شماره پانزدهم - فروردین ۱۳۹۷

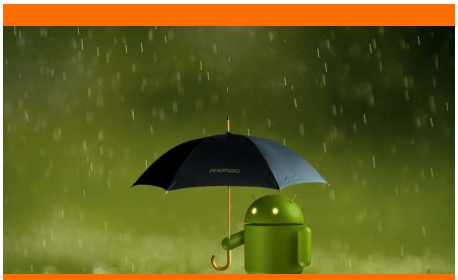
خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:

نقص هسته در برابر حفاظت از بدافزار

مایکروسافت نقص مهم هسته برنامه محافظتی خود را Patch کرد. مهاجم می تواند یک سیستم را کنترل کند و انواع آسیب ها را به وجود آورد. - صفحه ۲

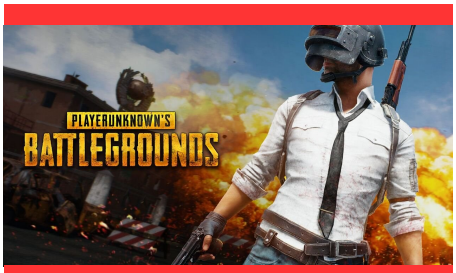


برخی از فروشندگان گوشی های اندروید در خصوص وصله های امنیتی روند درستی ندارند

محققان یک آزمایشگاه امنیتی در آلمان تحقیقات تازه ای را شروع کرده اند. بعد از مهندسی معکوس برروی کد سیستم عامل ۱۲۰۰ گوشی موبایل، Karsten Nohl و Jakob Lell متوجه شدند که برخی از شرکت‌های تولید کننده در خصوص وصله-های امنیتی روند درستی را طی نکرده اند. - صفحه ۲

بر طرف شدن چهار آسیب پذیری اساسی در محصولات Adobe

Adobe صبح روز سه شنبه چهار آسیب پذیری مهم را در محصولات Flash Player و InDesign به عنوان بخشی از بولتن امنیتی ماه آوریل April Security Bulletin که به طور منظم برنامه ریزی شده است، برطرف کرد. در مجموع، ۱۹ Adobe نسخه را برای محصولاتی از جمله Adobe Experience Manager، Adobe InDesign CC، Adobe Digital Editions و PhoneGap Push منتشر کرد. - صفحه ۳



بدافزاری که کامپیوتر شما را تا زمان نصب بازی PUBG، گروگان خواهد گرفت.

دنیای کامپیوترها تاریخچه‌ی طولانی از بدافزارهایی همچون جاسوس افزارها، ویروس‌ها و تبلیغ افزارها دارد. در تحقیقات اخیر از سوی تیم MalwareHunterTeam به مورد جالبی برخورده است. باج افزار جدیدی که فایل‌های کاربران را تا زمانی که آنان بازی PlayerUnknown's Battlegrounds را اجرا نکنند، رمزنگاری خواهد نمود. - صفحه ۴

Microsoft office، تروجان را بدون نیاز به Macroها اجرا می کند

نویسندگان بدافزار لزوما نیاز به فریب کاربران برای فعال کردن ماکروها برای اجرای کدمخرب ندارند. یک تکنیک جایگزین وجود دارد که یکی از مزایای دیگر ویژگی های دفاتر قانونی است. این ویژگی به نام تبادل اطلاعات دینامیکی مایکروسافت (DDE) نامیده می شود و اجازه می دهد که یک برنامه آفیس، دیتاهایی را از اپلیکیشن آفیس دیگر بارگذاری کند. - صفحات ۶ و ۷

نقص هسته در برابر حفاظت از بدافزار

مایکروسافت نقص مهم هسته برنامه محافظتی خود را Patch کرد. مهاجم می تواند یک سیستم را کنترل کند و انواع آسیب ها را به وجود آورد.

مایکروسافت یک آسیب پذیری اکتیو از راه دور را که بر روی سیستم محافظت فایلهای مخرب mpengine.dll تاثیر می گذارد را patch کرده است - که قابلیت اسکن، شناسایی و تمیز کردن برای نرم افزار های مختلف ضد ویروس و ضد جاسوسی مایکروسافت از جمله Windows Defender را فراهم می کند.

آسیب پذیری ها بحرانی حیاتی تلقی می شوند.

مایکروسافت می گوید برای بهره برداری از آسیب پذیری، یک فایل به طور خاص ساخته شده باید توسط یک نسخه ی unpatched از مایکروسافت Malware Protection Engine اسکن شود. مهاجم می تواند فایل را به طرق مختلف راه اندازی کند - با استفاده از یک وب سایت مخرب ،از طریق ایمیل، با آپلود آن به یک پوشه مشترک یا حتی از طریق یک سرویس پیام رسانی.

مهاجم که با موفقیت از آسیب پذیری سوء استفاده می کند می تواند سیستم کاربررا کنترل کرده و اقدام به نصب نرم افزار کند. مهاجمین بد تر نیز می توانند داده ها را مشاهده، تغییر یا حذف کنند و حتی میتوانند حساب های جدید با دسترسی کامل برای کاربرایجاد کنند.

به گفته مایکروسافت، به روز رسانی هسته، Microsoft Malware Protection بررسی و اسکن فایل های ویژه را اصلاح می کند.

به روز رسانی های هسته Microsoft Malware Protection معمولا یکبار در ماه منتشر می شوند، گرچه در مواردی مانند این، استثنائاتی نیز وجود دارد.

خوشبختانه، هیچ اقدامی توسط کاربران نهایی لازم نیست. مکانیسم ساخته شده برای شناسایی و استقرار به روز رسانی باید این پچ را به طور خودکار در عرض ۴۸ ساعت پس از انتشار منتشر کند، هرچند مایکروسافت می گوید که زمان دقیق آن بستگی به نرم افزار مورد استفاده، اتصال اینترنت شما و تنظیمات زیرساخت دارد.

گردآورنده: سمیه نیاخلیلی

بر طرف شدن چهار آسیب پذیری اساسی در محصولات Adobe

Adobe صبح روز سه شنبه چهار آسیب پذیری مهم را در محصولات Flash Player و InDesign به عنوان بخشی از بولتن امنیتی ماه آوریل April Security Bulletin که به طور منظم برنامه ریزی شده است، برطرف کرد.

در مجموع، ۱۹ Adobe نسخه را برای محصولاتی از جمله Adobe Experience Manager، Adobe InDesign CC، Adobe Digital Editions و PhoneGap Push منتشر کرد.

بر طبق Adobe، "از هر گونه سوءاستفاده کنترل نشده برای هر مسئله ای که در این بروزرسانی ها مطرح شده اطلاع ندارد". علاوه بر این، جزئیات خاصی برای هر CVE هنوز منتشر نشده است.

جدی ترین اشکالات مربوط به Adobe Flash Player۲۹.۰.۰.۱۱۳ و نسخه های قبلی است. Adobe ذکر کرد: "بهره برداری موفقیت آمیز می تواند منجر به اجرای کد دلخواه در سیستم کاربر شود."

نسخه های تحت تاثیر فلش پلیر عبارتند از Adobe Flash Player Desktop Runtime، Adobe Flash Player برای گوگل کروم و Adobe Flash Player برای Microsoft Edge و IE 11 شامل CVE-2018-4932 تا CVE-2018-4938.

سه مورد از چهار آسیب پذیری ای که دارای اهمیت هستند عبارتند از آسیب پذیری use-after-free (CVE-2018-4932) که می تواند یک حمله کد از راه دور را به وجود آورد، آسیب پذیری دیگر (CVE-2018-4935) شرایط را برای افشای اطلاعات ناخواسته فراهم میکنند و یک خطای خارج از محدوده (CVE-2018-4937) ایجاد می کند که می تواند شرایط مناسب برای حملات انجام شده با کد را ایجاد کند.

Mateusz Jurczyk و Silvanovich از گروه Google Project Zero برای پیدا کردن چهار اشکال Adobe Flash Player قدردانی شدند .از لین وانگ از دانشگاه Beihang نیز برای کشف یکی از آسیب پذیری های مهم Flash Player (CVE-2018-4932) قدردانی شد.

Adobe از کاربران Adobe Flash Player Desktop Runtime برای ویندوز، مکینتاش و لینوکس درخواست کرد برای به روز رسانی در Adobe Flash Player۲۹.۰.۰.۱۴۰ از طریق مکانیزم به روز رسانی محصولات یا با مراجعه به مرکز دانلود Adobe Flash Player اقدام کنند.

Adobe Flash Player برای مایکروسافت Edgeو اینترنت اکسپلورر ۱۱ نیز بعدا در روز سه شنبه منتشر خواهد شد.

یکی دیگر از آسیب پذیری های مهم، توسط Honggang Ren از آزمایشگاه FortiGuard Fortinet شناسایی شد که در InDesign CC Adobe یک اشکال فیزیکی حافظه (CVE-2018-4928) را شناسایی کرد که می تواند یک حمله اجرای کد دلخواه ایجاد کند.

Adobe نوشت: "این به روز رسانی یک آسیب پذیری مهم فیزیکی حافظه (CVE-2018-4928) را که توسط تجزیه نامناسب یک فایل inx به طور خاص ساخته شده است، حل می کند." توصیه می شود کاربران نصب نرم افزار خود را از طریق نرم افزار به روز رسانی Creative Cloud desktop ، و یا با رفتن به منوی راهنما InDesign و کلیک بر "Update" بروزرسانی کنند.

گردآورنده: حسین علیمرادی

بدافزاری که کامپیوتر شما را تا زمان نصب بازی PUBG، گروگان خواهد گرفت.

دنیای کامپیوترها تاریخچه‌ی طولانی از بدافزارهایی همچون جاسوس افزارها، ویروس‌ها و تبلیغ افزارها دارد. در تحقیقات اخیر از سوی تیم MalwareHunterTeam به مورد جالبی برخورده است. باج افزار جدیدی که فایل‌های کاربران را تا زمانی که آنان بازی PlayerUnknown's Battlegrounds را اجرا نکنند، رمزنگاری خواهد نمود.

به گزارش BleepingComputer reports، باج‌افزار PUBG RansomWare به کامپیوتر شما حمله خواهد کرد و فایل‌های موسیقی، تصاویر و اسناد قربانی را رمزگذاری خواهد کرد. فرمت این فایل‌ها همچنین به PUBG تغییر خواهد کرد. زمانی که این فرآیند پایان یافت، این باج افزار به شما یک پیغام نمایش می‌دهد که قربانی تنها قادر است از ۲ طریق فایل‌های خود را بازگرداند. یکی از این راه ها اجرا و بازی PUBG به مدت یکساعت است. راه حل دوم وارد نمودن کد بازگردانی فایل‌ها می‌باشد که در همان صفحه به قربانی نمایش داده می‌شود.

نویسنده‌ی این باج افزار یک پیغام غافل گیر کننده را به کاربر نمایش می‌دهد: "فایل‌ها، تصاویر، فایل‌های موزیک و اسناد شما رمزگذاری شده‌اند. فایل‌های شما توسط باج افزا PUBG رمزگذاری شده‌اند. اما نگران نباشید، بازکردن فایل‌های رمزنگاری شده دشوار نیست. من به پول احتیاج ندارم. تنها برای یک ساعت PUBG را بازی کنید."

براساس BleepingComputer، شما می‌توانید بازی برای ۳ ثانیه اجرا کرده و تمامی فایل‌های شما رمزگشایی خواهند شد و همه چیز به حالت نرمال برخواهد گشت.

با این وجود این برنامه جزو دسته بندی خطرناک قرار می‌گیرد. زیرا کامپیوتر شما را بدون اجازه تغییر می‌دهد و آن را تا زمانی که شما کارهای خواسته شده را انجام ندهید به عنوان یک قربانی نگه می‌دارد.

آنچه در این زمان مشخص نیست، این است که چگونه کاربر در ابتدا با این بدافزار مواجه می شود (یعنی چه سایت ها یا صفحاتی آن را گسترش می دهند)، یا تنها علاقهمندان به بازی PUBG که آن را نصب کرده‌اند تنها این بد افزار مواجه شده اند.

گردآورنده: محمد مرتضوی

برخی از فروشندگان گوشی های اندروید در خصوص وصله های امنیتی روند درستی ندارند

محققان یک آزمایشگاه امنیتی در آلمان تحقیقات تازه ای را شروع کرده اند. بعد از مهندسی معکوس برروی کد سیستم عامل ۱۲۰۰ گوشی موبایل، Karsten Nohl و Jakob Lell متوجه شدند که برخی از شرکت‌های تولید کننده در خصوص وصله-های امنیتی روند درستی را طی نکرده اند.

با توجه بررسی کد توسط محققین که آیا وصله‌های امنیتی برروی گوشی‌های موبایل به درستی نصب شده است یا خیر، در اکثر موارد محققین به این نتیجه رسیدند که این وصله های امنیتی برروی موبایل ها وجود ندارد.

بر اساس یافته ها برندهایی همچون شیائومی، وان پلاس و نوکیا به طور میانگین فاقد ۱ تا ۳ وصله نرم افزاری بودند. دستگاه هایی از اچ تی سی، موتورولا و ال جی به صور میانگین فاقد ۳ تا ۴ وصله امنیتی بودند. همچنین گوشی هایی از ZTE و TCL فاقد بیش از ۴ وصله امنیتی بودند.

این شرکت امنیتی همچنین ارتباطی بین فقدان وصله های امنیتی با قدرت پردازنده کشف کرد. به طور ساده، گوشی های ارزان قیمت با پردازنده های ضعیف تر دارای بیشترین آمار فقدان وصله ی امنیتی بوده اند. گوشی هایی با پردازنده ی سامسونگ دارای کمترین فقدان وصله های امنیتی بودند این در حالی است که گوشی هایی با پردازنده MediaTek به طور میانگین فاقد ۹.۷ وصله ی امینیتی بودند.

گوگل به Wired بیان کرده است که از تحقیقات SRL قدردانی می کند اما اشاره کرده است که برخی از تلفن های مورد بررسی ممکن است دستگاه هایی فاقد تایید اندروید باشند و بنابراین استانداردهای امنیتی گوگل نرسیده اند. همچنین گوگل اشاره نمود که گوشی های اندرویدی جدید دارای ویژگی های امنیتی هستند که از نفوذ هکرها به آن جلوگیری می کند، حتی اگر این گوشی ها آپدیت شده نباشند. از طرف دیگر گوگل اعلام نمود که وصله های امنیتی ممکن است برروی گوشی موجود نباشند زیرا فروشندگان می توانند ویژگی آسیب را به طور کامل از روی گوشی پاک کنند و نیازی به نصب وصله و تعمیر آن نباشد.

با این وجود، گوگل گفت که در حال کار با SRL برای بررسی بیشتر این موضوع است.

Karsten Nohl بیانات گوگل را تایید کرد و همچنین بیان نمود که در حال حاضر حتی هک کردن گوشی های بدون وصله های امنیتی نیز بسیار دشوار می باشد و از اقدامات امنیتی بسیاری در گوگل استفاده می کنند. Karsten Nohl بیان نمود: "حتی اگر برروی گوشی ها وصله های امنیتی نصب نشده باشد، اما این بدین منظور نیست که شما قادر به سو استفاده از آنان می باشید".

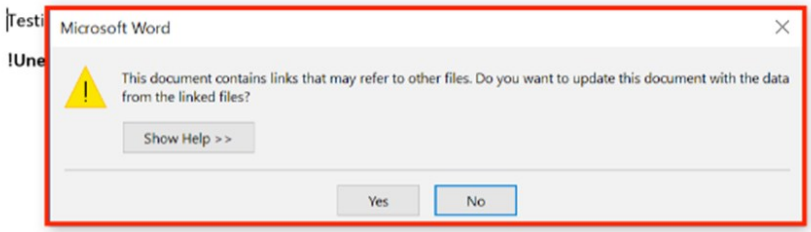
گوگل در رابطه با این موضوع بیانیه زیر را به The Verge صادر کرد:

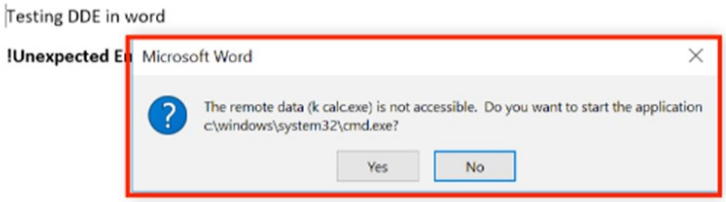
"ما می خواهیم از Karsten Nohl و Jakob Lell، بخاطر تلاش های مداوم خود برای تقویت امنیت اکوسیستم آندروید تشکر کنیم. ما با آنها همکاری داریم تا مکانیزم های تشخیص خود را بهبود بخشیم تا شرایطی را ایجاد نماییم که دستگاه به جای به روز رسانی امنیتی پیشنهاد شده توسط Google از یک به روز رسانی امنیتی متناوب داخلی استفاده کند. به روز رسانی های امنیتی یکی از لایه های بسیاری است که برای محافظت از دستگاه های اندرویدی و کاربران استفاده می شود. پلت فرم های حفاظتی ساخته شده، مانند سندباکس نرم افزاری و خدمات امنیتی همانند Google Play Protect، نیز به همان اندازه اهمیت دارند. این لایه های امنیتی همراه با تنوع فوق العاده اکوسیستم اندرویدی، به نتیجه گیری محققان می انجامد که سو استفاده از دستگاه های اندرویدی از راه دور همچنان یک مشکل اساسی است. "

گردآورنده: محمد مرتضوی

Microsoft office، تروجان را بدون نیاز به Macroها اجرا می کند

نویسندگان بدافزار لزوما نیاز به فریب کاربران برای فعال کردن ماکروها برای اجرای کدمخرب ندارند. یک تکنیک جایگزین وجود دارد که یکی از مزایای دیگر ویژگی های دفاتر قانونی است. این ویژگی به نام تبادل اطلاعات دینامیکی مایکروسافت (DDE) نامیده می شود و اجازه می دهد که یک برنامه آفیس، دیتاهایی را از اپلیکیشن آفیس دیگر بارگذاری کند. به عنوان مثال ، یک فایل ورد می تواند یک جدول که به وسیله کشیدن دیتا از یک فایل اکسل را برای هرباری که فایل ورد باز می شود؛ آپدیت کند.DDE یک ویژگی قدیمی است ولی DDE هنوز هم توسط برنامه های office پشتیبانی می شود و به کاربران این امکان را می دهد که دستورالعمل های ساده ای را با کشیدن داده ها و اطلاعاتی که به سند جدید تزریق می کنند؛ وارد کنند. مشکل این است که نویسندگان بدافزار می توانند فایل های ورد مخرب را با حوزه های DDE ایجاد کنند که به جای بازکردن یک برنامه آفیس دیگر، خط فرمان راباز کرده و کدمخرب را اجرا کنند. در شرایط عادی، برنامه های آفیس، دو اخطار را نشان می دهند.



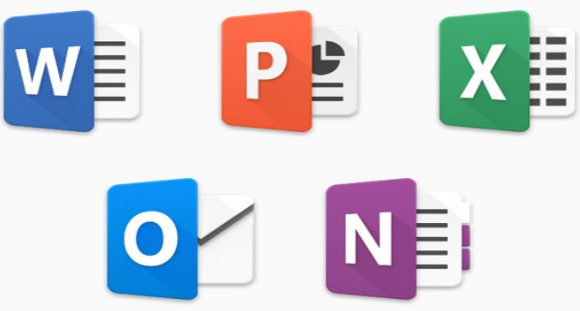


اولین هشدار در مورد سند حاوی لینک به سایر فایل هاست. درحالی که خطای دوم در مورد بازکردن یک خط فرمان از راه دور است. به گفته دو محقق امنیتی از Sense Post، پنجره دوم را می توان غیرفعال کرد تا هشدار ،فقط برای بار اول نشان داده می شود. این عامل به شدت قابلیت استفاده از DDE را افزایش می دهد.

مایکروسافت : این یک آسیب پذیری نیست.

Sense Post در اوایل سال جاری با مایکروسافت ارتباط برقرار کرد؛ اما این شرکت آسیب پذیری را در نظر نگرفت. دلیل اینکه مایکروسافت حملات DDE را به عنوان مسئله امنیتی نمی داند این است که آفیس قبل از بازکردن فایل ها، هشدار را نشان می دهد. این تنها مورد دیگری است که در آن نویسندگان بدافزار، یک راه خلاقانه برای سوء استفاده از یک ویژگی مشروع، مانند OLE و ماکرو پیدا کرده اند که مایکروسافت هم چنین به کاربران قبل از اجرا هشدار می دهد. کارشناسان امنیتی مانند دکتر Vesselin Bontchen با تصمیم مایکروسافت در خصوص دسته بندی حمله DDE موافقت می کنند.

ادامه در صفحه بعد.



گردآورنده: حسین علیمرادی

Microsoft office، تروجان را بدون نیاز به Macroها اجرا می کند

(ادامه...)

حملات DDE، مورد استفاده در گروه FIN7

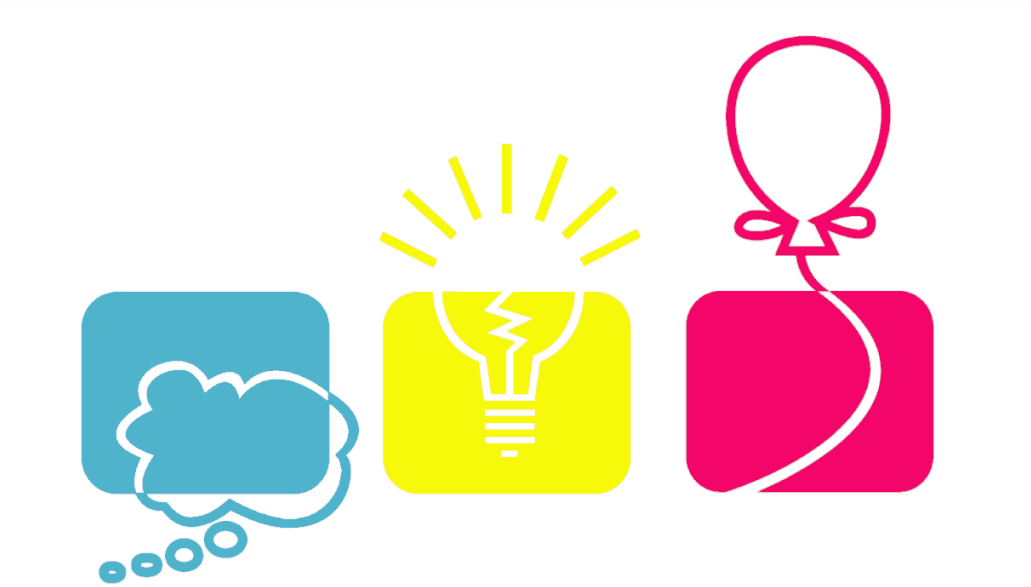
این نوع حملات از اوایل دهه ۹۰ میلادی آغاز شد. زمانی که DDE معرفی شد؛ ولی اخیرا در مارس ۲۰۱۷، هنگامی که یک تحقیق امنیتی بانام PwnDizz منتشر شد؛ یک گزارش در مورد راه هایی که نویسندگان بدافزار می توانستند از اسناد آفیس برای بارگذاری های پرداختی برسند؛ وجود داشت.این گزارش شامل ماکروها، اجزای OLE، اجزای Active X، اقدامات پاورپوینت DDE است. David Longenecken یک آموزش در مورد نحوه شناسایی حملات گذشته ی DDE را از طریق Logs Event منتشر کرد. David Stevens مجموعه ای از قوانین YARAرا منتشر کرد که شکارچیان بدافزار می توانند از شناسایی اسناد آفیس با استفاده از حملات DDE استفاده کنند. درحال حاضر، اکثر فروشندگان آنتی ویروس، آفیس را با حوزه های DDE به عنوان مشکوک یا مخرب تشخیص نمی دهند.

Kevin Beaumont تکنیک هایی را که حملات زنده توسط FIN7 مورد استفاده قرار گرفت را کشف کرد. گروهی از هکرها که در برخورد با سازمان های مالی متخصص بودند. Cisco Tabs تجزیه و تحلیل دقیق تر از این حملات انجام شده توسط همان گروه که قبلا توسعه دهنده نرم افزارهایDNS Messenger بودند؛ منتشر نمود. در حال حاضر کاربران باید مراقب بازکردن فایل های آفیس با لینک های DDE در صورتی که اسناد را از طریق ایمیل از افراد ناشناس دریافت می کنند؛ باشند.

اگر آن ها فایل را از یک فرستنده شناخته شده دریافت کرده باشند؛ چون ایمیل های جعلی بسیار شایع هستند؛ کاربران باید دوباره فرستنده را چک کرده و مطمئن شوند که آن ها واقعا فایل را ارسال نموده اند.

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 مرکز آپا خوارزمی:

@khu_cert

دانلود رایگان:

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