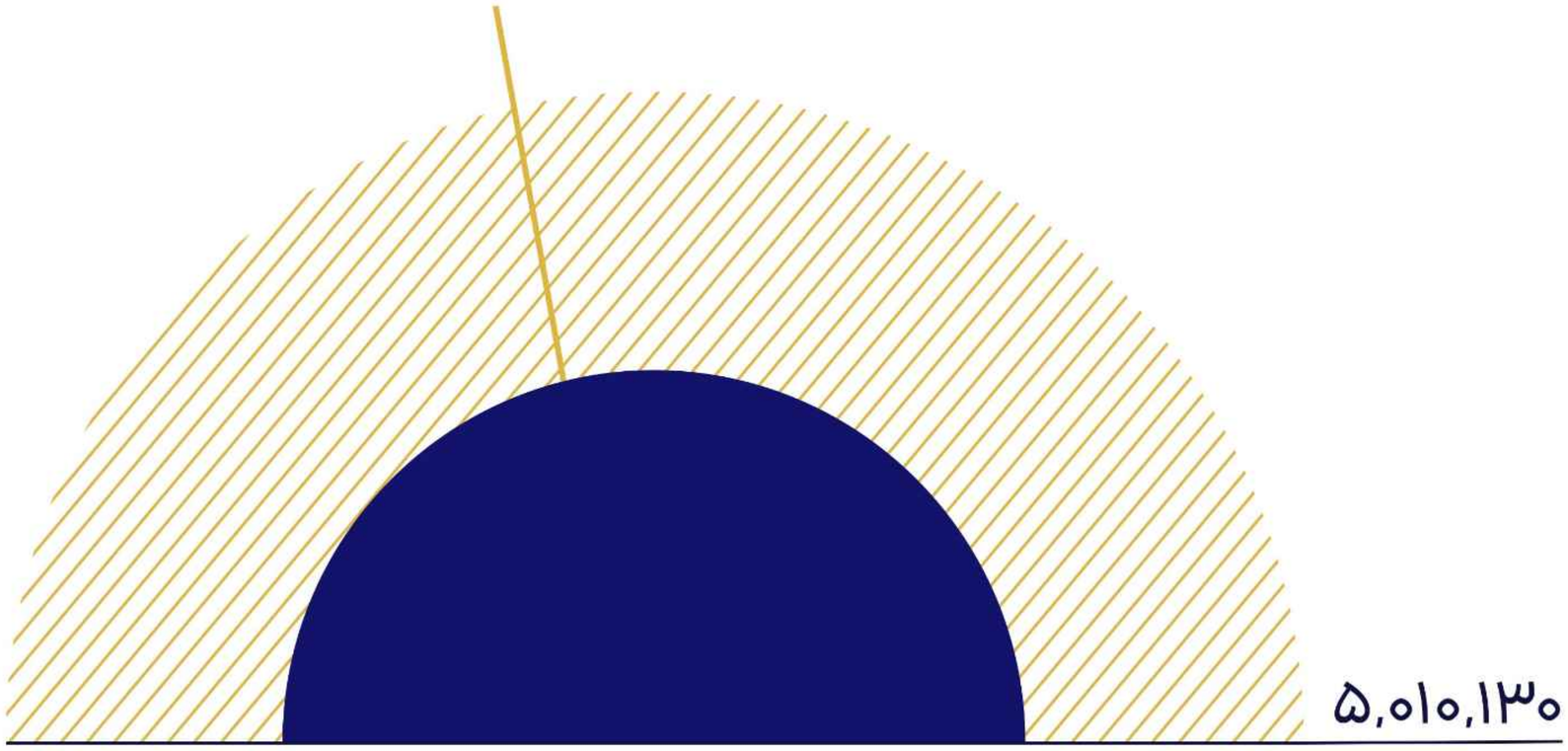
بیش از **۵,۰۱۰,۱۳۰** مقصد

تحت محافظت قرار گرفته‌اند.

۱۳ حمله بیش از **۱** روز به طول انجامیده است.



۵۷,۲۱۸ حمله به **۱۱,۴۴۶ مقصد** صورت پذیرفته است.



طبقه بندی مقاصد تحت حمله

%۱۸/۱۰
شرکت‌های ارائه‌دهنده خدمات اینترنت سیار

%۱۷/۳۴
کسب‌وکارهای اینترنتی

%۱۴/۶۸
شرکت‌های ارائه‌دهنده خدمات اینترنت ثابت

%۱۲/۷۷
درگاه‌های بر خط خدمات عمومی

%۳/۳۹
صنایع انرژی

%۳/۲۰
زیر ساخت های حیاتی ملی

%۷/۳۱
پیام رسان های بومی

%۱۱/۷۹
صنعت مالی، بانکی و بیمه

%۲/۹۸
خبرگزاری ها

%۳/۸۳
سایر صنایع

%۴/۶۱
درگاه های دولتی

/ تحلیل مبادی حمله

نقشه ارائه گردیده بیانگر مبادی حملاتی می باشد که به صورت **Symmetric**، **Direct** و بدون استفاده از تکنیک های **Spoof** و **Reflection** صورت پذیرفته است. با توجه به گستره و طیف متنوع حملات منع خدمت توزیع شده، اعمال سهم مبادی حملات مبتنی بر **Spoof**، **Reflection** و حملات نامتقارن **Amplification** در این نمودار سبب بروز خطای آماری و تحلیلی خواهد گردید.

بیش از **۶۴٪** از حملات تنها از **۱۰ کشور** صورت پذیرفته است.

شایان ذکر است

با توجه به توسعه روز افزون تجهیزات حوزه IOT و همچنین با عنایت به افزایش رو به رشد بات های مورد استفاده حملہ کنندگان، سهم قابل توجه کشور های مذکور در حملات صورت پذیرفته به کشور عزیزمان ایران، الزاما به معنای مدیریت و جهت دهی حملات توسط کشور های نامبرده نبوده و **بسیاری از این حملات با استفاده از تجهیزات آلوده متصل به شبکه و بدون آگاهی کاربران حقیقی صورت پذیرفته است.**

شرکت ارتباطات زیرساخت ضمن تقدیر از تمامی مدیران، نخبگان و متخصصان حوزه فناوری و امنیت سایبری، بر این باور است که پایداری و توسعه زیرساخت‌های حیاتی کشور تنها با تکیه بر دانش، خلاقیت و همت فرزندان این مرز و بوم میسر می‌باشد. دستاوردهای به‌دست‌آمده در این مسیر، گواه روشنی بر اهمیت اعتماد به توانایی‌های داخلی و بهره‌گیری از ظرفیت‌های بومی است که امروز به نقطه قوت کشور تبدیل شده‌اند.

این موفقیت مرهون تلاش‌های ارزشمند کارشناسان شرکت ارتباطات زیرساخت، حمایت و همفکری مدیران ارشد و همچنین همکاری بی‌نظیر بخش خصوصی در زمینه امنیت و توسعه فناوری‌های نوین است. بدین‌وسیله، از تمامی کارشناسان، نخبگان و همکاران بخش خصوصی که با همکاری صمیمانه و تعهدی بی‌مثال، در این مسیر نقش‌آفرینی کرده‌اند، صمیمانه قدردانی می‌شود.

همت و تلاش این عزیزان سرمایه‌ای گران‌بها برای امروز و آینده کشور است. امیدواریم با ادامه این مسیر و تقویت همکاری‌های بین‌بخشی، شاهد پیشرفت و مقاوم‌سازی هرچه بیشتر زیرساخت‌های دیجیتال کشور بوده و بتوانیم زمینه تامین امنیت و رفاه بیشتر جامعه را فراهم سازیم.

شرکت ارتباطات زیرساخت

/ وزارت ارتباطات و فناوری اطلاعات / شرکت ارتباطات زیر ساخت / **گزارش تحلیلی آماری** سامانه مقابله با حملات منع خدمت توزیع شده سیوان / دوره پاییز ۱۴۰۳