شماره سیزدهم - بهمن ۱۳۹۶

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:

حملات JackPot به عابر بانک‌ها

یک مقام مسئول در سرویس مخفی امریکا به رویترز بیان نمود: هکرهایی که احتمال میرود مربوط به تشکل مجرمان بین المللی باشند اخیرا با استفاده از حمله Jackpotting موفق به سرقت ۱ میلیون دلار از دستگاه های خودپرداز شده اند. - صفحه ۲

جزئیات جدید درمورد نفوذ به سیستم‌های Equifax

در گزارش اخیر Equifax به نمایندگان سنا، اذعان کرد رخنه‌ای که شرکت در سال گذشته، متحمل آن شده، ممکن است حاوی اطلاعات مهمی باشد که در سابق بر این ذکر نشده است. - صفحه ۵

هشدار لنوو به وجود نقصی در سیستم مدیریت Fingerprint در برخی از دستگاه‌هایش

شرکت لنوو در خصوص وجود یک نقص امنیتی با شدت بالا در برخی از دستگاه‌هاش هشداد داد. این نقص در نرم افزار Fingerprint Manager Pro یافت شده است و به هکرها امکان دور زدن سیستم احراز هویت از این روش بیومتریک را می دهد. - صفحه ۳

۵۰ پچ ماکروسافت در ویندوز، آفیس و مرورگرها برای فوریه ۲۰۱۸

به روزرسانی سه شنبه پچ مایکروسافت برای فوریه ۲۰۱۸، ۵۰ آسیب پذیری را در ویندوز و آفیس و مرورگرهای وب شرکت را نشان می‌دهد. - صفحه ۶

- **گروه سایبری PZChao، کشورهای آسیایی را با بدافزار استخراج بیت‌کوین، مورد حمله قرار می‌دهد!**

محققان امنیتی نوعی بدافزار سفارشی را یافتند که آسیا را طی چند ماه اخیر ویران کرده است و توانایی انجام وظایفی مانند سرقت رمزعبورها، استخراج بیت‌کوین و توانا ساختن هکرها برای کنترل از راه دور سیستم‌های درمعرض خطر را دارد.-صفحه ۴

حمله روز صفر و وصله امنیتی برای نسخه کاربر Bitmessage

به روز رسانی اخیر برای برنامه PyBitmessage مشکل اجرای کد از راه دور که در حملات از آن استفاده شده بود را برطرف می‌کند. Bitmessage پروتکل ارتباطی غیرمتمرکزی است که برای ارسال پیام‌های رمزنگاری شده به یک یا چند کاربر استفاده می‌شود. - صفحه ۶

حملات JackPot به عابر بانک‌ها.

یک مقام مسئول در سرویس مخفی امریکا به رویترز بیان نمود: هکرهایی که احتمال میرود مربوط به تشکل مجرمان بین المللی باشند اخیرا با استفاده از حمله Jackpotting موفق به سرقت ۱ میلیون دلار از دستگاه های خودپرداز شده اند.

این تکنیک شامل دسترسی فیزیکی به دستگاه و استفاده از بدافزارها، وسایل مخصوص الکترونیکی و یا هر دو برای کنترل و صدور دلار در یک زمان می باشد. نام Jackpotting از برنده شدن مقداری پول از دستگاه‌های Slot که شبیه خودپرداز می باشد گرفته شده است.

در سال ۲۰۱۰، هکری که به نام Barnaby Jack مشهور بود و در سال ۲۰۱۳ فوت نمود، توانست در برروی یک خودپرداز در کنفرانس کلاه سیاه‌ها این نوع حمله را انجام دهد. این مشکل در آسیا، اروپا و مکزیک تا این لحظه پا برجا می باشد. همچنین محقق امنیتی Brian Krebs بیان نمود که سرویس امنیت امریکا در این خصوص به موسسات مالی هشدار داده بوده است.

این حملات در سراسر کشورها از شمال غربی اقیانوس آرام و تا خلیج انگلستان در حال شکل گیری است. در چند روز گذشته ۶ حمله موفقیت آمیز صورت گرفته است. سرویس امنیت بیان نموده است که هکرها از وسیله ای مانند دستگاه اندوسکوپی برای اتصال لپ تاپشان به کامپیوتر موجود در خودپرداز استفاده می‌کنند. سپس آنان می‌توانند هارد درایو دستگاه خودپرداز را به وسیله بدافزار Ploutus.D آلوده نمایند. به محض اینکه کامپیوتر ریبوت شود خودپرداز قابلیت امکان ارائه خدمات به مشتریان را از دست می‌دهد و مجرمان می‌توانند آن را کنترل کنند و تمامی پول موجود در مخازن آن را خالی نمایند.

مجرمان، خود پردازهایی با سری Opteva ۵۰۰ و ۷۰۰ را مورد هدف قرار داده اند که به این آسیب پذیری دچار هستند. این خود پردازها همچنان از ویندوز XP استفاده می‌کنند.

گردآورنده: محمد مرتضوی

هشدار لنوو به وجود نقصی در سیستم مدیریت Fingerprint در برخی از دستگاه‌هایش

شرکت لنوو در خصوص وجود یک نقص امنیتی با شدت بالا در برخی از دستگاه‌هاش هشداد داد. این نقص در نرم افزار Fingerprint Manager Pro یافت شده است و به هکرها امکان دور زدن سیستم احراز هویت از این روش بیومتریک را می‌دهد.

شرکت لنوو مدل‌هایی از سری‌های ThinkPad، ThinkCenter و ThinkStation که نرم افزار نام برده بروی آنان فعال است را منتشر نمود. خبر خوب این است که تنها دستگاه‌هایی که ویندوز ۷، ۸ و ۸.۱ دارند از نرم افزار نام برده استفاده می‌کنند و دستگاه‌هایی با ویندوز ۱۰ به صورت Built-in از خاصیت Fingerprint پشتیبانی می‌کنند و در این صورت هیچ جای نگرانی نخواهد بود.

بر اساس گفته های شرکت لنوو، اطلاعات حساس مانند اطلاعات احراز هویت و اطلاعات Fingerprint در نرم افزار مذکور با الگوریتم رمزنگاری ضعیفی کد می‌شود. همچنین نرم افزار شامل پسوردهایی به صورت Hard Code می‌باشد که با عمل مهندسی معکوس و خواندن کد برنامه می‌توان پسورد رمزگشایی اطلاعات را به دست آورد.

با اینکه این نرم افزار تنها برروی ویندوزهای ۷، ۸ و ۸.۱ فعال است اما در حال حاضر هنوز هم کسب و کارهای زیادی از این سیستم عامل‌ها استفاده می‌کنند. خوشبختانه این نقص‌ها نمی توانند از راه دور مورد سو استفاده قرار گیرند و یک هکر نیاز به دسترسی فیزیکی به کامپیوتر دارد.

شرکت لنوو برای نرم افزار Fingerprint Manager Pro آپدیتی ارائه داده است (نسخه ۸.۰۱.۸۷) که این مشکل را مرتفع می‌نماید. از سوی دیگر هر فردی که یکی از لپ تاپ‌های زیر را داشته باشد و به ویندوز ۱۰ ارتقاع نداده باشد هنوز در خطر این آسیب پذیری خواهد بود و باید هرچه سریعتر بروزرسانی ها را دانلود و نصب نماید.

- ThinkPad L560
- ThinkPad P40 Yoga, P50s
- ThinkPad T440, T440p, T440s, T450, T450s, T460, T540p, T550, T560
- ThinkPad W540, W541, W550s
- ThinkPad X1 Carbon (Type 20A7, 20A8), X1 Carbon (Type 20BS, 20BT)
- ThinkPad X240, X240s, X250, X260
- ThinkPad Yoga 14 (20FY), Yoga 460
- ThinkCentre M73, M73z, M78, M79, M83, M93, M93p, M93z
- ThinkStation E32, P300, P500, P700, P900

گردآورنده: محمد مرتضوی

گروه سایبری PZChao، کشورهای آسیایی را با بدافزار استخراج بیت‌کوین، مورد حمله قرار می‌دهد!

محققان امنیتی نوعی بدافزار سفارشی را یافتند که آسیا را طی چند ماه اخیر ویران کرده است و توانایی انجام وظایفی مانند سرقت رمزعبورها، استخراج بیت‌کوین و توانا ساختن هکرها برای کنترل از راه دورِ سیستم‌های درمعرض خطر را دارد.

حملات PZChao که توسط محققان امنیتی با برنامه‌ی Bitdefender کشف شد، سازمان‌های دولتی، صنعتی، آموزشی و بخش‌های ارتباطاز راه دور را در آسیا و ایالات متحده هدف حمله قرار داده بود.

محققان بر این باورند که ماهیت، زیرساخت و ابزارهای شامل انواع تروجان GhostRAT که در حملات PZChao استفاده شده است، یادآور گروه بدنام هکرهای چینی، بنام **ببرآهنی** است.

حملات PZChao بوسیله‌ی تاکتیک‌هایی شبیه به تاکتیک‌های حمله‌ی ببر آهنی، درحال حمله به اهداف آسیایی و آمریکایی است، که برطبق نظر محققان، امکان بازگشت گروه بدنام چینی APT است.

حداقل از ماه جولای سال پیش، حملات PZChao در حال هدف قرار دادن سازمان-هایی بوده است که ضمیمه فایل VBS مخرب از طریق ایمیل‌های هدفمند را دریافت کرده‌اند.

اگر این فایل اجرا شده باشد، سند VBS فایل‌های اضافی را از یک سرورِ از راه دور با هاستِ "down.pzchao.com" که به IP ای در کره جنوبی (125.7.152.55) متصل است بر روی دستگاه ویندوزِ قربانی، دانلود می‌کند.

عملگرهای این تهدید در پسِ حمله، کنترل حداقل پنج زیردامنه‌ی مخرب از دامنه‌ی "pzchao.com" را داراست، و هر یک از آن‌ها برای میزبانیِ وظایف مخصوصی استفاده می‌شود، مثل دانلود، آپلود، عملیات مربوط به RAT، رساندن بدافزار DLL.

محققان می‌گویند فایل‌های مستقر شده توسط عملگرهای تهدید، "گوناگون و دارای قابلیت دانلود و اجرای فایل‌های دوتاییِ اضافی، جمع‌آوری اطلاعات شخصی و اجرای از راهِ دور فرامین در سیستم است".

اولین فایل نصب شده در دستگاه در معرضِ خطر، یک استخراج‌کننده‌ی بیت‌کوین است، که به شکل فایل اجرایی جاوا "java.exe" مخفی شده است، و این پول رایجِ پنهان را هر سه هفته ساعت ۳ صبح، وقتی اغلب افراد پشت سیستم‌هایشان نیستند، استخراج می‌کند.

همچنین برای سرقت رمزعبورها، این بدافزار در یکی از دو نسخه‌ی ابزار پاک‌کننده‌ی Mimikatz (بستگی به سازنده‌ی سیستم عامل دستگاه موردنظر دارد)، برای به دست آوردن رمزعبورها و فرستادن آنها به سرور کنترل و دستور، مستقر می‌شود.

اولین نهاییِ PZChao شامل نسخه‌ی سبُک اصلاح‌شده‌ی Ghost تروجان کنترل از راه دور(RAT) طراحی شده است و بسیار شبیه به نسخه‌های کشف شده در حملات سایبری مرتبط با گروه APT ببر آهنی رفتار می‌کند.

Ghost RAT مجهز به توانایی‌های عظیمی برای جاسوسی سایبری است، شامل:

- ثبت بلافاصله و آفلاین ضربه‌هایی که به کلیدها زده می‌شود.
- فهرست کردن تمام پردازش‌های فعال و پنجره‌های بازشده.
- شنود مکالمات از طریق میکروفون.
- ثبت تصاویر ویدیویی زنده از وبکم.
- مجوز خاموش و روشن کردن سیستم از راه دور.
- دانلود فایل باینری از اینترنت برای میزبانی از راه دور.
- مدیریت و سرقت فایل‌ها و...

تمام توانایی‌های بالا، به یک مهاجم از راه دور، اجازه‌ی بدست گرفتن کنترل سیستم مورد حمله، جاسوسی از قربانیان و برون‌نشت اطلاعات محرمانه را می‌دهد.

محققان می‌گویند درحالیکه ابزار مورد استفاده در PZChao کمی قدیمی شده است، "اما آن‌ها آزمایش حمله را پس‌داده‌اند و برای حملات آینده مناسب‌ترند".

گردآورنده: حسین علیمرادی

جزئیات جدید درمورد نفوذ به سیستم‌های Equifax

در گزارش اخیر Equifax به نمایندگان سنا، اذعان کرد رخنه‌ای که شرکت در سال گذشته، متحمل آن شده، ممکن است حاوی اطلاعات مهمی باشد که در سابق بر این ذکر نشده است.

در اواسط می ۲۰۱۷، عوامل مخرب از یک نقطه‌ضعف شناخته شده در چارچوب توسعه‌ی آپاچی استراتس (Apache Starts) استفاده کردند تا به به سیستم‌های Equifax دسترسی پیدا کنند. این شرکت می‌گوید این رخنه، حدود ۱۴۵ میلیون مشتری را تحت تأثیر قرار داده است –اغلب در آمریکا و همچنین کانادا و انگلستان- بخصوص اطلاعات شماره‌ی مشتریان، تاریخ تولد آن‌ها، آدرس‌ها و بعضی شماره‌ی گواهینامه‌ها، کارت‌های اعتباری و پرونده‌های دعاوی آن‌ها.

اسناد محرمانه‌ای که Equifax به کمیته‌ی مالی سنا ارسال کرده نشانگر اینست که احتمالا هکرها، شماره شناسایی قبوض، آدرس ایمیل‌ها، و حتی اطلاعات گواهینامه رانندگان را هم سرقت کرده باشند.

در پاسخ به گزارشات خبری، Equifax اظهار داشت اطلاعات به سرقت رفته هرگز شامل همه‌ی آن اطلاعاتی که ممکن است در معرض خطر باشند، نبوده است.

سناتور آمریکا، الیزابت وارن، از Equifax خواست تا در مورد "اطلاعات متناقض، گیج‌کننده و ناقص" ای که شرکت آماده کرده است، برای عموم و سنا، شفاف‌سازی کند.

طبق گفته‌ی سناتور وارن، Equifax به کمیته‌ی مالی گفته که در اوایل اکتبر، شماره پاسپورت‌ها نیز در جدول داده‌هایی که در دسترس هکرها قرار گرفته، بوده است، اما اکنون آژانس اخبار اعتباری ادعا می‌کند که پاسپورت‌ها در معرض خطر نبوده‌اند.

سناتور وارن نامه‌ای از این قرار به Equifax نوشت: "به این دلیل که شرکت شما به صدور ناقص، گیج‌کننده و متناقض بیانیه‌ها و مخفی کردن اطلاعات از کنگره و عموم مردم ادامه می‌دهد، واضح است که ۵ماه بعد از اعلان عمومی این رخنه، Equifax هنوز دارد به این پرسش ساده، پاسخ کاملی می‌دهد که: گستردگیِ دقیق این نفوذ چقدر بوده؟"

سناتور بمدت یک هفته به Equifax مهلت داده است تا فهرستی کامل و جامع از عناصر داده‌هایی که مطمئنا و یا احتمالا در این رخنه سرقت شده‌اند را به همراه زمانبندی اقدامات آن آماده کند تا بتوان حدود نفوذ را تخمین زد.

هفته‌ی گذشته، سناتور وارن گزارشی ۱۵ صفحه‌ای حاوی یافته‌های خود طی ۴ ماه تحقیق و بررسی روی نقاط ضعف Equifax منتشر کرد. تحقیقات این قانون‌گذار روشن کرد که شرکت، سیستم معیوبی را برای دفاع از حوادث امنیتی نصب کرده بود، هشدارهای خطر برای اطلاعات مشتری را نادیده گرفت، در خبر رسانی به موقع به سهامداران شرکت، موفق نبود و اطلاع و کمک‌رسانی ناکافی به مشتریان ارائه داد. این گزارش همچنین حاکی از این بود که Equifax از نقاط ضعف قرارداد فدرال برای اجبار IRS به امضای یک قرارداد، سود می‌برده است.

چندی پیش در امسال، سناتور وارن و مارک وارنر لایحه‌ای را تقدیم کردند که کمیسیون تجارت فدرال را در زمینه‌ی گزارش مالی بخاطر تکرار امنیت سایبریِ ضعیف، قادر به جریمه می‌کند. این لایحه در فقره‌ی رخنه در Equifax نوشته شد.

به گزارش رویترز، در اوایل این ماه، رئیس اداره‌ی حفاظت از مصرف کننده، میک مال‌ونی، مشکل نفوذ در Equifax را متوقف کرده بود. بدنبال انتشار این اخبار، ۳۲ سناتور برای درخواست اطلاعات بیشتر درمورد تحقیقاتش، نامه‌ای به او ارسال کردند.

گردآورنده: حسین علیمرادی

۵۰ پچ ماکروسافت در ویندوز، آفیس و مرورگرها برای فوریه ۲۰۱۸

به روزرسانی سه شنبه پچ مایکروسافت برای فوریه ۲۰۱۸ ، ۵۰ آسیب پذیری را در ویندوز و آفیس و مرورگرهای وب شرکت را نشان می‌دهد.

چهارده حفره‌ی امنیتی ارزیابی شناسایی شده است. از جمله آن‌ها: نقص افشای اطلاعات در مرورگر Edge، مشکلات حافظه در Outlook، آسیب پذیری اجرای کد از راه دور در Component Structured Query ویندوز و چندین مشکل حافظه در موتورهای اسکریپت مورد استفاده توسط Edge و Internet Explorer.

آسیب پذیری با شناسه CVE-2018-0771، به دلیل ساختار Edge است که درخواست‌های ریشه‌های مختلف را بررسی می‌کند.

دو نکته جالب توجه در این ماه کشف آسیب پذیری Outlook توسط نیکولاس در مایکروسافت است. نقص امنیتی با شناسه CVE-2018-0852، می‌تواند برای اجرای کد دلخواه در جلسه (session) کاربر با هدف بازکردن یک فایل بخصوص که با نسخه آسیب دیده از Outlook ساخته شده است، مورد سوء استفاده قرار گیرد.

Dustin Childs توضیح داد:

"کاربر نهایی که توسط چنین حمله ای هدف قرار می گیرد نیازی به باز کردن یا کلیک بر روی هر چیزی در ایمیل ندارد - فقط آن را در Preview Panel مشاهده می‌کند."

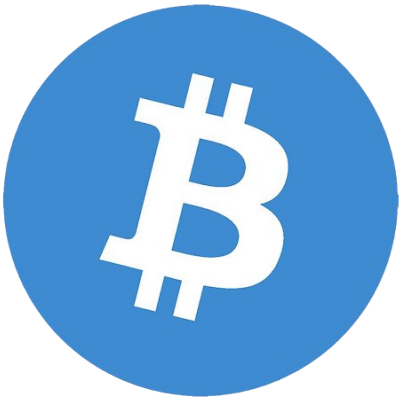
آسیب پذیری دوم Outlook که توسط Joly یافت شده (CVE-2018-0850) می‌تواند Outlook را مجبور به بارگیری یک ذخیره ی پیام محلی یا از راه دور کند. این نقص می تواند به صورت فرستادن یک ایمیل بخصوص ساخته شده به یک کاربر Outlook مورد سوء استفاده قرار گیرد.

"ایمیل باید به گونه ای طراحی شده باشد که Outlook را قادر سازد تا یک ذخیره ی پیام را بیش از SMB بارگیری کند. Outlook تلاش می‌کند تا پیام از پیش پیکربندی شده را در هنگام دریافت ایمیل بازکند. این بدان معنی است که یک مهاجم می‌تواند از طریق ارسال یک ایمیل، از آن بهره ببرد."

به روز رسانی سه شنبه مایکروسافت، مجموعه ای از ۳۴ آسیب پذیری شدید و دو متوسط را رفع می‌کند.

گردآورنده: حسین علیمرادی

حمله روز صفر و وصله امنیتی برای نسخه کاربر Bitmessage



به روز رسانی اخیر برای برنامه PyBitmessage مشکل اجرای کد از راه دور که در حملات از آن استفاده شده بود را برطرف می‌کند. Bitmessage پروتکل ارتباطی غیرمتمرکزی است که برای ارسال پیام‌های رمزنگاری شده به یک یا چند کاربر استفاده می‌شود. PyBitmessage برنامه رسمی Bitmessage ارائه شده برای کاربران است. توسعه دهندگان Bitmessage اخطاری مبنی بر رخنه روز صفر منتشر کرده‌اند که از آن علیه برخی کاربران PyBitmessage 0.6.2 سوء استفاده شده است.

این حفره امنیتی ناشی از خطای رمزنگاری پیام بوده و در نسخه 0.6.3.2 برطرف شده است. البته از آنجا که نسخه 0.6.1 این مشکل را ندارد، می‌توان برای حل مشکل این نسخه را جایگزین کرد.

Peter Šurda، یکی از اعضای تیم توسعه دهنده هسته Bitmessage، از جمله افرادی است که مورد هدف حملات قرار گرفته است. پیتر از کاربران درخواست کرده برای او پیامی ارسال نکنند چرا که کلیدهای خصوصی وی به احتمال زیاد توسط هکرها به سرقت رفته است. یک آدرس پشتیبانی جدید در PyBitmessage 0.6.3.2 اضافه شده است.

وی همچنین گفت: "اگر شما نگران این هستید که رایانه شما در معرض خطر است یا نه، همه رمزهای خود را تغییر و یک کلید جدید بسازید."

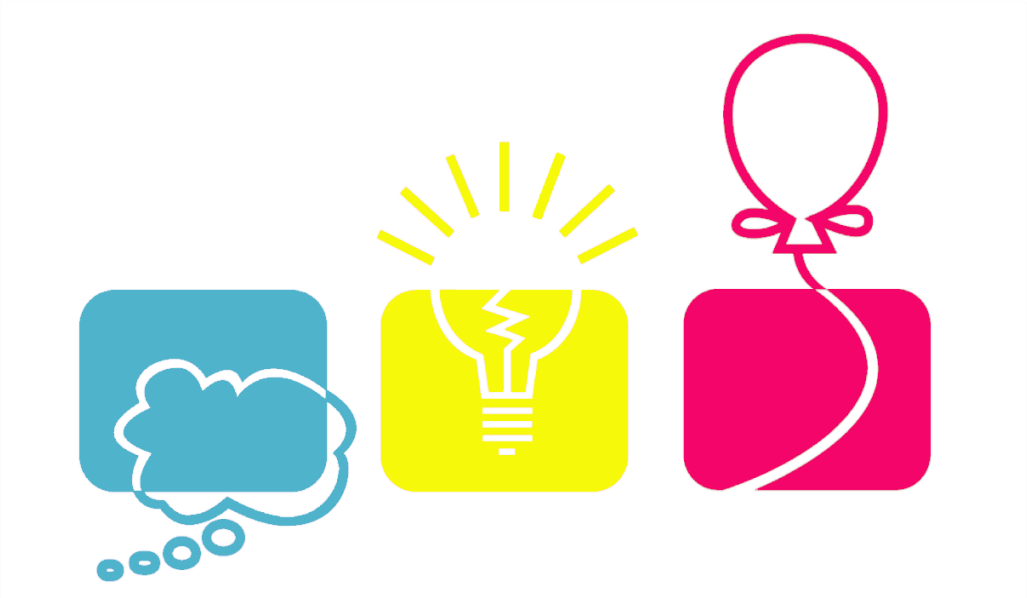
براساس گفته‌های Šurda مهاجمین در تلاش برای سوءاستفاده از این حفره به منظور دسترسی به کیف پول الکترووم و سرقت بیت‌کوین است. دریافت یک پیام مخرب موجب این سوءاستفاده می‌شود. مهاجم یک اسکریپت خودکار را اجرامی کند همچنین یک remote reverse shell را هم ایجاد یا تلاش در باز کردن آن دارد. اسکریپت خودکار به electrum/wallets متصل می‌شود اما هنگام استفاده از reverse shell مهاجم به سایر فایل‌ها هم دسترسی داشت.

تحقیق و بررسی در مورد این حملات در دست اقدام است و توسعه دهندگان گفته‌اند به محض روشن شدن موضوع اطلاعات بیشتری منتشر کنند.

Bitmessage در سال‌های گذشته به طور فزاینده‌ای محبوب شده است و این گزارش‌ها نشان می‌دهد که آژانس امنیت ملی ایالات متحده و سایر سازمان‌های اطلاعاتی نظارت کاملی بر آن دارند. در حالی که پروتکل اغلب توسط افرادی که به دنبال حفظ حریم خصوصی خود هستند استفاده می‌شود.

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.