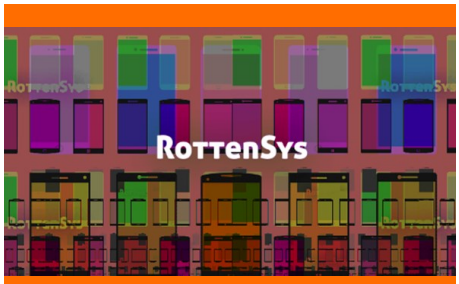
شماره چهاردهم - اسفند ۱۳۹۶

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:



بدافزار RottenSys

بدافزار RottenSysچینی در حال ساختن یک باتنت به بزرگی تقریباً ۵ میلیون گوشی هوشمند اندرویدی است.

در حال حاضر RottenSysبرای نمایش تبلیغات روی دستگاه کاربران استفاده می‌شود اما محققان شرکت Check Point مدارکی یافته‌اند که این کلاهبرداران در حال توسعه ماژولی برای جمع‌آوری همه گوشی‌های آلوده در یک باتنت غول‌پیکر هستند.

این باتنت قابلیت‌های گسترده‌ای از جمله نصب برنامه‌های اضافی و UI Automation دارد. البته بیم آن می‌رود که کلاهبرداران با استفاده از RottenSys اقدامات ناخواسته و بدتری نسبت به نمایش تبلیغات روی صفحه برای کاربران انجام دهند. - صفحات ۲ و ۳

حملات استخراجی رمزنگاری‌شده و ضربه آنها به تجارت

عبارت "استخراج رمزنگاری‌شده" معرف نوعی ارتباط با ارز رمزنگاری‌شده است. – آیا هکرها فقط افراد یا شرکت‌هایی که بیت‌کوین دارند را هدف قرار می‌دهند؟

نه کاملا. مثل هکرها، استخراجگران نیز برای همه خطرناکند. هکرها شرکت های تامین کننده آب و برق واقع در اروپا، سایت‌های دولتی انگلستان، کارخانه‌ای هسته‌ای در روسیه، و حتی یک واحد آسیب‌پذیر NSA را نیز مورد هدف حمله قرار دادند.

با نگاه به چشم‌انداز تهدید جهانی، بوضوح می‌توان دید که حملات استخراجی رمزنگاری‌شده، رو به افزایش است. - صفحات ۴، ۵ و ۶

تکنیک سرقت اطلاعات از بلندگو و هدفون

تیم تحقیقاتی دانشگاه بن-گوریون نِگِو در اسرائیل، روشی جدید در استخراج اطلاعات از رایانه‌های ایزوله شده‌ای که از بلندگو، هدفون، گوشی یا ریزگوشی را ارائه کردند.

سناریوهای حمله شامل سرقت بلندگو-بلندگو، بلندگو-هدفون و هدفون- هدفون می‌شود.

چنین حمله‌ای – با نام مستعار موسکیتو- با بهره گیری از تکنیکی بنام "بازیابی جک" امکان پذیر است که جک‌های صوتی خروجی را به جک‌های ورودی تبدیل می‌کند، به شکل موثری، بلندگوها را به میکروفون تبدیل می‌کند.- صفحه ۷

بدافزار RottenSys

بدافزار RottenSys چینی در حال ساختن یک باتنت به بزرگی تقریباً ۵ میلیون گوشی هوشمند اندرویدی است.

در حال حاضر RottenSys برای نمایش تبلیغات روی دستگاه کاربران استفاده می‌شود اما محققان شرکت Check Point مدارکی یافته‌اند که این کلاهبرداران در حال توسعه ماژولی برای جمع‌آوری همه گوشی‌های آلوده در یک باتنت غول‌پیکر هستند.

این باتنت قابلیت‌های گسترده‌ای از جمله نصب برنامه‌های اضافی و UI Automation دارد. البته بیم آن می‌رود که کلاهبرداران با استفاده از RottenSys اقدامات ناخواسته و بدتری نسبت به نمایش تبلیغات روی صفحه برای کاربران انجام دهند.

RottenSys از سال ۲۰۱۶ فعال شده است

اما هیچ وقت به این میزان خطرناکه نبوده‌است. این بدافزار اولین بار در سپتامبر ۲۰۱۶ ظاهر شد و کلاهبرداران بیشتر وقت خود را صرف پخش کردن آن در دستگاه‌های جدید کردند.

به آرامی تعداد قربانیان RottenSys افزایش یافت و بنا به گزارش Check Point این بدافزار تا کنون حدود ۵ میلیون دستگاه را آلوده کرده است.

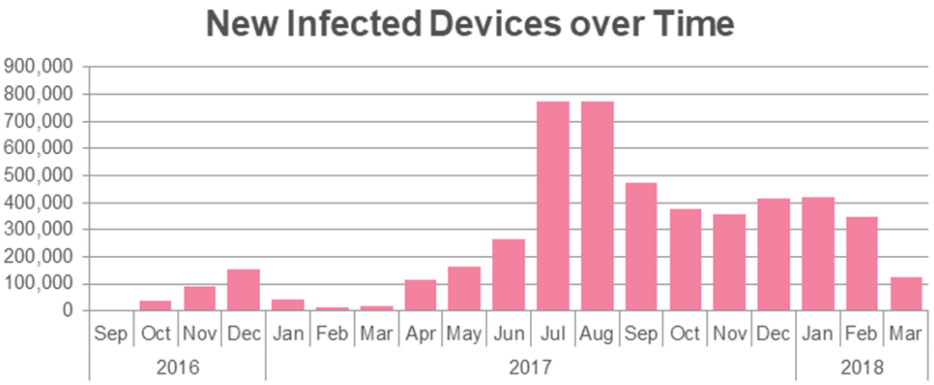
کامپوننت خطرناکی که ماه گذشته اضافه شد کنترل همه دستگاه‌ها را در اختیار مهاجمان می‌گذارد. طی دو سال گذشته RottenSys بیشتر روی ارسال تبلیغات تمرکز داشت.

محققان تخمین می‌زنند توسعه دهندگان این بدافزار در حال حاضر هر ده روز حدود ۱۱۵ هزار دلار درآمد دارند. این رقم براساس نمایش آگهی‌هایی بدست آمده است که محققان در طی تجزیه و تحلیل مشاهده کرده‌اند.

ادامه در صفحه بعد.

گردآورنده: حسین علیمرادی

بدافزار RottenSys (ادامه...)



RottenSys از مجازی سازی و پردازش‌های undead استفاده می‌کند

در گذشته خانواده‌های بدافزار اندرویدی دیگری هم مشاهده شده است اما تعداد کمی طوری مدیریت شدند که دستگاه‌های بسیاری را آلوده کنند.

بدافزار از دو پروژه متن باز که در GitHub به اشتراک گذاشته شده‌اند استفاده می‌کند. پروژه Small که یک فریم‌ورک مجازی‌سازی اپلیکیشن است و MarsDaemon که یک کتابخانه برای نگهداری برنامه‌ها به صورت undead است.

در گام اول RottenSys با استفاده از Small نگهدارنده‌های مجازی برای کامپوننت‌های خود می‌سازد و اجازه می‌دهد به صورت موازی اجرا شوند -کاری که سیستم عامل اندروند به صورت پیش‌فرض از آن پشتیبانی نمی‌کند- و به فرایند تحویل برنامه کمک می‌کند.

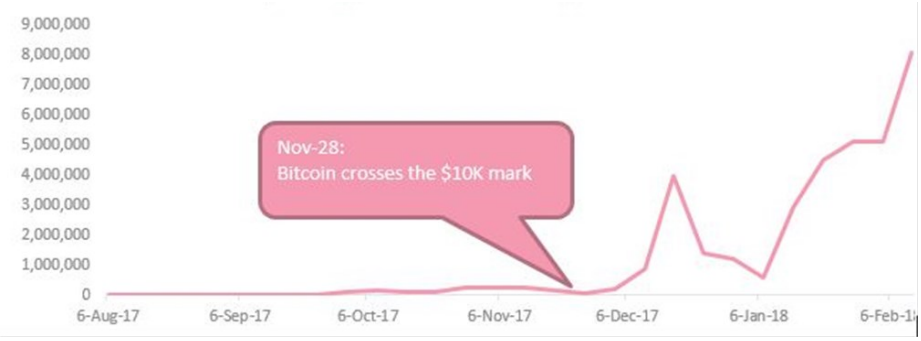
در گام دوم RottenSys با استفاده از MarsDaemon پردازش را حتی بعد از بستن آن توسط کاربر در حالت اجرا نگه می‌دارد و مطمئن می‌شود مکانیزم نمایش تبلیغات همیشه روشن است.

تنها نقطه ضعف این بدافزار روال نصب آن است. برنامه‌های آلوده با RottenSys تمایل دارند لیست بزرگی از مجوزها را درخواست کنند. کاربران بادقت به سادگی می‌توانند متوجه شوند و از نصب چنین برنامه‌هایی خودداری کنند اما متأسفانه همه کاربران اندروید حریم خصوصی را جدی نمی‌گیرند و معمولاً همه مجوزهایی که برنامه درخواست می‌کند به آن می‌دهند.

علاوه بر این هنوز مشخص نیست که سازندگان RottenSys چطور ممکن است از باتنت ساخته شده استفاده کنند و شاید به زودی شاهد استفاده از آن برای حملات DDoS باشیم مانند چیزی که سازندگان WireX با باتنتشان انجام دادند.

گردآورنده: حسین علیمرادی

حملات استخراجی رمزنگاری‌شده و ضربه آنها به تجارت



عبارت "استخراج رمزنگاری‌شده" معرف نوعی ارتباط با ارز رمزنگاری‌شده است. – آیا هکرها فقط افراد یا شرکت‌هایی که بیت‌کوین دارند را هدف قرار می‌دهند؟

نه کاملا. مثل هکرها، استخراجگران نیز برای همه خطرناکند. هکرها شرکت های تامین کننده آب و برق واقع در اروپا، سایتهای دولتی انگلستان، کارخانه‌ای هسته‌ای در روسیه، و حتی یک واحد آسیب‌پذیر NSA را نیز مورد هدف حمله قرار دادند.

با نگاه به چشم‌انداز تهدید جهانی، بوضوح می‌توان دید که حملات استخراجی رمزنگاری‌شده، رو به افزایش است.

حملات استخراجی اولین بار در سال ۲۰۱۱ با جایگاهی نسبتا ناچیز در میان دیگر حملات سایبری، ظهور کرد. با اینحال، از وقتی ارزش بیت‌کوین و مونرو صعود کرده، تجارت استخراج رمزنگاری‌شده نیز بشدت سودآور شده است. جدول زیر رشد هشداردهنده تعداد این حملات را بیان می‌کند.

این حملات، سازمان‌های سراسر جهان را هدف قرار می‌دهند. نقشه‌ی زیر، توزیع جهانی و شیوع حملات را در دسامبر ۲۰۱۷ نشان می‌دهد.

صنعت استخراج رمزنگاری‌شده

بطور خلاصه، با استفاده از تکنولوژی بلاک‌چین، استخراج، همان فرآیند سرقت معاملات جدید به درون دفترکل عمومی ارز-رمزنگاری‌شده است.

سرقت یک بلاک از معاملات، وابسته به حل یک معمای پیچیده است، و دفترکل به تنهایی، اساسا یک زنجیره از بلاک‌های معاملات مهرشده است و بعنوان یک بلاک‌چین شناخته می‌شود. به اولین استخراجگر(شخص یا رایانه) برای کامل کردن این محاسبات پیچیده، مقداری سکه‌ی ارزشمند اعطا می‌شود. اثبات ریاضیِ کار، که استخراجگر، معمای آن را با موفقیت حل کرده است، مثل یک مُهر برای معاملات عمل می‌کند.

با درخواست از استخراجگران برای حل این معماهای پیچیده‌ی کریپتوگرافی، فرآیند استخراج به ناچار درخواست محاسبات منبع-فشرده را دارد. استخراجگران، به نوبت، از راه قدیمی اما خوبِ "پول فیزیکی" انگیزه می‌گیرند.

در نتیجه، استخراج به یک تجارت بزرگ تبدیل شد، تجارت خیلی بزرگ.

هر ۱۰ دقیقه، بیت‌کوین یک بلاک معامله را در دفترکل خود انجام می‌دهد و به استخراجگر آن ۵/۱۲ بیت‌کوین هدیه می‌هد. با نرخ جاری معامله بیت‌کوین، حدود ۱۳۰هزار دلار هر ۱۰ دقیقه به استخراجگران پرداخت می‌شود، یا ۸/۶ میلیارد دلار در سال.

بله، درست خواندید. تجارت استخراج بیت‌کوین در سال درآمد ۸/۶ میلیارد دلاری تولید می‌کند.

و فقط بیت‌کوین یکی از ارزهای رمزنگاری‌شده است. هریک از این ارزها، اکوسیستم خود را تولید می‌کند. مثلا مونرو، سالانه به جمعیت استخراجگر خود، ۴۳۰ میلیون دلار پاداش می‌دهد.

ادامه در صفحه بعد

گردآورنده: حسین علیمرادی

حملات استخراجی رمزنگاری‌شده و ضربه آنها به تجارت (ادامه...)

جنبه‌ی جنایی استخراج رمزنگاری‌شده

بجای سرمایه‌گذاری در مراکز اطلاعاتی، مجرمین استخراج رمزنگاری‌شده، بوسیله‌ی هک کردن دستگاه‌های کاربران، از توان CPUی آنها برای انجام محاسبات بلاک‌چین خود و پاداش گرفتن استفاده می‌کنند.

قطعا وقتی کار به قربانیان استخراج برسد، همه چیز از دست می‌رود: رایانه‌ها، تلفن همراه، سرورها، سیستم‌های صنعتی، و حتی ماشین‌های تسلا. در هر CPU، استخراجگری مخفی، وجود دارد که منتظر گروگان گرفته شدن توسط هکرهاست.

چرا حملات استخراجِ رمزنگاری‌شده؟

سادگی، سودآوری و راه گریز.

حملات استخراجی، که اغلب از آنها تحت عنوان "جَک رمزگذاری‌شده" یاد می شود، پتانسیل بالایی برای تولید درآمدهای بالای مالی دارند.

انواع دیگر حملات ارز رمزنگاری‌شده

مجرمان تنها به تکنیک‌های استخراج در تورم متزلزل بها و محبوبیت این نوع ارزها بسنده نکرده‌اند.

سرقت کیف پول- دزدی مستقیم از کیف پول بیت‌کوین کاربر

انواع جدیدی از بدافزارها ظهور کرده‌اند که تلاش می‌کنند کلید خصوصی کیف‌پول را از رایانه‌ی کاربر بربایند. به محض اینکه مجرمین سایبری به کیف پول قربانی دست یافتند، براحتی می‌توانند سرمایه‌ی کاربر را به حساب خود انتقال دهند.

بعضی تروجان‌های مالی قدیمی مثل "تریکبات"، سریعا به روند بیت‌کوین پیوسته است، و امکانات جدیدی برای هدف قرار دادن کیف‌پول کاربر اضافه کرده است.

سرقت معاملات بیت کوینی

اگر بخواهید مقداری بیت‌کوین به کسی انتقال دهید، باید آدرس کیف پول آن فرد را در فرم پرداخت وارد کنید. هرچند این آدرس‌ها، طولانی و رمزنگاری شده، با اعداد و حروف تصادفی هستند تا کمتر به چشم آیند.

بدافزارها از روشی ساده استفاده می‌کنند: وقتی آدرس کیف‌پولی در کلیپبورد رایانه کپی می شود، بدافزار جای آن را با آدرس کیف‌پول رمزنگاری شده‌ی مهاجم عوض می‌کند. قربانی خوش‌خیال بعید است که متوجه تغییر آدرس شود و آن سرمایه، مستقیم به حساب مهاجم ریخته می‌شود.

سایت‌های تبادل ارزی هک‌کننده

سایت‌های تبادل ارزی بخش مهمی از اکوسیستم ارزهای رمزنگاری‌شده‌اند، چرا که میزبان کیف‌پول کاربر و دستیاری در معاملات بیت کوین هستند.

متأسفانه، سایت‌های تبادل ارز، غیرقابل کنترل‌اند و اغلب امنیت کافی ندارند. فقط در دو ماه اول سال ۲۰۱۸، شاهد سرقت ۱۷۰ میلیون دلار از بیت‌گریل و ۴۲۵ میلیون دلار از کوین‌چک بودیم.

به این دلیل که اغلب شرکت‌ها همچنان با پرداخت مستقیم ارزهای رمزنگاری‌شده موافقت نکرده‌اند، بعید است که تحت تاثیر حملات مختلفی که سعی در سرقت کوین یا دستکاری معاملات دارند قرار بگیرند.

سه نوع از حملات استخراجی، کسب و کار شما را تحت تاثیر قرار می‌دهند:

- **مصرف منابع سرور**

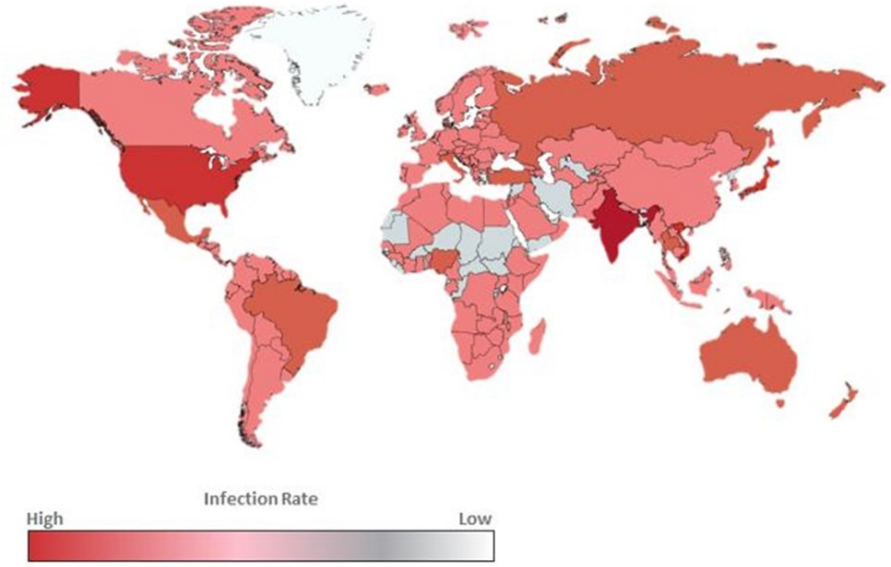
بدافزار استخراجگر، براحتی می‌تواند کل توان CPUی سرورهای شما را مصرف کند همچنین بشدت در دسترس بودن خدمات شما را کاهش و هزینه‌ی برق را افزایش دهد.

سرورهای شما باید بر روی یک ابر ارتجاعی میزبانی شوند، برای جبران نیروی محاسباتی از دست‌رفته، محیط، بدنبال تخصیص نمونه‌های اضافی است . متعاقبا هزینه‌های میزبانی ابری شما را افزایش می‌دهد. اگر سرورهای شما به شکل ارتجاعی تنظیم نشده باشند، حمله منجر به انکار کامل خدمات خواهد شد.

ادامه در صفحه بعد.

گردآورنده: حسین علیمرادی

حملات استخراجی رمزنگاری‌شده و ضربه آنها به تجارت (ادامه...)



- **کاهش بهره‌وری کاربر**

حملات استخراجی کاربران را به سه شکل اولیه هدف قرار می‌دهند:

۱. درست مثل سرورها، کاربران رایانه‌ها، تحت تاثیر بدافزار جست و جو گر رمزنگاری‌شده‌ای هستند که خودبخود روی سیستم‌عامل نصب می‌شوند.

۲. بدافزارهای موبایلی که حاوی کد استخراج هستند. گوشی‌های هوشمند برای تحمل بار سنگین محاسبات کریپتوگرافی موردنیاز برای استخراج، طراحی نشده‌اند. درواقع، فرایند استخراج می‌تواند حرارت موبایل را تا جایی که منجر به تغییر شکل آن شود، بالا ببرد.

۳. کاربران ممکن است سایتهای تحت تاثیر یا مخرب را باز کنند. این صفحات حاوی کد جاوااسکریپتی هستند که مرورگر کاربر را به یک دستگاه استخراج گر تشنه‌ی CPU تبدیل می کند.

نتایج همه‌ی این تکنیک‌های حمله یکیست: دستگاه کاربر کند و گرم می‌شود، علاوه براینکه کاربران بیش از پیش از عدم پاسخگویی به درخواستشان، ناامید می‌شوند.

- **تاثیر منفی بر اعتبار شرکت و رضایت مشتری**

در بسیاری موارد، هکرها، سرورهای وب یک سازمان را با تعبیه‌ی جاوااسکریپت استخراجگر در صفحات HTML سایت آنها آلوده می‌کنند.

اگر این اتفاق برای سازمان شما بیوفتد، شما اساسا بازدیدکنندگان سایت خود را هدف قرار می‌دهید! همه‌ی بازدیدکنندگان می‌بینند که رایانه و مرورگر آنها بطور غم‌انگیزی کند می‌شود، و همچنین CPU آنها تقریبا از کار می‌افتد. چنین اتفاقی می‌تواند منجر به تجربه‌ی بسیار ضعیف مشتری شود و تبلیغی که بر اعتبار شرکت تاثیر منفی دارد به بار آورد.

گردآورنده: حسین علیمرادی

تکنیک سرقت اطلاعات از بلندگو و هدفون

تیم تحقیقاتی دانشگاه بن-گوریون نِگِو در اسرائیل، روشی جدید در استخراج اطلاعات از رایانه‌های ایزوله شده‌ای که از بلندگو، هدفون، گوشی یا ریزگوشی را ارائه کردند.

سناریوهای حمله شامل سرقت بلندگو-بلندگو، بلندگو-هدفون و هدفون- هدفون می‌شود.

بازیابی دوباره‌ی جک، بازهم مشکل‌ساز می‌شود!

چنین حمله‌ای – با نام مستعار موسکیتو- با بهره گیری از تکنیکی بنام "بازیابی جک" امکان پذیر است که جک‌های صوتی خروجی را به جک‌های ورودی تبدیل می‌کند، به شکل موثری، بلندگوها را به میکروفون تبدیل می‌کند.

همین تیم تحقیقاتی، سال گذشته در پروژه‌ی قبلی خود بنام **بلندگو** درمورد بازیابی جک تحقیق کردند، که محققین در آن عادت داشتند هدفون‌ها را به میکروفون تبدیل کنند و صدا و مکالمه‌های محلی را ضبط کنند.

در این آزمایش، محققین استدلال می‌کنند که بدافزاری که موفق شده یک رایانه‌ی ایزوله‌شده را آلوده کند، می‌تواند فایل‌های محلی ذخیره‌شده را بشکل سیگنالهای صوتی تنظیم کند و آنها را به رایانه‌ای نزدیک از طریق بلندگوها، هدفون‌ها، گوشی‌ها یا ریزگوشی‌های متصل، منتقل کند.

رایانه‌ی دریافت‌کننده، که با بدافزار هم آلوده شده است، از بازیابی جک برای تبدیل بلندگوها، هدفون‌ها، گوشی‌ها یا ریزگوشی‌های متصل، به یک میکروفون موقتی استفاده می‌کند تا صدای تنظیم شده را دریافت و آن را به یک فایل اطلاعاتی تبدیل کند.

حمله موسکیتو، سرعت انتقال خیلی بالا را پشتیبانی می‌کند

محققین یک پروتکل سفارشی ایجاد کردند که اطلاعات باینری را به شکل سیگنال‌های صوتی تنظیم می‌کند، و این حمله را برای فواصل بین ۱ تا ۹ متری آزمایش کردند.

آنها شرح دادند که موفق به انتقال اطلاعات بین دو رایانه با سرعت متغیر بین ۱۸۰۰ تا ۱۲۰۰ بیت‌برثانیه در حالتیکه بلندگوها مقابل هم بودند و صدا را در باندهای فرکانس انتشار می‌دادند (کمتر از ۱۸کیلوهرتز) شدند.

وقتی بلندگوها مقابل هم نبودند، سرعت انتقال کاهش می‌یافت، و فاصله‌ی بین آنها زیاد می‌شد، یا فرکانس صوتی تغییر می‌کرد. علیرغم اینکه دو متغیر اول، بدیهی هستند، آخری نیاز به توضیح بیشتری دارد.

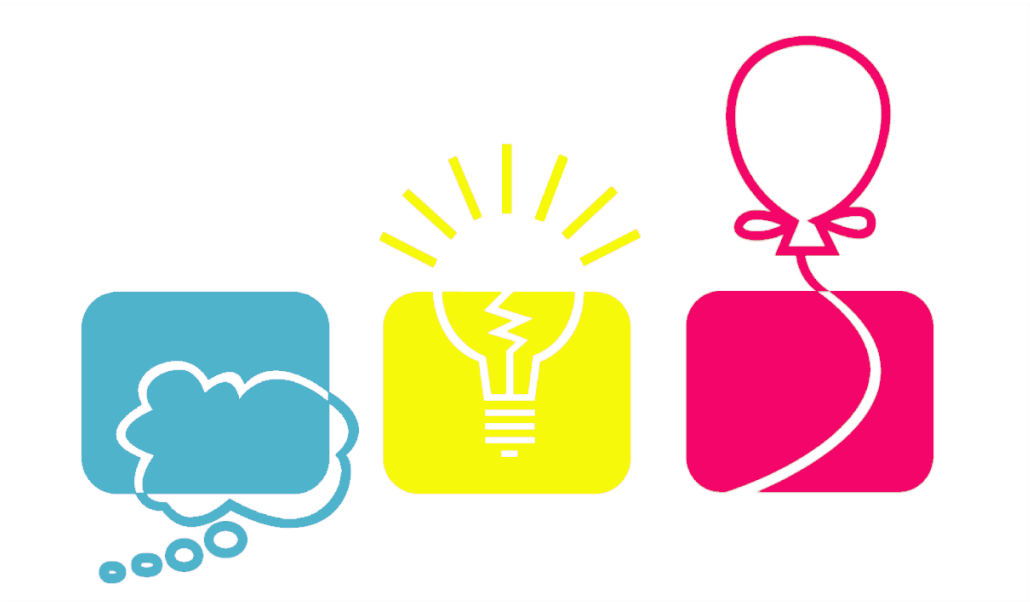
محققین عنوان کردند: "دلیل آن ایسنت که بلندگوها، و بطور خاص بلندگوهای خانگی، برای مشخصه‌های صوتی انسان ساخته شده‌اند، پس آنها در قبال محدوده‌ی فرکانس‌های شنیداری پاسخگو هستند."

سرعت انتقال همچنین حین استفاده از گوشی‌ها یا ریزگوشی‌ها کاهش یافت و برای هدفون‌ها نیز کمتر هم شد. چرا که هدفون‌ها، امواج صوتی را به یک سمت خاص هدایت می‌کنند، با محدود کردن موارد سرقت موثر به فاصله‌های خیلی خیلی کم، هنگامیکه هدفون‌ها بهم نزدیکند، و زمانیکه آنها صوت را فقط در فرکانس‌های شنیداری منتشر می‌کنند.

عوامل دیگری که سرعت انتقال داده را کم میکنند شامل نویزهای محیطی، مثل موسیقی، سخنرانی است، اما محققین گفتند که این نیز می‌تواند با تغییر فرکانس به بیش از ۱۸کیلوهرتز، اصلاح شود.

گردآورنده: حسین علیمرادی

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

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 تلگرام:

@khu_cert

دانلود رایگان:

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