



سرکوبگران اینترنت؛ نگاهی به عملکرد دادستانی و پیمانکاران سرکوب

پرده‌برداری از نقش نهادهای خصوصی،
دانشگاهی، قضایی و امنیتی در
سرکوب اینترنتی

گروه میان | تیر ۱۴۰۲

گروه میان یک سازمان غیرانتفاعی است که در سال ۹۱۰۲ تاسیس شد و در زمینه حقوق بشر کار فعالیت می‌کند. ماموریت ما افزایش ظرفیت جامعه مدنی برای ترویج حقوق بشر، حکمرانی خوب و عدالت اجتماعی از طریق حمایت و فناوری است.

Table of Contents

خلاصه اجرایی	۴
کارگروه تعیین مصادیق محتوای مجرمانه	۸
زیرساخت‌های فنی	۱۱
کارمندان و ساختار اداری	۱۴
گردان سایبری قوه قضاییه	۱۵
برگزاری کلاس‌های آموزشی برای مامورین سپاه	۱۶
نظارت بر قیمت‌گذاری اینترنت	۱۷
جمع‌آوری اطلاعات رنج‌های آی‌پی	۱۸
آیین‌نامه مدیریت نشانی‌های آی‌پی	۱۹
انواع درخواست سانسور و جمع‌آوری اطلاعات	۱۹
مرکز بررسی جرائم سازمان یافته سپاه پاسداران	۲۰
نظارت بر محتوای سایت‌ها داخلی	۲۰
پژوهشگاه امنیت ارتباطات و فناوری اطلاعات	۲۰
تشکل‌های مردم نهاد	۲۲
جمعیت توسعه‌گران فضای مجازی پاک	۲۳
پیمانکاران سانسور و سرکوب	۲۴
شرکت سحاب‌پرداز	۲۵
شرکت کیسان	۲۶
شرکت یافتار پژوهان پیش‌تاز	۲۸
قرارداد ۴۱۱۹؛ تحلیل ترافیک و سانسور اینترنت	۲۸
سامانه تارپس	۳۰
ابزار کمکی تحلیل متن	۳۱
پردازش تصویر	۳۳
شناسایی بدحجابی و «عربانی»	۳۵

شرکت دانش بنیان نیافام	۳۷
شرکت امن افزار شریف	۲۸
شرکت گروه دوران	۳۹
مشارکت در گروه کاری باز سازمان ملل متحد برای امنیت سایبری	۳۹
قراردادهای توسعه و فروش سیستم‌های سانسور و فیلترینگ	۴۱
قرارداد ۹۵-۹۶: تامین تجهیزات تفکیک ترافیک داخلی و خارجی	۴۱
سپاه پاسداران انقلاب اسلامی: قرارداد رمز کننده شبکه	۴۲
مسدود کردن فیلترشکن‌ها و وی‌پی‌ان‌ها	۴۲
شرکت فن‌آوری‌های تنظیم یار شریف	۴۳
تحلیل شبکه های اجتماعی توسط «لایف‌وب»	۴۶
اینترنت طبقاتی	۴۷
طرح گشایش شریف؛ آزمون اولیه اینترنت طبقاتی	۴۸
وی‌پی‌ان قانونی	۴۹
تحقیقات حقوقی و فنی	۴۹
پروپوزال فیلترینگ	۴۹
ربات شناسایی پست در اینستاگرام	۵۰
دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی	۵۱
راه‌کارهای حقوقی ساماندهی فضای مجازی	۵۳
مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای	۵۴
اپلیکیشن‌ها	۵۶
تپسی	۵۶
تم تم	۵۶
روبیکا	۵۷
کانال دو سر باخت	۵۸
گپ و آی گپ	۵۹
تلگرام طلایی	۶۰

خلاصه اجرایی

این گزارش با استفاده از تجزیه و تحلیل بیش از هشتاد هزار ایمیل لو رفته مربوط به کارگروه تعیین مصادیق محتوای مجرمانه (کمیته فیلترینگ) از سال ۲۰۱۴ تا ۲۰۲۲، کنترل و نظارت اینترنت در ایران را بررسی می‌کند. کمیته فیلترینگ یک نهاد قضایی زیر نظر دادستانی کل کشور است که مسوولیت سانسور اینترنت در ایران را به عهده دارد. این ایمیل‌ها در آبان ۱۴۰۱ توسط گروهی به نام **Anonymous Iran Ops** هک و **افشا** شد و در کانال تلگرام آنها **انتشار** یافت. این گزارش به اطلاعات منابع مورد اعتماد «گروه میان» در شرکت‌های فناوری ایرانی که به شرط ناشناس ماندن با ما صحبت کردند، تکیه دارد.

یافته‌های این گزارش در شرایطی است که در آن دولت ایران پروژه «اینترنت ملی» را برای تشدید کنترل خود بر فعالیت‌های آنلاین شهروندان دنبال می‌کند. این پروژه با نام شبکه ملی اطلاعات شناخته می‌شود و با محدود کردن دسترسی، سرعت یا مقرون به صرفه بودن، برای ایجاد یک محیط آنلاین که خدمات و برنامه‌های محلی را نسبت به خدمات بین‌المللی ترجیح می‌دهد، هدف‌گذاری شده است.

شبکه ملی اطلاعات تهدیدی جدی برای آزادی اینترنت ایرانیان است، زیرا به دولت قدرت بیشتری بر زیرساخت اینترنت، محتوای آنلاین و داده‌های شخصی کاربران و رفتارهای آنلاین می‌دهد. با این حال، شبکه ملی اطلاعات متکی به سرویس‌های توسعه‌یافته ایرانی است، از برنامه‌های پیام‌رسان تا برنامه‌های تاکسی آنلاین که بر روی سرورهای داخل کشور میزبانی می‌شوند. نکته مهم این است که تحریم‌ها، منع قانونی برای توسعه‌دهندگان ایرانی در زمینه استفاده از ابزارها، پلتفرم‌ها و زیرساخت‌های بین‌المللی ایجاد می‌کنند. به عبارت دیگر، آنها برای ایرانیان چاره‌ای جز استفاده از بسته‌های ناامن داخلی و زیرساخت‌های داده در راستای اهداف دولت ایران باقی نگذاشته‌اند.

در مقابل این پس‌زمینه، بازیگران و نهادهای اصلی که در تلاش‌های دولت ایران برای کنترل و سرکوب اینترنت مشارکت دارند، در ادامه خواهد آمد؛ در زیر، فهرستی از توصیه‌های گروه میان را ارائه کرده‌ایم که نشان می‌دهد چگونه دولت‌های ایالات متحده، اتحادیه اروپا و همچنین نهادهای چندجانبه مانند سازمان ملل می‌توانند به بهترین شکل از آزادی اینترنت در ایران حمایت کنند.

« **دادستانی کل کشور:** یک نهاد قضایی قدرتمند است که مسوولیت نظارت بر تمام دادسراهای کشور را بر عهده دارد و ریاست آن با عنوان دادستان کل، رییس کارگروه تعیین مصادیق محتوای مجرمانه و قانون جرایم رایانه‌ای است. این سازمان بر کمیته فیلترینگ نظارت دارد که اینترنت

را در ایران فیلتر و سانسور می‌کند و با شرکت‌ها و فناوری‌های مختلف برای توسعه ابزارهای نظارت و سرکوب همکاری می‌کند. دادستانی کل همچنین در شکل‌دهی و اجرای سیاست دیجیتال ایران نقش دارد و در تعاملات بین‌المللی در زمینه امنیت سایبری و حاکمیت اینترنت مشارکت داشته است. دادستانی کل به نقض حقوق بشر، سرکوب مخالفان و دخالت در مسائل شخصی همچون نحوه پوشش و ظاهر متهم شده است.

« **کارگروه تعیین مصادیق محتوای مجرمانه:** فیلتر و سانسور اینترنت در ایران توسط این نهاد قضایی که زیر نظر دادستانی کل کشور فعالیت می‌کند، انجام می‌شود. کمیته فیلترینگ دارای ساختار داخلی متشکل از ۲۱ عضو به نمایندگی از نهادهای مختلف جمهوری اسلامی است و موظف است هر شش ماه یکبار گزارش فعالیت‌های خود را به روسای سه قوه و شورای عالی امنیت ملی ارائه دهد. کمیته فیلترینگ با شرکت‌ها و صاحبان فناوری‌های مختلف برای توسعه ابزارهای نظارتی و سرکوبی همکاری می‌کند. شرکت‌هایی چون ساترا (سازمان تنظیم مقررات سمعی و بصری)، شرکت تیونینگ فناوری‌های یار شریف، نیافام، یافتار و گروه دوران از این جمله هستند.

« **شورای عالی فضای مجازی:** نهادی محوری در چشم انداز دیجیتال ایران که نقشی تعیین کننده در تدوین و اجرای سیاست‌های اینترنتی و دیجیتالی کشور ایفا می‌کند. شورای عالی فضای مجازی که به دستور رهبر ایران تاسیس شده است، به عنوان بالاترین سطح سیاست گذاری برای فضای مجازی در ایران فعالیت می‌کند و وظیفه مدیریت، نظارت و هماهنگی کلیه فعالیت‌ها و راهبردهای سایبری را بر عهده دارد. اعضای این سازمان را افراد مختلفی از بخش‌های دولتی، دانشگاهی و خصوصی تشکیل می‌دهند و اختیار تنظیم و نظارت بر زیرساخت‌ها و فعالیت‌های اینترنتی در ایران را به عهده دارد. این شامل حوزه‌هایی مانند امنیت اطلاعات، تجارت الکترونیک، خدمات دیجیتال و پیشگیری از جرایم سایبری است که شورای عالی فضای مجازی را به بازیگری کلیدی در شکل‌دهی آینده دیجیتال ایران تبدیل می‌کند.

« **معاون فنی در امور فضای مجازی دادستانی کل کشور:** معاونت فنی در امور فضای مجازی دادستانی کل کشور، مهره کلیدی در سیاست دیجیتال ایران است. این سمت در حال حاضر در اختیار جواد بابایی (از ۶ فروردین ۱۳۹۹) است که سمت قبلی وی ریاست دادسرای جرایم رایانه‌ای بوده است. بابایی هماهنگ کننده فعالیت سازمان‌ها و شرکت‌های مختلفی است که در این زمینه فعالیت می‌کنند. او همچنین بر توسعه پورتال دادستان کل نظارت می‌کند، وب سایتی که به شهروندان اجازه می‌دهد جرایم آنلاین را گزارش کنند. با این حال، ایمیل‌های فاش شده نشان می‌دهد که او علیرغم دست داشتن در سرکوب اینترنت، با سازمان ملل متحد همکاری می‌کند و برای این منظور به خارج

از کشور سفر می‌کند. به عنوان مثال مهدی امیری، مدیر فنی دفتر وی در انتخاب نمایندگان ایران در سازمان ملل در امور امنیت سایبری و حاکمیت اینترنت، با کمک «جمعیت توسعه دهندگان فضای سایبری (پاک)» نقش برجسته‌ای داشته است.

«**ساترا (سازمان تنظیم مقررات سمعی و بصری):** ساترا زیر نظر سازمان صدا و سیما که تحت نظر مقام معظم رهبری فعالیت می‌کند. این سازمان در سال ۱۳۹۵ با هدف نظارت بر تمامی محتوای صوتی و تصویری آنلاین منتشر شده در ایران تاسیس شد. در واقع این سازمان نقشی مشابه وزارت ارشاد اسلامی در رابطه با محتوای آنلاین دارد. ساترا پروژه‌های دیجیتالی متعددی را برای دولت انجام داده است، از جمله ایجاد سیستم مسدود سازی و سانسور اینترنت برای وبسایت‌های خارجی و توسعه پورتال دادستان کل. همچنین مشخص شده که ساترا در توسعه پروژه «مسدود کردن و سانسور اینترنت هوشمند» نقش محوری داشته است.

«**رسول جلیلی:** وی از سوی علی خامنه‌ای رهبر ایران، به ریاست دانشگاه صنعتی شریف و به عنوان عضو شورای عالی انقلاب اسلامی منصوب شده است. جلیلی در نقش‌های مختلف خود عملکرد موثری در شکل‌گیری سیاست دیجیتال ایران داشته است. او چندین ابتکار از جمله طرح «گشایش» (مخفف گسترش شبکه اینترنتی شریف) را که در واقع طرح اینترنت طبقاتی دانشگاه شریف رهبری کرده است. این طرح بحث‌برانگیز، سامانه‌ای را پیشنهاد می‌کند که در آن دسترسی به اینترنت به شکل تبعیض‌آمیزی بر اساس موقعیت‌های حرفه‌ای و اجتماعی افراد صورت می‌گیرد، در نتیجه اصول بی‌طرفی شبکه را نقض می‌کند و دسترسی به اطلاعات را برای اکثریت قریب به اتفاق ایرانیان محدود می‌کند. جلیلی همچنین در توسعه فناوری‌های تشخیص چهره و ابزارهای فیلترینگ و سانسور محتوای اینترنت کمیته فیلترینگ نقش داشت است. که نمایانگر نفوذ قابل توجه او در عرصه فضای مجازی در ایران است. جلیلی در اقدامی راهبردی تلاش داشته تا با پیشبرد فعالیت‌های خود در شرکت‌هایی که نام دانشگاه «شریف» را یدک می‌کشند، به این فعالیت‌ها مشروعیت بخشیده و به جلب اعتماد عمومی بپردازد.

«**شرکت تیونینگ فناوری های یار شریف:** این شرکت توسط رسول جلیلی با هدف کمک به تحقیق و توسعه ابزارهای مورد نیاز دادستانی کل کشور از جمله توسعه «سامانه مستندساز ادله الکترونیکی» ایجاد شده است. این شرکت در ایجاد ابزارهایی مشارکت دارد که می‌توانند از چت‌ها اسکرین شات بگیرند، اطلاعات حساب های مجازی را جمع آوری کنند و اطلاعات نادرست را تشخیص دهند. این شرکت همچنین برنامه‌های آموزشی برای جمع آوری شواهد علیه بازداشت شدگان و توسعه برنامه‌های شخص ثالث با قابلیت جمع آوری اطلاعات خصوصی کاربران ارائه می‌دهد.

« **نیروهای نظامی ایران:** نیروهای نظامی ایران، به ویژه سپاه پاسداران انقلاب اسلامی، به طور فعال در تدوین و اجرای اقدامات سانسور و نظارت اینترنتی مشارکت دارند. آنها همچنین در برنامه‌های آموزشی برای جمع آوری شواهد علیه بازداشت شدگان و توسعه برنامه‌های شخص ثالث با قابلیت جمع آوری اطلاعات خصوصی کاربران شرکت می‌کنند. آنها همچنین از طریق اقداماتی نظیر حمایت از لایحه طرح صیانت در مجلس و فشار بر شورای عالی فضای مجازی تلاش کرده‌اند اینترنت را نظامی کنند. طرحی که اما با مقاومت شدید فعالان جامعه مدنی مواجه شده کمپینی را در مخالفت با این لایحه ساماندهی کردند.

« **دانشگاه عالی دفاع ملی:** این نهاد نقش مهمی در تلاش‌های ایران برای سرکوب اینترنت و نظامی‌سازی فضای سایبری ایفا می‌کند. دانشگاه عالی دفاع ملی که توسط نیروهای مسلح ایران تاسیس شده است، در توسعه و اجرای استراتژی‌های مربوط به امنیت ملی، از جمله در حوزه دیجیتال، نقش اساسی دارد. این دانشگاه سهم قابل توجهی در تدوین تاکتیک‌ها و ابزارهای کنترل اینترنت دارد و آن را به سنگ بنای زیرساخت سرکوب اینترنت ایران تبدیل می‌کند.

« علاوه بر این، کمیته فیلترینگ با شرکت‌های مختلفی همکاری و فناوریهای زیادی برای توسعه ابزارهای نظارت و سرکوب استفاده می‌کند. نمونه‌هایی از این دست را در ادامه خواهید دید:

« **نیافام:** یک شرکت دانش بنیان است که راه‌های مبتنی بر وب را برای سازمان‌ها ارائه می‌دهد، مانند سیستم‌های پورتال هوشمند، سیستم‌های مدیریت محتوا، سیستم‌های چت آنلاین، سیستم‌های مدیریت ارتباط با مشتری و سیستم‌های پشتیبانی آنلاین. همچنین خدمات سئو حرفه‌ای و توسعه نرم افزار سفارشی را ارائه می‌دهد. ایمیل‌های فاش شده نشان دهنده تمایل نیافام برای همکاری با دادستانی کل کشور برای راه اندازی یک پورتال سازمانی با قابلیت‌های ویژه است. ویژگی‌های پیشنهادی شامل تشخیص چهره و شناسایی افراد به تصویر کشیده شده در تصاویر خبری، با هدف افزایش محتوای تولید شده است.

« **یافتَر:** این شرکتی است که از سال ۱۳۹۳ با هدف شناسایی مصادیق «بد حجابی» و «برهنگی» در تصاویر زنان، روی سیستم تحلیل تصویر کار می‌کند. این شرکت همچنین یک برنامه بلند مدت برای توسعه سیستم‌های خزنده وب برای جمع آوری داده‌ها از موتورهای جستجو مانند گوگل، یاهو و بینگ با هدف سانسور فعال دارد.

« **گروه دوران:** گروه دوران متخصص نرم افزار و خدمات شبکه کامپیوتری

است. این یک پیمانکار مسدود کننده و سانسور اینترنت است که نام آن در ایمیل های فاش شده است. شرکت مقدس بود توسط وزارت خزانه داری ایالات متحده به دلیل "سانسور یا سایر فعالیت هایی که آزادی بیان یا تجمع را محدود می کند." دوران همچنین قراردادهایی با ارائه دهندگان اینترنت برای ارائه ابزارهای تجزیه و تحلیل ترافیک تجهیزات سانسور منعقد کرده است.

« **پیامرسان گپ:** این یک پیام رسان مبتنی بر ابر رمزگذاری شده چند پلتفرمی است که ویژگی های مختلفی مانند چت، ایجاد گروه، ایجاد کانال، تماس های صوتی و تصویری، کیف پول، پلت فرم ربات، خدمات بازی و سرگرمی و ایجاد فروشگاه آنلاین را ارائه می دهد. با این حال، این پیام رسان اقدام به سانسور کرده و اطلاعات کاربران را در اختیار دادستانی کل کشور قرار داده است. مدیر عامل گپ مسنجر تابعیت بریتانیا را دارد و شرکت دیگری را در انگلیس تاسیس کرده است.

« این گزارش نتیجه گیری می کند که سیاست دیجیتال ایران با هدف استراتژیک برای کنترل و تنظیم اینترنت هدایت می شود، که در تلاش های آنها برای توسعه ابزارهای نظارتی پیچیده، راه اندازی دسترسی طبقه بندی شده به اینترنت و اجرای خدمات قانونی NPV مشهود است. هدف مقامات ایرانی نیز افزایش کنترل بر دسترسی به اینترنت و اعمال نفوذ در مجامع بین المللی و سازمان ملل است.

توصیه هایی برای شرکت های فناوری، ایالات متحده، بریتانیا، اتحادیه اروپا و سازمان ملل:

۱. ایالات متحده، بریتانیا و اتحادیه اروپا باید تحریم هایی را علیه افراد و نهادهای ذکر شده در بالا به دلیل نقش آنها در سانسور و سرکوب اینترنت در ایران اعمال کنند، مگر اینکه قبلاً تحریم شده باشند. اینها شامل:

۱. رسول جلیلی و شرکت هایش است که در توسعه ابزارهای سانسور و نظارت نقش دارند. با این حال، آنها همچنین باید از تحریم موسسات دانشگاهی مانند دانشگاه شریف که برای اتصال ایرانیان به جهان و پرورش نوآوری و آموزش حیاتی هستند، اجتناب کنند. تحریم این نهادها می تواند به جای حمایت از مردم و جامعه ایران به آنها آسیب برساند.

۱۱. به طور کلی، ایالات متحده، بریتانیا و اتحادیه اروپا باید به دقت آسیب‌های احتمالی تحریم‌ها بر شرکت‌های فناوری و مخابراتی مستقر در ایران یا خارجی یا نهادهای دولتی را ارزیابی کنند. تحریم‌ها می‌تواند نتیجه معکوس داشته باشد و دسترسی ایرانیان به اینترنت رایگان و امن را محدود کند، نه اینکه از آن محافظت کند. بنابراین، تحریم‌های آمریکا و اروپا باید از هدف قرار دادن فناوری‌های «سطح زیرساخت» که برای عملکرد اینترنت ضروری هستند، دوری کنند. تحریم‌های این فناوری‌ها می‌تواند به دولت ایران کمک کند تا اینترنت ایران را منزوی کند و رفتار کاربران را کنترل کند. نمونه‌هایی از فناوری‌های سطح زیرساخت عبارتند از دروازه‌های اینترنتی، ارائه‌دهندگان خدمات اینترنتی، ارائه‌دهندگان داده‌های تلفن همراه، خدمات ابری و مراکز داده.

۲. همه پلتفرم‌های دیجیتال، به‌ویژه برنامه‌های پیام‌رسان و رسانه‌های اجتماعی مانند واتس‌آپ، تلگرام، اینستاگرام و توییتر، باید ویژگی‌هایی را در نظر بگیرند که حریم خصوصی کاربر را افزایش می‌دهد، مانند گزینه‌ای برای غیرفعال کردن تصاویر صفحه. در حالی که سیگنال قبلاً این ویژگی را پیاده‌سازی کرده است، باید به طور گسترده‌تری به عنوان معیار استاندارد حفظ حریم خصوصی در همه پلتفرم‌های مشابه مورد استفاده قرار گیرد.

۳. شرکت‌های فناوری باید فعالانه به دنبال مشارکت با سازمان‌های جامعه مدنی و گروه‌های متخصص در آزادی اینترنت باشند. این همکاری‌ها، به‌ویژه با آن‌هایی که درک عمیقی از سیاست‌ها و زمینه‌های منحصربه‌فرد اینترنت ایران دارند، می‌تواند به این شرکت‌ها کمک کند تا به طور مستمر خط‌مشی‌ها و خدمات خود را برای محافظت بهتر از امنیت و حریم خصوصی کاربران ایرانی اصلاح کنند.

به ویژه، شرکت‌های فناوری مستقر در ایالات متحده و اتحادیه اروپا باید:

۱. دسترسی به زیرساخت‌های ابری خود را فعال کنید و از کانال‌های پرداخت جایگزین مانند ارز دیجیتال پشتیبانی کنید تا خدمات ایمن را برای ایرانیان داخل کشور ارائه دهید. این نه تنها امنیت کاربران ایرانی را تضمین می‌کند، بلکه آنها را قادر می‌سازد تا VPN‌های خود را با استفاده از زیرساخت‌های بین‌المللی راه‌اندازی کنند.

۱۱. پروکسی‌ها را در ابزارهای خود، به‌ویژه برنامه‌های ارتباطی امن مانند Wire یا پلتفرم‌های رسانه‌های اجتماعی مانند Pleroma ادغام کنید و آنها را به صورت رایگان در اختیار کاربران ایرانی قرار دهید. پروکسی‌ها می‌توانند به کاربران کمک کنند تا سانسور

را دور بزنند و به وب سایت‌ها و خدمات مسدود شده دسترسی پیدا کنند.

۳. دستورات عمل‌ها و بهترین شیوه‌ها را برای ادغام پراکسی‌ها در ابزارهای ارتباطی، با تأکید بر نیاز به رمزگذاری قوی، رابط‌های کاربری و حداقل تأثیر بر عملکرد و سرعت، توسعه و توزیع کنید.

۴. سیاستگذاران در اتحادیه اروپا و ایالات متحده باید به طور مشابه به دنبال تعامل با جامعه مدنی و جامعه آزادی اینترنت آگاه در مورد سیاست‌های اینترنتی ایران باشند تا از تصمیمات سیاسی آگاهانه‌تر و موثرتر اطمینان حاصل کنند. آنها همچنین باید فوراً بودجه‌ای را برای حمایت از VPN و سایر فناوری‌های دور زدن، که برای غلبه بر سانسور و دسترسی به اطلاعات در ایران ضروری هستند، اختصاص دهند. به ویژه، آنها باید:

۵. هم روی افزایش مقیاس VPN‌های موجود و فناوری‌های دور زدن سرمایه‌گذاری کنید و هم در توسعه موارد جدیدی که از معماری‌ها و تکنیک‌های نوآورانه برای مقاومت در برابر سانسور و مسدود کردن استفاده می‌کنند. نمونه‌هایی از این فناوری‌ها عبارتند از We-PN که به کاربران خارج از ایران اجازه می‌دهد تا اتصال اینترنتی خود را با کاربران داخل کشور به اشتراک بگذارند. VPN‌هایی که از سرورهای مبتنی بر ایران برای دور زدن خاموش شدن داده‌های تلفن همراه استفاده می‌کنند. دلتا چت، که از شبکه‌های ایمیل مستقر در ایران برای فعال کردن پیام‌های رمزگذاری شده ایمن در هنگام خاموش شدن اینترنت بین المللی؛ و Snowflake، یک سیستم VPN که کاربران را به شبکه عظیمی از سرورهای غیر متمرکز متصل می‌کند.

۱. روی دیش‌های ماهواره‌ای Starlink سرمایه‌گذاری کنید، که می‌تواند برای تعدادی از کاربران دسترسی نسبتاً رایگان به اینترنت در دوره‌های اختلال شدید فراهم کند.

۲. در پروژه‌های تحقیقاتی فنی سرمایه‌گذاری کنید که داده‌های شبکه ملی اطلاعات ایران را جمع‌آوری و تجزیه و تحلیل می‌کند تا بینش بیشتری در مورد زیرساخت‌ها، مسائل اتصال به شبکه و روش‌های سانسور به دست آورید. این تحقیق به توسعه دهندگان NPV و ابزار کمک می‌کند تا فناوری‌هایی را ایجاد کنند که در ایران بهتر کار کنند.

۳. روی برنامه‌هایی سرمایه‌گذاری کنید که امنیت دیجیتال ایرانیان را افزایش می‌دهد، مانند کمپین‌های عمومی، منابع در دسترس، میزهای کمک و کارگاه‌ها و جلسات آموزشی برای فعالان،

روزنامه‌نگاران و جامعه مدنی در داخل ایران. تغییر رفتار کاربران
بخش مهمی از استفاده ایمن از اینترنت در ایران است.

۶. گوگل باید بررسی کند و اقداماتی را برای جلوگیری از سوء استفاده
احتمالی از خدمات خود، مانند عملکرد جستجوی امن یا Safe Search،
به عنوان ابزاری برای اعمال سانسور توسط دولت ایران یا سایر نهادها
انجام دهد.

۷. دولت‌های بریتانیا و اتحادیه اروپا باید سیاست‌هایی را وضع و اجرا
کنند که باعث دلسردی و جلوگیری از استفاده از قلمرو آن به‌عنوان
پناهگاه امن برای کسانی شود که در توسعه ابزارهای سانسور و نظارت
که حقوق ایرانیان را نقض می‌کند، دست دارند.

۸. سازمان ملل متحد باید سیاست‌ها و مکانیسم‌های اجرایی
سخت‌گیرانه‌تری را برای جلوگیری از تأثیرگذاری بر سیاست‌های سازمان
ملل یا به دست آوردن صدایی در نهادهای مختلف آن توسط افرادی
که در نقض حقوق ایرانیان، به ویژه کسانی که در حال توسعه ابزارهای
سانسور و نظارت هستند، ایجاد کند.

۹. شرکت‌های فناوری باید به طور جامع سیاست‌های خود را در رابطه
با برنامه‌های کاربردی و API‌های شخص ثالث بررسی و تقویت کنند.
آنها باید اطمینان حاصل کنند که شرکت‌های مرتبط با دولت ایران
به این ابزارها برای تجاوز به حقوق ایرانیان از طریق اقدامات سانسور
و نظارت سوء استفاده نمی‌کنند.

۱۰. پلتفرم‌های رسانه‌های اجتماعی، مانند توییتر، باید سیاست‌های داده
خود را تقویت کنند تا اطمینان حاصل کنند که API‌ها و داده‌های
کاربران برای شرکت‌های تجزیه و تحلیل رسانه‌های اجتماعی مرتبط
با دولت ایران قابل دسترسی نیستند و در نتیجه از اطلاعات و حریم
خصوصی کاربران محافظت می‌کنند.

کارگروه تعیین مصادیق محتوای مجرمانه

کارگروه تعیین مصادیق محتوای مجرمانه یا کمیته فیلترینگ برای عمل به
ماده ۲۲ [قانون جرایم رایانه‌ای](#) در سال ۱۳۸۸ تاسیس شد. براساس این ماده،
کارگروه تعیین مصادیق محتوای مجرمانه باید هر پانزده روز با حضور ۱۲
عضو از نمایندگان سازمان‌ها و ارگان‌های حاکمیتی جمهوری اسلامی در دفتر
دادستانی کل کشور تشکیل جلسه داده و درباره فیلترینگ سایت‌های متخلف
رای‌گیری کند. این شورا همچنین موظف است هر شش ماه یکبار گزارش
کارها را برای روسای سه قوه و شورای عالی امنیت ملی بفرستد.

اعضای این شورا عبارتند از: وزیر یا نماینده وزارتخانه های آموزش و پرورش، ارتباطات و فناوری اطلاعات، اطلاعات، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، رئیس سازمان تبلیغات اسلامی، رئیس سازمان صدا و سیما و فرمانده نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی و یک نفر از نمایندگان عضو کمیسیون قضائی و حقوقی به انتخاب کمیسیون قضائی و حقوقی.

در میان ایمیل‌ها یک نامه از نظر سیاستگذاری سانسور اینترنت و تایید نام شرکت‌های پیمانکار فیلترینگ دارای اهمیت است.

در نامه‌ای با عنوان «**اهم راهکارها و پیشنهادهای اجرایی برای ساماندهی فضای مجازی**» با طبقه‌بندی «خیلی محرمانه»، راهکارهای «ساماندهی» اینترنت مطرح شده است. این راهکارها عبارت‌اند از:

« کاهش پهنای باند و مسدودسازی تدریجی نرم‌افزارها و پیام‌رسان‌های اجتماعی خارجی به ویژه اینستاگرام و واتس‌آپ- قطع یا اختلال موثر مکالمه صوتی و تصویری (Live Stream) اینستاگرام و واتس‌آپ

« مسدودسازی کامل، موثر و مستمر کلیه فیلترشکن‌ها، VPN‌های غیرمجاز و ابزارهای گریز از فیلترینگ

« واگذاری سامانه‌های فیلترینگ به ارائه دهندگان خدمات دسترسی و فراهم نمودن امکانات مربوط به نظارت قانونی و مستقیم دستگاه قضایی دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه

در این نامه شاهد هستیم که کاهش پهنای باند، یکی از سیاست‌های اصلی دولت ابراهیم ریسی است؛ به طوری که وزیر ارتباطات ایران ۰۲ اردیبهشت ۱۴۰۲ حداکثر نیاز پهنای باند خارجی در کشور را زیر ده درصد **اعلام کرد**. ما همچنین شاهد هستیم پروژه‌های مثل اینترنت طبقاتی - به عنوان جایگزینی برای فیلترشکن‌ها- برنامه آتی دسترسی به شهروندان اینترنت توسط حکومت است.

اما مهمترین بخش این نامه در زیر عنوان «مبانی فنی و اجرایی» بند دوم مطرح شده است. در این بخش از نامه ضمن نام بردن از شرکت‌های «یافتار پژوهان پیش‌تاز رایانش» و «داده پردازی دوران» به عنوان پیمانکاران فنی فیلترینگ نام برده شده است. در این نامه **آمده** است: «مسدودسازی کامل فیلترشکن‌ها از طریق مدیر کل امنیت شبکه و شرکت‌های پیمانکار فیلترینگ (**شرکت یافتار پژوهان پیش‌تاز رایانش و شرکت داده پردازی دوران**) بطور جدی پیگیری شود.»

در ادامه این **نامه** آمده است «براساس مصوبات جلسات ساماندهی فضای مجازی که در اوایل سال ۹۸ در محضر ریاست قوه قضائیه برگزار گردید، مقرر گردید در صورت استتکاف و یا ناتوانی وزارت ارتباطات از مسدود سازی فیلترشکن‌ها، با صدور دستور قضایی، این مسئولیت به سپاه پاسداران محول شود.»

در این نامه از سایفون به عنوان یکی از فیلترشکن‌های هدف برای مسدود کردن یاد شده است. همچنین درخواست شده است که اعمال فیلترینگ به شرکت‌های ارایه‌دهنده واگذار شود.

یک منبع که به شرط ناشناس بودن با فیلتربان صحبت کرده است، به فیلتربان گفت: «هر اپراتور موظف است با یک شرکت فیلترینگ قرارداد ببندد و ترافیکش را در اختیار آن شرکت قرار بدهند. ولی پیمانکار در روش و مسائل مرتبط با فیلترینگ الزاما حرف کارفرما را گوش نمی‌دهد، چون فیلترینگ روی مصرف ترافیک اثر دارد و این به معنی کاهش درآمد برای شرکت است. به همین دلیل است که اپراتورهای مختلف، فیلترینگ یکسان ندارند.»

این منبع ادامه داد: «مثلا شرکت دوران خدمات پیمانکار فیلترینگ مبین‌نت، ایرانسل، های‌وب، پارس‌آنلاین و آسیاتک را انجام می‌دهد. همراه اول با یافتار کار می‌کند و مخابرات هم با دوران همکاری دارد. خود شرکت زیرساخت هم این خدمات را از دوران دریافت می‌کند.»

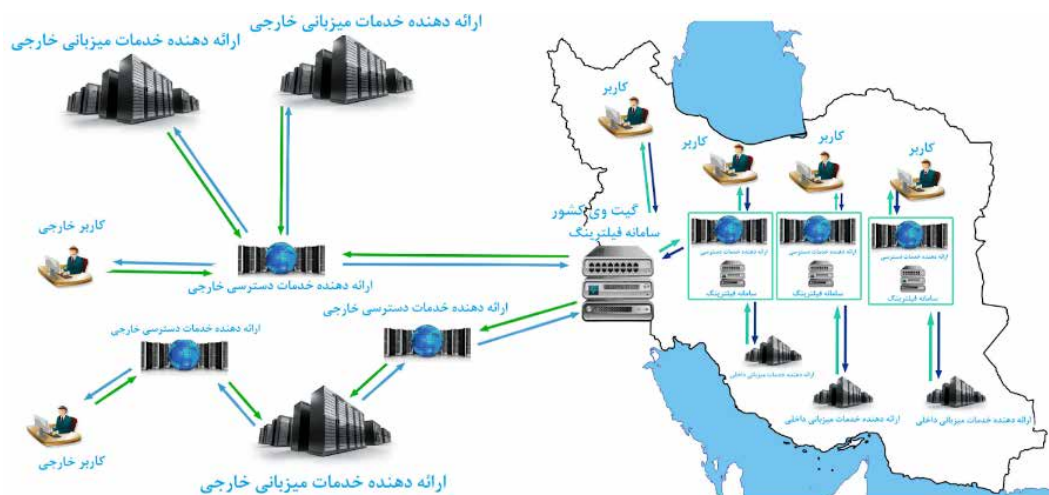
بر اساس تحقیقات فیلتربان، «سحاب‌پرداز» در سطحی بالاتر از این دو شرکت فعال است؛ به طوری که سیاست‌ها و معماری فنی را بررسی و اعلام می‌کند و دو شرکت دوران و یافتار پیاده‌سازی فنی را انجام می‌دهند.

در این نامه همچنین به «راهکارهای پیش‌نهادی گردش کار ستاد کل نیروهای مسلح به مقام معظم رهبری» اشاره شده که مشخص می‌کند، نیروهای نظامی ایران تلاش دارند تا بر فضای اینترنت کنترل پیدا کرده و اینترنت را نظامی کنند.

زیرساخت‌های فنی

طراحی‌های که از ایمیل‌های دادستانی به دست آمده است نشان می‌دهد که برنامه دادستانی و نهادهای تصمیم‌گیر در مورد اینترنت در ایران، سانسور اینترنت را در دو سطح ارایه‌دهنده‌های خدمات اینترنت و گیت‌وی کشور - که همان شرکت ارتباطات زیرساخت باشد- اعمال می‌کند.

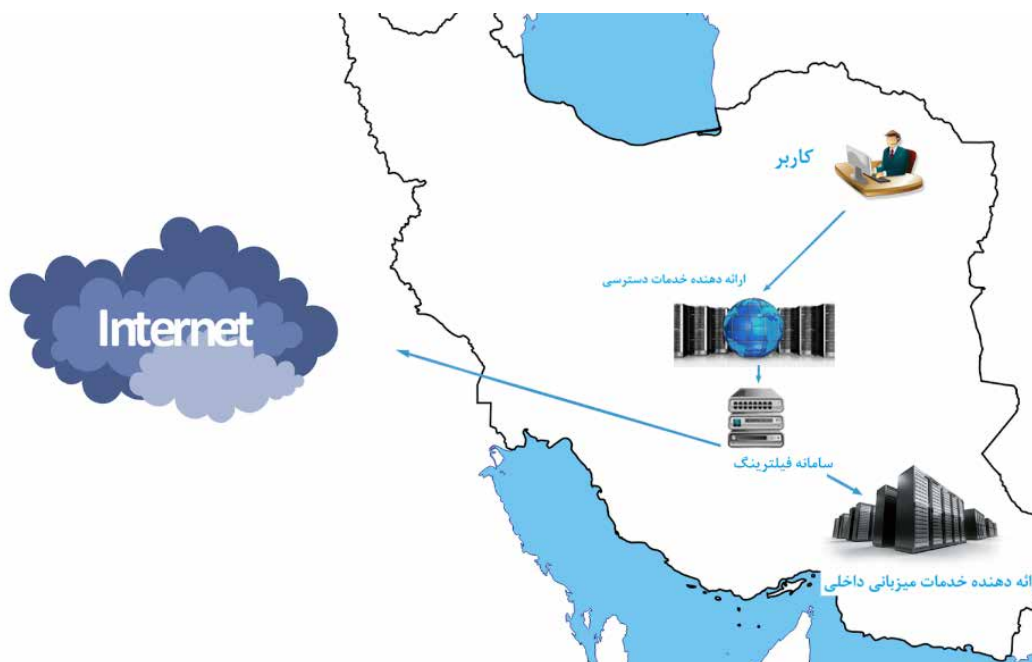
تمام کاربران برای دسترسی به اینترنت مجبور هستند از «گیت‌وی کشور» استفاده کنند و در داخل کشور فقط یک شبکه داخلی یا اینترنت که همان



نقشه ارتباط داخلی و خارجی شبکه ملی اطلاعات و نقاطی که سانسور اعمال می‌شود

شبکه ملی اطلاعات باشد، در دسترس است.

با وجود آنکه، آنچه گفته شد، اطلاعات جدیدی نیست، اما دسترسی به این نقشه‌ها نشان می‌دهد نتیجه تحلیل‌ها و تحقیق‌های در مورد ساختار اینترنت ایران صحت داشته است.



نقشه ارتباط داخلی و خارجی شبکه ملی اطلاعات و نقاطی که سانسور اعمال می‌شود

کارمندان و ساختار اداری

با بررسی ایمیل‌های ارسالی و دریافتی و همچنین یک فایل اکسل که شیفتهای کاری در زمان دورکاری کرونا را مشخص می‌کرد، برای نخستین بار به فهرستی از کارمندان اصلی کارگروه تعیین مصادیق محتوای مجرمانه به همراه سمت و حتی پروژه‌های که روی آن کار می‌کنند، دست یافتیم.

مهدی امیری، شاغل در اداره نظارت به عنوان معاون فنی معاونت امور فضای مجازی دادستانی کل کشور، عباس‌زاده، معاون اداره کل مدیریت منابع شبکه ملی اطلاعات و همچنین جواد بابایی معاون فضای مجازی قوه قضاییه، سه فردی هستند که بر اساس بررسی این ایمیل‌ها به نظر می‌رسد بالاترین سمت مدیریتی و قدرت تصمیم‌گیری را دارند.

جدول زیر از یکی از ایمیل‌هایی به دست آمده که در آن، برنامه و شیفت کاری کارمندان این کارگروه به همراه سمت و پروژه‌ای که روی آن کار می‌کردند را مشخص کرده است.

نام خانوادگی	وظیفه در دوران دورکاری
دویستی	پیش پردازشگر اجرا
دویستی	ربات استخراجگر اطلاعات هاست و دامنه
شعبان‌نیا	طراحی رابط کاربری واحد اجرا
مهدی صابری	سامانه سایت‌های مهم
مهدی صابری	سامانه اعتراضات (راوا)
عبداللهی	ثبت دستور در پنل
نساچی	لاگ گرفتن از تمامی وضعیت‌ها
نساچی	ثبت هاستینگ‌های شناسایی شده
نساچی	ارسال لینک به واحد رفع اثر
نساچی	کشف هاستینگ سایت مجرم
نساچی	نمایش مستندات رفع اثر
احمدی	ارسال تذکر به رصد و اظهارنظر
احمدی	ارسال به هاستینگ جهت شناسایی
احمدی	هشدار به واحد نظارت بر اجرا (مسدود سازی)
احمدی	هشدار به واحد نظارت بر اجرا (فیلتر)

احمدی	ارسال به واحد بازرسی
احمدی	TDL و SLD و تحقیقاتی
احمدی	تشخیص هوشمند مسدودی I2U
عبداللهی/ مهدی	ارسال دسته‌ای دستورات تذکر
صابری	ارسال دسته‌ای پالایش و رفع پالایش
عبداللهی/مهدی صابری	ارسال دسته‌ای مسدود سازی
عبداللهی/مهدی صابری	ارسال دسته‌ای دستورات کاربر محور
عبداللهی/مهدی صابری	ارسال دسته‌ای بلاک دامین
عبداللهی/مهدی صابری	ارسال اعتراض به راوا
عبداللهی/مهدی صابری	طراحی و توسعه پایگاه داده (فرایند دائم)
مهدی صابری / نساجی	تبدیل و انتقال مدیران سایت‌ها به ساماندهی جدید
دویستی	تبدیل و انتقال مدیران میزبان به ساماندهی جدید
دویستی	تبدیل کاربران ns با کاربران هاستینگ موجود در
دویستی / عبداللهی	سامانه های جدید
نساجی	بازبینی کل کدهای نوشته شده

گردان سایبری قوه قضاییه

در ایمیلی که به تاریخ ۱۶ آذر ۱۳۹۶ از مهدی صابری به عنوان مدیر فنی دادستانی به امیری ارسال شده، خطاب به خرم آبادی معاون وقت دادستانی کل کشور در امور فضای مجازی، پاسخنامه تشکیل گردان سایبری قوه قضاییه را داده است.

در این نامه آمده است: «پیرو دستور حضرت عالی در خصوص تهیه نظر یا پیشنهاد جهت طرح پژوهشی تشکیل گردان سایبری قوه قضاییه ج.ا.ا. به استحضار می‌رساند.» در این طرح که به نام «هسته اقدام سریع قوه قضاییه در فضای مجازی» معرفی شده، بسیج قوه قضاییه عامل این گردان معرفی شده است.

در این نامه وجود ارتش سایبری تایید می‌شود اما جزییاتی از آن مطرح نشده است. در بند ب در مورد استفاده از تجربه این نهاد نوشته شده است: «ب)

با توجه به وجود چندین سازمان هم عرض نظیر سازمان پدافند غیرعامل، فرماندهی امنیت سایبری سپاه پاسداران انقلاب اسلامی، ارتش سایبری ایران و ... باید حتما تجربیات این سازمان ها مد نظر قرار گرفته و نباید در این طرح همپوشانی صورت پذیر، همچنین حتی الامکان از دستاوردهای این مراکز بهره برداری شود.»

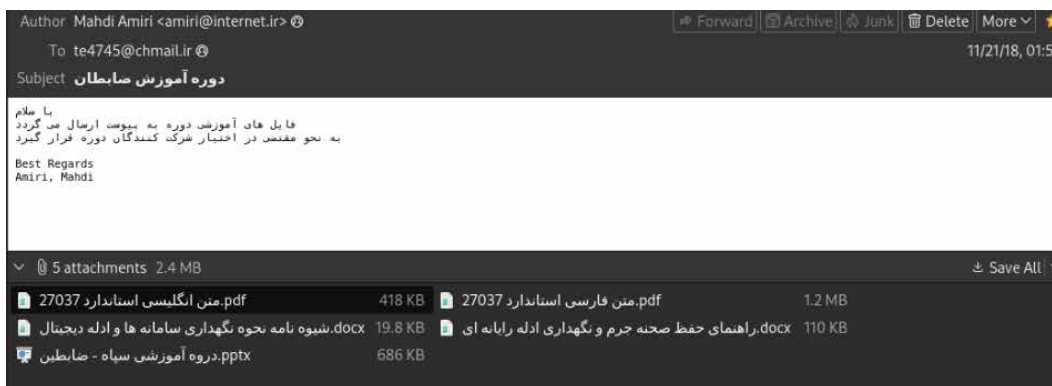


تصویر ایمیل تشکیل گردان سایبری دادستانی

برگزاری کلاس‌های آموزشی برای مامورین سپاه

دادستانی کشور **نامه‌ای** که به نشانی te4745@chmail.ir ارسال کرده و به نظر می‌رسد در پاسخ به موضوع برگزاری دوره‌های آموزشی برای آنچه که آنها «ضابطان قضایی» می‌نامند، مرتبط باشد.

در این **فایل‌ها** ما به یک پاورپوینت دست یافتیم. براساس نام این فایل که «دوره آموزشی سپاه» است، به نظر می‌رسد این کلاس آموزشی برای تقویت ماموران سپاه پاسداران انقلاب اسلامی با هدف آنچه که در فایل «حفظ صحنه جرم و اقدامات اولیه در حفاظت از ادله جرم» اعلام شده است.



ایمیل دوره آموزشی برای نیروهای سپاه پاسداران انقلاب اسلامی

نظارت بر قیمت‌گذاری اینترنت

تصمیم‌گیری در مورد سایت‌های نیم‌بهای داخلی یکی دیگر از مواردی است که با بررسی ایمیل‌های دادستانی برای نخستین بار مطرح می‌شود. در بین این ایمیل‌ها ما به ایمیلی برخوردیم که از طرف مهدی امیری برای بخش فنی دادستانی ارسال شده است که شامل فهرستی از سایت‌های پربازدید است که توسط وزارت ارتباطات و فن‌آوری اطلاعات با بررسی ترافیک کاربران ایرانی تهیه شده است.

فهرست نهایی و تایید شده این سایت‌ها در وبسایت سازمان فناوری اطلاعات ایران تحت عنوان «لیست دامنه‌های اینترنتی با میزبانی داخلی ثبت شده در سامانه» منتشر شده است.

بر اساس این ایمیل، عملاً دادستانی است که باید این فهرست را تایید کند در حالی که تا پیش از این تصور می‌شد که وزارت ارتباطات یا شورای عالی فضای مجازی تصمیم‌گیری در این مورد را برعهده دارند.

در بخش دیگری از این ایمیل‌ها مدیر پروژه خزشگر در شرکت یافتار به Safe Search اشاره می‌کند و اینکه چطور در صورت فعال بودن این حالت «محتوای غیراخلاقی» از نتیجه جستجو حذف خواهد شد.

او در ایمیل خود نوشته است: «در رابطه با عدم تناسب نتایج جستجو در تصاویر موتور جستجوی یاهو در برخی موارد باید توجه داشت که برخی موتورهای جستجو مانند گوگل، یاهو و Bing دارای قابلیت‌هایی به نام Safe Search هستند. این قابلیت به عنوان یک فیلتر بر روی نتایج موتور جستجو عمل می‌کند که با فعال شدن آن بنا به درخواست کاربر، موتور جستجو می‌تواند محتوای غیراخلاقی موجود را از نتایج خود حذف کرده و به کاربر نمایش ندهد.»

او ادامه می‌دهد: «با توجه به سیاست‌های پالایش در کشور ما، در صورتی که قابلیت Safe Search در موتور جستجوی یاهو توسط کاربر غیرفعال شود، قابلیت مذکور توسط سامانه پالایش فعال خواهد شد و در نتیجه محتوای غیراخلاقی موجود در موتور جستجو به کاربر نمایش داده نخواهد شد.»

این گفتگو در سال ۲۶ آبان ۱۳۹۴ انجام شده است. در نگاه اول و با توجه به موضوع گفتگو به نظر می‌رسد نامه درباره چگونگی استفاده از گوگل برای کشف محتوای «مجرمانه» باشد اما در محتوای نامه، به چگونگی استفاده از Safesearch به عنوان ابزاری برای اعمال سانسور اشاره شده است. در نهایت روز ۲۱ تیر ۱۴۰۱ [شرکت ارتباطات زیرساخت](#) شروع به دخالت و به سرقت بردن دی‌ان‌اس‌ها کرد تا به کاربرانی که از داخل ایران قصد بازدید از جستجوگر گوگل را دارند به اجبار به سایت «[جستجوگر امن گوگل](#)» هدایت کند تا از این ابزار به عنوان ابزاری برای سرکوب و سانسور اینترنت استفاده کنند.

Reply Reply All Forward Archive Junk Delete More

From Mahdi Amiri <amiri@internet.ir>

To technical administrator <tech-admin@internet.ir> 11/14/20, 00:35

Subject top list sites - Toprank Report Mehr 99 2- لیست سایتهای مهم

با سلام و احترام
به پیوست فهرست سایتهای پربازدید از سوی کاربران ایرانی که توسط وزارت ارتباطات تهیه شده است ارسال می‌گردد.
مقتضی است فهرست پیوست بررسی، تحلیل و اعلام نتیجه فرمایید تا پس از تایید نهایی به فهرست سایتهای مهم افزوده شود.
خواهشمند است با تحلیل فهرست پیوست و پس از تایید نهایی، لیست 150 سایت پربازدید کاربران ایرانی (مصوبه کارگروه)
اصلاح و مابقی نیز به سایتهای مهم از نظر دبیرخانه اضافه شود.
با سپاس
امیری

Best Regards
Amiri, Mahdi

1 attachment: Toprank Report Mehr 99 2- لیست سایتهای مهم.xlsx 18.3 KB Save

Toprank Report Mehr 99 2- لیست سایتهای مهم.xlsx 18.3 KB

تصویر ایمیل نظارت بر قیمت‌گذاری اینترنت و انتخاب سایت‌های داخلی

جمع‌آوری اطلاعات رنج‌های آی‌پی

۵۳۱ ایمیل در فاصله ۲۲ مهر ۱۴۰۰ تا ۲۴ شهریور ۱۳۹۹ از طرف مهدی امیری، مدیر فنی معاونت امور فضای مجازی دادستانی کل کشور ارسال شده که موضوع آن‌ها «اطلاعات رنج آی‌پی» است. این نامه‌ها خطاب به شخصی به اسم مهندس عباس‌زاده با سمت معاون اداره کل مدیریت منابع شبکه ملی اطلاعات ارسال شده و در آن اطلاعات مالک آی‌پی شرکت‌هایی درخواست شده که ادعا می‌شود «اقدام به اعمال مجرمانه» کرده‌اند.

آیین‌نامه مدیریت نشانی‌های آی‌پی

این آیین‌نامه استفاده از آی‌پی‌های غیرایرانی را که با هدف دور زدن سانسور اینترنت با روش تونل زدن استفاده می‌کند، ممنوع می‌کند و اعلام می‌کند «بر اساس ماده ۳ دستورالعمل ساماندهی دسترسی و تامین نیازمندی‌های اشخاص و گروه‌های تخصصی در فضای مجازی، هرگونه تونل و VPN به خارج از کشور مستلزم اخذ مجوز از کارگروه تعیین مصادیق محتوای مجرمانه می‌باشد.»

این آیین‌نامه در تاریخ ۱۸ شهریور ۱۳۹۹ تهیه شده است که می‌توان آن را از نشانه‌های برای راه‌اندازی اینترنت طبقاتی دانست. بر اساس این آیین‌نامه استفاده از محدوده خصوصی ۱۰/۸ فقط باید برای توسعه شبکه ملی اطلاعات مورد استفاده قرار بگیرد.

Author: Mahdi Amiri <amiri@internet.ir>
To: abbaszadeh@ito.gov.ir
Subject: آیین نامه مدیریت منابع عددی
8/9/20, 02:18

جناب آقای مهندس عباس زاده
با سلام و تحریک ایام
به بیست تصویر نامه مربوط به نظرات اصلاحی دادستانی کل کشور راجع به آیین نامه مدیریت منابع عددی ارسال می‌گردد
سماً مطالبی که در جلسه بحث در خصوص مدیریت یکپارچه منابع عددی و جلوگیری از ارائه خدمات به آن بی‌های بات نت و فیصله در جلسه مطرح شده بود در پیش نویس آیین نامه
ارسالی منعکس نشده است همینطور شواهدی که در جلسه مذکور راجع به ارتباط سیستم تعرفه گذاری ترجیحی و حمایتی با منابع عددی و ارزشگذاری محتوای مطرح شده بود نیز در این
آیین نامه به صورت منضم منعکس نشده است و به نظر می‌رسد این پیش نویس با طرح کاملی که در جلسه اشاره شد اطلاق ندارد
با آرزوی موفقیت
امیر
Best Regards
Amiri, Mahdi

2 attachments 839 KB
اصلاح آیین نامه مدیریت منابع عددی.pdf 400 KB
پیش نویس آیین نامه مدیریت منابع عددی - پیشنهادهای اصلاحی.pdf 439 KB

ایمیل آیین‌نامه مدیریت نشانی های اینترنت

انواع درخواست سانسور و جمع‌آوری اطلاعات مرکز بررسی جرائم سازمان یافته سپاه پاسداران

از بین درخواست‌های سانسور و فیلترینگ مواردی مانند درخواست فیلتر کردن سایت‌های فلزیاب، کانال‌های متعدد تلگرامی مانند آمدنیوز، تگ‌های متعدد اینستاگرام مشاهده می‌شود که عمدتاً توسط **گرداب (مرکز بررسی جرائم سازمان یافته سپاه پاسداران)** ارسال شده است. البته در این میان ایمیل‌های از طرف شهروندان معمولی نیز دیده می‌شود که درخواست فیلتر شدن برخی از محتواهای اینترنت عمدتاً با مضامین ضد مذهب و یا بی‌حجابی را ارسال کرده‌اند.

گرداب که وابسته به سپاه پاسداران انقلاب اسلامی است، نقش گسترده‌ای در سرکوب آنلاین و بازداشت و زندانی کردن شهروندان ایرانی به دلیل فعالیت‌های آنلاین آنها دارد.

نظارت بر محتوای سایت‌ها داخلی

فیلتر و سانسور تنها به یک آدرس اینترنتی یا شبکه اجتماعی محدود نیست. به عنوان نمونه ایمیل‌هایی بین این کارگروه و **رسیمو** که پلتفرمی برای ارتباط و تحلیل کسب‌وکارهاست، دیده می‌شود که در آنها دادستانی درخواست حذف اطلاعات برخی از شرکت‌ها و افراد را از این پلتفرم کرده است.

افرادی مانند بهروز فردوس، بهزاد فردوس، مهرزاد فردوس، میترا فردوس، و شرکت‌هایی مانند مجتمع صنعتی ماموت، حمل و نقل هاگ بار، گروه خودروسازان مایان، پیش ساخته سازان مهرسا، لیزینگ کارآمد، سازه و سوله ماموت، ماموت تلکا، رامان خودرو، ماموت دیزل، موسسه خیریه نیکان ماموت، گروه ماموت، آتین پارت افزار و تعداد دیگری از شرکت‌ها در میان

Reply Reply All Forward Archive Junk Delete More

From Rasmio platform <myrasmio@gmail.com>

To دادستانی <dadsetani@internet.ir> 6/12/21, 07:28

Subject Re: افشای سوابق و اطلاعات مدیران شرکت صنعتی ماموت

با سلام و احترام

خواهشمند است مراتب درخواست مذکور، از جمله مصوبه مورد اشاره، فهرست شرکت‌های اصلی و زیرمجموعه به همراه لینک صفحه آن‌ها در سامانه رسمیو را طی مکاتباتی ارسال فرمایید t@rasm.io رسمی خطاب به این شرکت (در سربرگ رسمی) و آدرس ایمیل تا بررسی‌های لازم انجام و اقدامات مقتضی معمول گردد.

با تشکر
ملک نژاد
مدیر عامل

On Wed, Jun 2, 2021 at 3:42 PM دادستانی <dadsetani@internet.ir> wrote:

مدیرعامل محترم شرکت پیشگامان رسمی پردازش دانا سلام علیکم
نظر به تمیمات و مصوبات اتخاذ شده، مقتضی است اقدام لازم در خصوص عدم افشای سوابق و اطلاعات مدیران شرکت صنعتی ماموت و شرکت های 32 گانه وابسته از سایت معمول گردید و نتیجه به این دادستانی اعلام شود rasm.io رسمیو
با تشکر / واحد اجرای دستورات دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه


ایمیل مدیریت محتوای سایت رسمیو


فهرست درخواستی دادستانی برای حذف از پلتفرم رسمیو بودند.

افرادی مانند بهروز فردوس، بهزاد فردوس، مهرزاد فردوس، میترا فردوس، و شرکت‌هایی مانند مجتمع صنعتی ماموت، حمل و نقل هاگ بار، گروه خودروسازان میان، پیش ساخته سازان مهرسا، لیزینگ کارآمد، سازه و سوله ماموت، ماموت تلکا، رامان خودرو، ماموت دیزل، موسسه خیریه نیکان ماموت، گروه ماموت، آتین پارت افزار و تعداد دیگری از شرکت‌ها در میان فهرست درخواستی دادستانی برای حذف از پلتفرم رسمیو بودند.

علت این حذف در هیچ‌کدام از ایمیل‌ها مشخص نشده است، اما این نمونه نشان می‌دهد که این کارگروه عملاً نقشی فراتر از تصمیم‌گیری برای مسدود کردن سایت یا اپلیکیشن دارد و بر روی محتوای سرویس‌های داخلی کشور نیز نظارت و اعمال قدرت می‌کند.



علت این حذف در هیچ‌کدام از ایمیل‌ها مشخص نشده است، اما این نمونه نشان می‌دهد که این کارگروه عملاً نقشی فراتر از تصمیم‌گیری برای مسدود کردن سایت یا اپلیکیشن دارد و بر روی محتوای سرویس‌های داخلی کشور نیز نظارت و اعمال قدرت می‌کند.


From Elham momeni <elhammomeni.2511@gmail.com> 

To dadsetani@internet.ir  6/28/21, 01:43

Subject سابقه سایت رسمیو .

حضور محترم جناب آقای قهرمانی
با سلام
با عنایت به مذاکره پیشین درخصوص بررسی سابقه سایت رسمیو در خصوص حذف اطلاعات شرکتهای تابعه ماموت به پیوست گزارش اطلاعات موجود تقدیم حضور میگردد
با تشکر

1 attachment: سابقه سایت رسمیو.xlsx 18.1 KB  Save 

 سابقه سایت رسمیو.xlsx 18.1 KB

ایمیل مدیریت محتوای سایت رسمیو

پژوهشگاه امنیت ارتباطات و فناوری اطلاعات

یکی از افرادی که بر اساس بررسی‌های ایمیل‌های دادستانی به نظر می‌رسد نقشی مهم در طراحی و تحقیقات برنامه‌های توسعه شبکه ملی اطلاعات داشته‌باشد، سیدهادی سجادی است که در سال ۳۹۳۱ به سمت سرپرست معاونت پژوهشگاه امنیت ارتباطات و فناوری اطلاعات منصوب شده است.

به نظر می‌رسد، پس از افشا شدن این ایمیل‌ها اطلاعات هویتی آقای سجادی از دسترس عموم خارج شده و در سایت پژوهشگاه ارتباطات و فن‌آوری اطلاعات تحت عنوان classified طبقه بندی شده است.

پژوهشگاه ارتباطات و فناوری اطلاعات در گذشته به اسم مرکز تحقیقات مخابرات شناخته می‌شد.

EN 

قوانین و مقررات

ارتباط با ما

پژوهشگاه

میز خدمت

صفحه اصلی

وزارت ارتباطات و فناوری اطلاعات
پژوهشگاه ارتباطات
و فناوری اطلاعات 

صفحه اصلی

سید هادی سجادی

There is currently no content classified with this term.

تصویر حذف اطلاعات سیدهادی سجادی از وبسایت پژوهشگاه ارتباطات و فناوری اطلاعات

تشکل‌های مردم نهاد

یکی از نکاتی که در میان ایمیل‌های دادستانی بسیار به چشم می‌خورد، حمایت از نهادهایی است که در ظاهر غیردولتی و مردمی هستند اما در عمل از حمایت‌های شدید دولت و به ویژه دادستانی برای ارتباط گرفتن با نهادهای بین‌المللی و اثرگذاری بر روند کار آنها استفاده می‌کنند.

به عنوان نمونه در ایمیلی که مهدی امیری مدیر فنی، معاونت امور فضای مجازی دادستانی کل کشور به محسن نیکبان از دانشگاه تهران در تاریخ ۳ خرداد ۱۴۰۱ ارسال کرده، فهرستی از شرکت‌های فعال در زمینه امنیت سایبری را معرفی کرده است.

براساس **ضمیمه** این نامه، معاونت پیگیری امور فضای مجازی در تاریخ ۳۱ اردیبهشت ۱۴۰۱ نامه‌ای به اشراق جهرمی، مدیر کل صلح و امنیت بین‌المللی وزارت امور خارجه ارسال کرده، که در آن فهرستی از شرکت‌های مورد تایید دادستانی فعال در حوزه امنیت سایبری فعالیت را معرفی کرده است که می‌توانند «در جلسات گروه کاری باز امنیت بین الملل اطلاعات و ارتباطات» شرکت کنند. این **شرکت‌ها** عبارت اند از:

- « [شرکت نرم افزاری امن پرداز \(یادویش\)](#)
- « [پژوهشکده امنیت رایا سامانه‌های شریف](#) وابسته به دانشگاه شریف
- « [شرکت امن افزار گسترش شریف](#) وابسته به دانشگاه شریف
- « [شرکت اطلاعات و ارتباطات امن مهیمن](#)
- « [دانشگاه صنعتی شریف](#)
- « [شرکت توسعه انفورماتیک فراز پژوهان](#)
- « [مرکز تحقیقات صنایع انفورماتیک](#)
- « [آزمایشگاه فناوران توسعه امن ناجی](#)
- « [شرکت پایش ابزار سیمرغ](#)

Author: Mahdi Amiri <amiri@internet.ir> Forward Archive Junk Delete More 5/24/22, 05:10
To: mohsenikbin@ut.ac.ir
Subject: معرفی تشکل‌های مردم نهاد و شرکت‌های غیردولتی فعال در عرصه امنیت سایبری

باسلام و احترام
ببرو مذاکرات تلفنی، به پیوسته تصویر نامه معرفی تشکل‌های مردم نهاد و شرکت‌های غیردولتی فعال و ماحینظر در عرصه امنیت فضای مجازی جهت مشارکت در
گروه کاری باز سازمان ملل متحد درخصوص امنیت سایبری ارسال می‌گردد
با آرزوی توفیق
امیری
Best Regards
Amiri, Mahdi

1 attachment: معرفی شرکت‌ها و موسسات غیردولتی حوزه امنیت سایبری توسط دادستانی کل.pdf 530 KB Save

تصویر ایمیل معرفی نهادهای مردم نهاد برای شرکت در مجامع بین‌المللی

جمعیت توسعه‌گران فضای مجازی پاک

جمعیت توسعه‌گران فضای مجازی پاک، سازمان دیگری است که در ایمیل‌های دادستانی به آن اشاره شده است.

بررسی‌ها در مورد این سازمان ما را به فعالیت‌های عیسی زارع‌پور در سال‌های قبل از وزارت ارتباطات، ما را به این سازمان می‌رساند.

حضور زارع‌پور در شرکت‌های خصوصی و همچنین سیستم دولتی در ایران نشان می‌دهد که او یکی از جدی‌ترین پشتیبانان شبکه ملی اطلاعات (اینترنت ملی) در ایران بوده است و با طرفداران این ایده نیز ارتباطات گسترده‌ای دارد. به عنوان نمونه، او از سال ۱۳۹۵ یکی از اعضای هیات‌مدیره (علی‌البدل) جمعیت توسعه‌گران فضای مجازی پاک است.

با توجه به این‌که شرکت از سال ۵۹۳۱ تاسیس شده، زارع‌پور را می‌توان به عنوان یکی از هسته‌های اصلی شکل‌گیری آن در نظر گرفت. افرادی که در این شرکت عضو هستند، همچون رسول جلیلی (مدیرعامل شرکت)، عضو حقیقی شورای عالی فضای مجازی و منیره حسینی خامنه (نایب‌رییس هیات‌مدیره شرکت)، از چهره‌های تاثیرگذار در حوزه حاکمیتی و همچنین فضای مجازی در ایران هستند. منیره حسینی خامنه، دختر آیت‌الله سید محمدحسینی خامنه، برادر بزرگتر آیت‌الله علی خامنه‌ای است.

فعالیت این شرکت عمدتاً در حوزه «گسترش ارزش‌ها و آرمان‌های انقلاب اسلامی»، «صیانت از ارزش‌های فرهنگی»، «تعمیم (گسترش) امر به معروف و نهی از منکر عنوان شده است.»

این سازمان در نامه‌ای که توسط شخصی به نام «پرهام فرهنگ وصال» به مهدی امیری مدیر فنی معاونت امور فضای مجازی دادستانی کل کشور ارسال شده است، ایشان به عنوان نماینده شرکت «جمعیت توسعه‌گران فضای مجازی پاک» معرفی شده است.

آقای وصال در ایمیل دیگری به آقای امیری خبر از ثبت این جمعیت به عنوان یک سازمان مردم‌نهاد در سازمان ملل با هدف شرکت در جلسات مرتبط با سازمان ملل می‌دهد.

Herewith, the SCS introduces its counsellor, Mr. Parham FARHANG VESAL, as the representative and contact point for all aspects of participation in the negotiating sessions and related matters. He can be reached at this e-mail address: pfvesal@vesalco.com

Thank you very much for your consideration.

Regards,

M. Habibi
SCS Board Chair



تصویر بخشی از نامه جمعیت توسعه‌گران فضای مجازی پاک و معرفی نماینده خارج از کشور به دادستانی



Dear Mr. Amiri,

Salaam -- Following up with our yesterday telephone conversation, this email comes to your kind attention.

In the attachment, please find the SCS's official letter for nomination in the participants' roster of the United Nations Ad Hoc Committee negotiating sessions on the elaboration of Cybercrimes Convention-to-be.

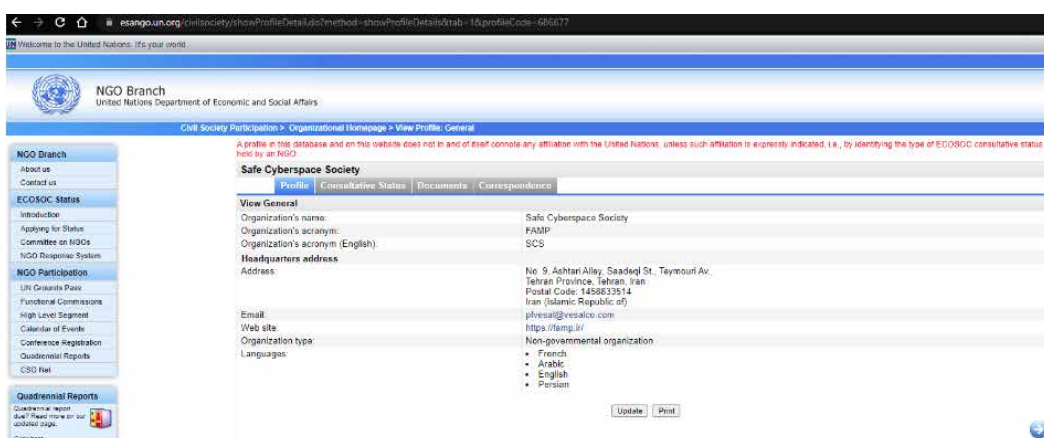
I truly appreciate your invaluable support of the NGOs and their developing role in the future of world governance and settlement of justice and equality for all.

Rest assured that I shall be available for any further documentation and/or information provision, in regard with this process.

Most sincerely,



تصویر ایمیل نماینده جمعیت توسعه‌گران فضای مجازی پاک در خارج از کشور به دادستانی



تصویر ثبت نماینده خارج از کشور جمعیت توسعه‌گران فضای مجازی پاک در سازمان ملل که به دادستانی ارسال شده

پیمانکاران سانسور و سرکوب

بررسی ایمیل‌های دادستانی تصویر روشن و دقیقی از وضعیت اعمال فیلترینگ در فاصله سال‌های ۲۰۱۴ تا زمان انتشار ایمیل‌ها توسط گروه هکری «ناشناس‌ها» به دست می‌دهد. با بررسی این ایمیل‌ها مشخص می‌شود که، چه شرکت‌های به صورت پیمانکار در پروژه‌های سرکوب اینترنتی با دادستانی همکاری داشتند.

لازم است تا ذکر کنیم که تمرکز ما بر روی شرکت‌های است که به توسعه ابزار سرکوب و سانسور نقش داشتند و به عنوان مثال به شرکت تبیان که فراهم کننده زیرساخت لازم برای وبسایت internet.ir متعلق به دادستانی، نیست.

شرکت سحاب‌پرداز

شرکت سحاب‌پرداز با نام کامل **سامانه گستر سحاب‌پرداز** یکی از بازیگران مهم فیلترینگ در ایران است که در سایتش، به عنوان یک شرکت در زمینه ارائه راهکار در حوزه «استراتژی و فناوری داده» به سازمان‌ها خدمات می‌دهد. این شرکت که از سال ۱۳۹۲ تاسیس شده، ادعا می‌کند که ۸۱۰ کارمند دارد و در حوزه‌های علم داده، کلان داده و سیستم‌های توزیع‌شده کار می‌کند.

این شرکت در آبان ۱۴۰۱ از طرف وزارت خزانه‌داری آمریکا به خاطر کمک به سانسور و ایجاد محدودیت در ایران **تحریم شد**. این شرکت در بیانیه‌ای در واکنش، هرچند تایید می‌کند که دولت ایران یکی از مشتریان است اما نمی‌پذیرد که محصولاتش در کاهش سطح دسترسی شهروندان ایران به اینترنت نقش داشتند.

شرکت کیسان

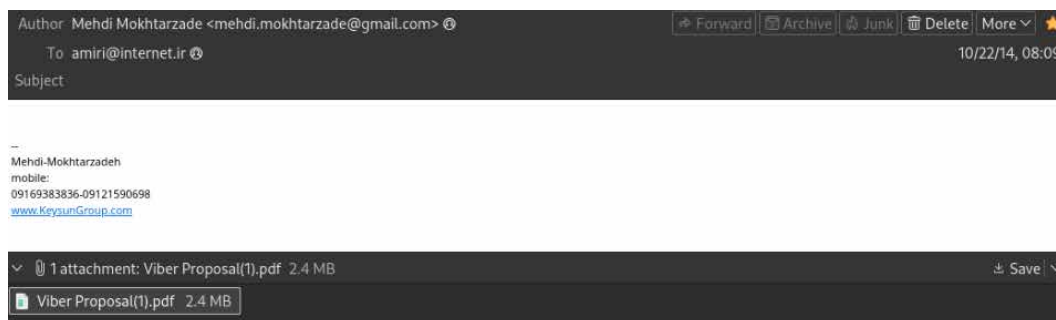
شرکت کیسان در **پروپوزال** ارسالی به تاریخ ۳۰ مهر ۱۳۹۳ به دادستانی پیشنهاد اجرای «پروژه آنالیز امنیتی نرم افزار وایبر» را مطرح کرده است.

وایبر پیام‌رسان بسیار محبوبی بود که به دلیل ایجاد اختلال‌های گسترده بر روی آن توسط مقامات ایرانی، کاربران خود از دست داد اما همچنان مورد استفاده برخی از کاربران در ایران است.

این شرکت پیشنهاد «اسپم کردن وایبر» را مطرح کرده و برای اجرای آن ۶۴ میلیون تومان بودجه درخواست کرده است. براساس این پیشنهاد، قرار بوده تا طی این پروژه شماره تلفن‌های ایرانی که عضو وایبر هستند را جمع‌آوری کنند.

این شرکت مزایای این پروژه را موارد زیر عنوان کرده است:

- « سناریوی اول: پیدا کردن فهرست کاربران وایبر در کشور هدف (شماره تلفن، عکس)
- « سناریوی دوم: ایجاد جنگ روانی با پخش اطلاعات به دست آمده در سناریوی اول



تصویر ارسال پروپوزال کیسان به دادستانی

- « سناریوی سوم: قدرت‌نمایی در حوزه فناوری اطلاعات و انتشار گزارش نقاط ضعف برنامه وایبر
- « سناریوی چهارم: ایجاد رعب و وحشت از طریق برنامه ارسال کد وایبر به کاربران وایبر
- « سناریوی چهارم: ایجاد رعب و وحشت از طریق برنامه ارسال تلفن وایبر به کاربران غیر وایبر
- « سناریوی ششم: ایجاد گروه و تخلیه اطلاعاتی اعضای گروه
- « سناریوی هفتم: ایجاد گروه و نفوذ و تخلیه اطلاعاتی به صورت فرد همراه
- « سناریوی هشتم: ارسال پیام اتوماتیک متنی، تصویری، موقعیت، فیلم و صوت به صورت تکی
- « سناریوی نهم: ارسال پیام اتوماتیک متنی، تصویری، موقعیت، فیلم و صوت به صورت گروهی
- « سناریوی دهم: نظر سنجی: دانشجویی پروژه قالب در الملی رفتارشناسی کاربران وایبر و سپس تخلیه اطلاعاتی
- « سناریوی یازدهم: اعلام نقاط ضعف وایبر به کاربران داخلی برای دقت بیشتر در استفاده از آن
- « سناریوی دوازدهم: ایجاد هانی پات (ما ۱۲۲ نفر با عکس و مشخصات خاص به صورت طعمه در وایبر فعال کنیم)
- « سناریوی سیزدهم: ارسال پیام مخرب (این سناریو باید با روش‌های دیگر ترکیب شود).

در زمانی که وایبر یکی از محبوب‌ترین پیام‌رسان‌های ایران بود مقامات ایرانی در پی نفوذ به این پیام‌رسان و خواندن پیام‌های خصوصی کاربران این پیام‌رسان و گروه‌های آنها بودند.

سردار سیدکمال هادیانفر رییس پلیس وقت فتا در تاریخ ۱۲ شهریور ۱۳۹۳ در مصاحبه با خبرآنلاین **گفته بود:** «باید بدانید که پیام‌های خصوصی در وایبر، واتس‌آپ و ... توسط پلیس فتا قابل کنترل است.»

Author: aram@aut.ac.ir
To: amiri@internet.ir
Subject: گزارش بحث‌های انجام شده با مسئول کمیته مصادیق در راستای ارائه راهکارهای بهبود فرآیند بررسی وجود مصادیق محتوای مخربانه در محتوای وب توسط کارشناسان کمیته مصادیق

با سلام و خسته نباشید
احتراماً گزارشی از بحث‌های انجام شده طی جلسات اخیر بین جنابعالی و اینجانب عباس آرام به نمایندگی از آقای حامد رضوانی، به پیوست ارسال می‌گردد
با احترام
عباس آرام

1 attachment: Proposal-Komite-Masadigh-all-13930619-10-40-final-Rezvani.docx 21.2 KB
Save
Unread: 0 Total: 3579

تصویر نامه عباس آرام به آذری جهرمی، مدیر وقت شرکت زیرساخت

شرکت یافتار پژوهان پیشتاز

شرکت «یافتار پژوهان پیشتاز رایانش» در ۰۲ فروردین ۱۳۹۲ تاسیس شد. [مصطفی رضوانی \(نسخه ذخیره شده\)](#) مدیرعامل فعلی این شرکت است. او پیش از این مدیر شرکت «امن افزار گستر شریف» بود.

قرارداد ۹۱۱۴؛ تحلیل ترافیک و سانسور اینترنت

در ایمیلی که به تاریخ ۱۸ آبان ۱۳۹۳ توسط عباس آرام ارسال شده است [فایلی ضمیمه](#) شده که در آن از توافق شرکت یافتار با محمدجواد آذری جهرمی، رئیس وقت شرکت ارتباطات زیرساخت صحبت شده است. این نامه را عباس آرام از طرف مصطفی رضوانی، مدیر شرکت یافتار به آذری جهرمی ارسال کرده است.

به نظر می‌رسد که این ایمیل به اشتباه برای دادستانی فرستاده شده است، چون چند ثانیه بعد از ارسال ایمیل اول - که درخواست پول بیشتر برای پیشبرد پروژه را از آذری جهرمی داشتند - ایمیل دیگری ارسال کردند و درخواست کردند که ایمیل قبلی را نخوانده، حذف کنند.

اما در نامه ارسالی به محمدجواد آذری جهرمی، عباس آرام نامه را با عبارت «مسیر اهداف بلند مشترک» پایان داده است که حکایت از همراهی کامل شرکت یافتار با سیاست‌های سانسور و تحلیل ترافیک اینترنت ایران دارد. در مورد قرارداد ۴۱۱۹ با عنوان «تحلیل پروتکل» خطاب به محمدجواد آذری جهرمی،

جناب آقای مهندسی جهرمی،
مدیریت عامل محترم شرکت ارتباطات زیر ساخت،

ای که دستت می رسد کاری بکن

پیش از آن کز تو نیاید هیچ کار
(البته سوء برداشت نشود، منظور این است که دیگر نیروی تحلیلی برای ما نمی اند و پیدا کردن نیرو هم در این شرایط چنان که می‌دانید "کز تو نیاید هیچ کار" است)

با توجه به اینکه در قرارداد 4119 در بخش تحلیل پروتکل، پرداخت هزینه سرویس نیازمند ارجاع کار از سوی کارفرما و تایید گزارش ارائه شده توسط پیمانکار از سوی کارفرما می باشد
و همچنین با توجه به اینکه شخص شما در جریان بسیاری از موارد تحلیل انجام شده بوده اید و دفتر صیانت در جریان بخش زیادی از این موارد نبوده است

و همچنین با توجه به اینکه مهلت یکساله سرویس تحلیل پروتکل در این قرارداد تا تاریخ 19 اسفند 95 به پایان می رسد
و همچنین با توجه به اینکه در متن قرارداد اذعان شده است که حداقل 20 درخواست سرویس تحلیل پروتکل در مدت یک سال ارجاع داده خواهد شد

و همچنین با توجه به اینکه تا کنون ارجاع سفارشی رسمی در این زمینه به ما داده نشده است و به تبع آن دریافتی نیز وجود نداشته است

و همچنین چنانکه می دانید نگهداشت نیرو کاری بس دشوار است و نیازمند مساعدت و همراهی توانگران و گوشه چشم گوشه نشینان و افسون افسونگران و توهم در بهشت بودن نیروها است
در صورتی که موارد پیوست را مصادیقی از بخش تحلیل پروتکل قرارداد مزبور می دانید،
التماس دعا داریم
وگرنه کماکان دعاگو هستیم.

کماکان امید است که ما همراهی خوب و قابل اتکا در مسیر اهداف بلند مشترک باشیم

چنانچه شاید و دانی
و شما راهبری خوب
چنانچه باید و دیدیم

و چه نعمتی برای همراه بهتر از راهبر خوب و مطمئن است
و چه نعمتی برای راهبر بهتر از همراه خوب و مطمئن است.

الیس الصبیح بقریب

نامه ارسالی از شرکت یافتار به آذری جهرمی در مورد تحلیل ترافیک اینترنت ایران

نوشته شده: «شخص شما در جریان بسیاری از موارد تحلیل انجام شده بوده اید و دفتر صیانت در جریان بخش زیادی از این موارد نبوده است.»

محمدجواد آذری جهرمی بعداً در دولت دوم حسن روحانی، وزیر ارتباطات و فن آوری اطلاعات شد. او متهم است که در گذشته به عنوان [بازجوی فنی](#) در جلسات بازجویی زندانیان سال ۸۸۳۱ حضور داشته است.

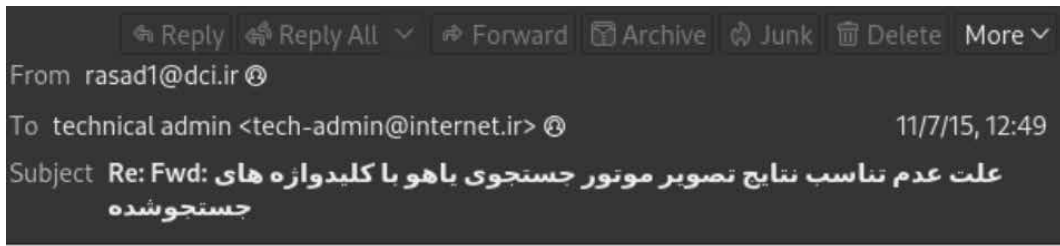
منظور از «دفتر صیانت»، بخش مسوول فیلترینگ در شرکت ارتباطات زیرساخت است. این موضوع را یک منبع که تحت شرایط گمنامی با فیلتربان صحبت کرد، تایید می‌کند. این منبع گفت: «در سطح مدیران رده بالای حوزه اینترنت، فیلترینگ با عناوین صیانت، پالایش و یا Policy Enforcement نامیده می‌شود.»

در این ایمیل صورت جلسه‌ای وجود دارد که به شکل یک سند روشن نشان‌دهنده فعالیت فنی شرکت یافتار در حوزه تحلیل ترافیک اینترنت و رفتار اینترنت، با هدف افزایش سانسور و فیلترینگ اینترنت است. سامانه تارپس

ما با بررسی ایمیل‌های دادستانی دریافتیم که شرکت یافتار سامانه‌ای به نام «تارپس» را برای دادستانی طراحی و پیاده‌سازی کرده است که هدف آن خزشگری در موتورهای جستجوی مطرح دنیا مانند گوگل و بینگ است. در این پروژه، مجموعه‌ای از کلیدواژه‌های مورد نظر دادستانی، با استفاده از API موتورهای جستجوی جهانی به صورت اتوماتیک فیلتر می‌شوند تا در نتیجه جستجوی به نمایش در آمده برای کاربر متن و تصویری که دادستانی «مجرمانه» می‌داند، سانسور شود.

در پی این پروژه به صورت اتوماتیک و با استفاده از یک بانک اطلاعاتی از کلیدواژه‌های مورد نظر دادستانی، بر روی این موتور جستجو و با استفاده از API این ابزارهای جهانی، محتوای تصویری و متنی در سطح جهان را که دادستانی آنها را «مجرمانه» می‌داند شناسایی و سانسور کنند.

فردی به نام حسن زاده که سمتش «مدیر پروژه خزشگر» در شرکت یافتار ذکر شده، به مدیر فنی دادستانی ایمیلی ارسال کرده و در مورد هدف این پروژه گفته: «هدف اصلی ما در استفاده از خزشگر و موتورهای جستجو یا هر ابزار دیگر با بکار بردن کلیدواژه‌های خاص، دستیابی سریعتر به محتوای مجرمانه و پالایش سایت مورد نظر از اینگونه محتوا بصورت یکجا و متمرکز می‌باشد، حال در مقابل پیشنهاد شما این سوال پیش می‌آید که در صورت استفاده از اینترنت بدون فیلتر، نحوه شناسایی و تفکیک موارد فیلتر با موارد باز، برای نتایج حاصل شده چگونه خواهد بود؟»



بسمه تعالی

سلام علیکم

ضمن تشکر از پیشنهادات شما لازم به توضیح است هدف اصلی ما در استفاده از خزشگر و موتورهای جستجو یا هر ابزار دیگر با بکار بردن کلیدواژه های خاص دستیابی سریعتر به محتوای مجرمانه و پالایش سایت مورد نظر از اینگونه محتوا بصورت یکجا و متمرکز می باشد، حال در مقابل پیشنهاد شما این سوال پیش می آید که در صورت استفاده از اینترنت بدون فیلتر، نحوه شناسایی و تفکیک موارد فیلتر با موارد باز، برای نتایج حاصل شده چگونه خواهد بود؟

با احترام - حسن زاده

تصویر گزارش نتایج خزشگر به دادستانی

ابزار کمکی تحلیل متن

از دیگر پروژه‌های که شرکت یافتار با دادستانی ایران پیش می‌برد پروژه تحلیل متن است. در ایمیل‌های که در مورد این پروژه صحبت می‌شود ما به [فایل پی‌دی‌اف](#) دست پیدا کردیم که با عنوان مجرمانه به امیری ارسال شده است.

این پروژه یک افزونه فایرفاکس است که می‌تواند از روی مرورگر نشانی سایتی را که باز است را بخواند، زبان متن را شناسایی کند، و متن را بر اساس معیارهای مشخص شده توسط دادستانی تحلیل کند.



تصویر ایمیل دادستانی به سازنده تحلیلگر متنی

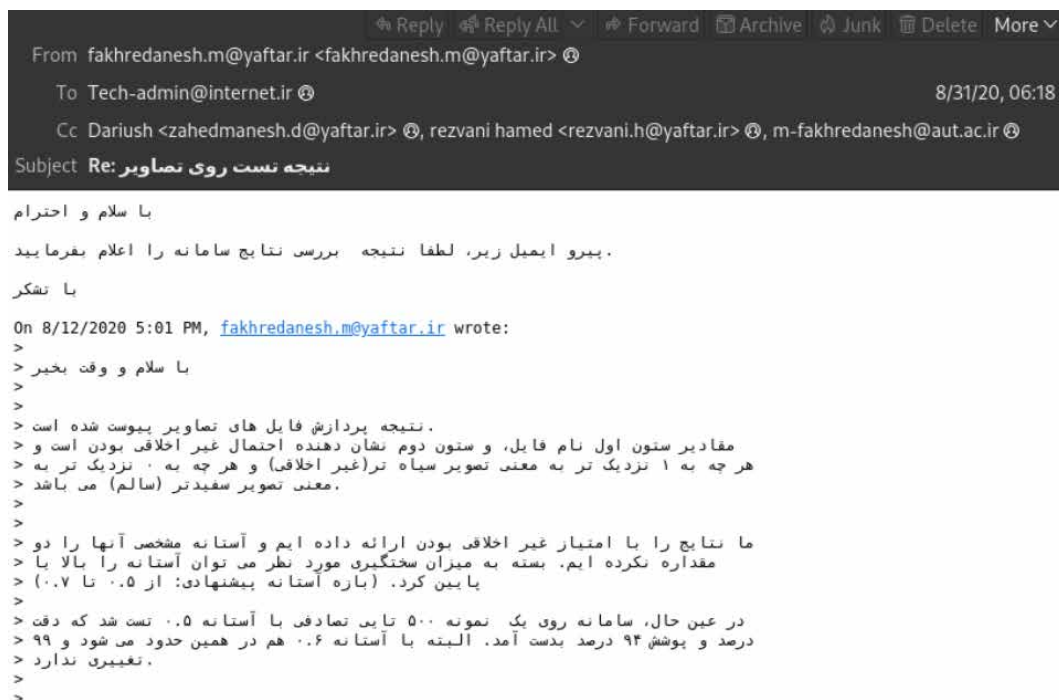
پردازش تصویر

در یکی از ایمیل‌ها، فردی به نام [محمد فخردانش](#) با ایمیلی متعلق به [دانشگاه امیرکبیر](#)، نتیجه پردازش فایل‌های تصویری را به دادستانی به عنوان نمونه ارسال کرده است.

در ادامه همان ایمیل، همان شخص این بار با ایمیلی متعلق به شرکت یافتار، از دادستانی درخواست کرده تا در همین موضوع به او پاسخ دهد.



تصویر ایمیل محمد فخردانش به دادستانی در مورد نتیجه پردازش فایل‌های تصویری



تصویر ایمیل محمد فخردانش از شرکت یافتار به دادستانی

Author Mahdi Amiri <amiri@internet.ir> Forward Archive Junk Delete More 9/14/15, 05:31
To mahdi.saberi@saberi@internet.ir
Subject Re: [Fwd: Re: **نرم افزار بردار شگر تصویر**]

Subject: Re: نرم افزار بردار شگر تصویر
From: saberi@internet.ir
Date: Tue, 09/08/2015 06:04 PM
To: saberi@internet.ir

با سلام،

در صورت امکان آواخر هفته بعد (ترجیحاً روز سه شنبه) وقتی برای دعوت مجتهد تصویر منس فراهمید. در ضمن با توجه به اینکه مدل تحول به صورت یک PC و یک نرم افزار کلاکت می باشد، هماهنگی با آرم جهت تحول را فراهم نمایید.
آیا این امکان وجود دارد که مجتهد در شرکت نصب باشد و با API ها و با واسطه پس برای دسترسی از راه دور فراهم گردد. با توجه به اینکه شرکت برای شما یک دستگاه مهم می باشد آیا توجه به آرایشی در این مدل مجتهد را می توان بر روی سخت افزار مناسب با GPU در شرکت نصب نمود و آرایک واسطه برای اتصال یک یا دسته ای از عکس ها و پردازش و بازگردان تابع استفاده نمود. قیمت دیگر این روش این است که روزی شما نرم افزار به صورت مستمر در محیط شرکت انجام می گردد و همواره از آخرین نسخه در سرویس استفاده می شود. مدل سرویس مدل معمولی است که در حال حاضر در دیتال در مورد مسائل مختلف در حال استفاده می باشد.

با تشکر
رضوان

تصویر ایمیل دادستانی در مورد نرم‌افزار پردازشگر تصویر

ما در ادامه دریافتیم که شرکت یافتار برای پردازش تصویری نیز با دادستانی ایران همکاری و پروژه‌های داشته است. عنوان این پروژه «[تحلیل نیازمندی‌ها](#) و [ارائه برنامه زمانبندی توسعه ابزار تشخیص تصاویر نامناسب کمیته مصادیق مجرمانه](#)» نوشته شده است.

در بسیاری از این ایمیل‌ها، افراد از نشانی ایمیلی استفاده کردند که متعلق به حامد رضوانی، در [دانشگاه امیرکبیر](#) است. به نظر می‌رسد بسیاری از

Author mahdi.saberi@saberi@internet.ir Forward Archive Junk Delete More 9/20/15, 03:46
To rezvani@aut.ac.ir
Cc amiri@internet.ir
Subject جلسه بردار شگر تصویر

بسمه تعالی
با سلام
عذر هماهنگی به عمل آمده با آقای امیری - جلسه بردار شگر تصویر چهارشنبه ساعت 8 الی 10
با احترام
مهدی امیری
1394.09.29

Author rezvani.m@yaftar.ir Forward Archive Junk Delete More 11/4/15, 09:08
To saberi@internet.ir, amiri@internet.ir

تصویر ایمیل جلسه در مورد پروژه پردازشگر تصویر

Author rezvani.m@yaftar.ir Forward Archive Junk Delete More 11/4/15, 09:08
To saberi@internet.ir, amiri@internet.ir
Subject LOM

جناب آقای صابری،

طبق درخواست یک LOM نمونه برای سیستم پردازش تصویر به پیوست ارسال شده است.

نکات زیر در مورد این LOM شایان توجه است:

- 1- با توجه به اینکه محدودیت قیمت با کارایی تعیین نشده است، یک سیستم با مشخصات نزدیک به سیستم موجود فعلی در شرکت پیشنهاد شده است. کارایی این سیستم حدود 400 عکس در ثانیه می باشد.
- 2- با توجه به اینکه محدودیت ذخیره سازی تعیین نشده بود، براساس زمان احتمالی مورد نظر برای ذخیره سازی، فضا در نظر گرفته شده است. اگر این سیستم یک روز کامل با تمام توان کار کند و هر عکسی به طور متوسط حدود 120 کیلوبایت باشد، حدود 4.2 ترابایت پروانه به فضای دیسک نیاز دارد. برای این سیستم حدود 18 ترابایت دیسک پیشنهاد در نظر گرفته شده است که با 5 می باشد و حدود 12 ترابایت فضای ذخیره سازی قابل استفاده می دهد که تقریباً برای 3 روز کافی است. همچنین حدود 3.6 ترابایت دیسک پردازش سریع تر در نظر گرفته شده است که با 40 می باشد و برای پردازش تصویر مورد استفاده قرار می گیرد. در صورتی که این میزان فضای ذخیره سازی بیشتر از نیاز می باشد، می توانید دیسک ها را با در نظر گرفتن ریسک از لحاظ تعداد با اندازه کاهش دهید.
- 3- این سیستم دارای یک GPU می باشد و قابل ارتقاء به دو GPU می باشد که سرعت پردازش را به 800 عکس در ثانیه می رساند. برداشت فعلی من این بوده است که نیاز فعلی مجموعه شما بیش از این نیست. در صورتی که نیاز بیش از این باشد، می توان دستگاه های دیگری از این نوع خرید یا اگر نیاز خیلی بیش از این است می توان از دستگاه های 56500 یا 5990 استفاده نمود که در هر ثانیه با GPU 4 قابل نصب است و حدود 4 بیغه در هر دستگاه قابل اضافه کردن است. البته راهکارهای برای افزایش این تعداد هم دارد. این راه حل بسیار حرفه ای تر است و به درد جاهایی می خورد که بخواهد gpu computing داشته باشند.
- 4- با توجه به میزان هزینه ای که در نظر گرفته اید، می شود مدل GPU، مدل پردازنده، میزان رم و ... را کم و زیاد کرد که به تناسب کارایی سیستم نیز تغییر خواهد نمود.
- 5- قیمت ها مربوط به 5.4 ماه پیش می باشد. بهیچ است برای گرفتن قیمت بروز، می توانید این لیست را به فراهم کننده تجهیزات خود بدهید تا قیمت جدید بدهد.

لطفاً برای معاملات آبی از این آدرس ایمیل استفاده نمایید.

با تشکر

> 1 attachment: LOM-Komiltee-940611-1815-Image.xlsx 11.6 KB Save

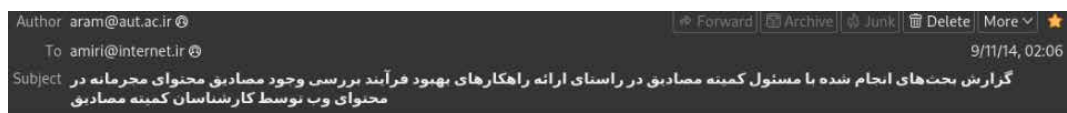
تصویر ایمیل شرکت یافتار به دادستانی در مورد سیستم پردازشگر تصویر

فعالیت‌های این شرکت توسط محقق‌های که در این دانشگاه کرده تحصیل بودند، انجام می‌شد.

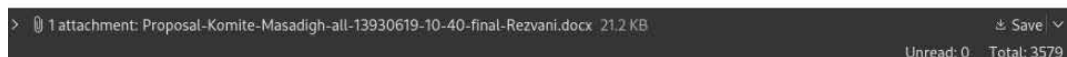
شناسایی بدحجابی و «عریانی»

ما در ادامه بررسی‌ها دریافتیم که عباس آرام گفته که او به نمایندگی حامد رضوانی، مدیر شرکت ادامه پروژه را برعهده دارد. او در این ایمیل [فایلی](#) را ارسال کرده که در آن این موارد به چشم می‌خورند:

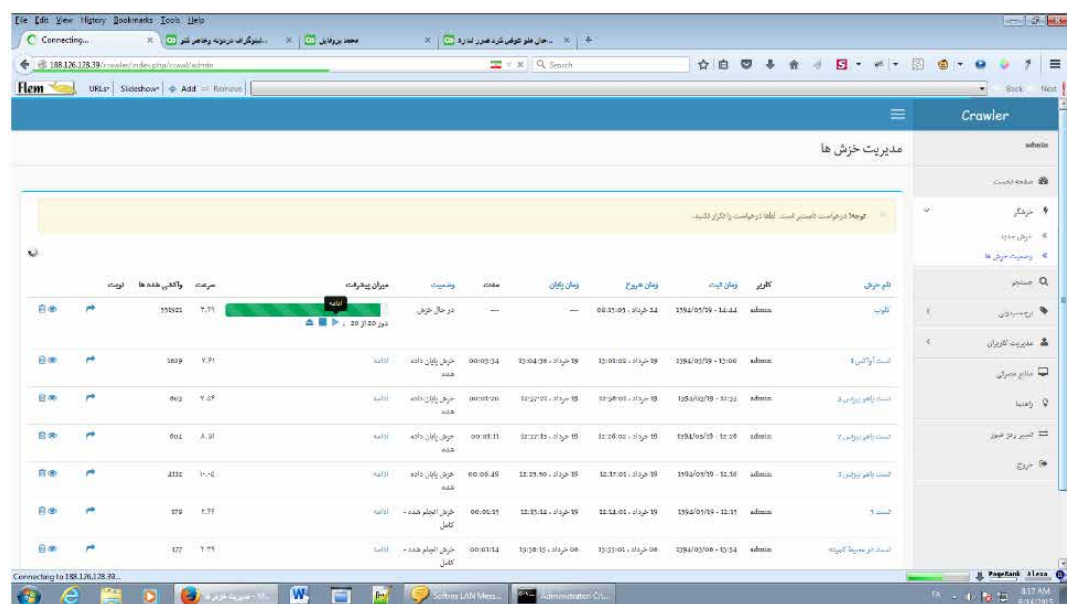
۱. ابزار کمکی برای تعیین مصادیق محتوای مجرمانه در صفحات وب با استفاده از تحلیل محتوای صفحه
۲. ابزار کمکی برای تعیین مصادیق محتوای مجرمانه در Upload Center ها با استفاده از خزش صفحات
۳. ابزار کمکی برای تعیین مصادیق محتوای غیراخلاقی در تصاویر با استفاده از روش‌های هوشمند



با سلام و خسته نباشید
احتراما گزارشی از بحث‌های انجام شده طی جلسات اخیر بین جنابعالی و اینجانب عباس آرام به نمایندگی از آقای حامد رضوانی، به پیوست ارسال می‌گردد
با احترام
عباس آرام



تصویر ایمیل عباس آرام به دادستانی در مورد پردازش تصویر بدحجابی و عریانی



تصویر وب‌اپلیکشن برنامه پردازش تصویر و خزشگر ساخته شده برای دادستانی توسط شرکت یافتار

ما در سایر ایمیل‌ها تصاویری از محیط این برنامه را مشاهده کردیم.

همچنین در **سند** دیگری با پرسش‌نامه‌ای روبه‌رو شدیم که از طرف این شرکت برای دادستانی ارسال شده است که به نظر می‌رسد هدف آن پیدا کردن درک بهتر از مصادیق مورد نظر دادستانی است.

در ابتدای این سند آماده است: «پاسخ‌های اعلامی جهت بهره برداری به منظور طراحی نرم افزارهای هوشمند پایشگر فضای مجازی می باشد و تمامی مصادیق و معیارهای مورد نظر کارگروه جهت پالایش محتوای مجرمانه را پوشش نمی دهد.»


در این مورد پرسش‌های زیر مطرح شده‌اند:

۱. a حدود پوشش زنان چیست؟ به عنوان مثال شرع، نوع پوشش زنان در صدا و سیما، نوع پوشش زنان در جامعه



۲. در پالایش عکس‌ها و برای مشخص کردن حدود پوشش و روابط، آیا ایرانی و خارجی بودن عکس‌ها تاثیر دارد؟ (بین عکس دو خانم ایرانی و خارجی در شرایط کاملا یکسان تفاوتی وجود دارد؟) در صورتی که پاسخ مثبت است، تفاوت چگونه باید اعمال شود؟

	<p>بله <input checked="" type="checkbox"/> خیر <input type="checkbox"/></p> <p>چنانچه نرم افزار بتواند با دقت بسیار زیاد تفاوت تصاویری که کاربرد پزشکی دارند از تصاویر غیر پزشکی را تشخیص دهد ، مطلوب خواهد بود اما اگر خطای زیادی دارد بنظر می رسد بهتر است تشخیص برعهده کاربر انسانی گذاشته شود. بر اساس تنصه ماده 15 قانون جرایم رایانه ای مفاد این ماده و ماده (14) شامل آن دسته از محتوایی که برای مقاصد علمی یا هر مصلحت عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا توزیع یا انتشار یا معامله می شود، نخواهد شد.</p>	<p>در صورتی که این تصاویر به شکل نقاشی باشد؟</p>
---	--	--

نمونه برخورد با تصویری پزشکی

	<p>بله <input checked="" type="checkbox"/> خیر <input type="checkbox"/></p> <p>موضوع بی حجابی و بدحجابی با توجه به پیچیدگی‌هایی که در تصمیم‌گیری دارد ، از اهداف تعیین شده برای روباتهای هوشمند پایشگر نمی باشد.</p>	<p>موی سر</p> <p>نحوه ی آراستن موی سر مهم است؟ آیا رنگ خاص موی سر مهم است؟</p>
---	--	--

نمونه روش برخورد با تصویر «بد حجاب»

	<p>بله <input type="checkbox"/> خیر <input checked="" type="checkbox"/></p>	<p>بوسیدن صورت</p>	<p>ارتباط دو جنس همسان روابط غیر معمول</p>
	<p>بله <input checked="" type="checkbox"/> خیر <input type="checkbox"/></p>	<p>بوسیدن لب‌ها</p>	

نمونه از روش برخورد با تصویر «ارتباط جنسی دو جنس همسان»

۳. تصاویری که برای نشان دادن بیماری قسمتی از بدن (مثلا سینه) را نشان می‌دهند؟
۴. در صورتی که این تصاویر به شکل نقاشی باشد؟
۵. عکس زن با لباس خانگی معمول (در حد بیرون بودن دست‌ها تا آرنج، یقه معمولی و مشخص بودن موها بدون آرایش خاص) ایرادی دارد؟

این پرسش‌ها وارد جزییات زیادی شده و در مورد تک تک اعضای بدن و نحوه پوشش آنها طرح سوال می‌کند تا مصادیق مورد نظر دادستانی را با جزییات تشخیص دهند. در برخی از موارد نمونه عکس‌های هم گذاشته شده است.

شرکت دانش بنیان نیافام

ایمیل‌های شرکت [دانش بنیان نیافان](#) نشان می‌دهد این شرکت در مورد راه‌اندازی پورتال سازمانی دادستانی آماده همکاری است.

این پورتال قابلیت‌هایی [قابلیت‌های \(لینک به نسخه ذخیره شده وبسایت این شرکت\)](#) مانند «قابلیت تشخیص چهره و هویت شخصیت‌های حاضر در تصاویر اخبار جهت غنی‌سازی محتوای تولید شده و تگ شدن نام شخصیت‌ها بر روی تصاویر در سایت [مشاهده ویدئو](#)» [\(لینک به نسخه ذخیره شده این محصول در سایت شرکت\)](#) که در [RFP ارسالی](#) این شرکت به دادستانی آماده همکاری است.

در این RFP که به صورت یک [فایل پی‌دی‌اف](#) برای دادستانی ارسال شده است، در بخش بهره‌مندی از هوش مصنوعی توانمندی‌های مانند تشخیص چهره افراد از درون تصاویر و فیلم‌ها، ایندکس صحیح تصاویر اشخاص در گوگل و موارد دیگری در مورد پردازش تصویر ذکر شده است.

From ahmadi@niafam.com Reply Reply All Forward Archive Junk Delete More
To 'technical administrator' <tech-admin@internet.ir> 1/19/20, 06:04
Subject RE: rfp dadsetani

From: technical administrator <tech-admin@internet.ir>
Sent: Sunday, January 19, 2020 12:41 PM
To: Ehsan Ahmadi <ahmadi@niafam.com>
Subject: rfp dadsetani

با سلام

طر جلسه ای که با جنابعالی و دوستان آن شرکت محترم در خصوص راه اندازی پورتال سازمان دادستانی کل کشور داشتیم، مقرر های این نهاد، خدمتون ارسال بشود که به پیوست می باشد rfp شد که

لطفاً زمان و هزینه های پیشنهادی ارسال فرمایید.

با تشکر

1398/10/29

> 1 attachment: dadsetani-NiafamProposal S981029.pdf 1.5 MB

Save

تصویر ایمیل شرکت نیافام به دادستانی و ارسال پروپوزال در مورد راه اندازی پورتال دادستانی

استفاده از تکنولوژی تشخیص چهره به عنوان یکی از اصلی‌ترین ابزارهای سرکوب و شناسایی مخالفان حکومت طی ماه‌های اخیر بارها از طریق مقامات ایرانی مطرح شده است.

در ایمیل دیگری که چند ماه بعد از ایمیل اول توسط احسان احمدی، رییس هیات‌مدیره و بازاریابی و فروش شرکت نیافان با موضوع «نسخه دمو» ارسال شده است. آقای احمدی در این ایمیل از اصلاح سیستم شرکت خود بر اساس بازخوردهای دادستانی صحبت کرده است.



امکانات کلی نرم افزار

جدا از امکانات فراوان نرم افزار اسپریت پورتال، در جدول ذیل به ویژگی‌های برجسته و بعضاً منحصر بفردی پرداخته شده است:

عنوان	توضیح مختصر
بهره‌مندی از فناوری هوش مصنوعی	• تشخیص چهره افراد درون تصاویر و فیلم ها (Face Recognition) بواسطه دانش شبکه‌های عصبی مصنوعی
	• تشخیص هویت افراد با استفاده از الگوریتم های Machine Learning
	• استفاده از قابلیت های تشخیص چهره در پردازش داده ها و ساختاردهی به اطلاعات
	• ایندکسینگ صحیح تصاویر اشخاص در گوگل
	• استفاده از الگوریتم های هوش مصنوعی جهت توسعه ابزارهای کمک‌کننده به محتوا نگاری
	• قابلیت پیشنهاد کلمات کلیدی برای مطالب، بواسطه Deep Learning

تصویر بخشی از پروپوزال شرکت نیافام ارسالی به دادستانی در مورد قابلیت تشخیص چهره

Reply Reply All Forward Archive Junk Delete More
From Ehsan Ahmadi <ahmadi@niafam.com>
To 'technical administrator' <tech-admin@internet.ir>
Subject RE: نسخه دمو

با سلام و عرض ادب

دادستانی محترم کل کشور

با سلام و عرض احترام

به استحضار میرسد پیرو فرمایش کارشناسان محترم دادستانی کل کشور پیرامون ارائه دمو مازول مدیریت فرایند نرم افزار اسپریت پورتال، شرکت نیافام نسبت به توسعه و آماده‌سازی فرایندساز بر اساس فرایند ارائه شده از سوی دادستانی اقدام نموده‌است و با توجه به تغییراتی که در جریان کاری به نیافام ابلاغ شده است و درخواستی که در زمینه طراحی قالب به نیافام ارائه شده‌است، زمان بیشتری جهت ارائه فرایند با کیفیت بهینه مورد نیاز است. گفتنی است انجام پروژه‌های مشتریان شرکت نیافام و عمل به تعهدات فعلی شرکت، به موازات توسعه نرم افزاری برای دادستانی کل کشور انجام می‌پذیرد و در صورت در اختیار داشتن زمان آزادتر، این امکان موجود بود که درخواست‌های آن سازمان محترم تا یکشنبه Workflow سریعتر عملیاتی شود. در نهایت به اطلاع می‌رسد در صورت افزایش مهلت شرکت نیافام برای ارائه هفته آینده، موارد خواسته‌شده به سطح کیفیت بهینه خواهد رسید. علیراجال، کارشناسان محترم دادستانی کل کشور می‌توانند با اطلاعاتی حساب کاربری ساخته‌شده وارد نرم افزار شوند و اقدامات صورت گرفته در جهت توسعه فرایند ثبت گزارش (با هویت) را مشاهده کرده و در صورت تأیید صحیح اقدامات صورت گرفته، دستور توسعه فرایند ثبت گزارش با شماره تلفن و بدون ثبت هویت را صادر نمایند.

تصویر ایمیل شرکت نیافام به دادستانی در مورد نسخه نمایشی سیستم تولید شده برای دادستانی

ایمیل‌های دیگر این شرکت نشان می‌دهد که [قرارداد همکاری](#) بسته شده است و پورتال دادستانی به مبلغ ۰۰.۰۰۲.۳۲۵ ریال توسط این شرکت با ویژگی‌های ذکر شده در RFP انجام شده است.

شرکت امن افزار شریف

در مورد رابطه این شرکت نکات زیادی وجود ندارد ولی ما به ایمیلی دست پیدا کردیم که یکی از کارمندان این شرکت که از وضعیت شغلی خود ناراضی است، ارسال کرده است. به نظر می‌رسد این کارمند از پیگیری شکایت خود در داخل شرکت ناامید شده و متن شکایت خود را به رسول جلیلی رییس دانشگاه شریف و عضو شورای عالی فضای مجازی که (سمت در این شرکت) و تعداد دیگری در دادستانی ارسال کرده است.

Author: R. Jalili <jalili@sharif.ir>
To: 'Mahdi Amiri' <amiri@internet.ir>, shirazi@amnafzar.ir
Cc: manafi@amnafzar.ir, mohamad.iranshahi@gmail.com
Subject: FW: ایرانشاهی - شرکت امن افزار گستر شریف

سلام بر آقای امیری و شرفراز
با عرض ارادت و آرزوی قبول طاعات
مرفوعه آقای ایرانشاهی که به بنده منعکس شده است تقدیم میگردد. متن کوتاهی کار نیمه‌رهنه شده است وگرنه کمترین انتظار کارمندان برای شرکت در ارتقا و رفاه مبعوض، به نحوی که به شرکت و ایشان انجام نشود مورد انتظار است. پاسخ تک جمعی به جمع دریافت کنندگان این نامه نیز نکات از دریافت و پیگیری خواهد نمود.
ارادتند و منتظر از رحمت همتون
Mohammad Iranshahi [mailto:mohamad.iranshahi@gmail.com] From:
Sent: Friday, October 14, 2016 9:20 AM
To: jalili@sharif.edu; amiri@amnafzar.ir
Subject: ایرانشاهی - شرکت امن افزار گستر شریف
جناب آقای دکتر جلیلی
با عرض سلام و وقت بخیر
اینجانب محمد ایرانشاهی از پرسنل شرکت امن افزار هستم که از سال 93 در این شرکت و در پروژه SOC مشغول بوده‌ام. ضمن احترام به تمامی رخصت و لطف حضرتعالی، لازم است با موضوعاتی را با شما مطرح نمایم.
متأسفانه شرایط بیرونی انسانی در مجموعه از لحاظ احترام به شخصیت و انسجام پرسنل، شیوه پرداخت ها، و ایجاد انگیزه و روحیه پیشرفت، در وضعیت بسیار نامناسبی قرار گرفته است. در چندماه اخیر تعداد زیادی از نیروهای متخصص مجموعه بهلت ناراضی شرکت را ترک کرده و عده دیگری نیز درصدد همین تصمیم می‌باشند.
اینجانب نیز پس از اعلام قبلی و استعفا از مجموعه، با کم لطفی بی سابقه ای از سوی مدیریت مجموعه و مدیر پروژه SOC مواجه شده و از تسویه حساب با من امتناع شده است. پس از اینکه دو ماه بدون عقد هیچ قراردادی با نام توان برای پیشبرد پروژه تلاش کرده‌ام. جناب دکتر امیری استانی آستاد کار دیده را منوط به دو ماه دیگر کار برای شرکت بدون هیچ گونه حق و حقوقی اعلام نموده اند....
علاقم بهشوری های متعدد دیده، هیچ پاسخ منطقی بر منطقی از مسئولین و مدیریت داده نشده و اینجانب از ورود به شرکت بی‌سرمه شده‌ام.
متأسفم که کارمزم علاوه قلب به ادامه فعالیت در شرکت محترم امن افزار و تحت اعلام این موضوع به جناب مهندس شرفراز، آوازخور به استناد از جهالت در راستای گرفتن حقوق قانونی ام از شرکت شده، ام لافها با تدبیر و منشی بزرگوارانه خود موضوع را مرتفع فرمایید.
در صورت نیاز خواهی بود

تصویر امیل شکایت از شرایط کار و مالی یکی از کارمندان شرکت امن افزار شریف به رسول جلیلی و دادستانی

همین موضوع نشان از همکاری این شرکت با کمیته تعیین مصادیق محتوای مجرمانه دارد.

شرکت گروه دوران


گروه دوران شرکت دیگری است که در ایمیل‌های لو رفته از دادستانی از آن به عنوان پیمانکار فیلترینگ یاد شده است. یک منبع آشنا با شرکت دوران تحت شرایط گمنامی به فیلترینگ گفت: «عمر نجفیان‌پور، علیرضا عابدی‌نژاد و محسن عتیق آدم‌های کلیدی فیلترینگ در دوران بودند.»

این شرکت در سال اکتوبر ۲۰۲۲ توسط دولت آمریکا به نقش داشتن در سانسور اینترنت تحریم شد.


اطلاعات موجود در صفحه لینکدین محسن عتیق، سابقه همکاری او با این شرکت را تایید می‌کند.

بر اساس همین اطلاعات او از سال ۲۰۰۶ تا ۲۰۱۹ به عنوان رهبر تیم فنی دوران مشغول به کار بوده است و هم اکنون ساکن شهر صوفیا در بلغارستان است و برای شرکت **Acronis** به عنوان مهندس امنیت کار می‌کند.

اطلاعات لینکدین شرکت دوران به ما نشان می‌دهد که تعداد دیگری از **کارمندان** این شرکت هم‌اکنون ساکن خارج از ایران هستند.




Mohsen A.
Lead Software / Security Engineer at Acronis | (CISSP)



Co-Founder, Technical Manager /Lead developer
Fortuna Network · Full-time
Jan 2018 - Aug 2020 · 2 yrs 8 mos
Tehran, Iran

Fortuna was a network security management and monitoring startup. The primary mission of this project was to develop high-performance security products for the SoHo and enterprises' clients.



Technical Team Lead
Douran · Full-time
2006 - Jul 2019 · 13 yrs 7 mos
Tehran Province, Iran

Network security analyst
Linux kernel developer
c / c++ developer
GO, developer

تصویر لینکدین محسن عتیق که نشان از همکاری او با شرکت دوران است

مشارکت در گروه کاری باز سازمان ملل متحد برای امنیت سایبری

شرکت دوران در تاریخ ۰۳ اردیبهشت ۱۴۰۱ از طرف دادستانی **مامور** شده است که در کارگروه کاری باز سازمان ملل متحد (Open-Ended Working Group) مورد امنیت سایبری ثبت‌نام کند.


قراردادهای توسعه و فروش سیستم‌های سانسور و فیلترینگ

دوران قراردادهای با همراه اول بابت تجهیزات فیلترینگ نیز بسته است. این قراردادها بر اساس سرعت تحلیل ترافیک و پیاده‌سازی فیلترینگ بسته شده است به صورتی که در صورت افزایش پهنای باند بر اساس سرعت پورت و سویچ، قیمت قرارداد هم افزایش پیدا می‌کند.

در این قراردادها از فیلترینگ عمدتاً با عناوینی مانند صیانت و یا پالایش یاد شده است. بر اساس اسنادی که فیلتربان به آنها دست یافته است، این شرکت از سال ۱۳۸۶ تا سال ۱۳۹۹ قراردادهای متعددی با شرکت‌های مانند همراه اول، ایرانسل، مخابرات، زیرساخت، مرکز فیزیک نظری (پژوهشگاه دانش‌های بنیادی)، رایتل و برخی دیگر از شرکت‌های ارائه دهنده خدمات اینترنت امضا کرده که ارزش تمام این قراردادها ۲/۰۸۴/۴۷۱/۸۱۳/۵۲۳ ریال (دو بیلیون و هشتاد و چهار میلیارد و چهارصد و هفتاد و یک میلیون و هشتصد و سیزده هزار و پانصد و بیست و سه ریال) بوده است. البته این تمام قراردادهای نیست که در این بازه زمانی بسته شده است.

برخی از این قراردادها نیز به دلار بسته شده، به عنوان نمونه دو قرارداد به ارزش ۹۰۱/۰۱۸ دلار در سال ۱۳۹۹ و دیگری ۳/۴۵۶/۰۰۰ دلار در سال ۱۳۹۷ بسته شده است.

برخی از این قراردادها به شرح زیر هستند.

Author: Mahdi Amiri <amiri@internet.ir>     More 
To: abedi@douran.com  5/23/22, 09:25
Subject: Fwd: مشارکت در گروه کاری باز سازمان ملل متحد برای امنیت سایبری: OEWG

جناب آقای دکتر عابدی
مدیرعامل محترم شرکت دوران
با سلام و احترام
به پیوست مستندات مربوطه در خصوص نحوه ثبت نام و مشارکت موسسات غیردولتی در گروه کاری باز سازمان ملل متحد راجع به امنیت سایبری ارسال می‌گردد.
لطفاً در صورت تمایل با توجه به محدودیت زمانی (تا سوم خردادماه سال جاری)، در اسرع وقت طبق دستورالعمل پیوست نسبت به ثبت نام اقدام فرمایید.
https://meetings.unoda.org/section/oewg-ict-2021-ngo-information_16382
https://forms.office.com/pages/responsepage.aspx?id=2zWeD09UYE-9zF6kFubccMjpoC_xkITnrRxnChY40tFUN18KSFNCWjcwTkVUNkcxw0LFESTdG03BEWS4u
<https://bit.ly/ICTOEWG22>
mail to prizeman@un.org

با تشکر
امیری

تصویر ایمیل دادستانی به شرکت دوران در مورد مشارکت در گروه کاری سازمان ملل

شماره قرارداد	سال	طرف قرارداد	مبلغ به ریال	قرارداد دلاری	نوع لایسنس
۱۶۷۸	۱۳۹۶	همراه اول	۲۵/۶۶۸/۰۰۰/۰۰۰	-	۸۰Gbps
۱۶۶۲	۱۳۹۶	همراه اول	۱۲/۸۳۴/۰۰۰/۰۰۰	-	۴۰Gbps
۵۹۹۷	۱۳۹۹	ایرانسل	۵۸۴/۲۸۸/۰۰۰/۰۰۰	۹۰۱/۰۱۸	فروش تجهیزات نرم‌افزاری و سخت افزاری امنیتی
۹۰۶۱/۴۹۹۶	۱۳۸۶	ایرانسل	۹۹/۶۱۶/۰۰۰/۰۰۰	-	-
۴۲۹۳	۱۳۹۷	ایرانسل	۲۶۰/۱۰۷/۲۰۰/۰۰۰	۰۰۰/۶۵۴/۳	۱۰۰Gbps
۴۴۲۴	۱۳۹۴	شرکت ارتباطات زیرساخت	۶۳/۰۴۱/۰۷۷/۴۰۰	-	-
۱۶۷۸	۱۳۹۶	همراه اول	-	-	۴۰G+۴۰G
		شرکت فن‌آوری اطلاعات	۸/۸۷۸/۹۱۵/۵۵۶	-	سیستم فیلترینگ داخلی فاز اول بر اساس مناقصه ۸۵/۱۷
۱۱۲۶		رایتل	۷/۴۶۷/۹۱۰/۰۰۰	-	«خرید لایسنس‌ها و انجام خدمات مهندسی، یکپارچه سازی و ارتقای ظرفیت سامانه «Policy Enforcement از ۸۰Gbps به ۱۶۰Gbps»
۷۳۱۹	۱۳۹۰	مرکز فیزیک نظری (پژوهشگاه دانش‌های بنیادی)	۶۹/۰۰۰/۰۰۰	-	۱۲۸Mb/ps
۱۹۹۱۹	۱۳۹۶	شرکت ارتباطات زیرساخت	۱/۷۰۱/۳۰۰/۰۰۰	-	دو دستگاه فایروال
۸۵۶۰	۱۳۹۶	شرکت ارتباطات زیرساخت	۵۰۱/۰۶۷/۸۹۵/۹۱۷	-	خرید تجهیزات ارتقا سخت‌افزاری و توسعه و ارتقا نرم‌افزای سیستم‌های پالایش ترافیک دیتای بین‌الملل فاز ۵
۶۵۸۷	۱۳۸۶	شرکت ارتباطات زیرساخت	۹/۴۹۴/۱۶۰/۰۰۰	-	پالایش داخلی ترافیک دیتای بین‌الملل
۱۲۷۷۳۶	۱۳۹۲	شرکت ارتباطات زیرساخت	۲۳/۹۲۴/۵۴۸/۰۰۰	-	خدمات پشتیبانی فیلترینگ فاز یک و تجهیزات تکمیلی
۲۰۱/۵۸۴	۱۳۹۳	شرکت ارتباطات زیرساخت	۳۵/۴۹۸/۱۸۱/۸۵۰	-	خرید تجهیزات بهسازی سرورهای فیلترینگ و تامین لیسانس نرم‌افزاری
۶۲۱۳	۱۳۹۴	شرکت ارتباطات زیرساخت	۰۰۲/۷۴۶/۲۷۳/۲۳۴	-	خرید سیستم‌های پالایش ترافیک فیلترینگ - فاز ۴
۹۶-۹۵	۱۳۹۵	شرکت مخابرات	۰۰۶/۷۷۹/۲۴۴/۸۱	-	تفکیک ترافیک داخلی و خارجی

مجموعه فنی تجهیزات نرم افزاری و سخت افزاری سیستم های اینترنت

(پیوست الف)

مشخصات فنی تجهیزات

عنوان	PN
بانک سخت افزاری فیلترینگ و DPI به همراه تمامی تجهیزات جانبی	DSGF-BLD3-HW

پستم فوق شامل تمامی تجهیزات سخت افزاری جهت راه اندازی یک بانک فیلترینگ بصورت کامل میباشد. تجهیزات آفل موزد نیل می باشد.

ردیف	شرح	نوع
۱	شاسی بلیت جهت بانک فیلترینگ و DPI	سخت افزار
۲	سرورهای مناسب برنده شاسی بلیت جهت بانک فیلترینگ و DPI به همراه تمامی تجهیزات داخلی مورد نیاز	سخت افزار
۳	۴ عدد سوئیچ ورودی و خروجی مشخصات هر سوئیچ : 8x 10Gb and 4x40Gb uplink ports	سخت افزار
۴	۱ عدد سوئیچ مدیریت	سخت افزار
۵	۸ عدد SFP+	سخت افزار
۶	۲ عدد External (۲ عدد)	سخت افزار
۷	۲ عدد External و Logger و گزارشگر (متناسب با پهنای باند)	سخت افزار
۸	۲ عدد سوئیچ External مدیریت	سخت افزار
۹	۱ عدد سرور تست	سخت افزار
۱۰	تجهیزات پست موزد نیاز	سخت افزار

عنوان	PN
لینکهای نرم افزاری فیلترینگ برای 100Gbps به همراه تمامی لینکهای جانبی	DSGF-100000-SW

تصویر خدمات فنی فیلترینگ به شرکت ایرانسل تحت عنوان سیانت



(پیوست الف)

مشخصات فنی تجهیزات

عنوان	PN
بانک سخت افزاری فیلترینگ به همراه تمامی تجهیزات جانبی	DSGF-BLD3-HW

پستم فوق شامل تمامی تجهیزات سخت افزاری جهت راه اندازی یک بانک فیلترینگ بصورت کامل می باشد. تجهیزات آفل موزد نیل می باشد.

ردیف	شرح	نوع
۱	شاسی بلیت جهت بانک فیلترینگ	سخت افزار
۲	سرورهای مناسب برنده شاسی بلیت جهت بانک فیلترینگ به همراه تمامی تجهیزات داخلی مورد نیاز	سخت افزار
۳	۴ عدد سوئیچ ورودی و خروجی مشخصات هر سوئیچ : 8x 10Gb and 4x40Gb uplink ports	سخت افزار
۴	۱ عدد سوئیچ مدیریت	سخت افزار
۵	۸ عدد SFP+	سخت افزار
۶	۲ عدد External (۲ عدد)	سخت افزار
۷	۲ عدد External و Logger و گزارشگر (متناسب با پهنای باند)	سخت افزار
۸	۲ عدد سوئیچ External مدیریت	سخت افزار
۹	۲ عدد سرور جیپی	سخت افزار
۱۰	۱ عدد سرور تست	سخت افزار
۱۱	تجهیزات پست موزد نیاز	سخت افزار

تصویر خدمات فنی فیلترینگ به شرکت ایرانسل تحت عنوان سیانت

در بین این قراردادها که عمدتاً در مورد توسعه سیستم های سانسور و فیلترینگ هستند دو قرارداد متفاوت دیده می شود.

قرارداد ۹۶-۹۵: تامین تجهیزات تفکیک ترافیک داخلی و خارجی

این قرارداد بین شرکت دوران و مخاطرات در سال ۱۳۹۵ به مبلغ ۱۸/۴۴۲/۹۷۷/۶۰۰ ریال بابت «خرید تجهیزات سخت افزار و نرم افزاری و خدمات پیاده سازی ایجاد امکانات تفکیک ترافیک داخلی از بین الملل مناطق شرکت مخاطرات» در استان های «خراسان رضوی، همدان، ایلام، خراسان جنوبی، چهارمحال و بختیاری، کرمان، خوزستان، کردستان، سیستان و بلوچستان، گلستان، گیلان و خراسان شمالی» بسته شده است.

تفکیک ترافیک سیاستی بود که در دولت حسن روحانی شروع شد. این سیاست عملاً امکان این را برای حکومت ایران فراهم کرد تا بتواند با حداقل آسیب به سیستم‌های داخلی جمهوری اسلامی بتواند اینترنت بین‌الملل را نه تنها راحت‌تر سانسور و مختل بکند، بلکه به راحتی بتواند اینترنت جهانی را قطع بکند.

بر همین اساس ما شاهد هستیم که از سال ۱۳۹۸ تا کنون جمهوری اسلامی ایران ده بار اینترنت جهانی را قطع کرده است که هر ده بار در پاسخ به تظاهرات خیابانی بوده است. تظاهرات‌های که تعداد بسیاری از شهروندان ایرانی در آن کشته، مجروح و زندانی شدند. به این ترتیب شرکت دوران نقش اساسی در نه تنها سرکوب اینترنت بلکه سرکوب معترضان در خیابان دارد.

سپاه پاسداران انقلاب اسلامی: قرارداد رمز کننده شبکه

قرارداد خرید تجهیزات رمز کننده و فایروال بین دوران و امیر توکلی از سپاه پاسداران انقلاب اسلامی به عنوان کارفرما در تاریخ ۱۳۹۴/۱۱/۱۲ بسته شده است. این قرارداد در مورد فروش، پشتیبانی، و آموزش ۱۰۰ دستگاه سخت‌افزاری رمز کننده شبکه ساخت شرکت دوران است. مبلغ این قرارداد ۱ میلیارد ریال است.

مسدود کردن فیلترشکن‌ها و وی‌پی‌ان‌ها

در [نامه‌ای](#) که از طرف مهدی امیری در دادستانی و در سال ۱۳۹۷ برای شرکت دوران ارسال شده، از آنها دعوت شده است تا در جلسه‌ای با هدف «بررسی اقدامات و نحوه عملکرد آن شرکت در حوزه پالایش محتوا و مسدود سازی فیلتر شکن‌ها و VPN‌های غیر مجاز» شرکت کنند.

در متن [نامه](#) آماده، از ماموریتی صحبت شده که به این شرکت داده شده است و توضیحات بیشتر درباره آن چنین است: «در اجرای ماموریت محوله از سوی دادستانی محترم کل کشور به این هیات تحقیق، مقتضی است به منظور بررسی اقدامات و نحوه عملکرد آن شرکت در حوزه پالایش محتوا و مسدودسازی فیلترشکن‌ها و VPN‌های غیر مجاز دستور فرماید نمایندگان مطلع و تام‌الاختیار آن شرکت در تاریخ ۱۳/۰۶/۹۷ ساعت ۱۰ ال‌غایت ۱۱ در محل دادستانی کل کشور به شناسایی ذیل حضور یابند.»

این نامه توسط رضا تقی‌پور با عنوان رییس هیات تحقیق دادستانی کل کشور رسیده است. رضا تقی‌پور بعداً عضو حقیقی شورای عالی فضای مجازی شد.

شرکت فن آوری های تنظیم یار شریف

شرکت «فن آوری های تنظیم یار شریف» یکی از پروژه هایی است که توسط رسول جلیلی، رییس دانشگاه شریف و عضو شورای عالی فضای مجازی راه اندازی شده است و هدف آن کمک به تحقیق و توسعه ابزارهای مورد نیاز دادستانی است.

شرکت فناوری های تنظیم یار شریف در تاریخ ۱۴ تیر ۱۴۰۱ [فایلی پی دی اف](#) با عنوان «پروپوزال فنی» سامانه مستندساز ادله الکترونیکی را به مدیر فنی معاونت امور فضای مجازی دادستانی کل کشور ارسال کرده است که در پاراگراف اول این پروپوزال، هدف از ساخت سامانه موسوم به «عدالت یار»، ایجاد «بستری جهت گردآوری و دسترسی به ادله الکترونیکی حقیقی و ارائه آنها به دادگاه» عنوان شده است.

بر این اساس ما برای اولین بار با ابزاری آشنا می شویم که دادستانی برای جمع آوری سند علیه افراد - و نه نهادها و شرکتها - استفاده می کند.

آنطور که در بخش نیازهای این سند نوشته شده است، یکی از نیازها «اسکرین شات از چت ها و پست ها، اطلاعات حساب ها مجازی، انتشار غلط اطلاعات» عنوان شده است. در ادامه آمده آمده است: «(حذف پیام) همچنین در بسیاری از پیام رسان ها پس از ارسال پیام، امکان حذف آنچه برای خود فرستنده و چه حتی برای گیرنده وجود دارد که باعث می شود هیچ رد و اثری از گفتگو باقی نماند.»

تحقیقات ما نشان می دهد که دسترسی به محتوای گفتگوی کنشگران مدنی و سیاسی پس از بازداشت، یکی از اولین اقدام های است که مامورین امنیتی جمهوری اسلامی انجام می دهند. این روند تا حدود یک تا دو سال پیش

جناب آقای امیری،
معاویت محترم مدیریت کل نظارت بر فضای مجازی دادستانی کل کشور،
با عرض سلام و احترام،
پیرو جلسه پیشین اینجانب با جنابعالی در اسفندماه 1400 و فرمایش شما منین بر ارائه پروپوزال فنی که پوشش دهنده چالش ها و راهکارها بر حسب هر پیام رسان باشد، پروپوزال نهایی خدمت شما به پیوست
این کپی ارسال می گردد.
بر این پروپوزال تمامی پیام رسان های داخلی و خارجی مورد بررسی دقیق قرار گرفته و پس از مشورت با صاحب نظران و خبرگان بسیار در پیام رسان های داخلی و شرکت های توسعه رهنده محصولات امنیت و شبکه راهکارهای منتخب ارائه گردیده و راهکارهای مزبور هم به طور خلاصه ارائه شده و از مجموعه روش ها حذف گردیده اند. با این حال، طبق تحقیق ها و مباحثه های انجام شده، در برخی قسمت ها نیاز به تصمیم گیری نهاد مسئول می باشد که کدام رویکرد پیاپی سازی اینجانب برود و کدام رویه امکان پذیرتر از سایر رویه ها می باشد. قسمت های گوناگون این پروپوزال عبارتند از:

- 1) **جدید**
- 2) **شرح نیاز:** کاربرد و نیاز جامعه - حذف پیام - پیام رسان ها - پیام رسان های داخلی
- 3) **کاربردها و چالش ها:** تلگرام - واتسآپ - اینستاگرام - بله - اینا
- 4) **راهکار حل مسئله:** راهکار فنی اول: طراحی و توسعه سامانه مستندساز ادله الکترونیکی - راهکار فنی دوم: طراحی و توسعه API و کد رهگیری برای پیام رسان های داخلی - راهکار های فنی بررسی شده و مردود - زیرساخت و پروتکل ایچکس ها
- 5) **آدرس و اطلاعات تماس**

طلی ماه های گذشته، نیازسنجی فنی و سیاستگذاری در این راستا در حد توان انجام شده است تا نمره کار هرچه رودتر حاصل شود. امید است تلاش های این مدت اینجانب در این مدت، مورد توجه و حمایت جنابعالی قرار گیرد و همکاری مناسبی شکل گیرد تا این صنعت عمومی مشمول خدمتی درخور و شایسته قرار گیرد.
خواهشمند جهت بررسی و بحث و تصمیم گیری در رابطه با نحوه پیاده سازی فنی، طلسمه ای با جنابعالی داشته باشم و راهکار نهایی مشخص گردد. لطفاً هرگونه پیشنهاد یا انتقاد مورد نظر خود را در این راستا به بنده انتقال دهید.
با احترام،
آرمان بهنام
شرکت فناوری های تنظیم یار شریف
جایان آزادی، جایان اسناد حبیب الله، بالابر از میدان حسین، پلاک 56، ایستگاه باواری شریف، ساختمان مرکز باواری صوت و تصویر (اومیک)
شماره تماس: 09391897972
تلفن: 02140665379
کد پستی: 1455714181

1 attachment: پروپوزال فنی سامانه مستندساز ادله الکترونیکی - دادستانی کل کشور.pdf 1.0 MB

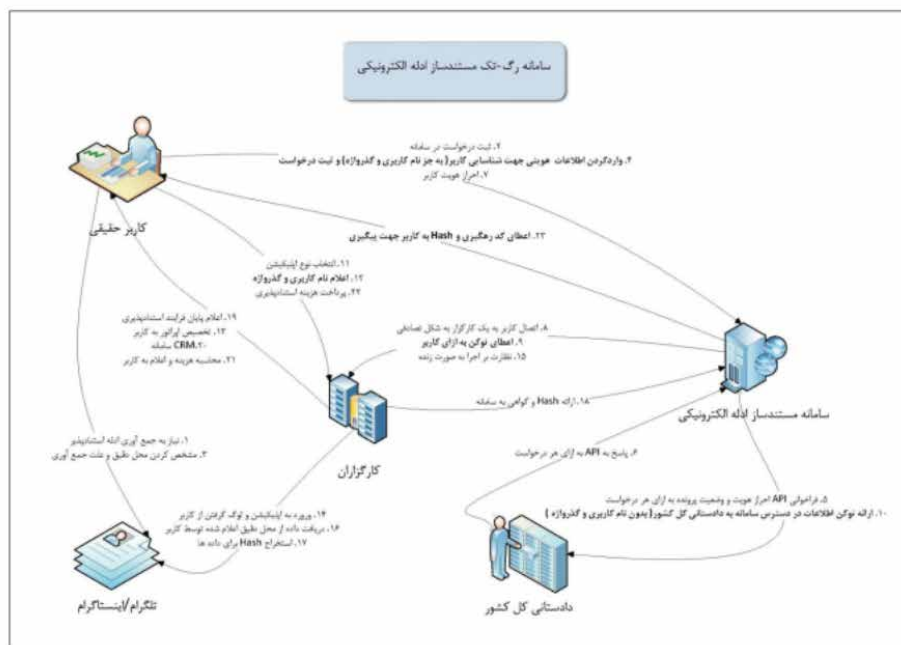
تصویر ایمیل شرکت «فن آوری های تنظیم یار شریف» به دادستانی و ارسال پروپوزال در مورد سامانه مستندساز ادله الکترونیکی

به این صورت بود که فرد پس بازداشت تحت فشار قرار می‌گرفت تا اطلاعات حساب خود را تحویل دهد و تفتیش حساب‌های آنلاین در زندان انجام می‌شد، اما اخیراً در محل بازداشت، اقدام به جمع‌آوری اطلاعات، چت‌هاها و ایمیل‌های کنشگران می‌کنند چرا که احتمال حذف این اطلاعات یا مسدود شدن حساب‌های کنشگران توسط نزدیکان آنها وجود دارد.

بنابراین چنین سیستمی عملاً دست مقامات قضایی و امنیتی را برای دسترسی به محتوای حساب‌های زندانیان بدون داشتن دستور قضایی و روند حقوقی باز خواهد گذاشت.

در ادامه این سند، شرکت «فناوری‌های تنظیم‌یار شریف» به بررسی تک‌تک پیام‌رسان‌ها مانند تلگرام، واتس‌اپ، اینستاگرام، بله، ایتا می‌پردازد و توضیح می‌دهد که روش کار این پیام‌رسان‌ها شامل امنیت، حذف پیام، ذخیره‌کردن پیام‌ها و سایر موارد چیست و چه چالش‌های را برای سیستمی که می‌خواهند طراحی کنند، ایجاد می‌کند.

 <p>تنظیم‌یار استارت‌آپ امنیتی و حقوقی</p>	<p>پروپوزال فنی "سامانه مستندسازی ادله الکترونیکی"</p>
<p>کارفرما : معاونت نظارت بر فضای مجازی دادستانی کل کشور</p>	<p>شرکت فناوری های تنظیم بار شریف</p>



شکل ۵. نمودار جریان فرآیند ارتباط بین نهادی در اجرای راهکار با ایجاد سامانه نظارت بر مستندسازی ادله الکترونیکی

تصویر نمودار جریان فرآیند ارتباط بین نهادی در مورد سامانه مستندسازی ادله الکترونیکی

مستندسازی ادله الکترونیکی

در نهایت راهکارهای این شرکت در مورد پیام‌رسان‌های داخلی شامل استفاده از API آنها و دسترسی به حساب‌های کاربران و در مورد سرویس‌های خارجی به عکس گرفتن از محتوای گفتگو و روش‌های مشابه است.

در بخش دیگری از [اسنادی](#) که در مورد این سامانه وجود دارد، روی حذف پیام تاکید شده است. به عنوان نمونه، در یکی دیگر از این اسناد آمده است: «در بسیاری از پیام‌رسان‌ها پس از ارسال پیام، امکان حذف پیام وجود دارد که باعث می‌شود هیچ رد و اثری از گفتگو باقی نماند و شاکی و متشاکی نتواند هیچگاه به آن استناد کند و احقاق حق نماید. همچنین دادگاه‌ها، مراجع قضائی و پلیس فتا نیز با وجود امکانات متعدد جهت استعلام از اطلاعات افراد، دسترسی به این داده‌ها ندارند. وجود این سامانه و در دسترس قرارگیری اپلیکیشن آن برای مردم، موجب جمع‌آوری سریع ادله الکترونیکی توسط فرد شده و امکان حل بسیاری مسائل و رفع دغدغه‌ها را به مردم می‌دهد.»

در ادامه راهکار حذف پیام را «ذخیره یک نسخه آفلاین از وب سایت‌ها، چت‌های پیام‌رسان‌ها و شبکه‌های اجتماعی در یک محیط امن» عنوان می‌کند. در ادامه آمده است: «برای این کار ساده‌ترین و مطمئن‌ترین روش تهیه عکس (Screenshot) یا فیلم از صفحه مورد نظر است.»

روش پیاده‌سازی این اپلیکیشن برای دسترسی به محتوای چت‌ها و ایمیل‌های گروه‌های هدف، پیاده‌سازی یک اپلیکیشن شخص ثالث ذکر شده است. در گزارش طراحی نوشته شده است: «طرح سامانه مستندساز عدالت یار با بهره‌گیری از مفهوم party-third و با هدف اعتماد سازی بین مردم و فضای مجازی و تسهیل فرآیند دادرسی پرونده‌ها به صورت فناوری reg-tech پیاده سازی می‌گردد.»

اپلیکیشن‌های شخص ثالث، اپلیکیشن‌هایی هستند که با استفاده از ابزاری‌های مشروع تهیه می‌شوند و با دریافت اجازه از مالک حساب به اطلاعات حساب او دسترسی پیدا کنند. به عنوان نمونه، شما می‌توانید با استفاده از [ابزارهایی که گوگل](#) در اختیار شما قرار می‌دهد، اپلیکیشن بسازید که حتی به محتوای ایمیل کاربر دسترسی داشته باشد. البته در زمان اجرای چنین اپلیکیشنی از کاربر برای دسترسی به حساب او اجازه گرفته می‌شود اما معمولاً کاربران به دلیل ضعف دانش و صرفاً با دیدن نام گوگل یا هر شرکت دیگری اعتماد می‌کنند و این اجازه را می‌دهند.

براساس همین روش در ادامه توضیح داده شده است: «علاوه بر محتواهای وب ذکر شده، محتوای شبکه اجتماعی نیز وجود دارد. این محتوا شامل چت بین دو شخص، چت در گروه و محتوای کانال‌های تلگرام، محتوای پست‌های اینستاگرام، محتوای تصویر و ویدئو در گالری و محتوای پیامک‌ها می‌باشد که علاوه بر راهکارهای ذکر شده، اپلیکیشن و وب سایت مورد نظر، دسترسی

به برنامه های نصب شده و برنامه های در حال اجرای سیستم می گیرد و با بررسی آن ها، اپلیکیشن های جعلی و اسکرین شات های جعلی از مبدا را تشخیص می دهد.»

در مورد هزینه تولید این سیستم، قیمت نهایی ۵۲۰ میلیون تومان برآورد شده و آمده است: «قیمت تمام شده محصول معادل ۲۵۰ میلیون تومان برای تحقیق و توسعه، ۳۶۰ میلیون تومان برای ساخت و اجرا و تست ها و ۱۹۰ میلیون تومان برای ایجاد محصولات ترویجی و معرفی و مستندسازی و آموزش این سامانه می باشد. مجموعاً قیمت تمام شده توسعه این محصول معادل ۸۰۰ میلیون تومان می باشد.»

نام و مشخصات کسانی که بر روی این سیستم کار می کنند، به این صورت ذکر شده است.

نام و نام خانوادگی	تحصیلات	دانشکده و دانشگاه رشته تحصیلی	نقش در پروژه
آرمان بهنام	کارشناسی ارشد	دانشگاه علم و صنعت ایران - دانشکده مهندسی صنایع	تعریف پروژه - ایده پردازی - مطالعات بازار - مدیریت پروژه - تعریف فرایند - تشریح راهکار و ساختار آن
محمود اقوامی پناه	دکتری	دانشگاه تهران	مهندسی کامپیوتر
کمیل شاه حسینی	دکتری	دانشگاه علم و صنعت	مهندسی کامپیوتر توسعه دهنده

یکی از روش های که توسط هکرهای حکومتی استفاده می شود، ایجاد چنین اپلیکیشن های است.

تحلیل شبکه های اجتماعی توسط «لایفوب»

شرکت **لایفوب** در ۲۵ دی ۱۳۹۸ **تحلیل مفصلی** از واکنش کاربران ایرانی در توئیتر، اینستاگرام و تلگرام نسبت به فاجعه سرنگونی هواپیمای اوکراینی ارایه کرده و به دادستانی فرستاده است. در بخشی از تحلیل این شرکت آمده است: «تا جایی که بر اساس نمایه تحلیل احساسات و عواطف توئیتر فارسی، احساسات منفی انسانی در این رسانه اجتماعی حتی از احساس خشم اعتراضات بنزینی آبان ماه نیز پیشی گرفت.»

یکی موارد مهم مورد اشاره در این گزارش «تحریک به اعتراض و تجمع (دانشگاه امیرکبیر و میدان آزادی)» است. بهاره هدایت، فعال سرشناس دانشجویی در این تجمع بازداشت شد و در ۴ مرداد ۱۳۹۹ به دلیل شرکت در این تجمع به اتهام تبلیغ علیه نظام از طریق نوشتن توییت‌هایش به ۸ ماه زندان محکوم شد.

لایفوب فراتر از تحلیل شبکه اجتماعی رفته و اقدام به ارزیابی تحلیلی سیاسی-محتوایی می‌کند. این شرکت از واکنش مسوولین جمهوری اسلامی نیز تحلیلی دقیق ارائه کرده است.

در بخشی دیگری از این گزارش آمده: «دو چهره دولتی یعنی وزیر فرهنگ و ارشاد اسلامی و مشاور رئیس جمهور در توییت‌هایی جداگانه، کوشش کردند سخنرانی سردار را لازم اما ناکافی بدانند. چهره‌های دیگر دولتی چندان در موضوع کنکاش نکردند و وزیرخارجیه به انتشار یک تصویر سیاه به معنی عزاداری بسنده کرد. اما اصالح طلبان در دو گروه سیاسی (شهین‌دخت مولوردی، محمود صادقی و ...) و اجتماعی (عباس عبدی، محمد فاضلی، محمدرضا جلایی‌پور و ...) نیز به شکلی عمومی همان سوژه «اعتماد عمومی» و «فروپاشی اجتماعی» را پیش بردند.»

آنها در ادامه تحلیل سیاسی خود را اضافه کرده‌اند: «اصلاح‌طلبان حتی در ماجرای تشییع پیکر سردار شهید قاسم سلیمانی که نماد و تجلی وحدت و همدلی جامعه و ضرورت گرفتن انتقام سخت از آمریکا بود، در تالش بودند پیام‌های همیشگی خود یعنی معرفی نشانه‌های دو قطبی و آنچه آنان «مخالفت با جنگ» می‌خوانند، برداشت کنند و به خورد جامعه بدهند. اگرچه اتفاق ناگوار مرگ ۶ نفر از هموطنان در مراسم تشییع در کرمان، به آنان کمک بسیاری کرد.»

اینترنت طبقاتی

اینترنت طبقاتی بازوی دیگری برای پیاده‌سازی سیاست‌هایی است که هدفشان قطره‌چکانی کردن پهنای باند بین‌المللی و جایگزین شدن این روش با فیلترشکن‌هاست.

فیلترشکن‌ها عملاً به یک بازی موش و گربه تبدیل شده‌اند. حکومت جمهوری اسلامی منابع زیادی را برای مسدود کردن فیلترشکن‌ها مصرف می‌کند اما به دلیل آنکه اکثر سرویس‌های محبوب فیلتر هستند، عمده ترافیک بین‌الملل ایران از طریق فیلترشکن‌ها منتقل می‌شوند.

مقامات ایرانی به این باور رسیده‌اند که برای پایان دادن به این بازی موش و گربه باید کنترل بازار فیلترشکن‌ها را در دست خود داشته باشند.

طرح دسترسی طبقاتی به اینترنت توسط محمدجواد آذری جهرمی، وزیر ارتباطات دولت دوم حسن روحانی در مجلس شورای اسلامی **مطرح** شد.

او با طرح این موضوع که فیلترشکن‌های چالشی هستند که باید برای آنها برنامه داشت، گفت: «بدون ساماندهی برخی حوزه‌ها نمی‌شود موضوع فیلترشکن‌ها را بررسی کرد. ما بارها در جلسات مختلف گفتیم [دسترسی‌ها را] طبقه‌بندی کنیم. نمی‌شود سطح سیستم برای پزشک، برای استاد دانشگاه یا برای خبرنگار با سطح یک کودک هشت، نه ساله برابر باشد.»

طرح گشایش شریف؛ آزمون اولیه اینترنت طبقاتی

در **نامه‌ای** که «زارعی» از دانشگاه شریف در تاریخ ۴۱ تیر ۱۴۰۱ به دادستانی ارسال کرده آمده است: «براساس مجوز شماره ۳۰/۳/۱۴۰۱/دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه دادستانی کل کشور (کارگروه) به صورت آزمایشی و به مدت یکسال از تاریخ ۱/۵/۱۴۰۱ در دانشگاه صنعتی شریف (دانشگاه) به منظور فراهم‌سازی امکان دسترسی به منابع پالایش‌شده برای جامعه مخاطبین منتخب در فضای فیزیکی یا مجازی مشخص با رعایت الزامات قانونی و در چارچوب قوانین و مقررات خاص مجوز مربوط و براساس این دستورالعمل اجرا می‌شود.»

زارعی که ارسال کننده نامه است، شکایت دارد که چرا این دسترسی هنوز فراهم نشده است.

این درخواست، به ارایه دسترسی به اینترنت بدون فیلتر برای گروهی از افراد در دانشگاه شریف مربوط می‌شود که قرار بود به صورت آزمایشی اجرا شود. این سرویس را می‌توان یکی از گام‌های اولیه در ایجاد اینترنت طبقاتی ارزیابی کرد.

برای پیاده‌سازی این سرویس، فهرستی از آی‌پی‌های این دانشگاه در لیست سفید قرار گرفته‌اند.

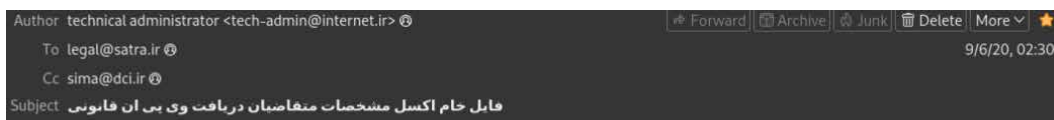


تصویر ایمیل زارعی از دانشگاه شریف در مورد فراهم کردن اینترنت طبقاتی برای این دانشگاه

وی‌پی‌ان قانونی

با وجود اینکه پیاده‌سازی اینترنت طبقاتی در دانشگاه شریف با استفاده از روش لیست سفید پیاده‌سازی شده بود، اما ایمیل دیگری که حدود یک سال قبل به [ساترا](#) ارسال شده است نشان می‌دهد در گذشته، ارایه اینترنت طبقاتی با استفاده از وی‌پی‌ان قانونی ارایه می‌شده است.

مدیر فنی دادستانی در ایمیلی به تاریخ ۱۷ شهریور ۱۳۹۹ خطاب به بخش حقوقی ساترا دو فایل اکسل فرستاده که درخواست‌کنندگان برای دریافت وی‌پی‌ان قانونی باید آنها را پر کنند.



با سلام
احتراما فایل های پیوست جهت تکمیل و ارسال اطلاعات متقاضیان درخواست وی پی ان قانونی برای گروه خبرنگاران صدا و سیما و گروه ارائه دهندگان خدمات صوت و تصویر فراگیر ارسال می‌گردد. لطفا همه قسمتها را با اطلاعات کامل صحیح تکمیل فرمایید. در غیر اینصورت ثبت نام صورت نمی‌پذیرد.
در صورت نیاز جهت راهنمایی بیشتر با شماره 02138582301 تماس حاصل فرمایید.



تصویر ایمیل دادستانی به ساترا و معرفی ساز و کار دریافت اینترنت طبقاتی برای خبرنگاران

این طرح برای نخستین بار با عنوان «وی‌پی‌ان قانونی» به عنوان یک راهکار فنی برای طبقه‌بندی دسترسی به اینترنت در تاریخ ۳۰ آبان ۱۳۹۸ و در واکنش به رفع مشکلات قطع اینترنت در آبان خونین ۱۳۹۸ [مطرح شد](#).

تحقیقات حقوقی و فنی

بخش زیادی از محتوای ایمیل‌های دادستانی مربوط به تحقیقات حقوقی و فنی در مورد محدودیت دسترسی به اینترنت یا جرم‌انگاری فعالیت در اینترنت است.

پروپوزال فیلترینگ

در ۱۴ دی ۱۳۹۳ [اصغر تاج‌الدین](#) با ایمیلی متعلق به دانشگاه زنجان tajoddin@zan.au.ir ([لینک ذخیره شده](#))، استادیار دانشگاه زنجان، به دادستانی ارسال کرده است و در آن اشاره کرده است که این ایمیل در پی پیشنهاداتی است که در جلسه‌ای حضوری در مورد آنها صحبت کرده بودند.



این ایمیل حاوی [پیشنهادهای](#) فنی آقای تاج‌الدین برای اعمال فیلترینگ و سانسور اینترنت با عنوان «طرح مدیریت دسترسی به محتوا در کشور» به دادستانی ارایه شده است.

بر اساس اطلاعات این فایل، این طرح «متعلق به شرکت توسعه سیستم سازی شرق» است.



بسمه تعالی
با سلام
طرح پیشنهادی براساس مواردی که حضوراً فرمودید تهیه و به پیوست آمده است.
الته هنوز شما تک اولیه بخش داشبورد را نیاورده ام و انشالله تا فردا ارسال می کنم
با تشکر ارادتمند شما
تاج الدین
1393/10/14

1 attachment: DACC-Proposal-1.docx 186 KB

تصویر ایمیل اصغر تاج‌الدین به دادستانی به همراه فایل پروپوزال طرح فیلترینگ

ربات شناسایی پست در اینستاگرام

محمدجواد آذری جهرمی در تاریخ ۵۲ بهمن ۱۳۹۳ ایمیلی به دادستانی ارسال کرده و در آن گزارشی از عملکرد ماشین شناسایی پست‌های اینستاگرامی ارایه داده است.

به نظر می‌رسد این ماشین در زمانی فعالیت می‌کرده است که اینستاگرام هنوز از پروتکل SSL/TLS استفاده نمی‌کرده و همین موضوع امکان فیلتر کردن صفحه‌های اینستاگرام را به حکومت ایران داده بود.

این پروژه تا سال ۱۳۹۷ همچنان ادامه داشته است. به این دلیل که در تاریخ ۹۱ آبان ۱۳۹۷ [نامه‌ای](#) از سوی جواد جاویدنیا سرپرست وقت معاونت



با سلام
نتایج بررسی برای بهره برداری ارسال میگردد

جهرمی

با سلام

نتایج بررسی به شرح ذیل تقدیم حضور می گردد

- **khaneye_maa** نام قبلی ایشان hairmod بوده و تبلیغات غیر اخلاقی داشته است. رفع فیلتر شد
- **which_brand** به نظر خطای ربات بوده است. رفع فیلتر شد
- **bolandgou** نام کاربری قبلی ایشان bolandgou_creative_house بوده و صفحه ایشان بیشتر سفید تشخیص داده شده بود با این حال به سبب تکرار درج آگهی غیر اخلاقی در نام جدید سیاه شده بود. رفع فیلتر شد
- **sepidclinic** در تاریخ ۲۰۱۲/۵/۱۸ توسط دادستانی وارد پایگاه داده ها شده در نتیجه رفع فیلتر نشد.
- **new.ideaa** نام قبلی ایشان jok.zirnafi و نام کامل ایشان 18++ بوده است. نیازمند دستور برای رفع فیلتر

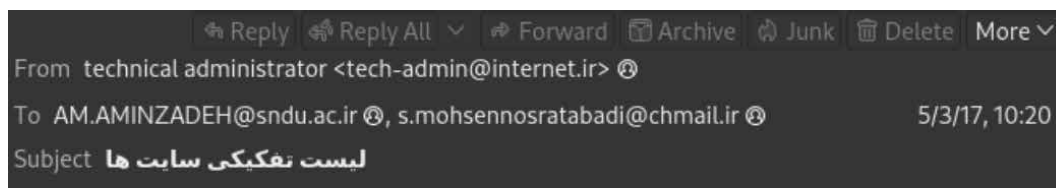
تصویر ایمیل ارسالی از محمدجواد آذری جهرمی به دادستانی و گزارش عملکرد ربات شناسایی پست‌های اینستاگرام

امور فضای مجازی دادستانی به رسول جلیلی ارسال شده و خبر از تشکیل جلسه‌ای «در خصوص طرح‌های مربوط به فیلترینگ هوشمند و نحوه مواجهه با اینستاگرام با حضور نمایندگان این دادستانی، ستاد کل نیروهای مسلح، سازمان اطلاعات سپاه پاسداران و برخی دیگر از اعضاء حقیقی شورای عالی فضای مجازی» داده است.

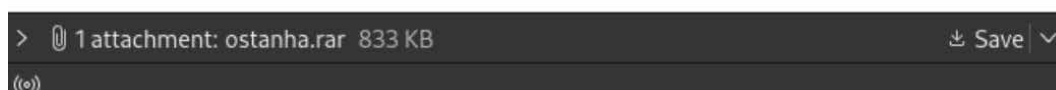
دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

در برخی از ایمیل‌های که مرتبط با موتور جستجوی ملی چاپار ارسال و دریافت شده است ما به فردی با نشانی ایمیل AM.AMINZADEH@sndu.ac.ir متعلق به [دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی](#) (دعا) برخوردیم. بررسی‌های ما نشان می‌دهد که این ایمیل متعلق به محمدعلی امین‌زاده، دانشجوی دکترای راهبردی فضای سایبر این دانشگاه است که مقالاتی در [فصلنامه ملی امنیت ملی](#) منتشر کرده است.

یکی از آخرین مقاله‌های او با عنوان «[فرصت‌ها و تهدیدهای اقتصادی جمهوری اسلامی ایران ناشی از توسعه فناوری‌های سایبری در افق ده ساله](#)» (لینک ذخیره شده) است که او این مقاله را همراه با رسول رضانی



بسمه تعالی
بیرو مذاکرات انجام شده لیست مورد نظر به بیوست ارسال می‌گردد
با احترام
۱۳۹۶/۰۱/۱۳



تصویر ایمیل دادستانی به محمدعلی امین‌زاده، دانشجوی دکترای راهبردی فضای دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی (دعا)

معاونت پژوهش دانشگاه پدافند هوایی خاتم الانبیاء (ص) آجا تهران ایران، و استادیار دانشگاه امام حسین نوشته است.

دانشگاه عالی دفاع ملی با نام کامل «دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی»، از دانشگاه‌های نیروهای مسلح جمهوری اسلامی ایران

است. این دانشگاه فعالیت خود را در سال ۱۳۷۱ به عنوان دانشگاه علوم استراتژیک آغاز کرد و از سال ۱۳۸۱ در زیرمجموعه ستاد کل نیروهای مسلح قرار گرفت.

این ایمیل می‌توان نشان‌دهنده همکاری نیروهای مسلح جمهوری اسلامی با پروژه‌های مربوط به اینترنت ملی و به عنوان نمونه موتور جستجوگر چاپار باشد.

باید یادآوری کنیم که یکی از اهداف کلان طرح صیانت واگذاری اینترنتی ایران به نیروهای مسلح و نظامی کردن اینترنت بود.

در ۸۲ مرداد ۱۳۹۹ طرح جرم‌انگاری فروش فیلترشکن از دادستانی به رضا تقی‌پور انواری (taghipour@sndu.ac.ir) از دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی ارسال شده و در آن اشاره شده که ارسال این طرح بر اساس «مذاکرات» قبلی بوده است.

مشخص نیست این دانشگاه نظامی چه نقشی در تدوین این طرح دارند اما



تصویر ایمیل دادستانی به رضا تقی‌پور انواری از دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی در مورد جرم‌انگاری وی‌بی‌ان

به نظر می‌رسد حداقل در طراحی چنین طرحی نقش مشورتی داشته باشند. در نمونه دیگری، متن قانون ترکیه راجع به شبکه‌های اجتماعی برای رضا تقی‌پور انواری ارسال شده است.

در سایر ایمیل‌ها دادستانی و تقی‌پور از این دانشگاه طرح‌های دیگری در مورد [شبکه ملی اطلاعات](#)، [فیلترینگ تلگرام](#)، و دسترسی به [داده‌های فیلترینگ](#) مطرح شده است.

در این نامه آمده است: «عطف به حکم مأموریت ابلاغی شماره ۱۴۰/۱۳۹۷/۱۳۹۳۵/۹۰۰۰ مورخ ۳۱/۵/۹۷، با ستحضار می‌رساند این هیأت از روز آغاز مأموریت، اقدامات اولیه لازم جهت دسترسی به اطلاعات و سامانه



تصویر ایمیل دادستانی به رضا تقی‌پور انواری از دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی در مورد شبکه‌های اجتماعی

های مورد نیاز، انجام بررسی‌های فنی و بازرسی حضوری از سامانه‌ها و مراکز وزارت ارتباطات و فناوری اطلاعات را بعمل آورده است لیکن از آنجا که مسئولین ذیربط، فراهم نمودن دسترسی به سامانه‌ها و اطلاعات مورد نیاز را منوط به انجام مراحل اداری و صدور مجوزهای لازم از سوی مراجع ذیربط در وزارتین اطلاعات و ارتباطات نموده‌اند و تاکنون اطلاعات خواسته شده جهت انجام تحقیقات مذکور واصل نشده است.»

در این نامه تقی‌پور درخواست تمدید مدت ماموریت را کرده است. همچنین درخواست کرده‌اند تا دادستانی به وزارت ارتباطات دستور دهد تا دسترسی به «سامانه‌های فیلترینگ و تحلیل ترافیک بین‌الملل کشور و اطلاعات مربوط به ترافیک نرم‌افزارهای پیام‌رسان اجتماعی خارجی و داخلی و فیلترشکن‌ها» را فراهم کند.

راهکارهای حقوقی ساماندهی فضای مجازی

در [سندی](#) که به عنوا راهکارهای حقوقی ساماندهی فضای مجازی در این ایمیل‌ها یافته شده است، راهکارهای زیر برای سانسور و ممانعت از دسترسی مردم به اینترنت و پیام‌رسان‌ها مطرح شده است.

۱. مسدود سازی کامل، مؤثر و مستمر کلیه فیلترشکن‌ها، VPN‌های



تصویر ایمیل دادستانی در مورد راهکارهای پیشنهادی برای ساماندهی فضای مجازی

غیرمجاز و ابزارهای گریز از فیلترینگ.

II. کاهش پهنای باند و مسدود سازی تدریجی گوگل پلی و پیام
رسان‌های اجتماعی خارجی به ویژه اینستاگرام و واتس‌آپ

III. قطع یا اختلال موثر مکالمه صوتی و تصویری (LiveStream)
اینستاگرام و واتس‌آپ

(مبانی حقوقی، فنی و اجرایی سازوکارهای مذکور پیوست می‌باشد)

برای اجرای موارد فوق به جلسه‌هایی با مشارکت دادستانی کل کشور، ستاد کل نیروهای مسلح و تاییدهای مکتوب آیت‌الله علی خامنه‌ای، رهبر ایران اشاره شده است. در ادامه آمده است: «اما از آنجا که دولت تمایلی به اجرای این مصوبات نداشته است و دستگاه قضایی نیز عزم جدی برای برخورد با تخلفات نداشته است در عمل این تدابیر و تصمیمات اجرا نشده است لذا پیشنهاد می‌شود به منظور پیگیری مستمر ساماندهی فضای مجازی اقدامات ذیل انجام شود».

بر همین اساس، پیشنهاد شده کمیته‌ای متشکل از نماینده دادستانی کل کشور، مرکز فناوری اطلاعات قوه قضائیه، سازمان اطلاعات سپاه پاسداران و دو نفر نماینده از جانب ریاست قوه قضائیه تشکیل جلسه دهند.

دادستانی همچنین پیشنهاد کرده این مورد از طریق «دسترسی برخط به سامانه کنترل ترافیک شبکه و با همکاری ضابطان (ترجیحاً سپاه پاسداران)» اجرا شود. بر اساس این نامه، اطلاعات دقیق از وضعیت ترافیک شبکه کشور «به طور انحصاری در اختیار اداره کل امنیت شبکه و اجا قرار دارد»، به همین جهت دادستانی کشور اعلام کرده است که این داده‌ها با دستور قضایی یا تصویب در شورای عالی فضای مجازی «دسترسی مستقیم رئیس کمیته نظارت به تجهیزات مانیتورینگ و تحلیل زنده ترافیک شبکه که در اختیار امنیت شبکه قرار دارد فراهم شود».

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای

بین ایمیل‌های که از مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای به دست آمده، ایمیلی با عنوان prison جلب توجه می‌کند. در متن ایمیل خطاب به امیری نوشته شده است:

«سلام از روی اطلاعات ارسالی شما بررسی سمت ما انجام شد و لیست پیوست مربوط به مشترکینی هستند که طی یک هفته در اون سایت (زندان رجایی شهر) بودن و جابجایی نداشتند. اگر شما یک نامه رسمی با حکم قاضی به ما بدید ما اینها رو قطع میکنیم»

روند کاری به این صورت بوده است که فردی به اسم مهاجر از سازمان تنظیم مقررات و ارتباطات رادیویی به اکبری در مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای ایمیلی ارسال کرده است که در آن «لیست مشترکینی که

Author: akbari@certcc.ir
To: amiri <amiri@internet.ir>
Subject: Fwd: prison

سلام از روی اطلاعات ارسالی شما بررسی سمت ما انجام شد و لیست پیوست مربوط به مشترکینی هستند که طی یک هفته در اون سایت (زندان رجایی شهر) بودن و جایابی نداشتند. اگر شما یک نامه رسمی با حکم فاضی به ما بدید ما اینها رو قطع میکنیم

From: "mohajer" <mohajer@cra.ir>
To: "akbari" <akbari@certcc.ir>
Sent: Saturday, June 2, 2018 1:11:22 PM
Subject: prison

با سلام
لیست مشترکینی که در بازه‌ی یک هفته‌ای تنها در محدوده مورد نظر بوده‌اند به پیوست ارسال می‌گردد
با تشکر

1 attachment: لیست مشترکین به تفکیک سلول.xlsx 8.8 KB
لیست مشترکین به تفکیک سلول.xlsx 8.8 KB

تصویر ایمیل مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای به دادستانی و ارسال لیست شماره تلفن های نزدیک به زندان رجایی شهر کرج

در بازه‌ی یک هفته‌ای تنها در محدوده مورد نظر بوده‌اند به پیوست ارسال می‌گردد. بعد از آن اکبری این اطلاعات را به دادستانی ارسال کرده است.

به نظر می‌رسد هدف از این کار، پیدا کردن زندانیانی باشد که از تلفن همراه استفاده می‌کردند. همین فرد در ایمیل دیگری راهنمای استفاده از سیستم سیام را برای مهدی امیری در دادستانی ارسال می‌کند.

سیام سامانه‌ای است که توسط سازمان تنظیم و مقررات رادیویی توسعه پیدا کرده است و بر اساس [گزارش اینترنت‌سیت](#) سامانه‌ای است که امکان پیدا کردن موقعیت جغرافیایی شهروندان را بر اساس شماره موبایل، موقعیت جغرافیایی و یا آی‌پی فراهم می‌کند.

Author: akbari@certcc.ir
To: amiri@internet.ir
Subject: سیام

1 attachment: Manual_User Machin Type_G_Ghazalayah_13970305.docx 129 KB
Manual_User Machin Type_G_Ghazalayah_13970305.docx 129 KB

تصویر ایمیل مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای به دادستانی در مورد پروژه سیام

بر اساس این ایمیل، ما امروز دریافتیم که مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای نیز در این برنامه نقش دارد.

اپلیکیشن‌ها

بخش زیادی از ایمیل‌هایی که ما بررسی کردیم روی اپلیکیشن‌ها موبایل متمرکز است.

تپسی

در ایمیلی که از طرف شرکت تپسی به دادستانی ارسال شده است، تپسی شکایت می‌کند که چرا دادستانی مانع استفاده رقیب این شرکت یعنی اسنپ از مسیریاب ویز نمی‌شود.

در این ایمیل سندی فنی نیز ضمیمه شده است که از نظر فنی اثبات می‌کند اسنپ از ویز استفاده می‌کند.



تصویر ایمیل تپسی به دادستانی در مورد ارسال اطلاعات کاربران به دادستانی

تم تم

در ایمیل دیگری شرکت سازنده اپلیکیشن پیام رسان تم تم که مدتی در ایران محبوب شده بود، اعلام می‌کند که محتوای مورد درخواست دادستانی را از پیام‌رسان خود حذف کرده است.

به نظر می‌رسد این محتواها پورنوگرافی بودند اما همین ایمیل نشان می‌دهد که این شرکت با دادستانی ایران همکاری داشته است.

در نامه دیگری شرکتی به نام هم‌میهن به دادستانی اعلام می‌کند که نماینده رسمی این پیام‌رسان در ایران است «و خود را موظف به انجام پالایش‌های لازم بر روی محتوای فارسی میداند و از این جهت تا کنون از سمت این پیام

Author: TamTam Messenger <prsupport@tamtam.chat>
To: Mahdi Amiri <amiri@internet.ir>, nezarat@internet.ir
Subject: گزارش اقدامات پیام رسان تم تم
12/12/18, 04:12

باسلام و احترام
جناب آقای مهندس امیری
به پیوست گزارش آخرین رسیدگی، حذف و بلائین های صورت گرفته پیام رسان تم تم در محتوای فارسی ارسال میگردد.
قابل ذکر است تاکنون بیش از 400 کانال فارسی دارای تعلف توسط ما بلائین، رسیدگی و پاکسازی شده اند.
باتشکر

TamTam Messenger

1 attachment: Porn Removal.txt 2.2 KB

Porn Removal.txt 2.2 KB

تصویر ایمیل تم تم به دادستانی و گزارش حذف محتوا بر اساس درخواست دادستانی

رسان بیش از ۴۰۰ کانال و محتوای فارسی مورد بررسی و پالایش قرار گرفته است که لیست آن به پیوست تقدیم میگردد.»

در ادامه نامه درخواست شده است تا مسدودیت این پیام رسان در کافه بازار برداشته شود.

روبیکا

روبیکا یکی از این محصولات است که در شرکت «**توسکا**» تولید می‌شود. بر اساس اسناد رسمی، سهامداران اصلی آن شرکت‌های «نقش اول کیفیت»، «ارتباطات سیار» و شرکت سرمایه‌گذاری توسعه نور دنا **هستند**. همه این شرکت‌ها زیرمجموعه یکی از اپراتورهای اصلی کشور یعنی «همراه اول» هستند که بیشتر مالکیت آن دولتی و در اختیار شرکت مخابرات ایران است.

کانال دو سر باخت

در نامه‌ای که به تاریخ ۹۱ اردیبهشت ۱۰۴۱ از طرف مهدی امیری، مدیر فنی معاونت امور فضای مجازی دادستانی کل کشور به مدیر روبیکا ارسال شده است، از او درخواست کردند تا کانال مشخصی با نشانی dosarbakht@ و با شماره تلفن مشخصی را ایجاد کنند تا آنچه که به گفته وی «محتوای آگاهی بخش در خصوص مضرات قمار و شرط بندی» است را در اپلیکشن‌های روبیکا و روبینو منتشر کنند.

بررسی‌های ایمیل‌های آقای امیری نشان می‌دهد دادستانی برای رفع

Author: Mahdi Amiri <amiri@internet.ir>
To: CEO@rubika.ir
Subject: کانال و صفحه دوسرباخت در روبیکا برای اطلاع رسانی مضرات قمار dosarbakht
9/5/22, 01:23

مدیرعامل محترم پیام رسان اجتماع روبیکا
با سلام

نظر به اینکه فعالیت قمارخانه های آنلاین به عنوان یک از فعالیتهای مجرمانه سازمان یافته فضای مجازی نقش ویرانگر و تبعات جبران ناپذیر اجتماعی، فرهنگی و اقتصادی برای شهروندان و کشور در پی داشته است، این دادستانی در نظر دارد محتوای آگاهی بخش در خصوص مضرات قمار و شرط بندی را در کانال و صفحه پیام رسان های اجتماع داخلی (به وبزه روبیکا) منتشر نماید و با دعوت از کاربران و موسسات مردم نهاد به مشارکت و نقش آفرینی در این امر، رویدادی مردمی در زمینه اطلاع رسانی عمومی از این بدیده شوم و خائمان سوز را با هشتگ و نام و نشان «دوسرباخت» فراهم نماید لذا پیشنهاد می شود در راستای مسئولیت اجتماعی و اهتمام آن مجموعه در پیگیری سالم سازی فضای مجازی و فرهنگ سازی و مقابله با جرائم فضای مجازی، شناسه ذیل در روبیکا و روبینو را به شماره +989026608478 احتیاط داده و نهیهای لازم جهت باز نشر و در معرض دید قرار گرفتن محتوای مذکور به عمل آید @dosarbakht

با تشکر
معاون مدیرکل نظارت بر فضای مجازی دادستانی کل کشور

Best Regards
Amiri, Mahdi

تصویر ایمیل دادستانی به روبیکا و سفارش ساخت کانال برای جمع‌آوری ویدیوهای اعتراف به شرکت در قمار

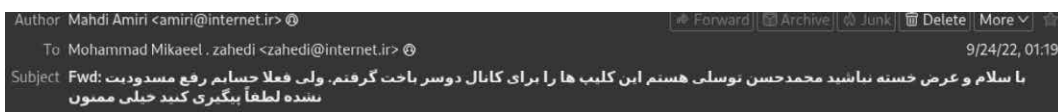
مسدودیت از حساب‌های بانکی افرادی که متهم به قماربازی هستند، آنها را مجبور می‌کند ویدیو از خود بگیرند و در آن، ضمن اعتراف به مشارکت در قمار، از این کار ابراز پشیمانی کنند. به عنوان نمونه، یکی از کسانی که قمار کرده در تاریخ ۹/۲۴/۲۲ چند فایل ویدیو از اعتراف و پشیمانی خود ارسال کرده است. او در متن ایمیل خود نوشته است: «با سلام و عرض خسته نباشید هستم این کلیپ‌ها را برای کانال دوسر باخت گرفتم. ولی فعلا حسابم رفع مسدودیت نشده لطفاً پیگیری کنید خیلی ممنون»



تصور ایمیل نمونه ویدیوهای اعتراف به قمار که به دادستانی ارسال شده

نمونه‌های از این نوع ایمیل‌ها در اینباکس آقای امیری بسیار است و در مواردی حتی او از محتوای این ویدیوها راضی نیست و درخواست می‌کند ویدیوها با توجه به مواردی که مطرح می‌کند اصلاح شوند. به عنوان نمونه در تاریخ ۹/۲۴/۲۲ آقای امیری اعلام می‌کند: «لطفاً با محمدحسن توسلی تماس بگیرید بگید هم از نظر محتوا اشکال داره و هم صدا ضعیف است و قابل شنیدن نیست. به مضرات قمار آنلاین اشاره کنند نه به اقدامات انجام شده.»

این نوع از اعتراف‌های اجباری از طرف شرکت در قمار و نه اداره یک وبسایت کلاهبرداری یا قمار، به نشانی ghomar@internet.ir ارسال شدند و مهدی امیری مسوول بررسی محتوای این اعتراف‌ها و تایید آنها است.



با سلام
لطفاً با محمدحسن توسلی تماس بگیرید بگید هم از نظر محتوا اشکال داره و هم صدا ضعیف است و قابل شنیدن نیست
به مضرات قمار آنلاین اشاره کنند نه به اقدامات انجام شده

Best Regards
Amiri, Mahdi

تصور ایمیل نمونه ویدیوهای اعتراف به قمار که به دادستانی ارسال شده که مورد تایید دادستانی نیست و درخواست ویدیو جدید کردند

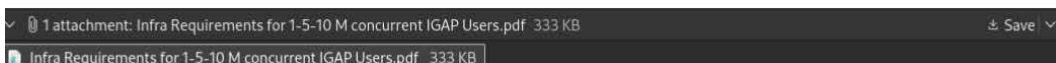


تصور ایمیل نمونه ویدیوهای اعتراف به قمار که به دادستانی ارسال شده

مهدی امیری در نامه‌ای به تاریخ ۶ شهریور ۱۴۰۱ برای محسن نیک‌بین، دانشجوی دکترای حقوق بین‌الملل عمومی در پردیس فارابی دانشگاه تهران، فهرست تشکلهای مردم‌نهاد و شرکتهای غیردولتی مورد تایید دادستانی را ارسال کرده است. هدف نهایی این است که نیک‌بین این لیست را برای «گروه کاری باز سازمان ملل متحد در خصوص امنیت سایبری» ارسال کند.

گپ و آی گپ

پیام‌رسان آی گپ در ایمیلی که به دادستانی ارسال کرده است نیازمندی‌های فنی خود را بیان داشته است و به نظر می‌رسد این گروه انتظار دریافت کمک داشتند.



تصویر ایمیل شرکت گپ به دادستانی و درخواست دریافت کمک فنی برای توسعه

در ایمیل دیگری، اطلاعات گروهی به نام «دختران دوئل» را در اختیار دادستانی قرار داده است.

بر اساس اطلاعاتی که مهدی انجیدنی مدیر این پیام‌رسان در حساب لینکدین خود گذاشته است، او موسس شرکت دیگری در انگلستان به اسم TS Information Technology است.



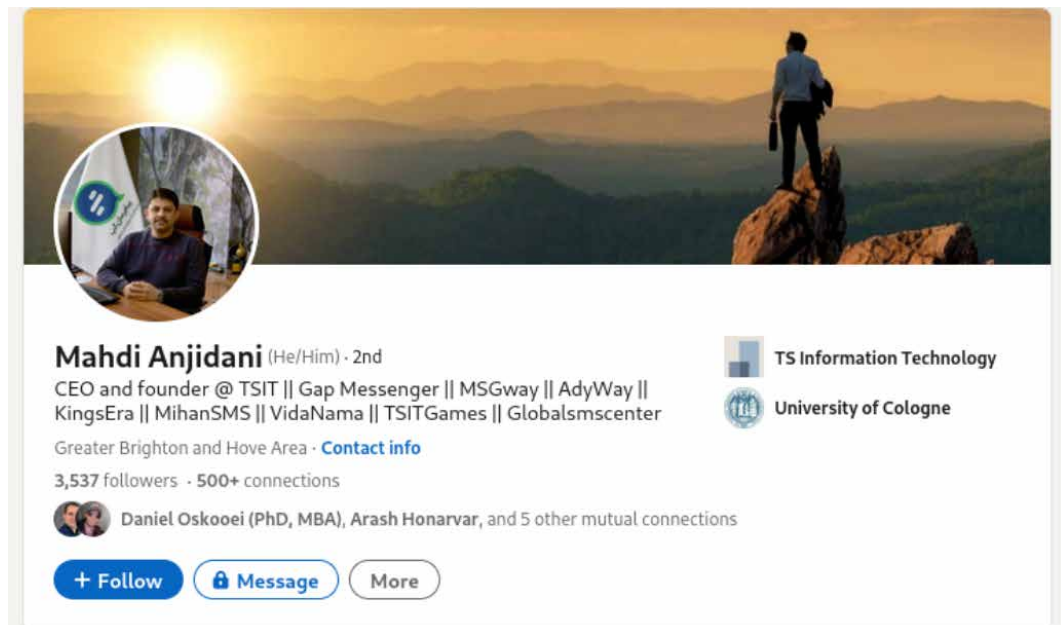
تصویر ایمیل شرکت گپ به دادستانی و ارسال اطلاعات کاربران این پیام‌رسان به دادستانی

اطلاعات موجود در وبسایت ثبت شرکت‌های دولت بریتانیا تایید می‌کند که او مدیر این شرکت است.

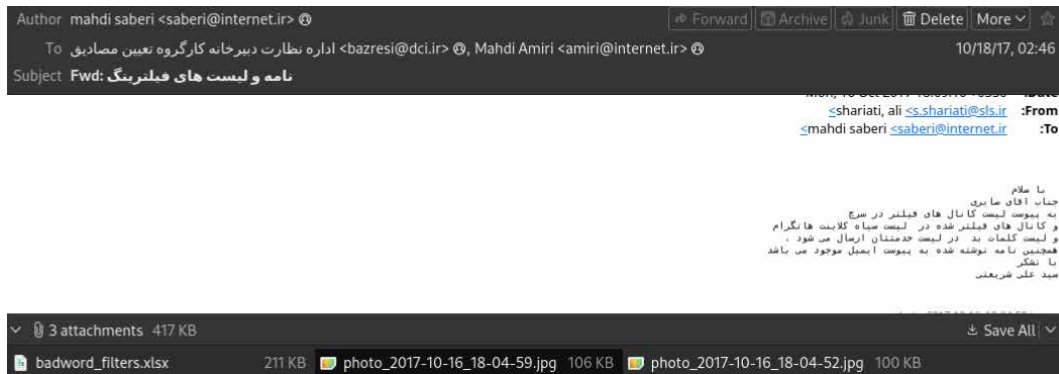
تلگرام طلایی

تلگرام طلایی اپلیکیشن جعلی بود که به گفته مقامات ایران تحت نظارت مقام‌های امنیتی از روی تلگرام ساخته شد. این اپلیکیشن بعداً به دلیل شنود و نقض حریم خصوصی از گوگل پلی حذف شده و تلگرام پیام هشدار را برای کاربران این اپلیکیشن منتشر کرد.

در نامه‌هایی (لینک [اول](#)، [دوم](#)) که این شرکت به دادستانی ارسال کرده، اعلام



تصویر صفحه لینکدین مدیر شرکت گپ



تصویر ایمیل دادستانی به تلگرام تلای و درخواست سانسور محتوا در این اپلیکیشن

کرده است آنها توان این را دارند که بستر فیلتر کلمات و کانال، و لیست سیاه بر روی کلاینت‌ها، تشخیص متن مستهجن، تشخیص تصاویر غیر اخلاقی را در تلگرام تلای ایجاد کنند.

پیش از این کمپین بین‌المللی حقوق بشر طی گزارش‌هایی، توان سانسور بر اساس کلمات کلیدی و کانال را به صورت فنی در تاریخ ۱۲ آبان ۱۳۹۷ [منتشر](#) کرده بود.