وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

خبرنامه سازمان فناوری اطلاعات

بازتاب خبری فناوری اطلاعات در رسانه ها

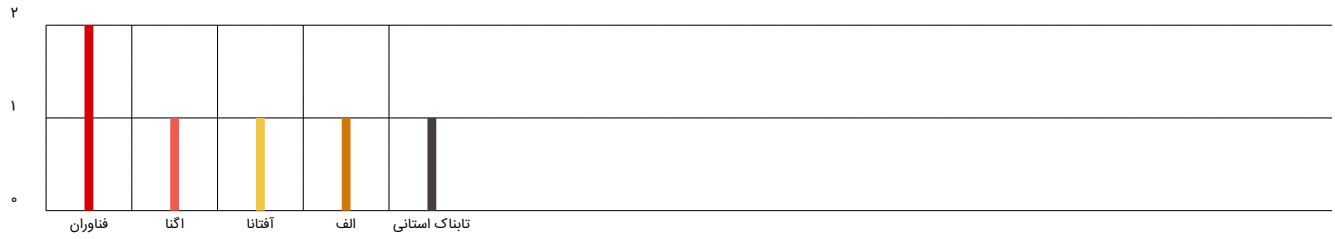
شماره: ۱۱۳۷

تاریخ:۹۷/۳/۶

اخبار فناوری اطلاعات روز ۹۷/۳/۶

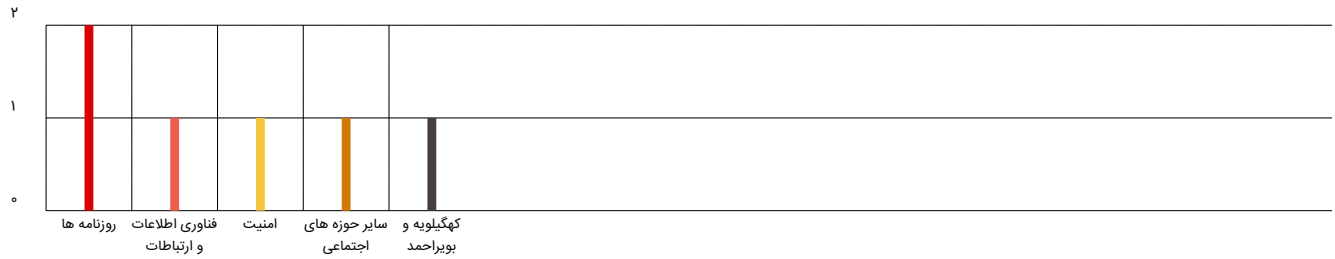
نوع منبع خبری

منابع خبری با بیشترین پوشش خبر



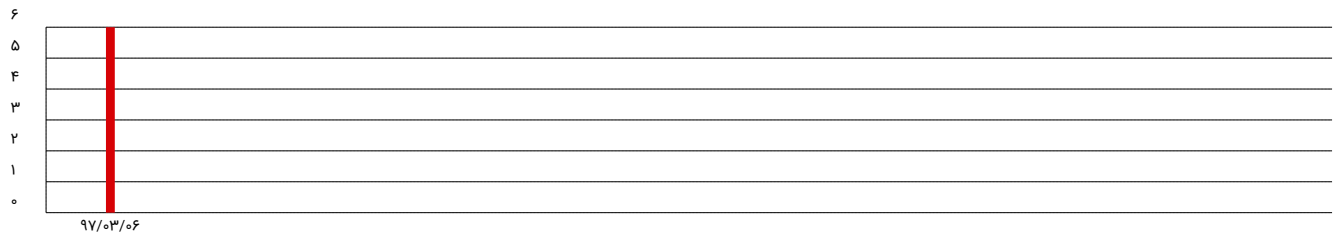
تعداد کل منابع : ۵

گروههای موضوعی با بیشترین پوشش خبری



تعداد کل گروه های موضوعی : ۵

براساس تاریخ



تعداد کل روزها: ۱

۱ هشدار در خصوص رواج احتمالی بدافزار VPNFilter

۲ امنیت گوشی‌های ZTE زیر سوال رفت

۳ ورج گرفتار DDos شد

۴ انتشار فراخوان عضوت در سه کمیسیون نظام صنفی رایانه‌ای تهران

۵ استقبال بی سابقه و گسترده فعالان صنعت فاوا از الکامپ ۲۴

۶ توضیحات جدید مرکز ماهر درباره حمله به سرورهای ایمیل سازمانی

هشدار در خصوص رواج احتمالی بدافزار VPNFilter

تابناک استانی
کهگیلویه و بویراحمد
۰۶ خرداد ۱۳۹۷ ۰۵:۴۸

خبرهای دریافتی و رصد و پایش انجام‌گرفته، حاکی از انتشار احتمالی بدافزار VPNFilter در ساعات و روزهای آینده در کشور است.

به گزارش تابناک کهگیلویه و بویراحمد و به نقل از پایگاه اطلاع رسانی شبکه خبر، مرکز ماهر با اعلام این هشدار تاکید کرد: گزارش‌های موجود حاکی از آن است که این بدافزار تاکنون بیش از ۵۰۰ هزار قربانی در جهان داشته است و این عدد نیز افزایش خواهد داشت.

براساس این گزارش قربانیان این بدافزار به یک نقطه جغرافیایی خاص تعلق ندارند و این بدافزار در تمامی مناطق فعال است.

بر پایه گزارش تابناک و بر اساس اطلاعات مرکز ماهر، روترهای Linksys, MikroTik, NETGEAR and TP-Link؛ عمده محصولات آلوده‌شده در ۵۴ کشور جهان هستند که در کنار برخی ابزارهای ذخیره‌سازی شبکه/NAS به این بدافزار آلوده‌شده‌اند.

لینک خبر در رسانه : http://resaneh.net/newsdetail/۱۹۶۸۳۵۲۹

الف

امنیت گوشی‌های ZTE زیر سوال رفت

الف

سایر حوزه های اجتماعی

۰۶ خرداد ۱۳۹۷ ۰۸:۲۴

به گزارش ایسنا به نقل از وب سایت Phone Arena، شرکت Avast Threat Labs که در زمینه امنیت سایبری و ارائه نرم‌افزارهای آنتی ویروس فعالیت می‌کند به تازگی اعلام کرده که بسیاری از گوشی‌های چینی ساخت شرکت زد تی ای (ZTE) میزبان یک بدافزار خطرناک تحت عنوان کوزیلون بوده‌اند که به‌صورت پیش فرض بر روی گوشی نصب شده بوده است.

شرکت چینی زد تی ای در ماه‌های اخیر تحت تاثیر دستور ترامپ مبنی بر ممنوعیت استفاده کارمندان و مقامات کاخ سفید و همچنین محدودیت برای کاربران آمریکایی در استفاده از این گوشی‌ها، دچار خسارات و دشواری‌های متعددی شده بود، حالا این خبر می‌تواند نمکی برروی زخم این تولیدکننده چینی باشد و آن را گرفتار بی اعتمادی و کاهش محبوبیت و درآمد از سوی کاربران کند.

از آنجا که در سال‌های اخیر اطلاعات محرمانه بسیاری از کارمندان و مدیران فعال در کاخ سفید و سایر دستگاه‌های دولتی ایالات متحده آمریکا افشا شده و دولت این کشور را با مشکلات بسیاری مواجه کرده، قانون‌گذاران این کشور چند ماه پیش لایحه‌ای را به منظور افزایش امنیت سایبری و جلوگیری از افشای اطلاعات محرمانه گوشی‌های کارمندان دولت ارائه داد که در آن خریداری وسائل الکترونیکی بخصوص گوشی‌های ساخت شرکت‌های چینی هوآوی و زد تی ای توسط تمامی کارمندان، کارکنان و مدیران در سازمان‌ها و دستگاه‌های دولتی، ممنوع اعلام می‌شود.

طبق این لایحه، تمامی دستگاه‌های دولتی از خرید و استفاده گوشی‌های همراه چینی که به گفته آنها از امنیت سایبری کمتری در قبال افشای اطلاعات محرمانه برخوردار است، منع خواهند شد.

قانون گذاران ایالات متحده آمریکا بر این باورند که گوشی‌های چینی این امکان را به هکرها و مجرمان سایبری می‌دهد تا به اطلاعات محرمانه و حریم خصوصی کاربران دسترسی پیدا کنند.

حالا شرکت اواست (Avast) نیز در گزارش خود عنوان کرده است این بدافزار تازه کشف شده، در بیش از ۱۸ هزار گوشی هوشمند ساخت ZTE که در بیش از ۱۰۰ کشور جهان از جمله روسیه، ایتالیا، آلمان، انگلستان و ایالات متحده آمریکا به فروش رسیده و توسط کاربران مورد استفاده قرار گرفته، به صورت پیش فرض نصب شده بوده است و این بدان معناست که میلیون‌ها کاربر در سراسر جهان تحت تاثیر این مساله و رخداد قرار گرفته‌اند. این امر می‌تواند به تنهایی حریم خصوصی بسیاری از کاربران را نقض کرده و اعتماد به شرکت سازنده را به کلی زیر سوال ببرد.

هنوز شرکت زد تی ای ZTE در واکنش به این ادعا پاسخی نداده است.

لینک خبر در رسانه : http://resaneh.net/newsdetail/۱۹۶۸۷۶۸۴

ارز دیجیتالی verge (ورج) با وجود تقویت الگوریتم‌های امنیتی ارز دیجیتالی بازهم مورد حمله سایبری، این‌بار از نوع DDos، قرار گرفت.

ارز دیجیتالی verge (ورج) با وجود تقویت الگوریتم‌های امنیتی ارز دیجیتالی بازهم مورد حمله سایبری، این‌بار از نوع DDos، قرار گرفت.

به گزارش افتانا (پایگاه خبری امنیت فناوری اطلاعات)، ارز دیجیتالی ورج (Verge) که به منظور بهبود عملکرد بلاک‌چین بیت‌کوین طراحی شده‌بود، مورد حمله سایبری اختلال سرویس توزیع شده (DDOS) قرار گرفت.

شرکت توسعه‌دهنده ارز ورج، این موضوع را با انتشار بیانیه‌ای در توییتر تایید کرد: «به نظر می‌رسد برخی از استخرهای ماینینگ تحت حمله اختلال سرویس توزیع شده قرار دارند و تعدادی از بلاک‌ها با تاخیر مواجه شده‌اند. همچنین برای حل این مشکل تلاش می‌کنیم.»

اوکماینر (Ocminer) در انجمن «BitcoinTalk» به هکری اشاره کرد که کدهای بلاک‌چین ورج را دست‌کاری کرده‌بود. مهاجم از باگ موجود در کد ورج بهره برده، زمان‌بندی‌های نامعتبر را روی بلوک‌ها تنظیم می‌کند، سپس به سرعت بلاک جدیدی را استخراج می‌کند.

این نخستین‌بار نیست که ارز ورج مورد حمله قرار گرفته‌است؛ بلکه در آوریل ۲۰۱۸ با حمله دیگری نیز مواجه شده‌بود. در آن زمان ۲۰ میلیون واحد از این ارز (بیش از ۱.۱ میلیون دلار در طول آن دوره) به سرقت رفت.

کارشناس ارشد امنیت در «نت اسکوت آربور» (NETSCOUT Arbor) که یک شرکت امنیت سایبری متخصص در حملات اختلال سرویس توزیع شده است، گفت: «مجرمان سایبری سریعا به راه‌های جدیدی برای پیشرفت می‌رسند، بنابراین جای تعجب نیست که هکرها در حال توسعه بازارهای بدافزار ارز دیجیتالی برای استفاده از فرصت‌ها هستند.»

همچنین اعلام شد به منظور فریب شبکه، مهاجم با استفاده از زمان‌بندی‌های نامعتبر کنترل دو عدد از پنج الگوریتم پروتکل ورج را به دست گرفت. در کمتر از چند ساعت مهاجم توانسته ۳۵ میلیون ارز را به ارزش ۱.۷۵ میلیون به نرخ ارز فعلی به دست آورد.

منتقدانی چون اوک ماینر ادعا می‌کنند: «ارتقای اخیر یک اقدام موقت بود و آسیب‌پذیری اساسی در سیستم ورج را نمی‌توان نادیده گرفت. علاوه‌بر این ارز موجود در بازار حدود ۷۵۲ میلیون است و از زمان حمله قیمت آن سریع کاهش یافته و احتمالا بدتر هم خواهدشد.»

لینک خبر در رسانه : http://resaneh.net/newsdetail/۱۹۶۹۱۲۴۸

کمیسیون های فروشگاه ها، فین تک و تولید و عرضه محتوای سازمان نظام صنفی رایانه ای استان تهران برای دور جدید فعالیت خود عضو می پذیرد.

فناوران- سازمان نظام صنفی رایانه ای استان تهران از تمام کسب وکارهای حوزه فروشگاهی دعوت کرده است که حداکثر تا پایان وقت اداری روز چهارشنبه ۱۸ خردادماه ماه برای عضویت در این کمیسیون ثبت نام کنند. همچنین مهلت ثبت نام برای عضویت در دو کمیسیون فین تک و تولید و عرضه محتوا نیز تا روز چهارشنبه ۲۳ خرداد اعلام شده است.

حوزه فعالیت کمیسیون فروشگاه ها، بررسی مشکلات و مسایل صنفی، ساماندهی بازاراین حوزه و همچنین کمک به بهبود فضای کسب و کار و تعامل دوسویه میان فعالان فروشگاهی در حوزه فناوری اطلاعات و ارتباطات اعلام شده است. کمیسیون فین تک نیز با هدف بررسی مشکلات و مسایل صنفی، ساماندهی بازار این حوزه و همچنین کمک به بهبود فضای کسب و کار و تعامل دوسویه میان فعالان کسب و کارهای حوزه بانکداری وپرداخت الکترونیکی تشکیل می شود.

بر اساس این گزارش، فعالیت کمیسیون تولید و عرضه محتوا، بررسی مشکلات و مسایل صنفی این بخش از کسب و کار، ساماندهی بازار، کمک به بهبود فضای کسب و کار و نیز تعامل دوسویه میان فعالان کسب و کار در حوزه های خدمات ارزش افزوده، VoD،IPTV و Aggregator ها اعلام شده است.

گفتنی است که براساس آئین نامه جدید فعالیت کمیسیون ها در سازمان نظام صنفی رایانه ای استان تهران، انتخاب و معرفی نهایی اعضای هر کمیسیون سازمان پس از برگزاری انتخابات داخلی آن، منوط به تصویب و تایید نهایی فهرست اعضا و رئیس منتخب کمیسیون توسط هیات مدیره است.

همچنین بر اساس این آیین نامه رئیس کمیسیون اختیار دارد راساً در خصوص موارد مرتبط با حوزه فعالیت خود در رسانه ها مصاحبه و موضعگیری کرده و اعضای صنف را در جریان اخبار مربوط قرار دهد.

ثبت نام الکامپ بیست و چهارم دیروز به پایان رسید و براساس اعلام ستاد اجرایی الکامپ، استقبال فعالان بخش های مختلف حوزه فاوا برای حضور در الکامپ بسیار چشمگیر بوده است.

فناوران - بر این اساس، استقبال گسترده ای از سوی شرکت های پرداخت الکترونیک به ثبت رسیده است و شاهد حضور شرکت های فن آوا، به پرداخت ملت، پرداخت الکترونیک سداد، پرداخت الکترونیک سامان کیش، تجارت الکترونیک پارسیان، کارت اعتباری ایران کیش، فناوران هوشمند بهسازان فردا و غیره هستیم. علاوه بر اینها بانک ملت نیز در این دوره نمایشگاه ثبت نام کرده و حضور خواهد داشت.

در میان ثبت نام کنندگان این دوره الکامپ می توان اسامی سه اپراتور تلفن همراه رایتل، همراه اول و ایرانسل را مشاهده کرد. همچنین شرکت های انتقال داده های نداگستر صبا، آسیاتک، گسترش ارتباطات مبنا، فن آوا، داتک و غیره نیز از رسته اینترنتی ها در الکامپ ثبت نام کردند.

از میان شرکت های امنیتی اسامی شرکت های امن افزار گستر شریف، اندیشه نگار پارس، داده پردازان دوران و شرکت فنی و مهندسی امن پردازان کویر دیده می شود.

پارک علم و فناوری پردیس، شهرک علمی و تحقیقاتی اصفهان، پارک علم و فناوری یزد، پارک علم و فناوری دانشگاه تهران و مرکز تخصصی آپا– واحد علوم و تحقیقات دانشگاه آزاد اسلامی نیز در میان ثبت نام کنندگان قرار دارند.

همینطور شرکت مخابرات ایران نیز در این دوره از نمایشگاه الکامپ حضور خواهد داشت.

علاوه بر اینها شرکت های فعال در حوزه نرم افزارهای مالی و اداری، پشتیبانی، ارایه کنندگان خدمات مشاوره، تجارت الکترونیک، شبکه، تولیدکنندگان محتوا و خدمات ارزش افزوده، شرکت های امنیتی، آموزشی، تولیدکننده باتری و UPS و غیره مشارکت قابل توجهی در این دوره نمایشگاه به ثبت رساندند.

این در شرایطی است که ثبت نام دو سالن الکام استارز و الکام گیمز از دیروز شنبه پنجم خرداد ماه آغاز شده است و همچنین دستگاه ها، نهادها و سازمان های دولتی ارایه دهنده خدمات دولت الکترونیک نیز در سالنی مستقل با همین عنوان در نمایشگاه مستقر خواهند شد.

بیست و چهارمین نمایشگاه الکامپ به همت سازمان نظام صنفی رایانه ای کشور در تاریخ ششم تا نهم مرداد ماه در محل نمایشگاه های دایمی تهران برگزار خواهد شد.

توضیحات جدید مرکز ماهر درباره حمله به سرورهای ایمیل سازمانی

اگنا

فناوری اطلاعات و ارتباطات

۰۶ خرداد ۱۳۹۷ ۱۲:۲۷

> اگنا- مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای بار دیگر با اعلام اطلاعیه ای، در مورد افزایش شدت حملات سایبری به سرورهای ایمیل در کشور، توضیح داد.

اگنا- مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای بار دیگر با اعلام اطلاعیه ای، در مورد افزایش شدت حملات سایبری به سرورهای ایمیل در کشور، توضیح داد.

مرکز ماهر اول خردادماه با اعلام گزارشی نسبت به افزایش شدید حمله به سرویس دهنده‌های ایمیل سازمانی هشدار داد و توصیه کرد که مدیران سیستم نسبت به بررسی وضعیت امنیتی سرورهای ایمیل خود و اجبار کاربران در انتخاب رمزهای عبور مناسب و پیچیده اقدام کنند. همچنین لازم است سیاست مسدودسازی حساب کاربری در صورت چندین بار تلاش با رمز عبور ناموفق (account lockout) فعال باشد.

در این زمینه این مرکز بار دیگر توضیحات جدیدی به هشدار قبلی اضافه و اعلام کرد: ایمیل سرورهای مورد استفاده در سطح سازمان‌ها و شرکت‌ها در کشور از نظر نرم‌افزار و نحوه پیاده سازی بسیار متنوع هستند و نمی‌توان به سادگی ادعا کرد که اکثر سرویس دهنده‌ها متصل به active directory یا directory service های دیگر هستند.

در اطلاعیه منتشر شده اشاره‌ای به جزئیات و چگونگی پیاده سازی قابلیت Lockout نشده است. در توصیه ارائه شده نیز منظور مسدود سازی دسترسی از طریق حساب ایمیل است. بدیهی است مدیران سیستم لازم است تنظیمات و توصیه‌های دریافتی را با مطابقت با نیازمندی‌ها و شرایط زیرساخت خود بکار ببندند.

متاسفانه همه سرویس دهنده‌های ایمیل مورد استفاده، قابلیت شناسایی و مسدودسازی آدرس های با تلاش ناموفق را ندارند. علاوه بر این با توجه به دسترسی مهاجمان به شبکه های بزرگ بات و IPهای متعدد با سویاستفاده از این ظرفیت، مهاجم می تواند حمله brute force خود را با آدرس های متعدد ادامه دهد.

در هر صورت بدون شک تمام کاربران ترجیح خواهند داد حساب کاربری آنها در صورت وقوع حمله موقتا مسدود شود تا اینکه مورد نفوذ و سویاستفاده مهاجم قرار گیرد.

لازم است مدیران سیستم ضمن نظارت بر رویدادنماهای ثبت شده در سرور ایمیل، در صورت مواجه با اختلالات مشابه موضوع را به اطلاع مرکز ماهر برسانند.

گفته شده است که حملات سایبری کشف شده از نفوذ به ایمیل سرورها در قالب brute force روی رمز عبور از طریق پروتکل‌های imap و pop۳ و نیز حمله DOS از طریق ارسال دستورات پی‌درپی imap و pop۳ صورت می‌گیرد.

لینک خبر در رسانه : http://resaneh.net/newsdetail/۱۹۶۹۴۰۲۹