گزارش اَبر دِراک
از وضعیت اینترنت سال ۱۳۹۹
در ایران

عناوین

مقدمه

گزارش سالانه با استفاده از پردازش و تحلیل داده‌های فعالیت کاربران اَبر دِراک براساس بازدید از وب‌سایت‌های فعال بر بستر اَبر دِراک در اینترنت تهیه می‌گردد و ارائه‌دهنده تصویری از عادت‌ها و رفتارهای کاربران اینترنت است که شامل رتبه‌بندی‌هایی از ارائه‌دهندگان خدمات هاستینگ (میزبانی)، تامین‌کنندگان اینترنت و ... است.

این گزارش براساس جمع‌آوری و تحلیل داده‌های مراکز داده اَبر دِراک نظیر لاگ‌های سرورهای لبه (Edge Server)، توزیع کنندگان بار (Load Balancers)، زیرساخت‌های DNS و زیرسیستم‌های مانیتورینگ (NOC و SOC) در طول یک سال تولید شده است.

در تهیه‌ی این گزارش سعی شده است تا حد امکان اطلاعات مورد نیاز کارشناسان و فعالان اینترنت و شبکه، گردآوری و بررسی شود. نتیجه‌ی این بررسی‌ها دید بهتری برای کارشناسان و فعالان حوزه‌ی IT کشور به همراه دارد و امکان تحلیل دقیق‌تری از شبکه فناوری اطلاعات کشور را فراهم می‌کند.

از سال گذشته به دلیل همه‌گیری کرونا، روش‌ها و سبک زندگی مردم دچار تغییراتی گردید. وجود این سبک جدید زندگی در رفتارهای کاربران در اینترنت نیز بروز پیدا کرده است. نمونه‌هایی از این تغییر رفتار در تحلیل‌های به‌دست آمده از داده‌های کاربران اَبر دِراک به وضوح دیده می‌شود.

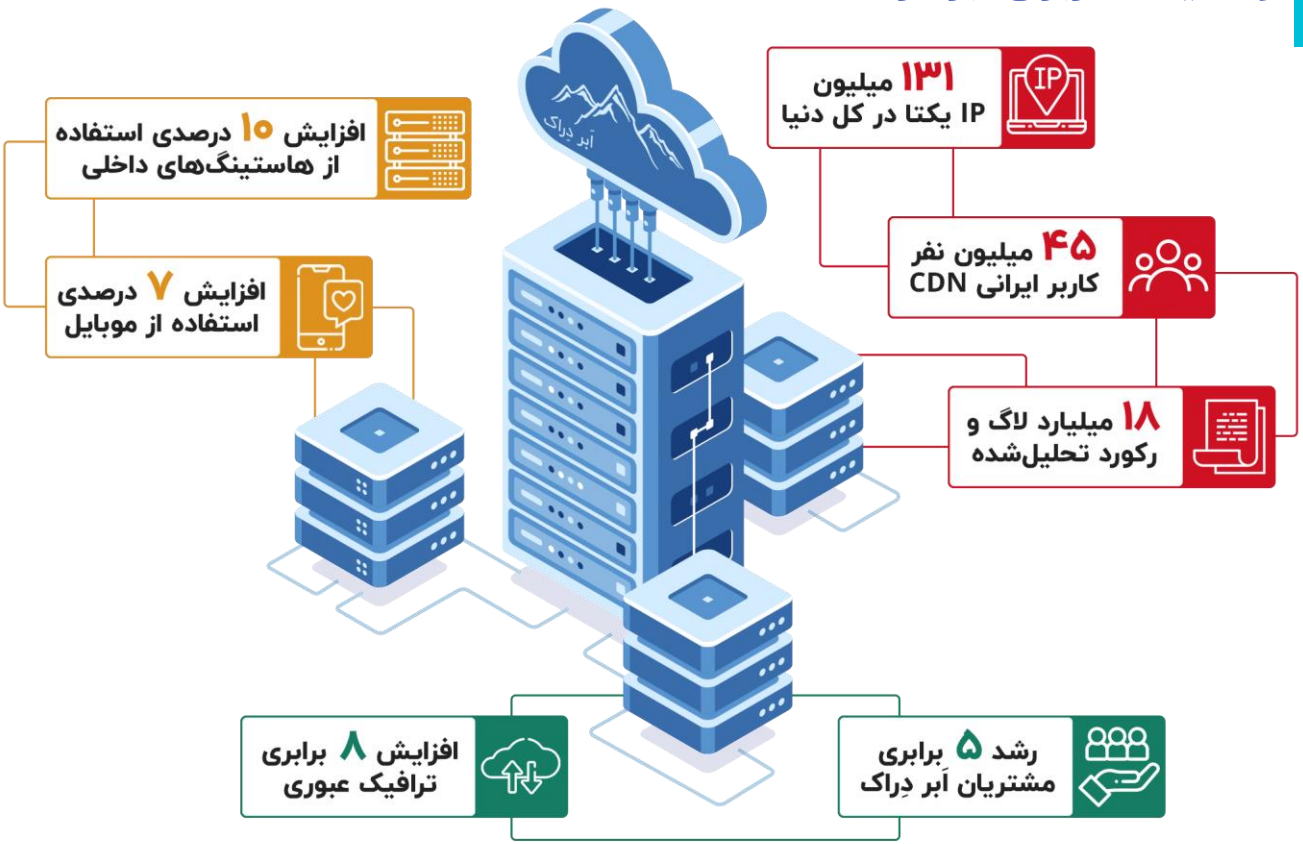
مقدمه

بر اساس تحلیل اطلاعات بدست آمده از این گزارشات، درصد حملات DDoS داخلی از ایران توسط دستگاه‌های آلوده به نرم‌افزارهای مخرب (Botnet) در تجهیزات همراه (تمامی دستگاه‌های هوشمند) از ۱۵ درصد به ۲۴ درصد افزایش داشته و همزمان با رشد دو برابری روبرو شده است.

همچنین تعداد حملات با حجم ترافیکی بالا نسبت به مدت مشابه سال قبل کاهش داشته و در مقابل حملات با تعداد درخواست زیاد مخرب افزایش قابل توجهی داشته‌اند.

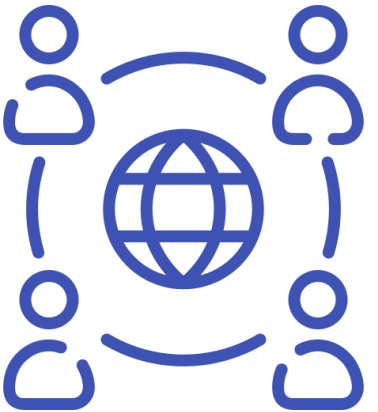
تحلیل اَبر دِراک از این موضوع، اهمیت نیاز به مقاوم‌سازی کسب‌وکارها در سطح اینترنت با استفاده از فناوری‌های امنیت ابری را نشان می‌دهد. چرا که در روش‌های سنتی، مقابله با حملات حجمی به‌وسیله‌ی مدیران فنی و با هماهنگی مراکز داده‌ی میزبان و با استفاده از راهکارهایی مانند BlackHoling رفع می‌گردید؛ اما در روش جدید حملات که با تعداد زیاد درخواست کم حجم صورت می‌پذیرد پیچیدگی‌های فنی بیشتری را برای مقابله با حمله و دفع آن در مقابل کسب‌وکارها قرار می‌دهد.

وضعیت کاربران اَبر دِراک



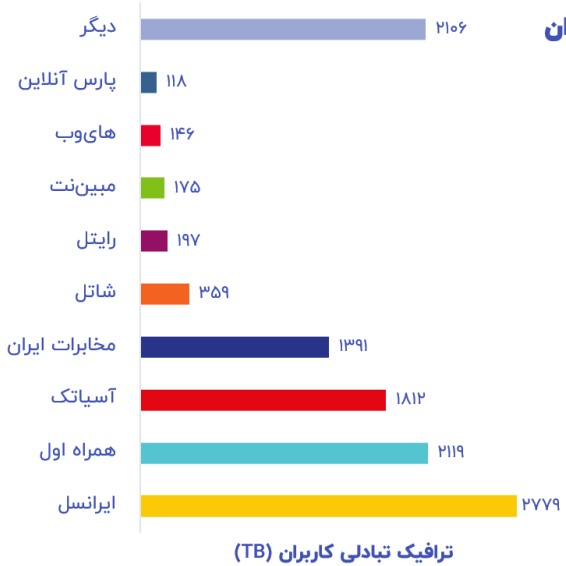
بخش اول

کاربران اینترنت

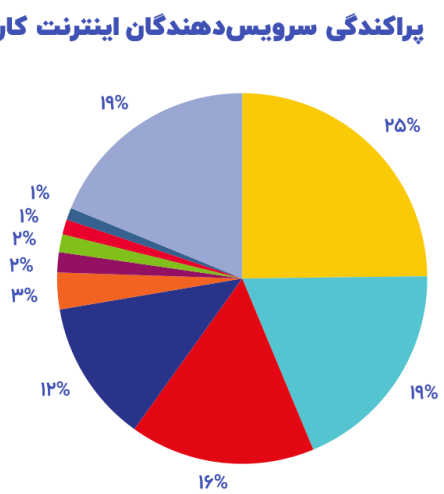


استفاده کاربران از سرویس‌دهندگان اینترنت (ISPها)

بر اساس این داده‌ها، کاربران اینترنت در سال **۱۳۹۹** بیش‌تر از سال **۱۳۹۸** از اپراتورهای همراه استفاده کرده‌اند. ایرانسل و همراه اول از گروه اپراتورهای همراه هر دو در صدر رتبه‌بندی قرار دارند و آسیاتک و مخابرات ایران از گروه اپراتورهای ثابت رتبه‌های بعدی را به خود اختصاص داده‌اند. مطابق با این داده‌ها، **۴** اپراتور ذکر شده دسترس‌پذیرترین ارائه‌دهندگان خدمات اینترنت برای کاربران ایرانی هستند.



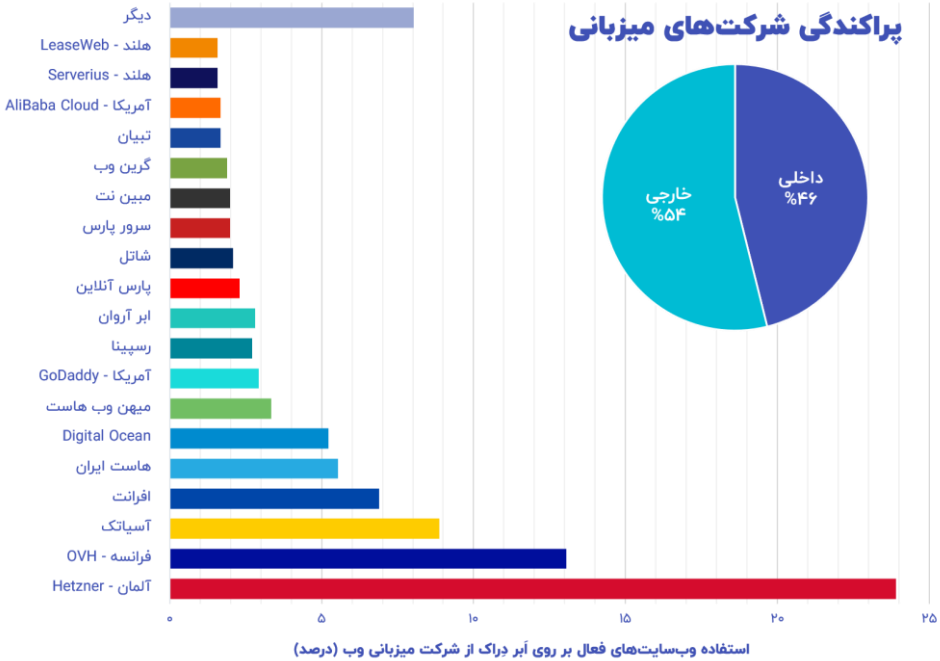
ترافیک تبادلی کاربران (TB)



استفاده صاحبان وب‌سایت‌ها از شرکت‌های ارائه‌دهنده خدمات میزبانی وب

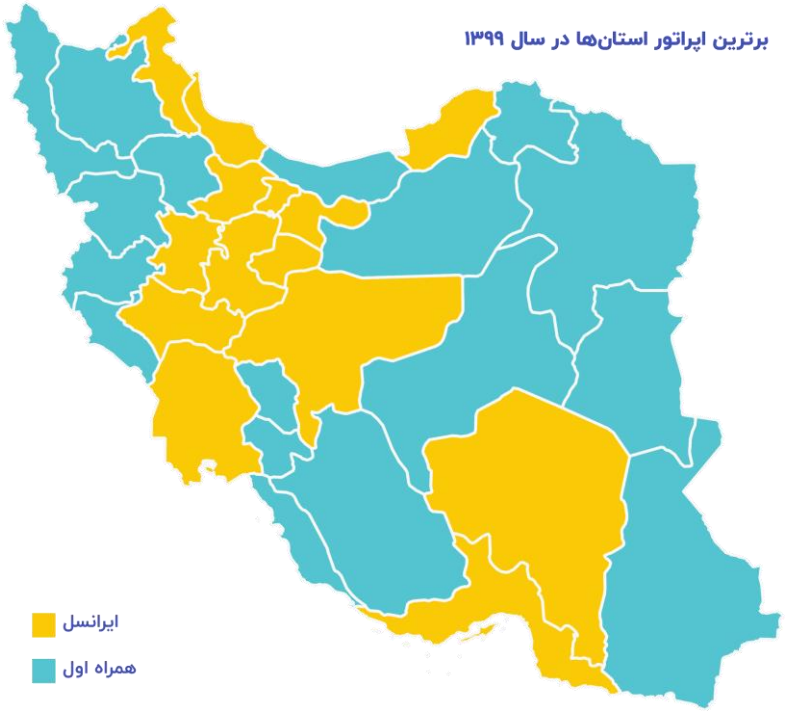
مطابق این گزارش، هرچند کیفیت سرویس‌دهی شرکت Hetzner آلمان و OVH فرانسه همچنان برای صاحبان وب‌سایت‌ها بیش از هر سرویس‌دهنده‌ی دیگری مورد پذیرش است، اما استفاده از میزبان‌های داخلی به نسبت دوره مشابه در سال قبل با ۱۰ درصد رشد روبرو بوده است.

نکته قابل توجه اینکه حتی بعد از رخداد آتش‌سوزی برای مرکز داده‌ی OVH در زمستان ۱۳۹۹، استفاده از این سرویس‌دهنده، دستخوش تغییرات چندانی نبوده و اقبال کاربران تا زمان انتشار این گزارش سیر نزولی نداشته است.



بیشترین استفاده کاربران از تامین‌کنندگان اینترنت در ایران

دو اپراتور سیار با تسلط بازار ۸۰ درصدی و بر اساس بیش‌ترین استفاده در هر استان کشور در این نقشه نمایش داده شده است.

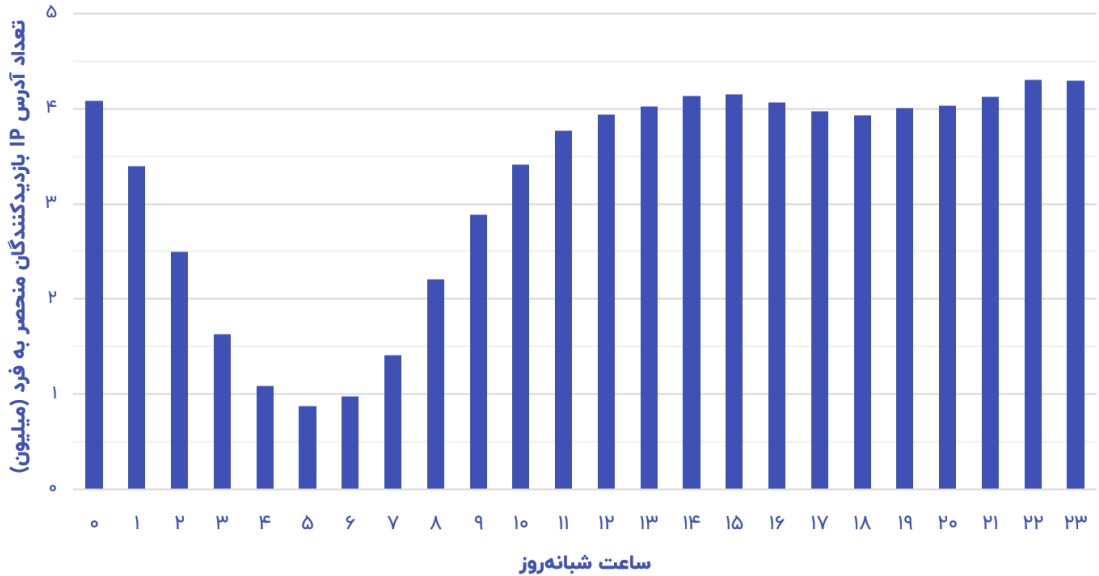


بیشترین استفاده کاربران از تامین‌کنندگان اینترنت در ایران

تامین‌کننده‌های ارتباطات ثابت محلی با بیش‌ترین تعداد کاربر به علاوه تعداد سایر تامین کننده‌ها با مجموع بیش‌تر از ۹۰ درصد از کاربران در استان‌ها و بر اساس داده‌های تحلیلی اَبر دِراک در این نقشه نمایش داده شده‌اند.

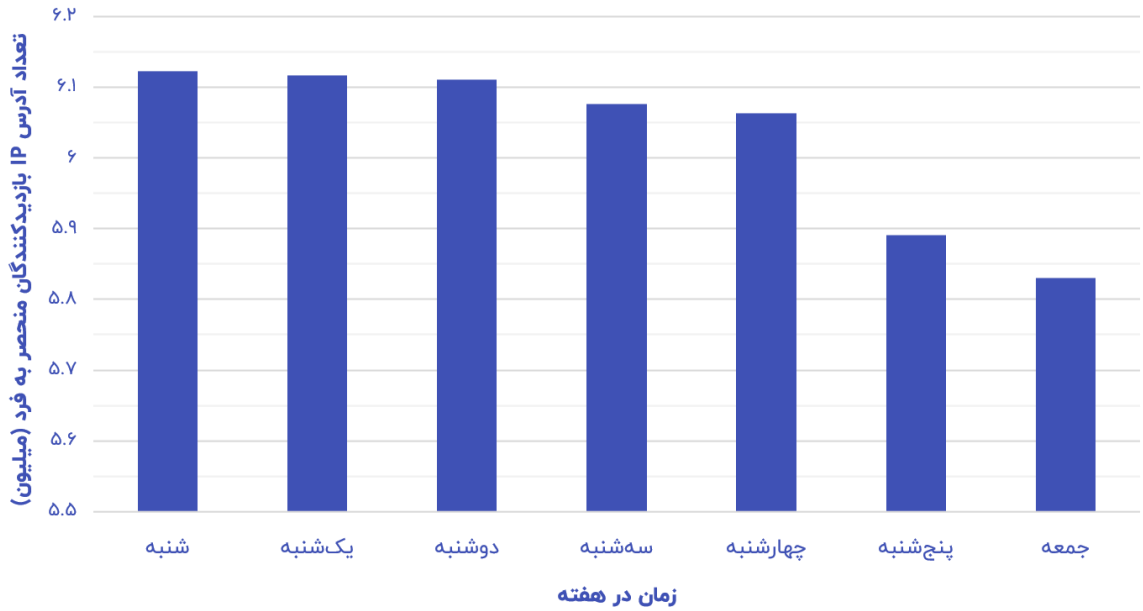
زمان استفاده از اینترنت برای کاربران ایرانی

گسترش استفاده کاربردی از اینترنت در سال گذشته و جایگزینی فعالیت‌های حضوری با روش‌های مشابه اینترنتی به دلیل شرایط کرونا، ساعات افزایش بار ترافیکی اینترنت را از ۱۷ ساعت در روز به ۲۰ ساعت افزایش داده است.
اختلالات سرعت و کیفیت اینترنت در سال گذشته برای اپراتورها به دلیل افزایش همزمانی و همچنین افزایش ساعت‌های پربار بوده که این تغییر رفتار به نسبت دوره مشابه در سال ۱۳۹۸ موید این موضوع می‌باشد.



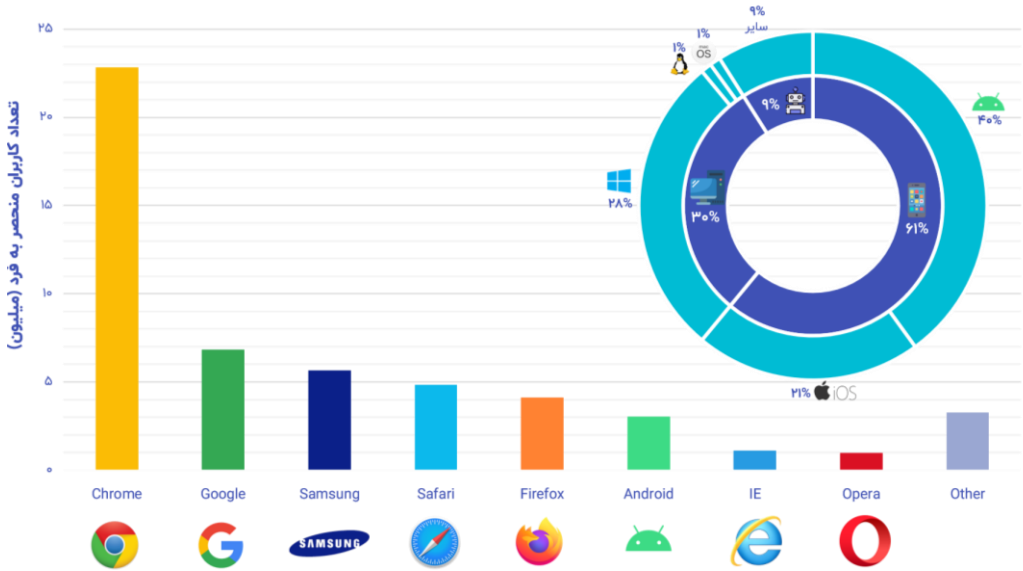
زمان استفاده از اینترنت برای کاربران ایرانی

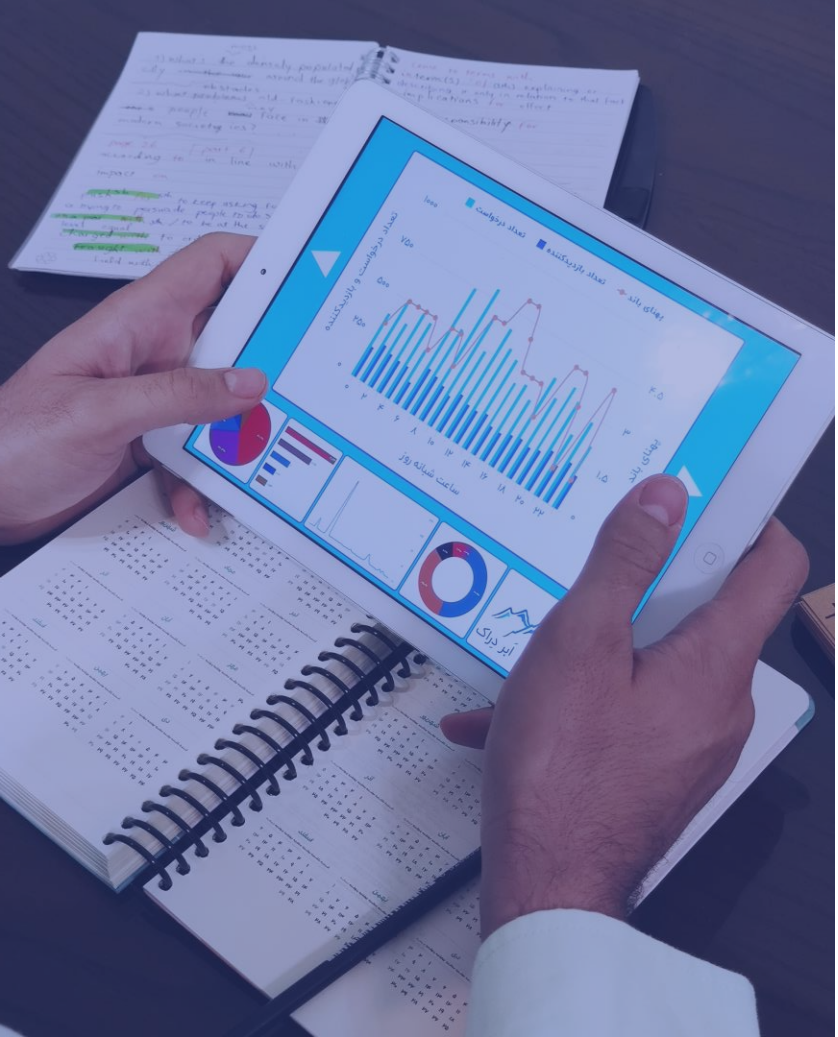
نمودار توزیع تجمعی کاربران اینترنت ایرانی در روزهای مختلف هفته هم نشان از افزایش استفاده از اینترنت نسبت به سال ۱۳۹۸ دارد. این داده‌ها بنا به روزهای تعطیل هفتگی در هر کشور نمایش‌های متفاوتی دارند. بازدید کاربران ایرانی در سال ۱۳۹۹ در روزهای غیر تعطیل رشد بالایی داشته و همچنین در روزهای تعطیل هم به نسبت مدت مشابه در سال قبل با رشد قابل توجهی روبرو بوده است.



مرورگرهای رایج کاربران ایرانی

گوگل‌کروم همچنان محبوب‌ترین مرورگر برای ایرانیان است و ۴۷ درصد استفاده‌ی کاربران را به خود اختصاص داده است. استفاده‌ی گسترده از تلفن‌های همراه و مخصوصا گوشی‌های مبتنی بر سیستم‌عامل اندروید، مرورگرهای موجود بر روی این گوشی‌ها را در رده‌های بعدی استفاده قرار داده است.





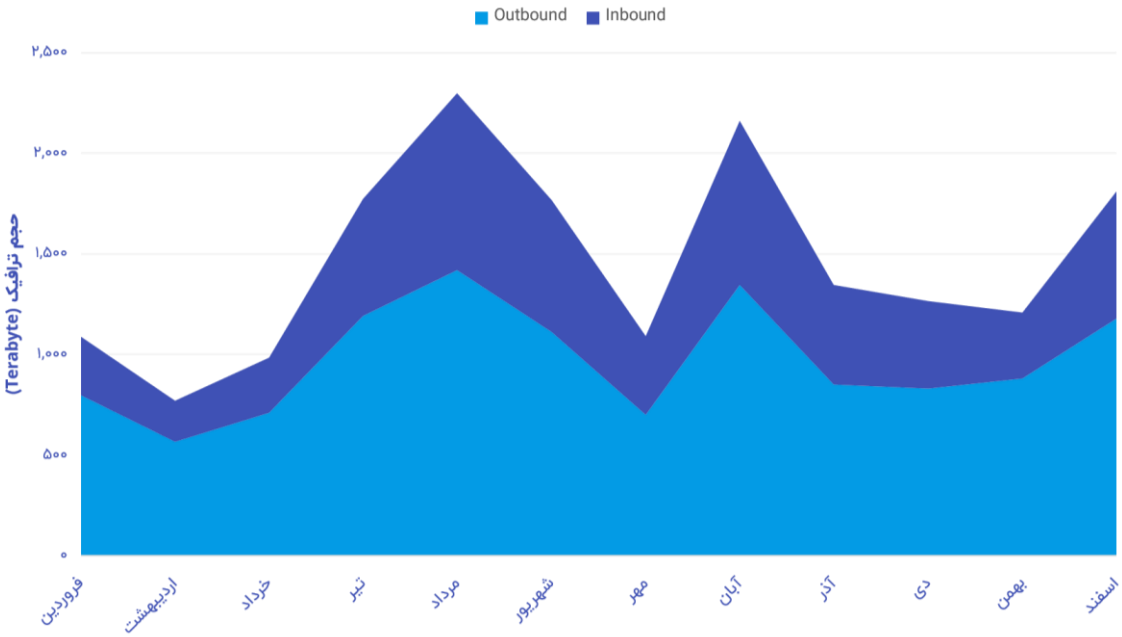
بخش دوم

عملکرد اَبر دِراک

ترافیک تبادلی شبکه‌ی اَبر دِراک

نقاط اوج این نمودار در مِردادماه و آبان‌ماه حاکی از رشد استفاده‌ی کاربران از اینترنت در ایران (وب‌سایت‌های فعال بر بستر اَبر دِراک) در سال گذشته است.

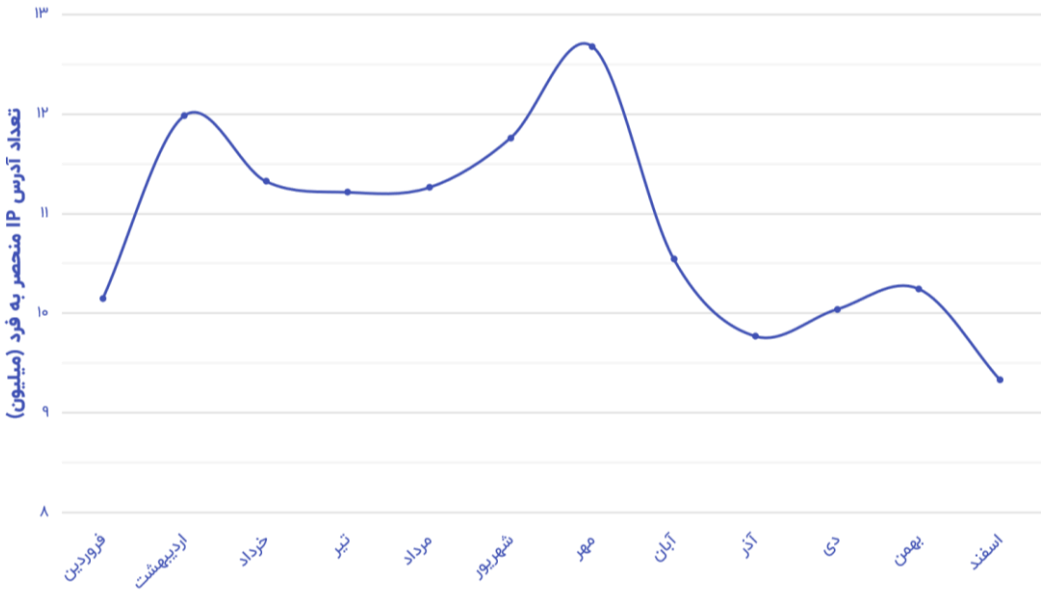
زیرساخت‌های اَبر دِراک رشد ۷ برابری را در حجم ترافیک تبادلی نسبت به سال قبل داشته است.



کاربران منحصر به فرد

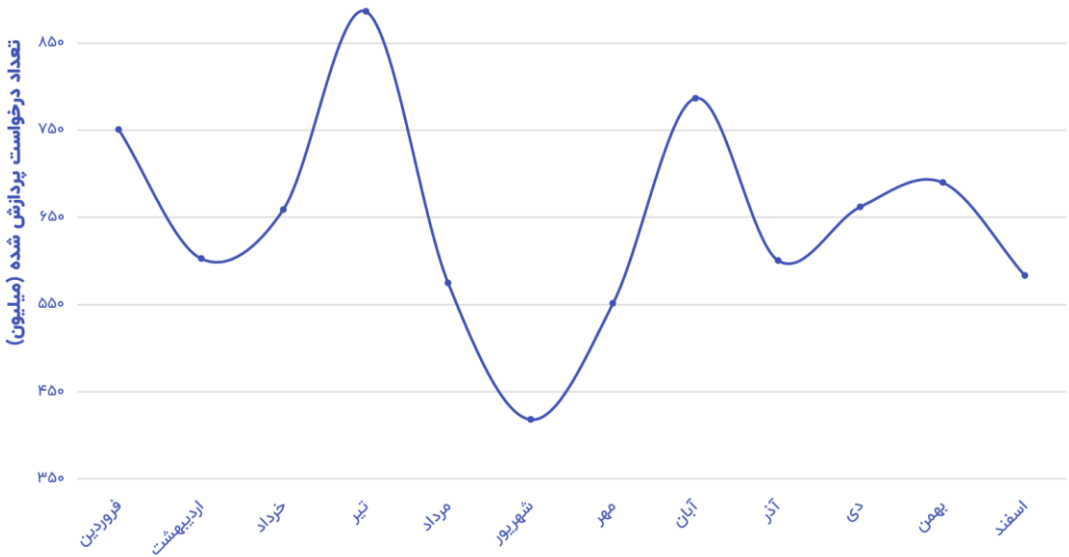
کاربر یکتا، در این نمودار، به آدرس یکتای اینترنتی (IP Address) اطلاق می‌گردد که در هر ماه حداقل یک بار از یکی از وب‌سایت‌های قرار داشته بر بستر اَبر دِراک بازدید کرده‌اند.

میزان کاربران فعال نهایی اَبر دِراک در سال ۹۹ نسبت به سال قبل ۵/۵ برابر افزایش داشته است.



درخواست‌های پردازش‌شده توسط اَبر دِراک

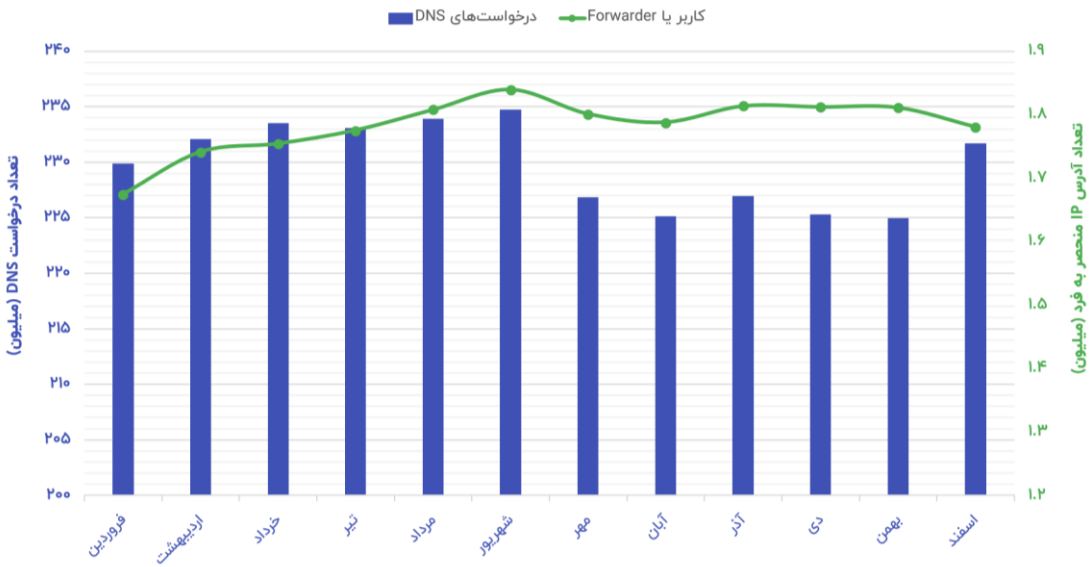
این نمودار نشان‌دهنده‌ی تعداد درخواست‌های کاربران از اَبر دِراک است که توسط اَبر دراک پردازش و پاسخ داده شده‌اند. این درخواست‌ها بدون در نظر گرفتن پاسخ‌گویی از Cache یا سرور اصلی نمایش داده شده‌اند.
در اینجا نیز مطابق با نمودار ترافیک تبادلی، اوج درخواست‌های پردازش شده در اَبر دِراک در زمان‌های قرنطینه در تیر و آبان ۹۹ است.



درخواست‌های DNS

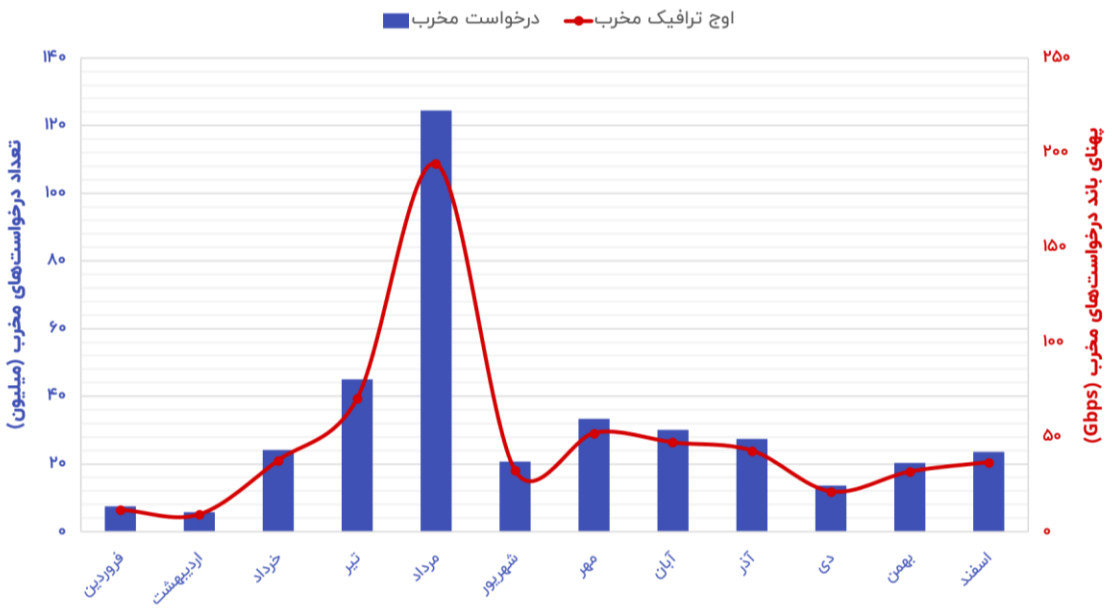
سرویس Cloud DNS اَبر دِراک در کنار راهکار CDN حجم زیادی از درخواست‌های کاربران را پاسخ می‌دهد. نمودار زیر بیانگر نحوه توزیع پاسخ‌های اَبر دِراک به درخواست‌های مختلف DNS کاربران در ماه‌های مختلف سال ۹۹ است.

رشد ۶ برابری IPهای منحصر به فرد به نسبت سال گذشته، نشان‌دهنده‌ی استفاده‌ی بیشتر کاربران مختلف ایران و دنیا از CDN اَبر دِراک است.



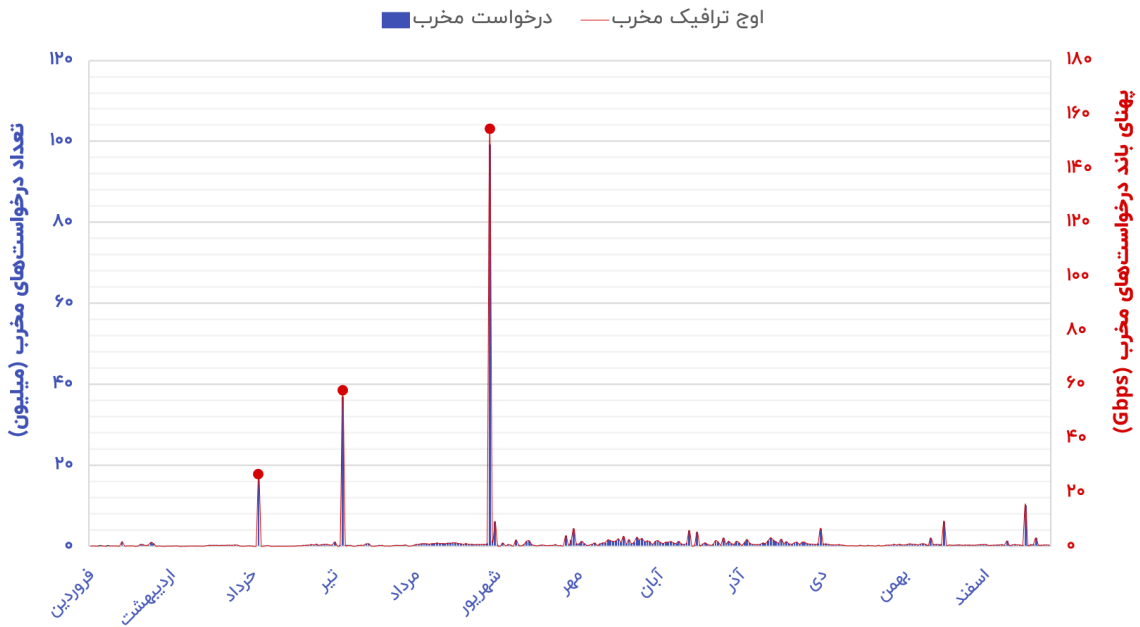
حملات منع سرویس دفع شده

حملات صورت گرفته به وب‌سایت‌های استفاده کننده از بستر اَبر دِراک نسبت به مشابه سال قبل افزایش چشم‌گیری داشته است. ۱۲۰ حمله مخرب توسط سرویس امنیت ابری اَبر دِراک دفع شده که بزرگ‌ترین حجم ترافیک حملات انجام شده ۲۱۰ گیگابیت بر ثانیه بوده است.



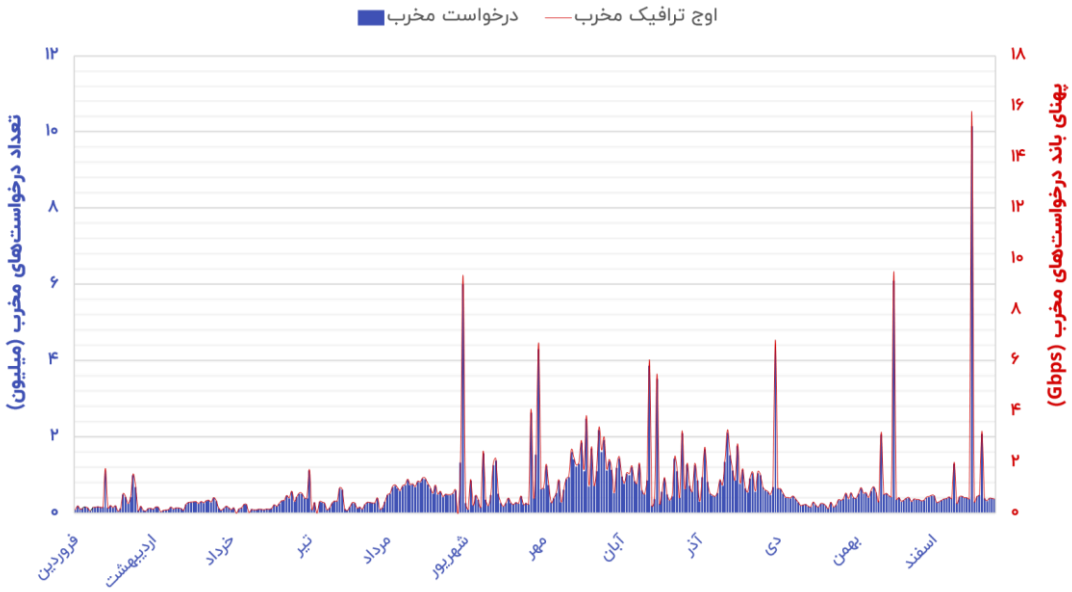
حملات منع سرویس دفع شده روزانه – بزرگ‌ترین ها

در این نمودار ۳ عدد از بزرگ‌ترین حملات و مقیاس آن ها نسبت به سایر حملات نمایش داده شده است.



حملات منع سرویس دفع شده روزانه - سایر

در مقایسه با مدت مشابه سال قبل تعداد حملات روز به روز افزایش یافته و عمده‌ی حملات به سمت حملات با رفتار ارسال درخواست‌های زیاد متمرکز شده‌اند. به همین دلیل استفاده از سرویس‌های امنیتی برای مقابله با این حملات بیشتر از قبل مورد نیاز کسب‌وکارها می‌باشد. نکته دیگر در بررسی حملات این است که دیگر تنها وب‌سایت‌های بزرگ و با بازدیدکننده بالا هدف این حملات نیستند و وب‌سایت‌های کوچک‌تر هم مکررا مورد حمله‌های منع دسترسی قرار می‌گیرند.



اردیبهشت ماه ۱۴۰۰

www.derak.cloud

@derakcloud