

رویداد

مبارزه با کالای قاچاق بعد از ۱۵ آبان

● **فارس:** به گفته رئیس اتحادیه فناوران رایانه تهران، آغاز طرح مبارزه با کالای قاچاق در صنف رایانه از ۱۵ مهر به اول آبان موکول شده و در این فرصت اطلاع‌رسانی و بازرسی درون‌صنفي برای برخورد انجام شده است. مهدی میرمهدی در این باره بیان کرد: با هماهنگی انجام‌شده بین اتحادیه و اتاق اصناف، آغاز طرح مبارزه با کالای قاچاق در صنف رایانه از ۱۵ مهر به اول آبان موکول شده و از روز گذشته آغاز شد. او افزود: در این مدت اطلاع‌رسانی کامل درباره جمع‌آوری کالای قاچاق به واحدهای صنفی انجام شد و بازرسی‌های صنفی افزایش یافت تا با اقدامات درون‌صنفي، واحدها برای آغاز طرح مبارزه با کالای قاچاق آماده شوند. او ادامه داد: در این بازرسی‌ها سندیت کالا از طریق فاکتور فروش بررسی می‌شود و درباره کالاهایی که واردات آنها معتبر نبود، دستور جمع‌آوری از واحد صنفی صادر شده است. به گفته او، برای کاهش ضرر و زیان، به واحدهای صنفی توصیه شد پیش از اجرای طرح اگر کالاهایی از این نوع دارند آن را با قیمت کمتر یا در شهرستان به فروش برسانند و از واحد صنفی جمع‌آوری کنند. او گفت: معتقدیم در صنف رایانه کم‌اظهاری وجود دارد اما به دلیل تعرفه گمرکی مناسب، قاچاق در این بازار نداریم.

صرفه جویی ۵ میلیون یورویی با شبکه توزیع محتوای داخلی

● **ایستا:** مدیرعامل اپراتور سوم ارتباطی از راه‌اندازی شبکه توزیع محتوا (CDN) به وسیله رایتل و صرفه‌جویی پنج میلیون‌یورویی این اپراتور خبر داد. سیدمجید صدری با اعلام این خبر گفت: اپراتور سوم تلفن همراه برای تأمین زیرساخت مورد نیاز خود در زمینه محتوا از پتانسیل بومی و شرکت دانش‌بنیان یکی از دانشگاه‌های طرازاول کشور استفاده کرده است. او ادامه داد: به‌این‌ترتیب استفاده از شرکت خارجی که هزینه‌ای برابر پنج میلیون یورو برای تأمین محتوای چندرسانه‌ای فیلم، کلیپ، سریال و کانال‌های تلویزیونی بر شرکت تحویل می‌کرد، حذف شده است. او بیان کرد: پیش از این، سیستم مورد نیاز در کشور موجود نبود و این شرکت دانش‌بنیان با حمایت رایتل برای اولین‌بار در کشور نسبت به طراحی و ساخت آن اقدام کرده و موفق شد و از این پس می‌توان با استفاده از سیستم داخلی برای توزیع محتوا استفاده کرد. او افزود: اپراتور سوم در حال‌حاضر برخی پورتال‌ها را با استفاده از بستر این شبکه راه‌اندازی تجاری کرده است و نصب و راه‌اندازی این سامانه به شرکت‌های تولیدکننده محتوا مانند شرکت‌ها و سازمان‌های فعال در زمینه تولید محتواهای چندرسانه‌ای، سریال یا فیلم‌های سینمایی کمک می‌کند تا محتواهای چندرسانه‌ای و فرهنگی خود را با استفاده از شبکه رایتل در معرض استفاده از عموم مشترکان این اپراتور قرار دهند و فضای کسب‌وکار جدیدی شکل بگیرد.

برگزاری اجلاس توسعه‌دهندگان وب فارسی

● **شرق:** اجلاس توسعه‌دهندگان وب فارسی ۲۲ آذر با شرکت فعالان وب و توسعه‌دهندگان فضای مجازی از سراسر ایران، به وسیله کانون توسعه‌دهندگان فضای مجازی برگزار می‌شود. حمیدرضا همتی، رئیس کانون توسعه‌دهندگان فضای مجازی، در نشست خبری، بیان کرد: محورهای اصلی برگزاری این اجلاس کسب‌وکارهای اینترنتی، اقتصاد فضای مجازی، امنیت سایبری، سیستم‌های تحت وب و طراحی و توسعه وب است. او گفت: در حاشیه این اجلاس با برگزاری پانلی تخصصی به بررسی فعالیت‌های استارت‌آپ‌های در حال رشد و چالش‌ها و راهکارهای راه‌اندازی استارت‌آپ در ایران خواهیم پرداخت. علاقه‌مندان برای کسب اطلاعات بیشتر و حضور در بزرگ‌ترین گردهمایی توسعه‌دهندگان فضای مجازی باید به وب‌سایت اجلاس به نشانی <http://www.pwconf.ir> مراجعه کنند.

ورود MTN به ایرانیان نت

● **تسنیم:** بعد از گذشت ماه‌ها سکوت و اظهارات سربسته درباره ورود سرمایه‌گذار خارجی به اپراتور چهارم ایران، اما شواهد گویای توافق ایرانیان‌نت با اپراتور چندملیتی MTN «ام‌تی‌ان» است و به‌زودی باید منتظر خبر تمدید انحصار پروانه این اپراتور برای بار دیگر هم باشیم. در این راستا، وزیر ارتباطات هم از مذاکره مسئولان اپراتور چهارم با چند شرکت خارجی برای واگذاری سهام خبر داد. مدت‌هاست بحث مذاکره ایرانیان‌نت با «ام‌تی‌ان» مطرح شده و حتی پیش از سال جاری در گزارش‌های سازمان «مذاکرات همکاری ایرانیان‌نت و «ام‌تی‌ان» به دور پایانی رسید»، گفته شد طرح تجاری ایرانیان‌نت مورد موافقت اپراتور خارجی قرار نگرفته و از این جهت قرار شده طرح تجاری مشترکی با این شرکت خارجی تدوین نشود. حال با توجه به نگاهش‌شدن طرح تجاری مشترک میان این دو شرکت، ظاهراً یکی از پیش‌شرط‌های آن برای سرمایه‌گذاری مجدد در ایران، افزایش مدت زمان انحصار پروانه اپراتور چهارم است. براساس اظهارات یک مقام مسئول اپراتور چندملیتی «ام‌تی‌ان» در نظر دارد در قالب طرح تجاری مشترک ۴۹ درصد سهام ایرانیان‌نت را اختیار کند و اکنون نیز توافقات آنها نهایی شده است.

حمله سایبری وسیع به شرکت خدمات اینترنتی «داین»، برخی از سرویس‌های اینترنتی پربازدید مانند توییتر، آمازون و نت‌فلیکس را مختل کرد. حمله سایبری که نه‌فقط اثر آن را کاربران آمریکایی احساس کردند، بلکه در دیگر کشورها نیز کاربران با کاهش سرعت اینترنت مواجه شدند. خبرگزاری رویجه‌وله در این باره می‌نویسد: شرکت داین که خدمات اینترنتی در اختیار سایت‌های پربازدید قرار می‌دهد، می‌گوید حمله حدود ساعت هفت صبح به وقت شرق آمریکا آغاز شد و چندین ساعت ادامه داشت. علاوه بر سواحل شرقی آمریکا، حملاتی در لندن نیز گزارش شده است. آمازون گزارش داد در آلمان، آمریکا و ژاپن اختلالاتی به وجود آمده است. به گفته مدیران شرکت «داین»، این

حمله با روشی انجام شده که در آن مهاجمان با ارسال درخواست‌های جعلی و پرشمار برای بازدید، یک سرویس اینترنتی را از دسترس خارج می‌کنند. شرکت داین اعلام کرده تمرکز این حمله عمدتاً سواحل شرقی آمریکا بوده است. وبگاه «تک‌کراچ» که در مباحث مربوط به اینترنت و فناوری تخصص دارد، اعلام کرده کاربران اروپایی به صورت یکسان مورد حمله قرار نگرفته‌اند. همچنین اعلام شده هنوز معلوم نیست کدام فرد یا گروه مسئول این حمله است. این حمله سایبری، از جمله برخی از پایگاه‌های اینترنتی نظیر وب‌سایت شبکه خبری «سی‌ان‌ان» و روزنامه «نیویورک‌تایمز» را هم هدف قرار داد. بنا بر گزارش رسانه‌ها، علاوه بر این، برخی وب‌سایت‌ها مانند «نت‌فلیکس»، ارائه‌کننده فیلم و سریال و وب‌سایت Airbnb، ارائه‌کننده اتاق و همچنین «ردیت» نیز مختل شده‌اند. خبرگزاری رویترز نیز گزارش داد هرک‌ها با اجرای حملات پیچیده و دامنه‌دار علیه زیرساخت‌های اینترنت در آمریکا، دسترسی مردم این کشور به ده‌ها سایت

چرا از نت‌ورک‌مارکتینگ می‌ترسیم؟

رضا خاقان: اگر به سایت وزارت بازرگانی، صنایع و معادن مراجعه کنید، متوجه می‌شوید بخشی باعنوان بازاریابی شبکه‌ای وجود دارد. فعلاً اسامی حدود ۲۲ شرکت دارای مجوز به همراه مشخصات نمایندگی‌ها و محصولات‌شان، آنجا فهرست شده‌اند. همچنین در این بخش قوانین حاکم بر این شرکت‌ها برای اطلاع مراجعه‌کننده منتشر شده و حتی به تفکیک و جزئیات، موارد تخلفاتی که ممکن است در این شرکت‌ها رخ دهد، آمده است. اگر به سایت «ایران‌هشدار» هم مراجعه کنید، هم اسامی شرکت‌های بازاریابی شبکه‌ای، تاریخ صدور و انقضای مجوز، نام مدیرعامل و کالاهایی را که می‌توان عرضه کرد، می‌بینید. اگر شرکتی به هر علتی از قواعد و قوانین بازاریابی شبکه‌ای تخطی یا تخلفی کرده باشد، همان‌جا گزینه‌ای به نام «تعداد اخطار دریافتی» وجود دارد. شما به‌راحتی می‌توانید شرکتی را ببینید که به علت تعدد اخطار، لغو مجوز شده یا شرکتی که تا‌به‌حال یکی، دو اخطار گرفته ولی مجوز فعالیتش لغو نشده و در مقابل، تعداد بیشتری شرکت هم تاکنون اصلاً اخطاری دریافت نکرده‌اند. علاوه بر این نظارت‌ها، اگر به سایت هریک از این ۲۲ شرکت هم که مراجعه کنید، متوجه می‌شوید نشان مجوز بازاریابی شبکه‌ای جلو دید مخاطب به صورت چشم‌گزن خودنمایی می‌کند. اگر نشان به رنگ سبز است، یعنی شرکت اجازه فعالیت دارد. اگر به رنگ زرد بود یعنی یک جای کارش ایراد دارد و به او زمان داده شده تا آن را برطرف کند، اگر به رنگ قرمز بود، یعنی شرکت فعلاً تا مدتی برای رفع ایراد به طور موقت تعطیل شده است. این شرکت‌ها مجوز دارند تا محصول خود را به شیوه مستقیم به فروش برسانند، یعنی خریدار به جای مراجعه به فروشگاه، محصول را از سایت سفارش می‌گیرد و دریافت می‌کند.

با همه این توضیحات، چرا در ایران ما همچنان فوبیای بازاریابی شبکه‌ای داریم؟ این همه نت‌ورک‌هراسی از کجا می‌آید؟ پاسخش ساده است؛ «شرکت‌های هرمی». بسیاری از ما که زمانی خود یا نزدیکانمان در شرکت‌های هرمی فعال بوده‌اند، فکر می‌کنند بازاریابی شبکه‌ای همان‌طور که با شرکت‌های هرمی، حقه، کلک و از دست دادن سرمایه و اتلاف وقت و حتی خطرات احتمالی دیگر است.

این درحالی است که شرکت‌های هرمی در همه دنیا غیرقانونی است، ولی بازاریابی شبکه‌ای

قدمتی ۵۰ساله دارد.

یک نفر می‌گفت به علت آن سابقه ناخوشایند

برطرف‌دار را برای ساعت‌های متمادی غیرممکن کردند. بر این اساس، دسترسی مردم این کشور به سایت‌هایی مانند توییتر، پی‌پال، نت‌فلیکس، اسپاتیفای و ... برای ساعت‌های متمادی در روز جمعه ناممکن شد. این حملات با نصب یک بدافزار موسوم به Mirai روی وب‌کم‌ها، ایزار ضبط داده‌های دیجیتال و... صورت گرفت و ثبات جهانی اینترنت را به طور جدی در معرض خطر قرار داد. هدف اصلی این حملات شرکت Dyn در New Hampshire بوده است که زیرساخت‌های اینترنت را در این کشور اداره می‌کند و وظیفه مسیریابی ترافیک بی‌سابقه‌ای روی سایت‌های هدف ایجاد کردند تا کاربران بتوانند به آنها دسترسی پیدا کنند

بر عهده دارد. مهاجمان با سوءاستفاده از صدها هزار ابزار و وسیله متصل به اینترنت که قبلاً به بدافزار Mirai آلوده شده بودند، ترافیک بی‌سابقه‌ای روی

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

حمله هرک‌ها به زیرساخت‌های اینترنت آمریکا دسترسی کاربران دنیا را با مشکل مواجه کرد

اینترنت آمریکا از پای درآمد



سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند. با این کار دسترسی به این سایت‌ها ابتدا در شرق آمریکا و سپس در کل این کشور و بخش‌هایی از اروپا مختل شد. کابل یورک، مدیر استراتژی شرکت Dyn، حملات یادشده را پیچیده و چالش‌برانگیز توصیف کرده و تحقیقات وزارت امنیت داخلی آمریکا و پلیس فدرال آمریکا در این زمینه در جریان است. حملات هکری قبلی مشابه این به وسیله رسانه‌های آمریکایی به روسیه نسبت داده شده و این‌بار نیز رسانه‌های مذکور انگشت اتهام را به سمت روسیه دراز کرده و مدعی هستند هدف نهایی از این اقدامات ایجاد اختلال در زمان برگزاری انتخابات ریاست‌جمهوری آمریکاست. در تقریباً همه ایالات این کشور رای‌دادن با استفاده

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

سایت‌های هدف ایجاد کردند تا کاربران نتوانند به آنها دسترسی پیدا کنند.

از اینترنت برای نظامیان و افراد خارج از آمریکا مجاز است. حملات مذکور از نوع distributed denial-of-service attack یا DDos بوده است. در جریان این حملات با ایجاد ترافیک مصنوعی شدید روی سایت‌های هدف از دسترسی کاربران به آنها جلوگیری می‌شود. کارشناسان امنیتی مدت‌هاست درباره پیامدهای امنیتی خطرناک همه‌گیرشدن اینترنت اشیا هشدار می‌دهند. با گسترش ابزار متصل به اینترنت و با توجه به امنیت پایین بسیاری از این ابزار، می‌توان آنها را در قالب شبکه‌های منسجم به پایگاهی برای مختل‌کردن کل اینترنت مبدل کرد. نیویورک‌تایمز نیز به نقل از تحلیلگران غربی این حملات را مجدداً به دولت روسیه نسبت داده و مدعی است حمله مذکور مقدمه‌ای

برای حمله اصلی به زیرساخت‌های کلیدی اینترنت در آمریکا در زمان برگزاری انتخابات ریاست‌جمهوری این کشور است. کارشناسان امنیتی هشدار می‌دهند تکرار این حملات در روزهای برگززاری انتخابات ریاست‌جمهوری در آمریکا می‌تواند مانع از ثبت آرای مردم ایالات متحده شود و شاید بهتر باشد در این دوره رای‌گیری اینترنتی صورت نگیرد. در ۳۱ ایالت و هم‌طور منطقه کلمبیا رای دهی نظامیان و شهروندان خارج از آمریکا از طریق اینترنت هم ممکن است. مردم ایالت آلاسکا هم می‌توانند از طریق اینترنت رای خود را ثبت کنند. در یک ماه اخیر مقامات آمریکایی بارها روسیه را به هک‌کردن کمیته ملی دموکراتیک وابسته به حزب دموکرات و سرقت اطلاعات ایمیل‌های همکاران هیلاری کلینتون و خود وی با هدف تأثیرگذاری بر انتخابات آمریکا، متهم کرده‌اند. گفته می‌شود اوپاما دستور حملات تلافی‌جویانه را خطاب به آژانس امنیت ملی آمریکا صادر کرده بنابراین احتمال وقوع یک نبرد سایبری جدی بین دو طرف بالا گرفته است.

بازار

J7 Prime میان‌رده پرچم‌دار

● **بدنه** تمام‌فلزی با زبان طراحی پرچم‌داران و سنسور اثرانگشت، این گوشی میان‌رده را به محصولی خوش‌دست و درعین‌حال امن تبدیل می‌کند، محصولی که به‌زودی عرضه می‌شود. خانواده ۲۰۱۵ سری J و پس از آن سری ۲۰۱۶ موفقیت بسیاری در بازارهای جهانی داشتند و این گوشی‌های میان‌رده جزء پرفروش‌ترین گوشی‌های هوشمند در بازار میان‌رده‌ها بودند که به هرچه بهترشدن وضعیت فروش بر بازار گوشی‌های مانند نسخه ۲۰۱۶ گوشی J7 با بدنه تمام‌فلزی وارد بازار می‌شود. طراحی بدنه به‌گونه‌ای است که این گوشی ۱۵.۵اینچی به‌خوبی در دست جای بگیرد و هنگام کار با یک‌دست مشکلی به وجود نیابد. البته سامسونگ در J7 Prime از زبان طراحی پرچم‌داران خود استفاده کرده تا حسی منحصربه‌فرد را به کاربر منتقل کند. دوربین اصلی طوری در بدنه جای گرفته است که هیچ‌گونه برآمدگی روی قاب پشتی احساس نشود و ظاهری کامل، صاف و یک‌دست داشته باشد. از نظر ضخامت هم این گوشی با ضخامتی ۸.۱ میلی‌متری جزء گوشی‌های باریک محسوب می‌شود که روی حاشیه سمت چپش دو درگاه سیم‌کارت قرار گرفته است و یک درگاه مجزای کارت حافظه که تا سقف ۲۵۶ گیگابایت حافظه اضافی را پشتیبانی می‌کند.

حافظه داخلی این گوشی ۱۶ گیگابایت است که با توجه به حجم اطلاعات در دنیای امروزی ممکن است برای برخی کاربران کم باشد. برای رفع این مشکل می‌توان از کارت‌های حافظه میکرواس‌دی استفاده کرد و خبر خوب اینجاست که برای این کار نیازی به قربانی‌کردن سیم‌کارت دوم نیست، چراکه سامسونگ یک درگاه مجزا برای کارت حافظه جانبی در J7 Prime قرار داده که می‌توان تا سقف ۲۵۶ گیگابایت حافظه اضافی را به گوشی اضافه کرد. پروزنده هشت‌هسته‌ای با فرکانس ۱.۶ گیگابایتی حافظه رم سه‌گیگابایتی در کنار پردازنده گرافیکی Mali، تیم پردازشی گلکسی J7 Prime را تشکیل می‌دهند. گلکسی J7 Prime به دو دوربین ۱۳ و هشت‌مگاپیکسلی مجهز است که هردو آنها آپ‌رچر (دیافراگم) f/1.9 دارند. برای گرفتن سلفی‌های عریض (wide) می‌توانید روی دوربین جلوا این گوشی حساب باز کنید و با استفاده از حالت Beauty Mode سلفی‌های بهتر و زیباتری از خود بگیرید.




پهنای باند
مسیر اختصاصی شما



اینترنت یک، آسایت

شرایط فروش، درجه یک

۱۵۴۴asiatech.ir



بزرگترین دیتاسنتر محتوایی در کشور