شماره بیست و سوم - آذر ۱۳۹۷

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:

نقص اطلاعاتی موجود در Quora بیش از ۱۰۰ میلیون کاربر را تحت تاثیر قرار داد!

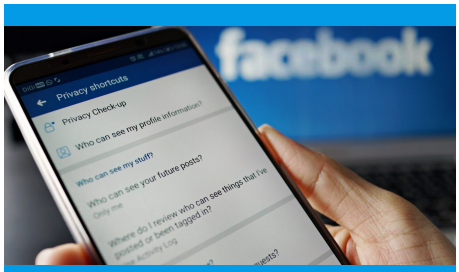
پس از هک اخیر در هتل های زنجیره ای ماریوت و تلاش برای نفوذ به اطلاعات مشتریان Dell، Quora اعلام کرده است که بیش از ۱۰۰ میلیون از سوابق کاربران در هفته گذشته به سرقت رفته است. - صفحه ۲

باج افزار WannaCry همچنان در هزاران کامپیوتر به طور خاموش زنده است!

حتی بعد از گذشت ۱۸ ماه همچنان باج افزار WannaCry کسب و کارهای موجود در سراسر جهان را تهدید می‌کند. بر اساس گزارش Kryptos Logic بیش از نیم میلیون کامپیوتر در سراسر جهان هنوز آلوده می‌باشند. - صفحه ۳

رهیابی دانش آموزان چینی با GPS های کارگذاشته شده در لباسشان!

ده مدرسه در Guizhan و منطقه‌ی Guangxi Zhuang از یونیفرم‌های هوشمند استقبال کرده‌اند. این یونیفرم‌ها با داشتن ۲ رهیاب برروی شانه‌هایشان قابلیت مانیتور کردن مکان دانش آموزان را به صورت ۷ روز هفته و ۲۴ ساعت روز دارا می‌باشند. - صفحه ۴



ارسال اطلاعات کاربران بدون اجازه به فیسبوک!

فیس بوک همچنان در حال ردگیری نرم افزارهایی است که کاربران حتی در صورتی که اکانت فیس بوک ندارند، اجرا می‌کنند. این امر ۶۱٪ از اپلیکیشن‌ها را تحت تاثیر قرار می‌دهد و یک عمل غیر قانونی بر اساس قوانین GDPR است. - صفحه ۵

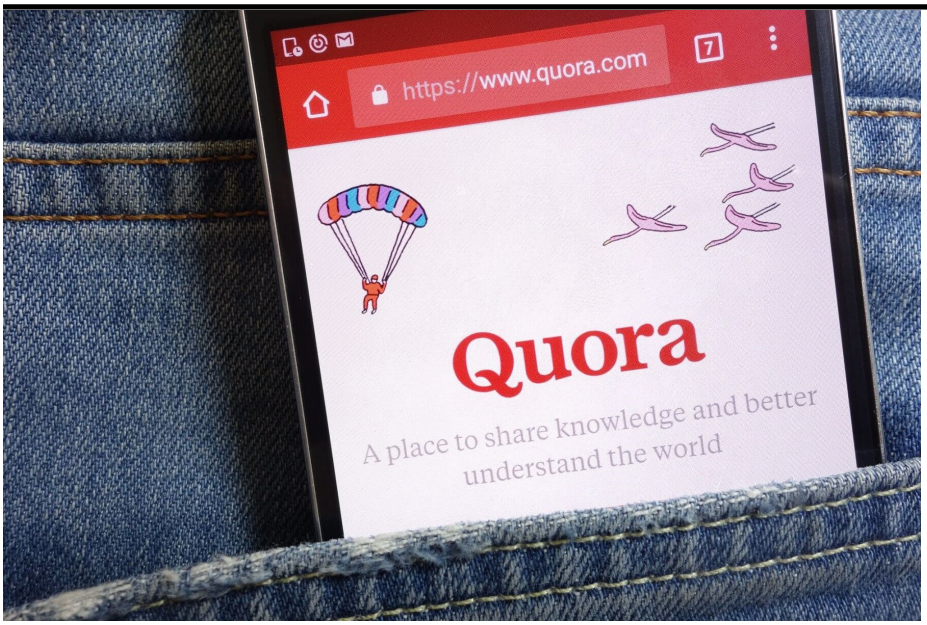
دور زدن سیستم امنیتی Office 365 تنها با یک کاراکتر!

محققان امنیتی تکنیکی ساده که منجر به دور زدن سیستم امنیتی Office 365در خصوص بررسی لینک‌ها می‌شود را به تازگی کشف نموده‌اند که در حال حاضر برای آن هیچ روش مقابله‌ای همچنان ایجاد نشده است. - صفحه ۶

نشت اطلاعات ۲۰۲ میلیون شهروند چینی جویای کار

محققان امنیتی چندی پیش دریافتند که دیتابیس عظیمی از اطلاعات مربوط به ۲۰۲ میلیون شهروند چینی بدون هیچ احراز هویتی در دسترسی مردم برروی اینترنت قرار گرفته است. - صفحه ۷

نقص اطلاعاتی موجود در Quora بیش از ۱۰۰ میلیون کاربر را تحت تاثیر قرار داد!



پس از هک اخیر در هتل های زنجیره ای ماریوت و تلاش برای نفوذ به اطلاعات مشتریان Dell، Quora اعلام کرده است که بیش از ۱۰۰ میلیون از سوابق کاربران در هفته گذشته به سرقت رفته است.

این وب سایت پرسش و پاسخ نوشته است که "دسترسی غیرمجاز به یکی از سیستم های ما توسط یک برنامه شخص ثالث مخرب" در تاریخ ۳۰ نوامبر رخ داده است. داده های لو رفته شامل: "نام، آدرس ایمیل، پسوردهای رمزگذاری شده (هش شده)، داده ها وارد شده از شبکه های مرتبط؛ محتوای عمومی و اقدامات، مانند سوالات، پاسخ ها، نظرات، رای ها، محتوای غیر عمومی و اقدامات، مانند درخواست پاسخ، پیام های مستقیم (توجه داشته باشید که درصد کم از کاربران Quora چنین پیام هایی را ارسال یا دریافت کرده اند)"

هرچند که پسوردهای به سرقت رفته همگی هش شده هستند اما Quora بیان نمود که بهتر است تا کاربران پسوردهای خود را تغییر دهند.

Adam D'Angelo، مدیر اجرایی Quora گفت که این شرکت اقداماتی را برای رسیدگی به این مسئله انجام داده است، اگرچه تحقیقات ما ادامه دارد و ما همچنان به پیشرفت های امنیتی ادامه خواهیم داد.

Quora هرکسی را که ممکن است تحت تاثیر این نقص قرار گرفته باشد از سیستم خارج نموده و اگر از یک روش احراز هویت استفاده می کرده، پسوردشان را نامعتبر کرده است.

همچنین D'Angelo اضافه نمود: "مسئولیت ما این است تا مطمئن شویم رخ دادهایی مثل این دیگر اتفاق نمی افتد و ما نتوانستیم این مسئولیت را به خوبی برآورده کنیم."

همچنین شرکت Dell که تحت تاثیر حمله ی سایبری اخیر قرار گرفته است ادعا کرده است که هیچ اطلاعاتی از کاربران به سرقت نرفته است. این شرکت یک بازنشانی کلی از تمامی رمزهای Dell.com انجام داده است و کاربران قبل از اینکه بتوانند به اکانت خود دسترسی داشته باشند نیاز بوده تا چندین مرحله احراز هویت انجام دهند.

گردآورنده: محمد مرتضوی

باج افزار WannaCry همچنان در هزاران کامپیوتر به طور خاموش زنده است!

حتی بعد از گذشت ۱۸ ماه همچنان باج افزار WannaCry کسب و کارهای موجود در سراسر جهان را تهدید می‌کند. بر اساس گزارش Kryptos Logic بیش از نیم میلیون کامپیوتر در سراسر جهان هنوز آلوده می‌باشند. این باج افزار تقریبا به طور کامل در انگلستان و ایالات متحده ریشه کن شده است اما پیش بینی می‌شود که مشکلات گسترده‌ای در بخش‌های دیگری از جهان وجود دارد.

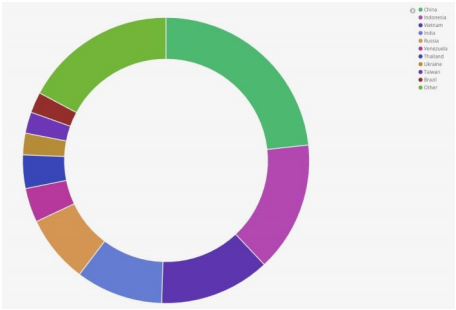
در حدود یک سال و نیم از انتشار اولیه‌ی باج افزار WannaCry می‌گذرد اما همچنان این باج افزار هزاران کامپیوتر را در سراسر دنیا تهدید می‌کند. داده‌های اخیر نشان می‌دهد که هزاران هزار کامپیوتر آلوده به بدافزار هستند. این در حالی است که در حال حاضر این بدافزارها غیر فعال و خاموش هستند.

این بدافزار به لطف یک محقق امنیتی به نام Marcus Hutchins در Kryptos Logic غیر فعال است. به گزارش Bleeping Computer، وی با کشف کدهای موجود در بدافزار توانست دامنه‌ای که بدافزار به آن رجوع می‌کند را کشف نماید. این دامنه ثبت نشده بود. وی با ثبت این دامنه توانست دکمه‌ی فعال سازی را از آن خود کند.

باج افزار WannaCry به طور متناوب از این آدرس Ping می‌گیرد. تا زمانی که دامنه در دسترس است این باج افزار فایل را رمزگذاری نخواهد کرد. اگر این سایت Down شود این باج افزار فعالیت خود را شروع خواهد کرد.

Kryptos Logic این دامنه را برای محافظت از آن در مقابل حملات DDoS به Cloudflare داده است.

در طول یک هفته، این سایت ۱۷ میلیون بار پینگ شده است که این پینگ‌ها از ۶۳۰۰۰۰ آی پی یکتا از ۱۹۴ کشور در دنیا



بوده است. چین، اندونزی، ویتنام ۳ کشوری هستند که بیشترین آلودگی را دارند.

این دامنه در طول هفته بیش از اواخر هفته فعال می‌باشد.

Kryptos Logic ابزاری دارد که TellTale نامیده می‌شود و می‌تواند تشخیص دهد که آیا سیستم شما آلوده به باج افزار WannaCry است یا خیر. مدیران شبکه می‌توانند با استفاده از این نرم افزار آی پی های درون سازمانی را مانیتور نمایند. این نرم افزار از لینک زیر قابل دانلود می‌باشد.

https://telltale.kryptoslogic.com/

گردآورنده: محمد مرتضوی

رهیابی دانش آموزان چینی با GPS های کارگذاشته شده در لباسشان!

ده مدرسه در Guizhan و منطقه‌ی Guangxi Zhuang از یونیفرم‌های هوشمند استقبال کرده‌اند. این یونیفرم‌ها با داشتن ۲ رهیاب برروی شانه‌هایشان قابلیت مانیتور کردن مکان دانش آموزان را به صورت ۷ روز هفته و ۲۴ ساعت روز دارا می‌باشند.

اگر دانش آموزی سعی نماید در طول ساعات درسی، مدرسه را ترک کند، هشداری مخابره خواهد شد. همچنین اگر دانش آموز سعی کند مدرسه را بدون این یونیفرم ترک نماید این هشدار فعال خواهد شد. جالب است بدانید که اگر دانش آموزان از رفتن به مدرسه خودداری کنند، والدین آنان از این اتفاق با خبر خواهند شد. از ویژگی‌های مهم دیگر این یونیفرم، این است که اگر دانش آموز در کلاس بخوابد، این هشدار مجدد فعال خواهد گردید.

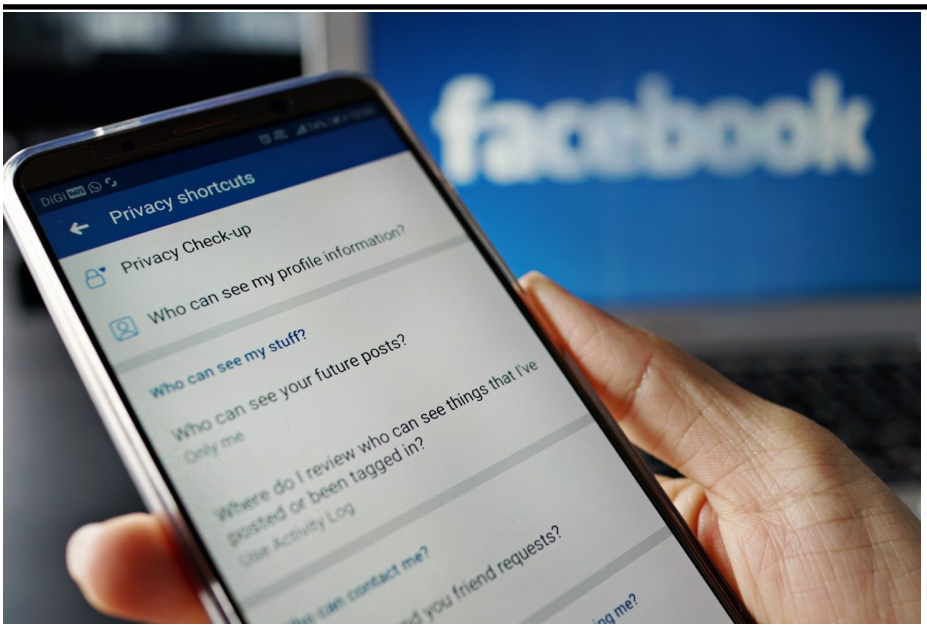
نیاز به گفتن نیست که مدیران مدارس و والدین به داده‌های این یونیفرم‌ها دسترسی دارند. سرپرست Renhuai Lin Zongwu بیان نموده است که آنان محل دقیق دانش آموزان را بعد از ساعات مدرسه چک نخواهند کرد. وی همچنین بیان نموده است که از زمان معرفی این یونیفرم‌ها حضور دانش آموزان افزایش چشمگیری داشته است.

براساس گفته‌های Yuan Bichay، مدیر تولید شرکت Guizhan Guangu Technology، هر کدام از این یونیفرم‌ها قابلیت شسته شدن بیش از ۵۰۰ بار در دمای ۱۵۰ درجه‌ی سانتی گراد را دارند. همچنین از این یونیفرم‌ها می‌توان برای پرداخت پول به صورت الکترونیک در داخل مدارس استفاده نمود که باعث می‌شود والدین و مدرسه قابلیت مشاهده‌ی این پرداخت‌ها را داشته باشند.

این اقدام باعث تعجب و همچنین پرسش‌های زیادی در فضاهای مجازی از جمله یکی از معروفترین شبکه‌های اجتماعی چین یعنی Weibo شده است. کاربران در خصوص اینکه این اقدام یک عمل مخالف با حقوق بشر است سوال می‌کنند و برخی از اینکه چقدر زمان نیاز است تا همه‌ی دانش آموزان و افراد بالغ از این لباس با قابلیت رهیابی استفاده کنند متعجب هستند.

گردآورنده: محمد مرتضوی

ارسال اطلاعات کاربران بدون اجازه به فیسبوک!



فیس بوک همچنان در حال ردگیری نرم افزارهایی است که کاربران حتی در صورتی که اکانت فیس بوک ندارند، اجرا می‌کنند. این امر ۶۱٪ از اپلیکیشن‌ها را تحت تاثیر قرار می‌دهد و یک عمل غیر قانونی بر اساس قوانین GDPR است.

علارغم قوانین حریم خصوصی جدید، مطالعات جدید نشان می‌دهد که بسیاری از اپلیکیشن‌های مشهور اندروید اطلاعات کاربران را به Facebook ارسال می‌کنند. این اطلاعات بدون توجه به آنکه کاربر دارای اکانت Facebook است یا خیر ارسال می‌گردد. این اطلاعات به محض باز شدن برنامه و پیش از آنکه کاربر حق انتخابی داشته باشد و یا بتواند تنظیمات حریم شخصی را فعال کند ارسال می‌شوند. حریم خصوصی بین المللی این مطالعات را هدایت کرده است و نتایج آن نشان می‌دهد که حداقل ۶۱٪ از اپلیکیشن‌هایی که آنان تست کرده‌اند داده‌هایشان را برای Facebook ارسال می‌نمایند. این اطلاعات شامل جزئیاتی نظیر اینکه چه اپلیکیشن‌های اجرا شده‌اند، چه زمانی این اپلیکیشن‌ها اجرا شده‌اند، چه کسی آنان را اجرا کرده است و چه مدت از این اپلیکیشن‌ها استفاده شده است، می‌باشد.

برای مثال اگر شخصی برنامه‌ی Indeed را باز کند، به نظر می‌رسد که آن شخص جویای شغل است. اگر کسی برنامه‌ی Qibla Connect را باز کند به نظر می‌رسد که وی مسلمان است.برنامه‌های دیگری همچون Duolingo، Kayak، Shazam، Spotify، TripAdvisor، Yelp و ... نیز بررسی شدند. قوانین کوکی‌های Facebook دو متد را برای افرادی که کاربر فیس بوک نیستند پیش نهاد می‌دهد که کاربران بتوانند با ارسال اطلاعات مخالفت کنند. اما حریم خصوصی بین الملل طی بررسی‌های خود متوجه شده است که هیچ یک از این دو گزینه در اطلاعات ارسالی هیچ تغییری ایجاد نمی‌کند. زمانی که داده‌های مربوط به برنامه‌ای که کاربر اجرا نموده است معمولی باشد، Facebook می‌تواند این اطلاعات را با سایر داده‌ها با جزئیات بالا ترکیب نماید و یک پروفایل تبلیغاتی برای کاربر ایجاد نماید. این نقص حریم خصوصی مربوط به اپلیکیشن‌ها و برنامه‌ها نمی‌باشد، بلکه به Android SDK فیس بوک مربوط است که توسط برنامه نویسان مورد استفاده قرار می‌گیرد. در ۲۸ ژوان، فیس بوک اعلام نمود که آنان با آپدیت Android SDK خود، تنها در صورت توافق کاربر، اقدام به ارسال اطلاعات آنان خواهد کرد. هرچند که این امر باعث بر طرف شدن نقض قوانین شد اما خیلی از برنامه‌ها همچنان از نسخه‌های قدیمی این SDK استفاده می‌کنند. حتی بعد از آپدیت شدن این برنامه‌های قدیمی، مقدار تنظیم شده‌ی اولیه‌ی آنان تغییر نخواهد کرد و همچنان به ارسال اطلاعات خواهند پرداخت.

گردآورنده: محمد مرتضوی

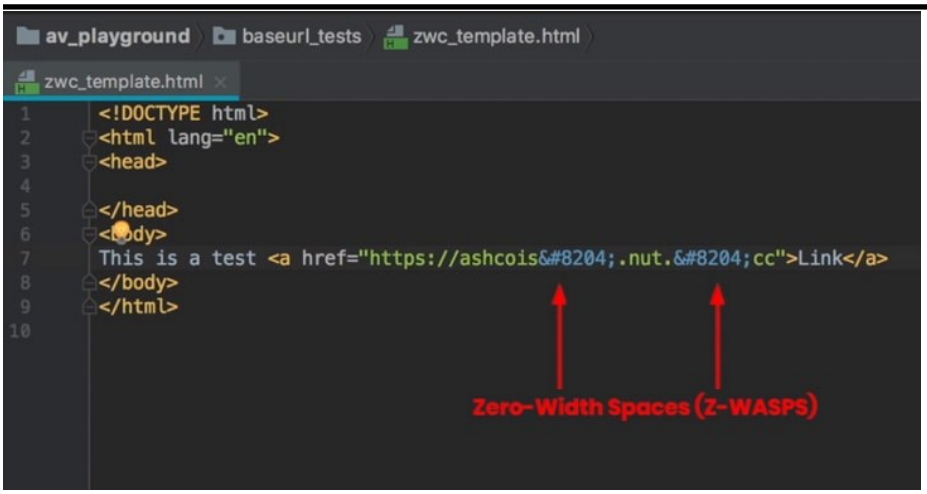
دور زدن سیستم امنیتی Office 365 تنها با یک کاراکتر!

محققان امنیتی تکنیکی ساده که منجر به دور زدن سیستم امنیتی Office 365 در خصوص بررسی لینک‌ها می‌شود را به تازگی کشف نموده‌اند که در حال حاضر برای آن هیچ روش مقابله‌ای همچنان ایجاد نشده است. لینک‌های ایمن یک راه حل برای جلوگیری از تهدیدات در Office 365 می‌باشد که توسط مایکروسافت ارائه گردیده است. این مکانیزم، لینک‌های وارده را با لینک‌های امن مایکروسافت جایگزین می‌کند تا از تهدیدات جلوگیری شود.

بنابراین، هربار که کاربر برروی یک لینک کلیک می‌کند، این لینک به مایکروسافت ارسال می‌شود. پس از ارسال، این لینک توسط مایکروسافت بررسی امنیتی می‌شود.

اگر اسکنرهای امنیتی مایکروسافت بتوانند عنصری خطرناک در آن لینک پیدا کنند، در هشداری به کاربر، وجود این عناصر اطلاع داده می‌شود. در غیر اینصورت، کاربر به لینک اصلی ارجاع داده می‌شود.

محققان امنیتی شرکت Avanan توانسته‌اند به روش دور زدن این سیستم امنیتی در



Office 365 دست پیدا کنند. به این روش Zero - Width Space ویا ZWSPs می‌گویند.

- (Zero-Width Space)
- ‌ (Zero-Width Non-Joiner)
- ‍ (Zero-Width Joiner)
- (Zero-Width No-Break Space)
- ０ (Full-Width Digit Zero)

این روش توسط تمامی مرورگرهای به روز پشتیبانی می‌شود. کاراکتر ZWSPs یکی از کاراکترهای غیر قابل چاپ می‌باشد که معمولا برای شکستن خط در کلمات طولانی استفاده می‌شود. این کاراکترها از این قرار هستند:

بر اساس تحقیقات به عمل آمده، مهاجمان با اضافه کردن این عبارات به لینک‌های مخرب در حملات فیشینگ، سیستم امنیتی مایکروسافت را دور می‌زنند و این سیستم قابلیت تشخیص این لینک‌ها را نخواهد داشت.

بنابراین، زمانی که کاربر برروی این لینک‌ها کلیک می‌کند، مستقیما به سایت‌هایی با عناصر مخرب و فیشینگ هدایت خواهد شد.

گردآورنده: محمد مرتضوی

نشت اطلاعات ۲۰۲ میلیون شهروند چینی جویای کار

محققان امنیتی چندی پیش دریافتند که دیتابیس عظیمی از اطلاعات مربوط به ۲۰۲ میلیون شهروند چینی بدون هیچ احراز هویتی در دسترسی مردم برروی اینترنت قرار گرفته است.

این دیتابیس ۸۵۴.۸ گیگابایتی برروی MongoDB و در یک میزبان هاستینگ آمریکایی قرار داشته است.

در مجموع، این دیتابیس شامل ۲۰۲۷۳۰۴۳۴ رکورد درباره افراد جویای شغل از چین می‌باشد که شامل اطلاعاتی نظیر نام کامل، تاریخ تولد، تلفن تماس، آدرس ایمیل، وضعیت تاهل، اطلاعات گواهینامه رانندگی و تجارب حرفه‌ای و کاری آنان می‌باشد.

Bob Diachenko مدیر تحقیقات امنیتی در Hacken.io این دیتابیس را در حدود ۲ هفته‌ی پیش کشف کرده است که در زمان کوتاهی بعد از اطلاع وی به توییتر، امن گردید.

با این حال لاگ مربوط به MongoDB حداقل ۱۲ آی پی را نشان می‌دهد که قبل از Offline شدن این دیتابیس به آن دسترسی داشته‌اند.

اگرچه هنوز منبع داده‌ها نا مشخص است اما به نظر می‌رسد که شخصی با استفاده از ابزار قدیمی جمع آوری رزومه که data-import نامیده می‌شود اقدام به جمع آوری اطلاعات تمامی افراد جویای شغل در وب سایت‌های چینی همانند bj.58.com کرده است.

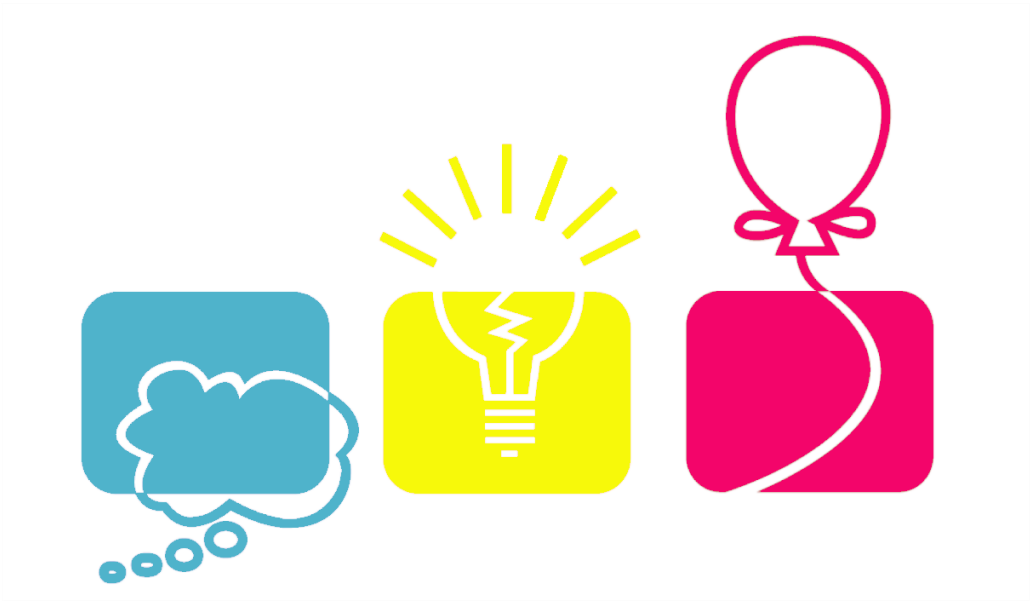
Diachenko معتقد است که فرمت داده‌های جمع آوری شده دقیقا همانند فرمت ابزارهای جمع آوری داده می‌باشد.

Diachenko اقدام به برقراری ارتباط با تیم bj.58.com کرده است که به وی گفته شده است که منشاء این اطلاعات، سایت آنان نمی‌باشد.

این اولین باری نیست که نمونه‌های MongoDB برروی اینترنت پخش می‌شوند. در سال‌های اخیر، چندین گزارش مبنی بر نشت اطلاعات برروی اینترنت اعلام گردیده است.

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

محسن نادری

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:

http://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.