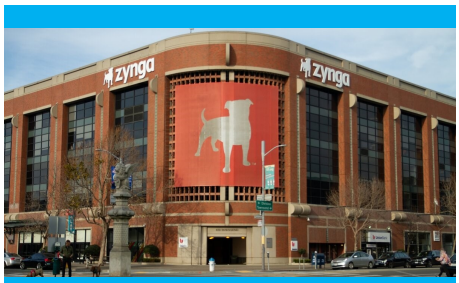
شماره سی و دوم - شهریور ۱۳۹۸

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:



Zynga هک شد!

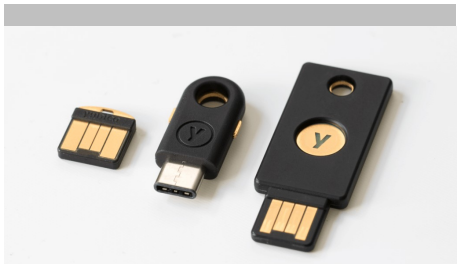
نمونه‌ای از داده‌ی کاربران شامل نام آنان، آدرس ایمیل، IDهای افراد، پسوردهای هش شده، توکن ریست پسوردها، شماره تماس افراد، ID فیس بوک کاربران و IDهای اکانت کاربران Zynga برای سایت خبری The Hacker News ارسال گردیده است که تایید می‌کند این سایت هک شده است.- صفحه ۲

دیتاسنتری برای جرائم سایبری در پناهگاه سابق ناتو!

مسئولین آلمان اخیرا یک دیتاسنتر مربوط به جرائم سایبری که به صورت پنهانی در پناهگاه ۵۰۰۰ متر مربعی سابق ناتو قرار داشت با حمله پلیس به منطقه از دسترس خارج گردید. - صفحه ۳

گوگل و ISPها در مقابل هم بر سر DNSهای رمزنگاری شده!

گوگل و موزیلا هردو خواهان آپدیت به روز رسانی مرورگرهایشان برای استفاده از ترافیک رمزنگاری شده در سطح DNS هستند. آنان اعلام کرده‌اند که با این کار حریم شخصی کاربران، بیشتر رعات خواهد شد و کاربران کنترل بهتری برروی اینکه چه کسی عادات رفتاری آنان را می‌بینند خواند داشت. اما ISPها علاقه‌ای به قفل کردن این اطلاعات ندارند و از قانون گذاران امریکایی خواسته‌اند تا از این اتفاق خودداری کنند. - صفحه ۴

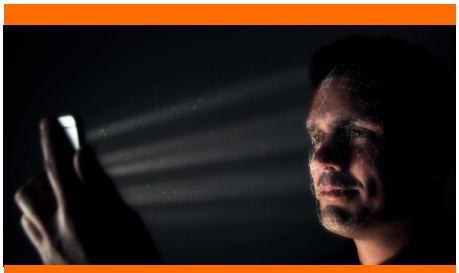


استفاده از کلیدهای امنیتی Yubico برای ورود به سیستم‌های ویندوزی

از کلیدهای Yubico قبلاً برای محافظت از Gmail، Dropbox، مدیران رمز عبور و موارد دیگر استفاده شده است و همچنین می توانید برای ورود به سیستم‌های Mac و Linux استفاده شود. - صفحه ۵

برنامه‌هایی با آیکون مخفی در Google Play Store

قرار دادن کد تبلیغ در یک برنامه روشی همه گیر است که توسعه دهندگان می‌توانند هزینه های خود را برای ارائه برنامه‌های رایگان یا ارزان جبران کنند. با این حال، برخی از سازندگان برنامه‌ها آنچه را که اساساً برنامه‌های تبلیغاتی مزاحم هستند را ایجاد کرده و آن به عنوان برنامه‌ای مفید نشان می‌دهند. - صفحه ۶



قفل صورت Pixel 4 به میزان Face ID آیفون ایمن نیست!

با اینکه تا کنون گوشی Pixel 4 منتشر نشده است اما شخصی توانسته است تا یک مشکل امنیتی در آن پیدا نماید. ویژگی بازگشایی قفل از طریق اسکن صورت در این گوشی حتی با چشم‌های بسته هم کار خواهد کرد. - صفحه ۷

Zynga هک شد!

نمونه‌ای از داده‌ی کاربران شامل نام آنان، آدرس ایمیل، IDهای افراد، پسوردهای هش شده، توکن ریست پسوردها، شماره تماس افراد، ID فیس بوک کاربران و IDهای اکانت کاربران Zynga برای سایت خبری The Hacker News ارسال گردیده است که تایید می‌کند این سایت هک شده است.

Zynga، توسعه دهنده بازی‌های اجتماعی، جدیدترین شرکت فناوری است که قربانی نقض ویرانگر داده‌ها گردیده است.

هکر سریالی "Gnosticplayers" به این سایت خبری گفته است که وی موفق به دستیابی به دیتابیسی حاوی بیش از ۲۱۸ میلیون رکورد اطلاعات کاربران دنیای بازی به همراه دوستانشان شده است.

Zynga در ابتدای سال ۲۰۰۷ تاسیس گردیده است که تنها چند سال بعد با بازی FarmVille به محبوبیت بالایی دست پیدا کرد، بازی که با آن توانست مالکیت MyMiniLife را هم نیز به دست آورد.

Zynga بیان نموده است که آنان بلافاصله تحقیقات را آغاز کرده‌اند و از شرکت ثالثی برای انجام تحقیقات و جرم یابی سایبری استفاده کرده‌اند.

توسعه دهنده این کمپانی گفته است که همچنین برای محافظت از حساب‌های کاربری آسیب دیده از ورود نامعتبر، اقداماتی انجام شده است. ام حداقل کاربران باید رمزعبور Zynga خود را فوراً تغییر دهند.

Zynga تا کنون از انتشار جزییات در خصوص این حمله خود داری نموده است.

گردآورنده: محمد مرتضوی

دیتاسنتری برای جرائم سایبری در پناهگاه سابق ناتو!

مسئولین آلمان اخیرا یک دیتاسنتر مربوط به جرائم سایبری که به صورت پنهانی در پناهگاه ۵۰۰۰ متر مربعی سابق ناتو قرار داشت با حمله پلیس به منطقه از دسترس خارج گردید.

این دیتاسنتر شامل تعداد بیشماری از وب سایت‌های غیرقانونی فروش مواد، اسلحه، داده‌های سرقت شده، اسناد و سایر مواد می-باشد.

این حمله روز جمعه گذشته در شهر کنار رودخانه ترابن-تراباخ به انجام رسید. براساس گزارش‌ها، بیش از ۶۰۰ عضو نیروی انتظامی در این عملیات شرکت داشتند. پلیس توانست با موفقیت از وسایل محافظتی این منطقه همچون درهای آهنی، نرده‌ها، سیم‌های خاردار و دوربین‌های مداربسته و همچنین "محافظت دیجیتال" این مرکز عبور و به داخل آن رخنه کند.

طبق گزارش‌ها، پلیس حدود ۲۰۰ سرور، تلفن همراه، اسناد و مقدار زیادی پول نقد کشف و ضبط کرده است. همچنین ۱۳ نفر که گفته می‌شود اقدامات شرورت کارانه در این مرکز دستگیر داشتند، دستگیر شدند.

به گفته‌ی پلیس، WallStreetMarket پیش از آنکه در ابتدای سال جاری از دسترس خارج شود، دومین فروشگاه زیر زمینی در دنیا بود که برروی این سرورها میزبانی می‌شده.

رییس دادستانی عمومی در کوبلنز بیان کرده است که این کار تنها همانند خراش ایجاد کردن به سطح شبکه‌های زیر زمینی است و پردازش اطلاعات موجود در داخل آن می‌تواند ماه‌ها ویا سال‌ها به طول انجامد.

گفته می شود یک مرد ۵۹ ساله هلندی که در این پناهگاه زندگی می‌کرده است، رهبری این مجموعه را به عهده دارد. مقامات می-گویند که وی با جنایات سازمان یافته در هلند ارتباط دارد و اولین بار این سرورها را در سال ۲۰۱۳ در ترابن-تراباخ تنظیم و راه اندازی کرده است.

گردآورنده: محمد مرتضوی

گوگل و ISPها در مقابل هم بر سر DNSهای رمزنگاری شده!

گوگل و موزیلا هردو خواهان آپدیت به روز رسانی مرورگرهایشان برای استفاده از ترافیک رمزنگاری شده در سطح DNS هستند. آنان اعلام کرده‌اند که با این کار حریم شخصی کاربران، بیشتر رعات خواهد شد و کاربران کنترل بهتری برروی اینکه چه کسی عادات رفتاری آنان را می‌بینند خواند داشت. اما ISPها علاقه‌ای به قفل کردن این اطلاعات ندارند و از قانون گذاران امریکایی خواسته‌اند تا از این اتفاق خودداری کنند.

استفاده از درخواست‌های نام دامنه به صورت رمزنگاری توسط گوگل و موزیلا در حال فراگیری است اما این درخواست در کنگره تبدیل به یک چالش شده است.

براساس منابع موجود در The Wall Street Journal، کمیته قضایی مجلس نمایندگان آمریکا در حال تحقیق برروی مرورگر گوگل کروم با ساختار استفاده از DNS برروی پروتکل رمزنگاری شده‌ی TLS هستند.

براساس ادعای این غول جستجو، این تکنولوژی از شنود سارقین اطلاعات و شرکای تجاری سوم شخص برروی نام دامنه‌ای پیشگیری می‌کند.

شرکت‌های سرویس دهنده‌ی اینترنت از این بابت نگران هستند که قطع دسترسی آنان به داده‌هایی که کاربران مورد جستجو و مرور قرار می‌دهند، برای گوگل یک مزیت ناعادلانه است. زیرا گوگل می‌تواند از این داده‌ها برای نمایش تبلیغات استفاده خواهد کرد. بنابراین ISPها به کنگره درخواست کرده‌اند که موضوع را به دلایل ضد انحصاری بررسی کند.

در ۱۳ سپتامبر کمیته قضایی در نامه‌ای از گوگل سوال کرد که آیا آنان می‌خواهند از داده‌های رمزگذاری شده برای مقاصد تجاری استفاده کنند یا خیر؟ در حالی که شرکت گوگل همچنان پاسخی به این نامه نداده است، در بیانات خود گفته است که این حرکت کنترل بیشتری را به مصرف کنندگان می‌دهد. همچنین گوگل ادعا می‌کند که مردم را وادار به استفاده از DNS رمزگذاری شده نمی‌کند.

در تاریخ ۱۹ سپتامبر، ائتلافی از ISPها نامه‌ای به کنگره ارسال کردند که ابراز نگرانی کردند که این پروتکل می‌تواند گوگل را به عنوان ارائه دهنده اصلی جستجوی DNS متمرکز کند، به طور واقعی رقابت را متوقف می‌کند.

این ائتلاف خواستار جلوگیری از پیاده سازی این سرویس توسط گوگل شدند.

EFF با حمایت خود از DNS رمزنگاری شده مطرح کرد که استفاده از DNS بر پروتکل‌های رمزنگاری شده همچون TLS و HTTPS آخرین حفره‌ی بزرگ امنیتی در دنیای اینترنت است.

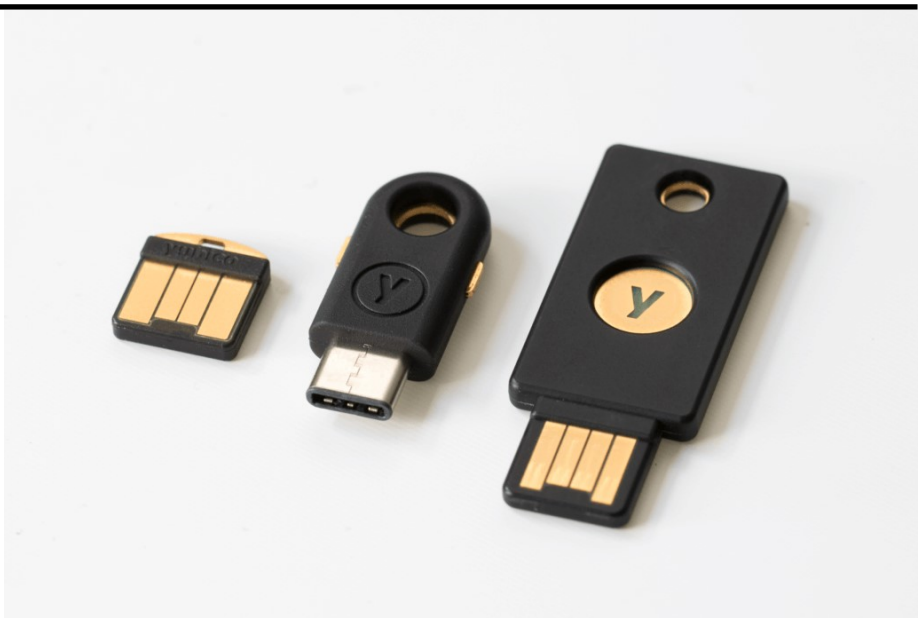
EFF همچنان بیان کرده است که برای جلوگیری از انحصار این امر توسط گوگل بهتر است تمامی ISPها این خدمت را ارائه نمایند.

گوگل قصد دارد تا به آرامی و در گام اول تنها برای یک درصد از کاربران گوگل کروم این ویژگی را در ماه اکتبر فعال نماید.

شرکت فایرفاکس نیز در مرورگر موزیلای خود در حال پیاده سازی این ویژگی است و احتمال می‌رود که تا سال آینده این ویژگی به بهره برداری برسد.

گردآورنده: محمد مرتضوی

استفاده از کلیدهای امنیتی Yubico برای ورود به سیستم‌های ویندوزی



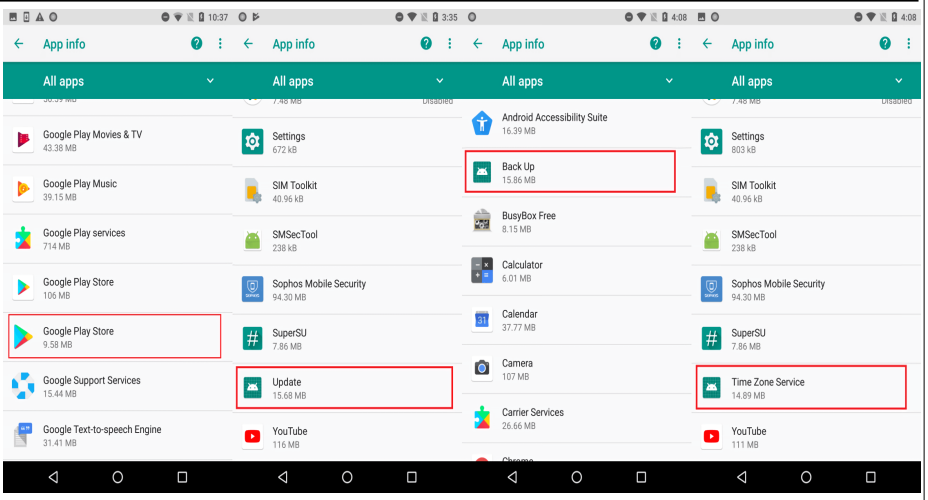
از کلیدهای Yubico قبلاً برای محافظت از Gmail، Dropbox ، مدیران رمز عبور و موارد دیگر استفاده شده است و همچنین می توانید برای ورود به سیستم‌های Mac و Linux استفاده شود. پس از شش ماه آزمایش، این شرکت اکنون یک نسخه پایدار از Yubico Login for Windows Application را منتشر کرده است.

Yubico می‌نویسد که این برنامه برای افرادی طراحی شده است که دارای حساب های محلی در رایانه‌های ویندوز ۷، ویندوز ۸.۱ یا ویندوز ۱۰ هستند. پس از نصب بر روی دستگاه ویندوز، از کلید Yubico می توان بعنوان لایه دوم تأیید اعتبار استفاده کرد. کاربران هنوز هم باید رمزهای عبور خود را تایپ کنند، اما برای تکمیل مراحل ورود به سیستم، باید USB را وارد کنید.

در اوایل این هفته، گوگل اعلام کرد که طی سال گذشته با Yubico همکاری کرده است تا یک کلید سخت افزاری USB-C را تهیه کند. ۴۰ دلار قیمت دارد، با دستگاه های Android، Chrome OS، macOS و Windows سازگار است و در کنار انواع موجود USB-A / NFC و Bluetooth / USB Titan Security Key / NFC به فروش می‌رسد.

گردآورنده: امیرحسین ضرغامی

برنامه‌هایی با آیکون مخفی در Google Play Store



قرار دادن کد تبلیغ در یک برنامه روشی همه گیر است که توسعه دهندگان می‌توانند هزینه های خود را برای ارائه برنامه‌های رایگان یا ارزان جبران کنند. با این حال، برخی از سازندگان برنامه‌ها آنچه را که اساساً برنامه-های تبلیغاتی مزاحم هستند را ایجاد کرده و آن به عنوان برنامه‌ای مفید نشان می‌دهند.

محققان تهدید در SophosLabs مستقر در استرالیا اخیراً ۱۵ برنامه را کشف کردند که به نظر نمی‌رسد به جز نمایش تبلیغات انبوه در دستگاه‌های Android، کاری انجام دهند. این برنامه‌ها دارای اسامی و توضیحات محصولی همچون برنامه‌ی QR خواندن تا برنامه‌های ویرایش تصویر هستند.

آنچه که این برنامه ها را حتی توطئه آمیز تر می‌کند این است که آن‌ها آیکون‌های خود را مخفی می‌کنند تا حذف آن‌ها از تلفن سخت تر شود. برخی از آن‌ها حتی خود را در تنظیمات با نام‌ها و نمادهای مختلف استتار می‌کنند.

Sophos نمونه‌ای از برنامه‌هایی به نام Flash On Calls & Messages را معرفی نمود. هنگامی که این برنامه راه اندازی شود، پیامی را نمایش می‌دهد که می‌گوید: "این برنامه با دستگاه شما ناسازگار است!" سپس آن برنامه App Store را باز می‌کند و Google Maps را نشان می-دهد تا کاربر را فریب دهد که مشکل از برنامه مربوط به نقشه است.

پس از آن، آیکون خود را پنهان می‌کند تا در Luncher دیده نشود. برنامه‌های دیگر موجود در لیست نیز این کار را انجام می دهند، اگرچه برخی از آن‌ها در راه اندازی اولیه این کار را انجام نمی‌دهند. برخی از آن‌ها قبل از مخفی کردن آیکون منتظر خواهند ماند تا نصب کامل شود.

بدتر این است که این برنامه‌ها با استفاده از نام و آیکون دیگری در تنظیمات Android سعی در فریب کاربر و جلوگیری از حذف خود دارند. نه نفر از ۱۵ نفر از توسعه دهندگان این برنامه‌ها از این روش برای جلوگیری از شناسایی استفاده کرده اند. این برنامه از نام‌هایی همانند Backup، Update، Google Play Store و... برای خود استفاده کرده‌اند.

۱۵ برنامه مخرب کشف شده، از Google Play حذف شده است. با این حال، آمار بازار Play نشان داد که این برنامه‌ها در مجموع قبلاً در بیش از ۱.۳ میلیون دستگاه در سراسر جهان بارگیری و نصب شده‌اند.

گردآورنده: محمد مرتضوی

قفل صورت Pixel 4 به میزان Face ID آیفون ایمن نیست!

با اینکه تا کنون گوشی Pixel 4 منتشر نشده است اما شخصی توانسته است تا یک مشکل امنیتی در آن پیدا نماید. ویژگی بازگشایی قفل از طریق اسکن صورت در این گوشی حتی با چشم‌های بسته هم کار خواهد کرد.

ویژگی بازگشایی قفل گوشی بر اساس اسکن صورت در گوشی‌های Pixel 4 بسیار سریع است. سنسورهای Radar در کسری از ثانیه و به محض برداشتن گوشی، شروع به پردازش کرده و به سرعت قفل گوشی را باز می‌کنند.

سیستم بازگشایی قفل صفحه در Pixel 4 همانند Face ID در اپل می باشد که دارای مشکلات مشابهی می‌باشند. اما براساس گزارش BBC، گوشی Pixel 4 عملیات قفل گشایی را حتی با چشمانی بسته نیز انجام خواهد داد این در حالی است که اگر در آیفون شما مستقیما به سنسور نگاه نکنید قفل صفحه باز نخواهد شد.

گوگل در صفحات پشتیبانی خود تایید کرده است که این ویژگی بی نقص نیست و این موضوع صحت دارد.

ممکن است شرایط زیادی برای سو استفاده از این نقص نباشد اما ممکن است این نقص زمانی استفاده شود که صاحب گوشی خواب است.

گوگل برای این موضوع هیچ تدابیری را در نظظر نگرفته است و به احتمال زیاد تا هفته آینده این محصول به همین گونه که هست منتشر و به فروش رسد. اما گوگا اعلام کرده است که این مورد نیز همانند سایر ویژگی-است که این مورد نیز همانند سایر ویژگی‌های این شرکت به مرور زمان بهبود خواهد یافت.

تا رفع این مشکل می‌توان این ویژگی را غیر فعال کرد. در زمان غیرفعال کردن این ویژگی کاربر مجبور است تا از رمز عبور برای قفل گشایی گوشی خود استفاده نماید.

برای غیرفعال کردن این ویژگی به آدرس زیر باید مراجعه نمود:

Settings > Display > Advanced > Lock screen display

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.