شماره سی و سوم - مهر ۱۳۹۸

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

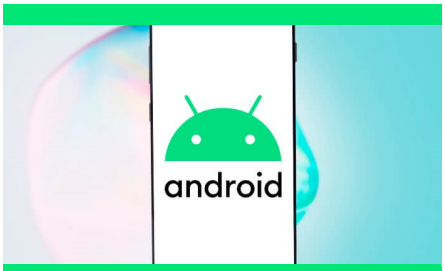
در این شماره خواهید خواند:

حمله Strontium حداقل به ۱۶ سازمان ورزشی و ضد دوپینگ

با آمادگی ژاپن برای بازی های المپیک ۲۰۲۰ توکیو، هکرها سرعت و پختگی حملات خود را افزایش داده اند. مرکز اطلاعات تهدید مایکروسافت اعلامیه‌ای درباره آنچه که به نظر می رسد حمله سایبری هماهنگ که به سازمان های ورزشی و ضد دوپینگ ملی و بین المللی ارسال شده است، صادر کرده است.- صفحه ۲

باج افزار با نام جعلی آپدیت برای ویندوز!

گروهی که به تازگی در فضای اینترنت شروع به فعالیت کرده‌اند مردم را فریب می‌دهند که باید سیستم عامل ویندوز خود را بروزرسانی کنند.. سپس اقدام به نصب باج افزار برروی کامپیوتر قربانیان می‌کنند. - صفحه ۵



جاسوسی از طریق دوربین موبایل‌های اندرویدی

محققان شرکت تست امنیتی Checkmarx از چندین آسیب پذیری هشدار دهنده در برنامه های دوربین چندین فروشنده گوشی های هوشمند اندرویدی از جمله گوگل و سامسونگ پرده برداشتند. این آسیب پذیری از آن زمان تا به حال برطرف شده است و می توانید آخرین نسخه برنامه را بروز رسانی کنید. - صفحه ۳

افشای اطلاعات ۱ میلیون نفر از کاربران T-Mobile

در آخرین ماه سال ۲۰۱۹ همچنان نشت اطلاعات یکی از داغ‌ترین مباحث موجود در میان کارشناسان امنیت و هکرها می‌باشد. اما این بار این رخداد برای شرکت بزرگ اپراتوری T-mobile رخ داده است و بیش از یک میلیون نفر از کاربران شرکت T-mobile اطلاعاتشان افشا و در دسترس مهاجمین قرار گرفته است. - صفحه ۶

Disney+ هک شد!

پیاده سازی سرویس‌های استریم با بیش از ۱۰ میلیون کاربر همواره دارای مشکلات فراوانی بوده است و Disney+ هم از این قاعده مستثنی نیست. علاوه بر مشکلات تکنیکی، گزارشاتی موجود است که اطلاعات صدها اکانت کاربری توسط هکرها، به سرقت رفته است. - صفحه ۴

سیستم‌های دولتی لوئیزیانا درگیر باج افزار!

مهاجمان اینترنتی شهرهای زیادی از امریکا را تحت حملات خود قرار دادند. این بار نوبت به لوئیزیانا رسیده است تا هدف باج افزارها شود. در تعدادی توئیت، فرماندار جان بل ادواردز نوشت که تیم امنیت سایبری دولت در پاسخ به یک حمله باج افزاری تبلیغاتی که برروی برخی از سرورها تأثیر داشته است در حال فعالیت هستند. - صفحه ۷

حمله Strontium حداقل به ۱۶ سازمان ورزشی و ضد دوپینگ

با آمادگی ژاپن برای بازی های المپیک ۲۰۲۰ توکیو، هکرها سرعت و پختگی حملات خود را افزایش داده اند. مرکز اطلاعات تهدید مایکروسافت اعلامیه‌ای درباره آنچه که به نظر می رسد حمله سایبری هماهنگ که به سازمان های ورزشی و ضد دوپینگ ملی و بین المللی ارسال شده است، صادر کرده است. به نظر می‌رسد این کار یک گروه مشهور هکر روسی است که پس از آنکه ورزشکاران المپیک روسی متهم به تقلب در طی این رقابت ها شدند، در پی تلافی در آمدند.

مایکروسافت ادعا می کند که یک گروه هکر شناخته شده به نام Strontium یا Fancy Bear حداقل به ۱۶ سازمان ورزشی و ضد دوپینگ حمله کرده است. این حملات ماه گذشته پس از آن آغاز شد که آژانس جهانی مبارزه با دوپینگ اعلام کرد که روسیه با ممنوعیت تمام مسابقات مهم ورزشی از جمله مسابقات جهانی و المپیکهای آتی که قرار است سال آینده در توکیو برگزار شود روبرو است.

مرکز اطلاعات تهدید این شرکت اولین حمله را در تاریخ ۱۶ سپتامبر مشاهده کرد و هیچ سازمانی را که مورد هدف قرار گرفته است، معرفی نکرده است. این حملات شامل ترکیبی از در هم شکستن رمزعبور، فیشینگ ، بهره برداری از دستگاه های IoT و همچنین نرم افزارهای منبع باز و بدافزارهای سفارشی بود. این روش ها بطور معمول توسط استرانسیوم علیه دولت ها ، اتاق های فکر ، گروه های حقوق بشر و سازمان های مختلف دیگر استفاده می شود.

خبر خوب این است که بیشتر حملات ناموفق بودند. مایکروسافت به سازمان های آسیب دیده اطلاع داد و پیشنهاد داد تا به افرادی که درخواست کمک کردند کمک کند. برای محافظت از خود در برابر هک های Strontium ، این شرکت توصیه می کند که در همه حساب های ایمیل خود از تأیید هویت دو عاملی استفاده کنند و یاد بگیرید چگونه نقشه های فیشینگ را شناسایی کنند ، تا خطر نشت اطلاعات حساس از سازمان خود را برطرف کنند.

دولت روسیه قبلاً با حمله هایی که اطلاعات پزشکی صدها ورزشکار تقریباً از ۳۰ کشور جهان و همچنین یک سازمان تسلیحات شیمیایی و نیروگاه هسته ای آمریکا را هدف قرار داده بود. مایکروسافت امیدوار است که بحث های بین المللی را درباره اقدامات امنیت سایبری که می تواند از حملات آینده جلوگیری کند ، شایان ذکر است که CrowdStrike دریافت که هکرهای تحت حمایت دولت روسیه سریعتر از سایر کشورها هستند.

گردآورنده: امیرحسین ضرغامی

جاسوسی از طریق دوربین موبایل‌های اندرویدی

محققان شرکت تست امنیتی Checkmarx از چندین آسیب پذیری هشدار دهنده در برنامه های دوربین چندین فروشنده گوشی های هوشمند اندرویدی از جمله گوگل و سامسونگ پرده برداشتند. این آسیب پذیری از آن زمان تا به حال برطرف شده است و می توانید آخرین نسخه برنامه را بروز رسانی کنید.

این تیم تحقیقات خود را با نگاهی به برنامه دوربین Google در گوشی های Pixel 2 XL و Pixel 3 آغاز کردند. آن‌ها آسیب پذیری های متعددی در رابطه با مشکلات دور زدن مجوز مشاهده کردند که به مهاجمی امکان می‌دهد از برنامه استفاده کند تا از طریق یک برنامه سرکش عکس بگیرد و فیلمبرداری کند.

این حمله حتی اگر تلفن قربانی قفل شده باشد، صفحه خاموش و هنگام تماس صوتی نیز امکان پذیر است.

از دیگر سناریوهای حمله این است که دسترسی به عکس ها و فیلم های ذخیره شده و حتی جمع آوری داده‌های GPS که بتوان موقعیت مکانی کاربر را پیدا کرد. این روش همچنین در برنامه دوربین سامسونگ نیز انجام پذیر است.

برای نشان دادن آسیب پذیری‌های مختلف، تیم Checkmarx یک برنامه اثبات مفهوم را طراحی کرد و شبیه یک برنامه معمول آب و هوا بود. با استفاده از آن، آن‌ها با موفقیت توانستند بدون اطلاع کاربر ، عکس و فیلم، داده GPS بگیرند و حتی صدا را از هر دو طرف مکالمه در حین مکالمه صوتی نیز ضبط کنند.

تیم Checkmarx با مسئولیت پذیری تمام یافته‌های این آسیب پذیری را به Google اطلاع داد که تأیید کردند که این موضوع فقط به برنامه دوربین آن‌ها محدود نمی‌شود، بلکه به اکوسیستم عمومی Android بر می‌گردد.

گوگل در بیانیه‌ای که به Checkmarx صادر کرد، گفت که این موضوع از طریق بروزرسانی Play Store به برنامه Google Camera در ژوئیه سال ۲۰۱۹ بر روی دستگاه‌های Google تأثیرگذار رسیدگی شده است، این پچ در دسترس همه شرکا قرار گرفته است. هم گوگل و هم سامسونگ آن‌ها آسیب پذیری Checkmarx را بعد از انتشار وصله امنیتی تأیید کردند که مشکل برطرف شده است.

گردآورنده: امیرحسین ضرغامی

Disney+ هک شد!

پیاده سازی سرویس‌های استریم با بیش از ۱۰ میلیون کاربر همواره دارای مشکلات فراوانی بوده است و Disney+ هم از این قاعده مستثنی نیست. علاوه بر مشکلات تکنیکی، گزارشاتی موجود است که اطلاعات صدها اکانت کاربری توسط هکرها، به سرقت رفته است.

در روز شروع، کاربران Reddit و Twitter گزارش داده‌اند که از ناحیه‌ی کاربری خود خارج شده‌اند و تمامی پسوردهای آنان تغییر پیدا کرده است. اطلاعات هویتی این کاربران برروی گروه‌های هک از ۳ تا ۷ دلار قیمت گذاری شده است.

بر اساس ادعای Diseny آنان هک نشده‌اند و هیچ شواهدی مبنی بر افشای اطلاعات پیدا نکرده‌اند. براساس سخنان یکی از اعضای این کمپانی: "ما به طور مداوم سیستم‌های امنیتی خود را بازرسی می‌کنیم و وقتی به سیستم مشکوک می‌شویم، حساب کاربری را قفل می‌کنیم و کاربر را برای انتخاب یک رمز عبور جدید راهنمایی می‌کنیم."

برخی از کاربران تحت تاثیر این جریان اقرار کرده‌اند که از حساب کاربری دیگران استفاده می‌کردند. اما برخی از کاربران از پسوردهای یکتا و غیر تکراری استفاده می‌کردند.

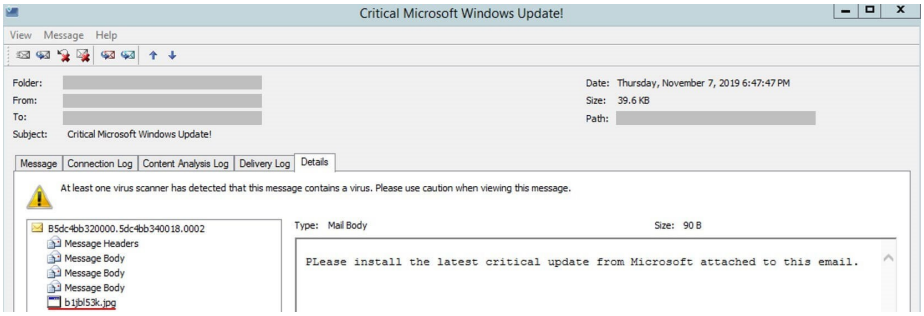
شاید هکرها از طریق اطلاعات احراز هویتی لو رفته از سایر وب سایت‌ها به اطلاعات کاربران دسترسی پیدا کرده‌اند یا شاید هم آنان از ابزارهایی همچون Keylogger ها استفاده کرده‌اند. براساس بیانات Disney: "میلیون‌ها نام کاربری و رمزعبور از نقص‌های پیشین موجود در سایر کمپانی‌ها لو رفته است. پیش از فعال سازی سرویس Disney+، که این اطلاعات در فضای وب به فروش رسیده است."

براساس ادعای Disney تنها تعداد کمی از کاربران این سیستم استریم تحت تاثیر قرار گرفته‌اند.

حال با تمامی شواهد موجود این کمپانی ادعا می‌کند که نشت اطلاعات از طریق همکاران وی و نرم افزارهای سوم شخص صورت گرفته است. حال باید دید که در آینده چه ابعاد دیگری از این هک اطلاع رسانی خواهد شد..

گردآورنده: محمد مرتضوی

باج افزار با نام جعلی آپدیت برای ویندوز!



گروهی که به تازگی در فضای اینترنت شروع به فعالیت کرده‌اند مردم را فریب می‌دهند که باید سیستم عامل ویندوز خود را بروزرسانی کنند.. سپس اقدام به نصب باج افزار برروی کامپیوتر قربانیان می‌کنند.

محققان SpiderLabs ایمیل‌های اسپمی کشف کرده‌اند که با عنوان جدیدترین بروز رسانی سیستم عامل مایکروسافت به قربانیان ارسال شده و از آنان می‌خواهد تا آپدیت‌های حیاتی مورد نیاز را دانلود و نصب نمایند. شرکت مایکروسافت به هیچ عنوان به روز رسانی‌های خود را از طریق ایمیل به کاربران ارسال نمی‌کند.

این ایمیل شامل تنها یک جمله است با ۲ حروف بزرگ در اول آن که این کار آن را بیش از پیش غیرواقعی می‌کند.

از دریافت کنندگان تقاضا می‌شود تا برروی دکمه‌ی Update کلیک کنند. بعد از کلیک برروی این دکمه یک فایل با پسوند jpg. دانلود می‌شود که یک فایل اجرایی Net. برای دانلود سایر محتوای مورد نیاز برروی سیستم قربانی است.

با کلیک برروی این فایل یک فایل اجرایی دیگر دانلود می‌گردد. نام این فایل bitcoingenerator.exe از یک کاربر با نام misterbtc2020 در گیت هاب. این فایل جدید هم نیز یک فایل Net. همانند قبلی می‌باشد.

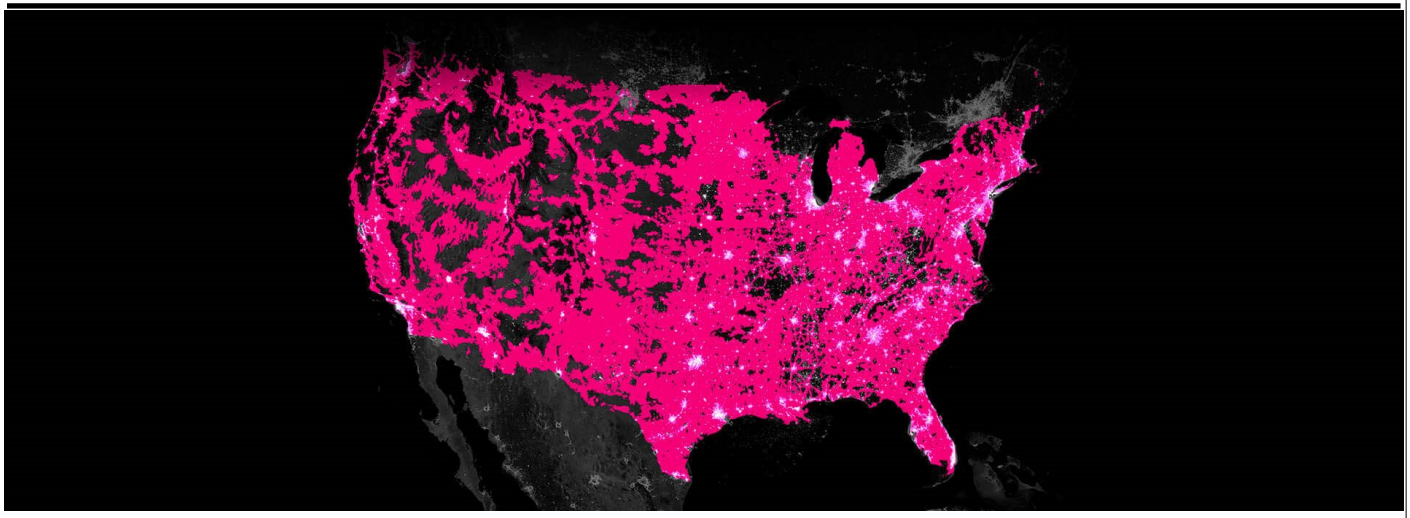
فایل bitcoingenerator.exe، اقدام به رمزنگاری تمامی فایل‌های کاربر و تغییر پسوند آنان می‌گردد. این باج افزار همچنین پسوند آنان می‌گردد. این باج افزار همچنین یک نسخه از خود را در شاخه اصلی هر درایو با نام bot.exe قرار می‌دهد.

قربانی یک فایل با نام Cyborg_DECRYPT.txt برروی دسکتاپ خود می‌تواند پیدا کند که مبلغ ۵۰۰ دلار را برای باز کردن قفل فایل‌ها درخواست کرده است.

زمانی که محققان امنیتی ساختار این فایل را مورد بررسی قرار می‌دادند آن‌ها سه نمونه دیگر و یک Builder یافت کردند. حتی یک ویدیو YouTube شامل یک لینک به Builder برروی گیت هاب یافت گردید که دارای ۲ مخزن (Repository) بود: یکی با فایل باینری Builder و دیگری با یک لینک به نسخه‌ی روسی این باج افزار.

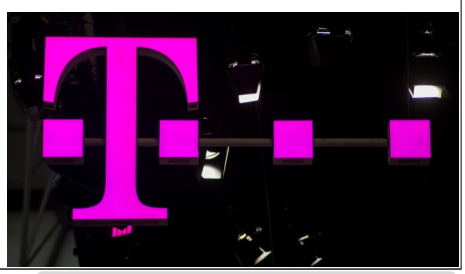
گردآورنده: محمد مرتضوی

افشای اطلاعات ۱ میلیون نفر از کاربران T-Mobile



در آخرین ماه سال ۲۰۱۹ همچنان نشت اطلاعات یکی از داغ‌ترین مباحث موجود در میان کارشناسان امنیت و هکرها می‌باشد. اما این بار این رخداد برای شرکت بزرگ اپراتوری T-mobile رخ داده است و بیش از یک میلیون نفر از کاربران شرکت T-mobile اطلاعاتشان افشا و در دسترس مهاجمین قرار گرفته است.

تیم امنیتی T-mobile این دسترسی مخرب به داده‌های کاربران را از دسترس خارج کرده است و اقدامات صورت گرفته را طی یک گزارش به مقامات ارائه نموده است. داده‌های قابل دسترسی توسط مهاجمان شامل نام، آدرس، صورتحساب، شماره تلفن، شناسه حساب و جزئیاتی مانند میزان پرداخت و ویژگی‌هایی است که در آن قرار دارد.



هیچ گونه اطلاعات مالی یا رمزعبوری در معرض دید و نشت قرار نگرفته است و این شرکت به کاربرانی که داده‌هایشان در معرض حمله قرار گرفته است هشدار داده است. این شرکت طبق مقررات ارتباط از راه دور به کاربران اطلاع داده است.

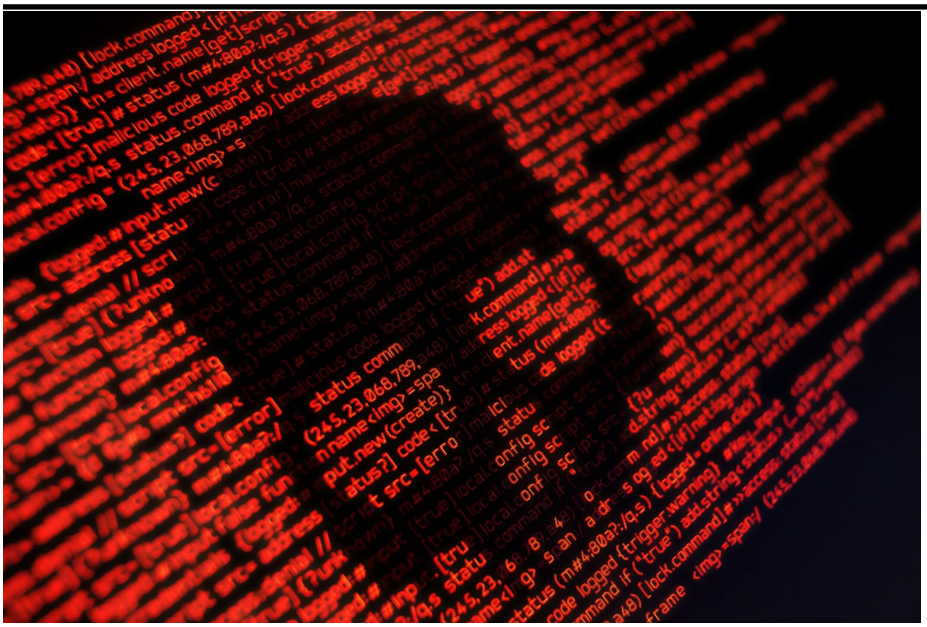
مقیاس کلی این حمله ۱.۵ درصد از ۷۵ میلیون کاربر این شرکت برآورد شده است. تیم امنیتی برای اولین بار متوجه این حمله در اوایل ماه جاری شده است. با این حال، T-Mobile نگفته است که چه مدت حمله قبل از متوقف شدن در جریان بوده است. در حالی که داده های در معرض آسیب خیلی خطرناک و حیاتی نیست، اما می‌تواند برای سرقت هویت آنلاین و کلاهبرداری استفاده شود.

این حمله به دنبال نقض داده‌های فیس بوک است که شماره‌تلفن ۴۰۰ میلیون کاربر را افشا کرده و وجود یک حادثه DoorDash که در آن مهاجمان توانستند به جزئیات مالی نزدیک به ۵ میلیون تاجر و مشتری دست پیدا کنند.

طبق معمول در این نوع شرایط ، بهتر است رمز ورود خود را تغییر دهید حتی اگر توسط T-Mobile به شما اطلاع داده نشده باشد. همچنین هرگز از گذرواژه‌های خود در سرویس‌ها یا وب سایت‌های مختلف مجدد استفاده نکنید.

گردآورنده: محمد مرتضوی

سیستم‌های دولتی لوئیزیانا درگیر باج افزار!



مهاجمان اینترنتی شهرهای زیادی از امریکا را تحت حملات خود قرار دادند. این بار نوبت به لوئیزیانا رسیده است تا هدف باج افزارها شود.

در تعدادی توئیت، فرماندار جان بل ادواردز نوشت که تیم امنیت سایبری دولت در پاسخ به یک حمله باج افزاری تبلیغاتی که برروی برخی از سرورها تأثیر داشته است در حال فعالیت هستند.

در هنگام شناسایی این حمله، دفتر خدمات فناوری (OTS) سرورهای دولتی را برای احتیاط خاموش کرد و این امر بر ایمیل‌ها، وب سایت‌ها و سایر برنامه‌های آژانس‌های دولتی تأثیر گذاشت.

فرماندار همچنین افزود: "قطع سرویس به دلیل واکنش تهاجمی به OTS برای جلوگیری از گسترش آلودگی اضافی سرورهای دولتی است، نه به دلیل حمله باج افزار."

سرورهای دولتی که مدیریت ارتباطات ایمیلی و برنامه‌های داخلی را بر عهده دارند، تحت تأثیر قرار گرفتند، همچنین چندین وب سایت از جمله اداره وسایل نقلیه موتوری، دفتر اصلاحات، دفتر فرمانداری ایالت لوئیزیانا و موارد دیگر نیز تحت تاثیر قرار گرفت.

دفتر امور کودکان و خانواده لوئیزیانا نیز چندین ساعت تحت‌تاثیر قرار گرفت.

در ماه جولای، لوئیزیانا با حمله باج افزار که سه مدرسه را تحت تأثیر قرار داد، مواجه شد و منجر به اعلام وضعیت اضطراری در سطح کشور شد. همانطور که OTS حمله اخیر را کشف و متوقف کرد، چنین اقدام شدیدی لازم نبود.

برخلاف بسیاری از موارد دیگر باج افزارهایی که به سیستم‌های دولتی رخنه کرده‌اند، هیچ گونه تخرب داده‌ای از این حمله وجود ندارد و از دولت باجی گرفته نشده است. در اوایل سال جاری، در شهر Riviera Beach در فلوریدا، به پرداخت ۶۰۰،۰۰۰ دلار به هکرها موافقت شد، همچنین در یکی دیگر از مکان‌های فلوریدا، Lake City نیز حدود ۵۰۰۰۰۰ دلار بیت کوین به هکرها از سوی دولت پرداخت کردند.

در ماه آگوست، بیش از ۲۰ نهاد دولتی محلی در تگزاس تحت تأثیر "حمله باج افزاری هماهنگ" قرار گرفتند. از اکتبر سال جاری، ۸۱ حادثه باج افزاری که دولت‌های محلی آمریکا را تحت تاثیر قرار داده است، رخ داده 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

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.