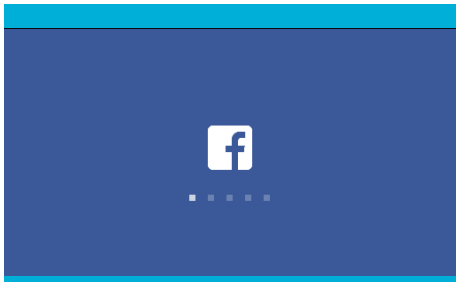
شماره بیست و هشتم - اردیبهشت ۱۳۹۸

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:

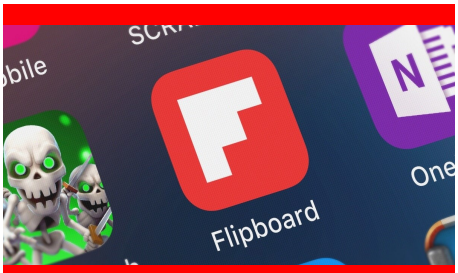


حذف ۲.۱۹ میلیارد از حساب‌های جعلی فیس بوک

فیس بوک با استفاده از یک رویکرد سه جانبه برای مبارزه با حساب‌های جعلی از سیستم های تشخیص شبکه‌های اجتماعی به محض ورود به سیستم، تقلب‌های بالقوه را بررسی می‌کند و می‌تواند آن‌هایی را که سه مرحله اول را پشت سر می‌گذارند حذف کند. - صفحه ۲

برخی از گذرواژه های G Suite از سال ۲۰۰۵ به صورت متن ساده ذخیره شده!

پس از اینکه فیس بوک و توییتر نیز به این موضوع اعتراف کردند، گوگل گفت این یک اشکال است که موجب ذخیره برخی از کلمات عبور به صورت متن ساده می‌شود. این مسئله که فقط بر روی بخشی از کاربران سازمانی G Suite تأثیر گذاشته، است. - صفحه ۳

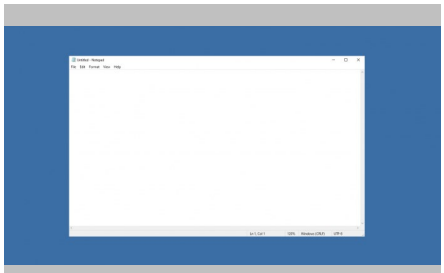


فعالیت هکرها برروی سرورهای Flipboard به مدت ۱۰ ماه

Flipboard یکی دیگر از غول‌های فناوری است که اخیرا اطلاعات مهم کاربران خود را نشر داده است. داده‌هایی که در معرض خطر قرار دارند عبارتند از نام کاربر، کلمه عبور، آدرس های ایمیل و توکن دیجیتالی که برای پیوند حساب‌های شخص ثالث به Flipboard استفاده می‌شوند. - صفحه ۴

محدود کردن دسترسی به اطلاعات شخصی توسط Google

رسوایی جمع آوری اطلاعات که در سال گذشته در فیس بوک رخ داد، تاثیری وسیع در صنعت فناوری به همراه داشت. اما مردم در مورد حفاظت از اطلاعات شخصی خود آگاهی بیشتری دارند و این امر باعث می‌شود که شرکت‌ها سطح دسترسی توسعه دهندگان به اطلاعات مشتری را محفوظ نگه دارند- صفحه ۵



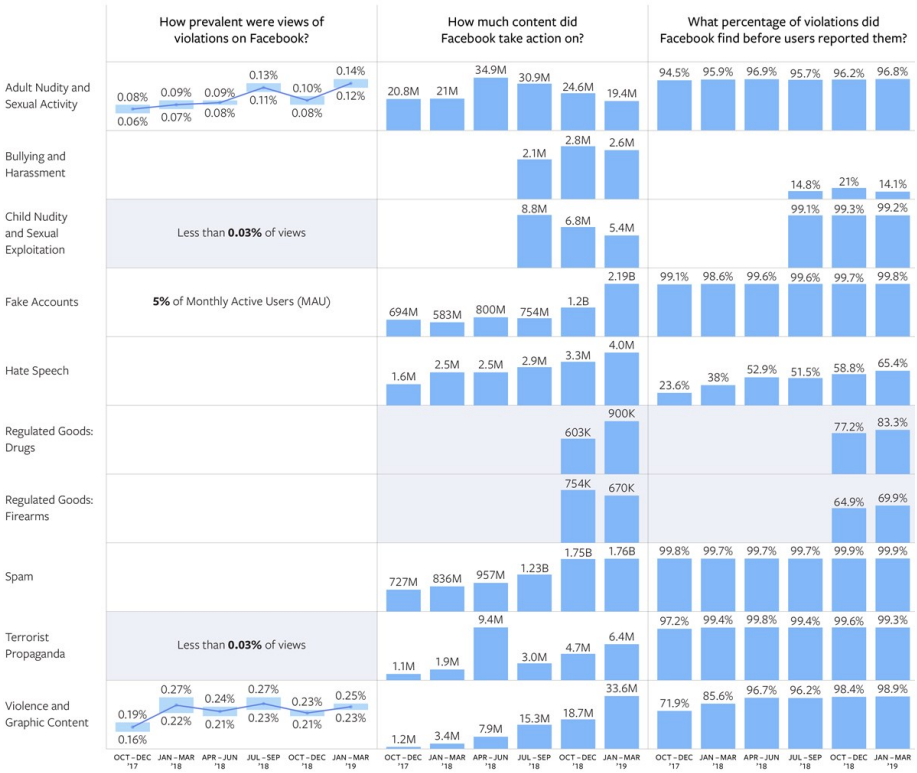
وجود آسیب پذیری Notepad

یک مشکل حافظه‌ای در برنامه‌ی محبوب مایکروسافت به نام Notepad می‌تواند منجر به باز شدن بخش Shell از راه دور شود. این باگ توسط Tavis Ormandy یکی از اعضای تیم پروژه‌ی Zero کشف شده است.- صفحه ۶

ورود باج افزار Shade به امریکا!

باج افزار Shade که تا کنون کسور روسیه را هدف قرار داده بود، اکنون در امریکا و ژاپن دیده شده است. این باج افزار برای اولین بار در سال ۲۰۱۴ توسط آزمایشگاه امنیتی Kaspersky کشف گردید اما اخیرا این باج افزار فعالیت خود را به بیرون از مرزهای روسیه گسترش داده است. - صفحه ۷

حذف ۲.۱۹ میلیارد از حساب‌های جعلی فیس بوک



فیس بوک با استفاده از یک رویکرد سه جانبه برای مبارزه با حساب‌های جعلی از سیستم های تشخیص شبکه‌های اجتماعی به محض ورود به سیستم، تقلب‌های بالقوه را بررسی می‌کند و می‌تواند آن‌هایی را که سه مرحله اول را پشت سر می‌گذارند حذف کند.

فیس بوک در سه ماهه اول سال ۲۰۱۹ فیس بوک ۲.۱۹ میلیارد از حساب‌های تقلبی را غیرفعال کرد، که در گذشته فقط ۱.۲ میلیارد حساب فاقد اعتبار بود. نتیجه حملات خودکار از کاربران جعلی بسیار بد است که سعی در ایجاد حجم زیادی حساب‌ها در یک بار دارند.

الکس شولتز، ازتیم آنالیز در فیس بوک، هشدار داده است که "تعداد حملات حساب های جعلی که توسط اقدامات ساده انجام می شود بسیار بالا است. اگر یک کاربر جعلی، تلاش کند یک حمله را ایجاد کند و صد میلیون حساب جعلی ایجاد کند، ما آن‌ها را به محض ایجاد حذف می کنیم. صد میلیون حساب تقلبی ایجاد شده اما هیچ کس در پشت این حساب‌ها قرار نگرفته است و از این رو، ما هیچ گونه آسیبی به کاربران واقعی-مان وارد نمی‌کنیم"

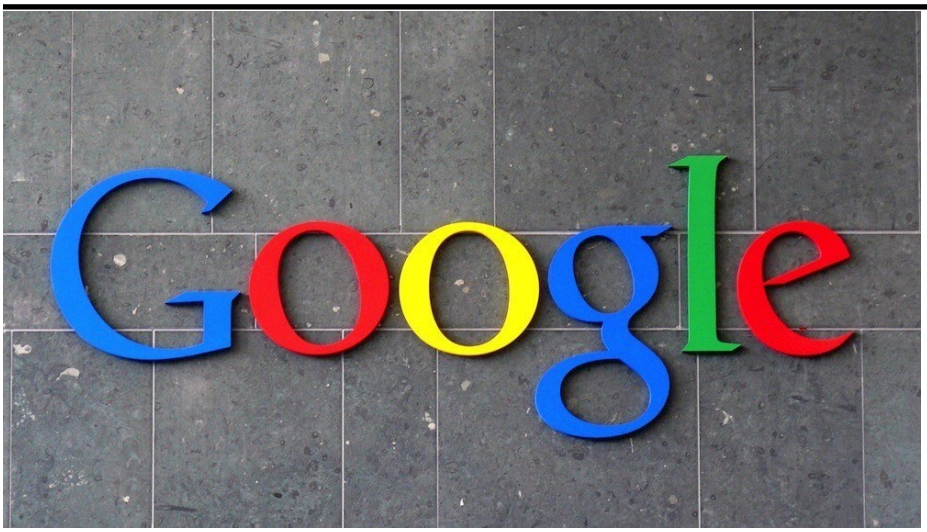
فیس بوک نیز آمار و ارقام شایع در خصوص مواردی چون محتوای برهنگی، فعالیت جنسی و همچنین خشونت را به اشتراک گذاشت. برآورد شده است که از ۱۰،۰۰۰ باری که افراد محتوا را مشاهده کردند، ۱۱ تا ۱۴ بار آن، حاوی مطالبی از برهنگی و فعالیت جنسی بوده است.

فیس بوک علاوه بر این، برای اولین بار شاخص‌های شیوع تروریسم جهانی و برهنگی کودکان و استثمار جنسی را به اشتراک گذاشت.

تعداد هر کدام از این دسته‌ها برای اندازه گیری با استفاده از تکنیک‌های استاندارد برای فیس بوک بسیار زمان بر بوده است.

گردآورنده: امیرحسین ضرغامی

برخی از گذرواژه های G Suite از سال ۲۰۰۵ به صورت متن ساده ذخیره شده!



پس از اینکه فیس بوک و توییتر نیز به این موضوع اعتراف کردند، گوگل گفت این یک اشکال است که موجب ذخیره برخی از کلمات عبور به صورت متن ساده می‌شود. این مسئله که فقط بر روی بخشی از کاربران سازمانی G Suite تأثیر گذاشته، https://gsuite.google.com/ از سال ۲۰۰۵ تا کنون وجود داشته است. خوشبختانه برای Google و کاربران آن شواهدی وجود ندارد که هیچ کدام از کلمات عبور به طور نامناسبی لو رفته باشد.

این مشکل از یک ویژگی حذف شده در حساب‌های شرکت G Suite بوجود آمده است. گوگل مدیران دامنه را مجاز دانسته بود بنابراین تازه واردان می توانستند به سرعت در روز اول وارد حساب خود شوند. اما یک خطا در هنگام اجرای این ویژگی در سال ۲۰۰۵ به وجود آمد که به این معنی بود که کنسول مدیریت یک کپی از این کلمات عبور را در متن ساده ذخیره می کرده.

علاوه بر این، گوگل به طور تصادفی با این خطا مواجه شد ولی می‌گوید از رمزهای عبور مشتریان G Suite سوء استفاده نشده و آن ها را تا حداکثر ۱۴ روز بعد ژانویه ۲۰۱۹ به صورت رمز شده ذخیره می‌کند و هیچ مدرکی از دسترسی نامناسب به مشتریان وجود ندارد.

در حالی که کلمه عبور متن ساده در سرورهای امن Google به صورت داخلی ذخیره شده است، این شرکت با مدیران G Suite تماس گرفته و به آن‌ها گفته است که برسی کنند و هرگونه حساب کاربری که ایجاد می شود مجدد تنظیم شود.

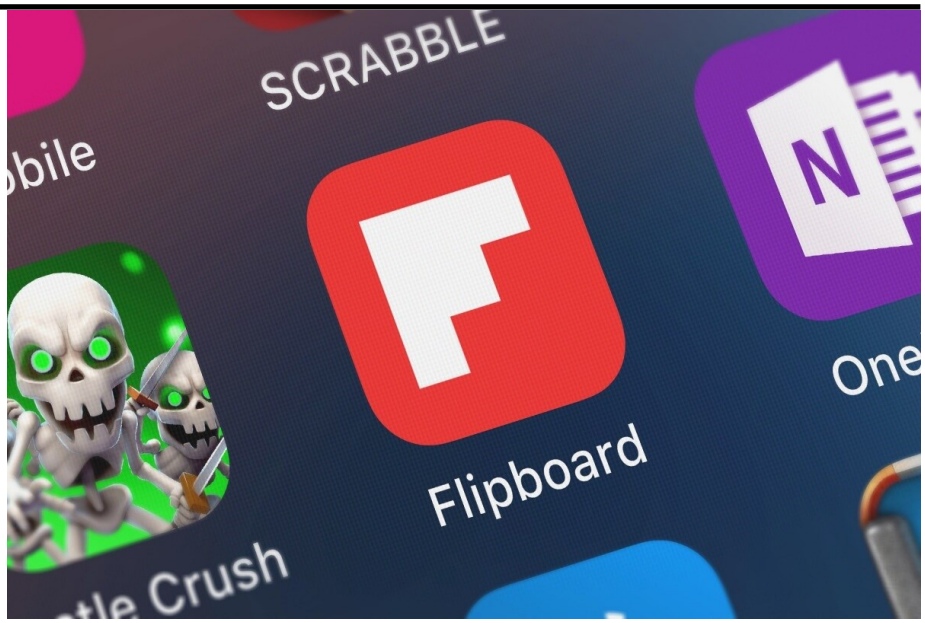
در ماه مارس، فیس بوک اعلام کرد که "صدها میلیون کاربر فیس بوک Lite، ده ها میلیون کاربر دیگر فیس بوک و دهها هزار کاربر Instagram رمزهای عبور خود را در یک فرمت قابل خواندن بدون رمزگذاری ذخیره کرده‌اند."

توییتر نیز مسائل مشابهی را تجربه کرده است. این سایت رمز ۳۳۰ میلیون کاربر را در سال گذشته پس از یک اشکال در سرور پسوردها به صورت متن ساده ذخیره می-کرد.

در حالی که این مسئله تنها بر یک زیرمجموعه از کاربران G Suite تأثیر گذاشته و هیچ کلمه عبوری به سرقت نرفته است، این امر همچنان برای گوگل رسوایی بزرگی خواهد بود. این شرکت اذعان می کند که "به استانداردهای خود و همچنین مشتریان خود عمل نکرده است."

گردآورنده: امیرحسین ضرغامی

فعالیت هکرها برروی سرورهای Flipboard به مدت ۱۰ ماه



Flipboard یکی دیگر از غول‌های فناوری است که اخیرا اطلاعات مهم کاربران خود را نشر داده است. داده‌هایی که در معرض خطر قرار دارند عبارتند از نام کاربر، کلمه عبور، آدرس های ایمیل و توکن دیجیتالی که برای پیوند حساب‌های شخص ثالث به Flipboard استفاده می‌شوند.

این شرکت بیان کرده است در حالی که مشکوک به فعالیت‌های غیر احراز شده برروی سرورهای خود در ۲۳ آپریل شدند متوجه شدند یک مهاجم در تاریخ ۲ ژوئن ۲۰۱۸ و ۲۳ مارچ ۲۰۱۹ و همچنین در تاریخ ۲۱-۲۲ آپریل ۲۰۱۹ به اطلاعات دیتابیس آنان دسترسی داشته است.

کاربرانی از ۱۴ مارچ ۲۰۱۲ ایجاد شده اند ویا پسورد خود را تغییر داده‌اند پسوردشان با استفاده از bcrypt هش شده است. پیش از آن تاریخ نیز پسورد کاربران با استفاده از الگوریتم SHA-1 هش شده است.

Flipboard هنوز در حال شناسایی اکانت-هایی است که درگیر این نقص شده‌اند. این شرکت دارای ۱۵۰ میلی.ن کاربر فعال در ماه است که بر اساس بیانات این شرکت، تمامی این اکانت‌ها در این نقص شریک نیستند. همچنین این شرکت بیان نموده است که به زودی پشورد تمامی کاربران را ریست خواهد کرد.

گردآورنده: محمد مرتضوی

محدود کردن دسترسی به اطلاعات شخصی توسط Google

رسوایی جمع آوری اطلاعات که در سال گذشته در فیس بوک رخ داد، تاثیری وسیع در صنعت فناوری به همراه داشت. اما مردم در مورد حفاظت از اطلاعات شخصی خود آگاهی بیشتری دارند و این امر باعث می‌شود که شرکت‌ها سطح دسترسی توسعه دهندگان به اطلاعات مشتری را محفوظ نگه دارند. حال این روسوایی متوجه‌ی شرکت Google شده است و محققان امنیتی بسیاری در طول سال‌ها، نگرانی‌های خود را در خصوص استفاده‌ی صحیح از اطلاعات در محصولات Google بیان نموده‌اند.

گوگل در سال گذشته اعلام کرد Project Strobe، به بررسی ریشه و شاخه‌ای از دسترسی توسعه دهنده‌های شخص ثالث به دستگاه اندرویدی و داده‌های حساب Google را مشغول است. این غول جستجو قبلا چندین سایت جدید را اجرا کرده است و اکنون توجه خود را به Chrome تغییر داده است.

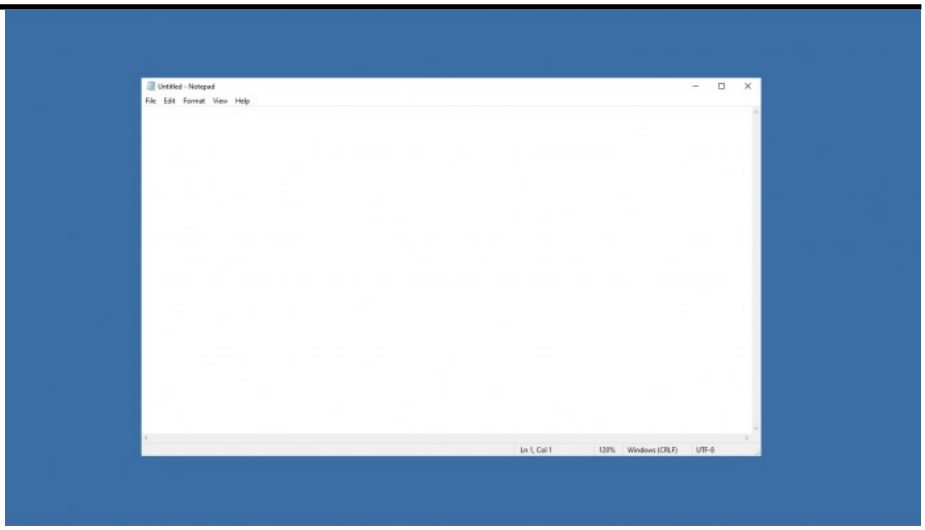
گوگل نیاز دارد که فقط درخواست دسترسی به اطلاعات مورد نیاز برای پیاده سازی ویژگی های خود را در صورتی که بیش از یک مجوز برای اجرای یک ویژگی استفاده شود، این مجوز باید از مجوزهای دسترسی به حداقل مقدار داده استفاده کند.

گوگل گفته است که همیشه توسعه دهندگان را برای استفاده از این رفتار تشویق کرده است، اما در حال حاضر، الزام لازم برای همه برنامه‌های افزودنی به این شکل است. گوگل همچنین ماموریت دارد که برنامه‌های افزونه ای که برای محتوای کاربر ارائه شده و ارتباطات شخصی را ارسال می‌کنند، باید از یک خط مشی رازداری تبعیت کنند و اطلاعات را به طور ایمن ارسال کنند.

مرورگرها به یک برند محبوب برای حملات رو به رشد فیشینگ و مهندسی اجتماعی تبدیل شده‌اند، بسیاری از حملات از افزونه‌های قانونی استفاده می‌کنند که بعدا با کد مخرب به روز رسانی می‌شوند.

گردآورنده: امیرحسین ضرغامی

وجود آسیب پذیری Notepad



یک مشکل حافظه‌ای در برنامه‌ی محبوب مایکروسافت به نام Notepad می‌تواند منجر به باز شدن بخش Shell از راه دور شود. این باگ توسط Tavis Ormandy یکی از اعضای تیم پروژه‌ی Zero کشف شده است.

وی در توییت خود بیان نمود که به دلیل وجود یک نقص امنیتی که در حافظه رخ می‌دهد می‌توان به خط فرمان و یا Shell از راه دور دست یافت.

وی همچنان بیان نمود که این آسیب پذیری از سال ۱۹۸۵ با این نرم افزار همراه می‌باشد و هیچکس تا کنون به آن پی نبرده است.

وی بیان نمود:" من نخستین فردی هستم که خط فرمان Shell را از درون Notepad اجرا نموده‌ام. این نقص یک آسیب پذیری حافظه‌ای می‌باشد و من آن را به Microsoft اعلام نموده‌ام. این آسیب پذیری تمام آخر هفته‌ی من را درگیر خود نمود"

این محقق بیان نمود که جزییات مربوط به این آسیب پذیری در ۹۰ روز آینده انتشار خواهد یافت.

وی همچنین بیان نمود که: "این آسیب پذیری یک باگ جدی می‌باشد و ما به مایکروسافت ۹۰ روز مهلت داده‌ام تا آن را مرتفع سازد."

قرار است تا بعد از بررسی‌های مایکروسافت، اطلاعات مربوط به این آسیب پذیری به طور کامل در اختیار سایرین قرار داده شود. اگر مایکروسافت نتواند که این آسیب پذیری را طرف مدت ۳ ماه برطرف کند، در آن زمان تمامی مراحل این آسیب پذیری منتشر خواهد شد.

برخی محققان معتقدند مهم نیست که چه شدت نقص موجود در Notepad جدی است، مشکل اصلی برای مهاجمان این است که می‌توانند Notepad را راه اندازی کرده و یک فایل را تجزیه و تحلیل کنند.

ممکن است نقص حافظه‌ای دفترچه یادداشت وجود داشته باشد و ممکن است خطرناک باشد، اما باید روی رایانه هدف قرار بگیرد و برنامه ویرایش متن را راه اندازی کند، بنابراین استفاده موفقیت آمیز از این نقص از راه دور واقعا نمی تواند امکان پذیر باشد.

حال باید ۳ ماه منتظر بود و دید که آیا بنا به ادعای این محقق امنیتی آیا این آسیب پذیری به همین میزانی که بیان شده است جدی است یا خیر؟

گردآورنده: محمد مرتضوی

ورود باج افزار Shade به امریکا!

باج افزار Shade که تا کنون کسور روسیه را هدف قرار داده بود، اکنون در امریکا و ژاپن دیده شده است.

این باج افزار برای اولین بار در سال ۲۰۱۴ توسط آزمایشگاه امنیتی Kaspersky کشف گردید اما اخیرا این باج افزار فعالیت خود را به بیرون از مرزهای روسیه گسترش داده است.

براساس تحقیقات Kaspersky، باج افزار Shade تاکنون ۵ کشور دیگر غیر از روسیه را تحت تاثیر قرار داده است که عبارتند از ایالات متحده، ژاپن، هند، تایلند و کانادا.

باج افزار Shade توسط ایمیل آلوده گسترش می‌یابد. در اواخر ماه فوریه سال ۲۰۱۹ این ایمیل‌های آلوده شامل لینکی به یک آرشیو و یا پیوست یک فایل PDF می‌باشد. این لینک یا فایل پیوست شامل یک فایل جاوا اسکریپت ویا جاوا می‌باشد که برای دریافت فایل‌های مورد نیاز این باج افزار طراحی شده است.

زمانی که یک قربانی به این باج افزار آلوده می‌شود، در ابتدا تصویر پشت زمینه ویندوز وی تغییر می‌گردد و ۱۰ فایل برروی دسکتاپ آن ایجاد می‌گردد که دارای نام-های README1.txt تا README10.txt می‌باشند. پیغامی که در تصویر پشت زمینه وجود دارد حاوی متن

" attention! All the important files on your disks were encrypted. The details can be found in README.txt files which you can find on any of your disks"

می‌باشد.

تمامی فایل‌های README.txt دارای یک متن ثابت می‌باشد.

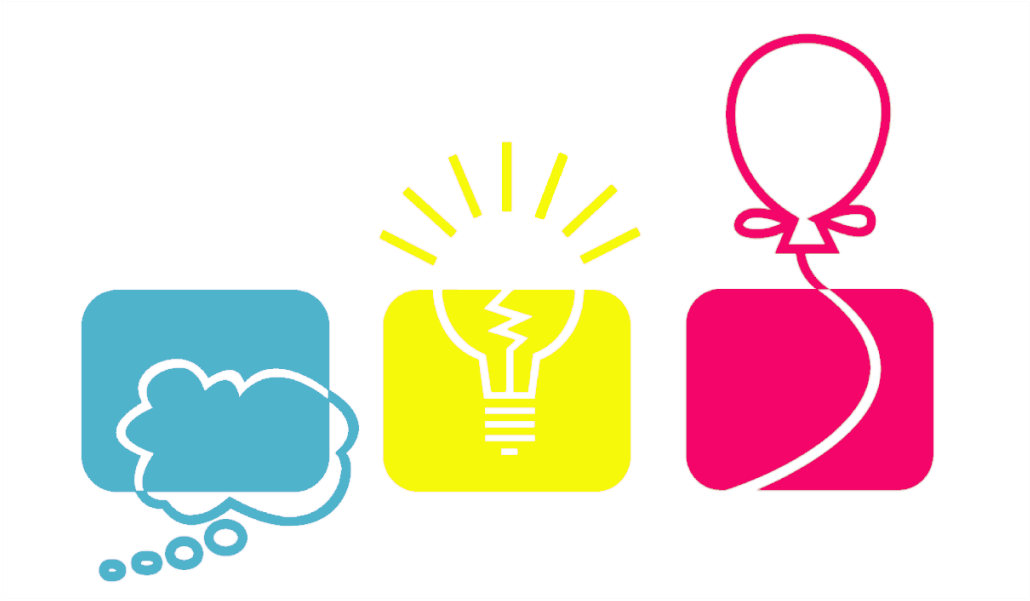
اهداف جدید

اخیرا ایمیل‌هایی که حاوی محتوا و لینک‌های آلوده می‌باشد به سایر کشورهای نیز ارسال گردیده است. این امر نشان دهنده‌ی این است که توسعه دهندگان تمایل دارند تا کسب و کار خود را به سایر کشورها گسترش دهند.

تحقیقات کارشناسان امنیت نشان می‌دهد که یکی از راه‌های گسترش این بدافزار پورت ۸۰ می‌باشد. در تصویر موجود می‌توانید میزان گسترش این بدافزار را در کشورهای مختلف مشاهده نمود.

گردآورنده: محمد مرتضوی

KHARAZMI CERT COORDINATOR CENTER



مرکز آپا دانشگاه خوارزمی

رییس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

امیرحسین ضرغامی

محسن یزدی‌نژاد

فاطمه الهی

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

پست الکترونیک:

cert@khu.ac.ir

وب سایت:

https://cert.khu.ac.ir/

کانال مرکز آپا خوارزمی:

@khu_cert

دانلود رایگان:

دانلود رایگان مجموعه کامل خبرنامه‌ها از طریق اسکن کد زیر در دسترس است.