شماره سی و پنجم - تیر ۱۴۰۱

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

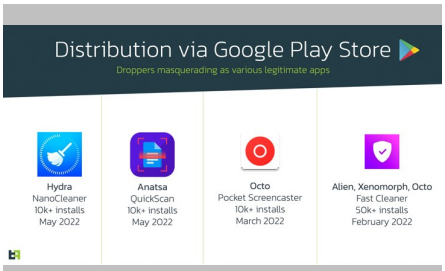
در این شماره خواهید خواند:

کابوس جدیدی برای آفیس: Follina

مشکلات و آسیب پذیری‌های آفیس هیچ گاه تمامی ندارد. کاربران زیادی هرساله در معرض این خطرات قرار می‌گیرند. از طرف دیگر مهاجمین زیاد، آفیس را به چشم یک گنجینه می‌بینند که از طریق آن می‌توان انواع حملات را برروی قربانیان پیاده سازی کرد. - صفحه ۲

قوانین جدید دولت هند!

تیم CERT هند، روز پنجشنبه دستورالعمل‌های جدیدی را منتشر کرد که بر اساس آن از ارائه‌دهندگان خدمات، واسطه‌ها، مراکز داده و نهادهای دولتی درخواست کرده تا حوادث امنیت سایبری، از جمله نشت داده‌ها را در عرض شش ساعت گزارش کنند. - صفحه ۵



جدیدترین وضعیت بدافزارهای موبایل

در جدیدترین گزارش امنیتی سال ۲۰۲۲ برروی گوشی‌های موبایل، کشورهای اسپانیا و ترکیه بیشتر از سایر کشورها هدف حمله‌ی تروجان‌های بانکی برروی دیوایس‌های اندروید قرار گرفته‌اند. در این لیست به ترتیب سایر کشورهای لهستان، استرالیا، ایالات متحده، آلمان، بریتانیا، ایتالیا، فرانسه و پرتغال نیز وجود دارند. - صفحه ۳

۱۰ سال جاسوسی

محققان امنیتی یک کمپینگ جاسوسی کشف کرده‌اند که توسط یک گروه هکری، تحت حمایت چین مدیریت می‌شوند. این کمپینگ از سال ۲۰۱۳ دولت‌ها، سیستم‌های آموزشی و سازمان‌های مخابراتی را هدف قرار می‌دادند. - صفحه ۶

سلطه‌ی رایانش ابری، چالش‌های امنیتی!

پذیرش رایانش ابری در دهه گذشته به سرعت در حال رشد بوده است و به زودی استفاده از رایانش ابری برای نرم افزارهای کاربردی، نرم افزارهای زیرساختی، خدمات فرآیند کسب و کار و زیرساخت های سیستم، به نقطه عطفی دست خواهد یافت که در دو یا سه سال آینده از سایر گزینه‌های فناوری سنتی پیشی می‌گیرد. - صفحه ۴

امکان سرقت تسلا با کلیدهای شخصی

سال گذشته، تسلا به‌روزرسانی‌ای را منتشر کرد که راه‌اندازی وسایل نقلیه خود را پس از باز شدن با کارت‌های کلید NFC آسان‌تر کرد. اکنون، یک محقق امنیتی نشان داده است که چگونه می‌توان از این ویژگی برای سرقت خودروها سوء استفاده کرد. - صفحه ۷

کابوس جدیدی برای آفیس: Follina

مشکلات و آسیب پذیری‌های آفیس هیچ گاه تمامی ندارد. کاربران زیادی هرساله در معرض این خطرات قرار می‌گیرند. از طرف دیگر مهاجمین زیاد، آفیس را به چشم یک گنجینه می‌بینند که از طریق آن می‌توان انواع حملات را برروی قربانیان پیاده سازی کرد.

اما آسیب پذیری جدیدی که در آفیس باعث نگرانی کاربران شده است و هنوز برای آن هیچ وصله‌ی نرم افزاری از سوی مایکروسافت ارائه نشده است، آسیب پذیری با شناسه CVE-2022-30190 می‌باشد که با نام Follina شناخته می‌شود.

این آسیب پذیری به مهاجم امکان اجرای کد دلخواه برروی کامپیوتر شخصی قربانی را می-دهد.

این آسیب‌پذیری توسط محقق مشهور امنیت سایبری، کوین بومونت، «Follina» نامیده شد. بر اساس تحلیل وی، یک سند آلوده با استفاده از قابلیت الگوهای Word امکان دریافت یک فایل HTML را از هر وب سروری فراهم می‌کند و در نهایت با استفاده از قابلیت ms-msdt MSProtocol امکان بارگذاری و اجرای کدهای PowerShell فراهم خواهد شد.

طبق صحبت‌های این محقق امنیتی مشکل اصلی اینجاست که آفیس کدهای مخرب را با استفاده از msdt حتی در زمانی که macroها غیرفعال باشند اجرا می‌کند.

به طور خلاصه، این آسیب پذیری روز صفر اجازه اجرای کد را در طیف وسیعی از محصولات مایکروسافت می‌دهد که می تواند در سناریوهای مختلف حمله مورد سوء استفاده قرار گیرد. علاوه بر این، این آسیب‌پذیری "مرز غیرفعال کردن ماکروها را می‌شکند" و تشخیص آن بسیار ضعیف است.

این آسیب پذیری برروی نسخه‌های متفاوتی از سیستم عامل ویندوز با موفقیت اجرا شده است. یکی عواملی که این ضعف امنیتی را بسیار مهم جلوه می‌دهد تست موفق آن برروی ویندوز ۱۰ با macro غیرفعال و Defender فعال است.

اما برای جلوگیری از این آسیب پذیری تا زمان ارائه‌ی یک وصله‌ی امنیتی، مایکروسافت دستورعمل زیر را ارئه کرده است:

- اجرای cmd با دسترسی admin
- اجرای دستور زیر برای تهیه‌ی نسخه‌ی پشتیبان از رجیستری در یک فایل

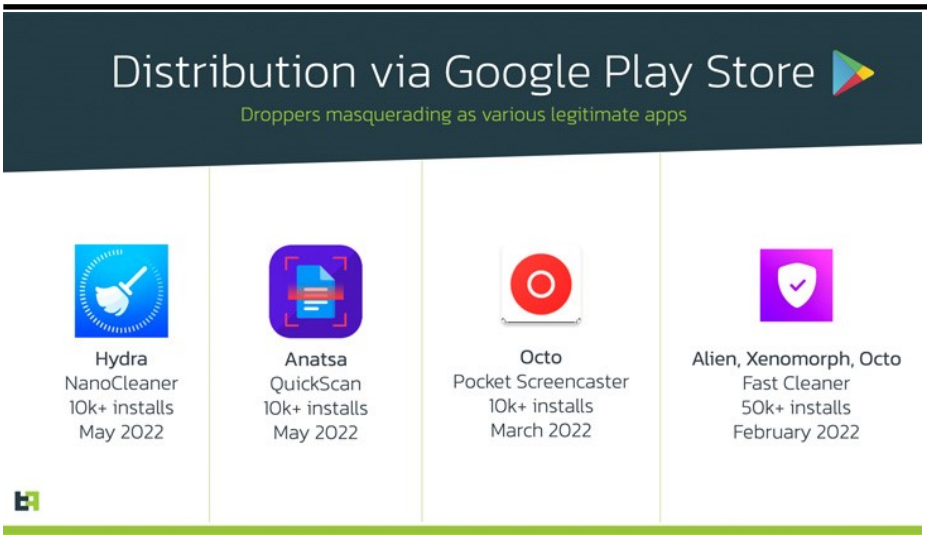
reg export HKEY_CLASSES_ROOT\ms-msdt نام فایل

- اجرای دستور زیر

reg delete HKEY_CLASSES_ROOT\ms-msdt /f

گردآورنده: محمد مرتضوی

جدیدترین وضعیت بدافزارهای موبایل



طبق بررسی‌های صورت گرفته در جدیدترین گزارش امنیتی سال ۲۰۲۲ برروی گوشی‌های موبایل، کشورهای اسپانیا و ترکیه بیشتر از سایر کشورها هدف حمله‌ی تروجان‌های بانکی برروی دیوایس‌های اندروید قرار گرفته‌اند. در این لیست به ترتیب سایر کشورهای لهستان، استرالیا، ایالات متحده، آلمان، بریتانیا، ایتالیا، فرانسه و پرتغال نیز وجود دارند.

طبق گزارش شرکت امنیت سایبری هلندی ThreatFabric: نگران‌کننده‌ترین موضوع توجه فزاینده به حملات On-Device Fraud یا تقلب در دستگاه مربوط می‌شود.

فقط در پنج ماه اول سال ۲۰۲۲، خانواده‌های بدافزارهایی که از سیستم عامل اندروید برای انجام کلاهبرداری سوء استفاده می‌کنند، بیش از ۴۰ درصد افزایش داشته است، که تشخیص آن‌ها با استفاده از موتورهای امتیازدهی سنتی تقلب تقریبا غیرممکن می‌باشد.

فعال‌ترین تروجان‌های بانکی عبارتند از:

- Hydra
- FluBot
- Cerberus
- Octo
- ERMAC

همانطور که در لیست بالا اشاره شد، این تروجان‌ها در قالب ابزارهایی مفید به کاربران ارائه می‌شدند که اسامی آنان به شرح ذیل است:

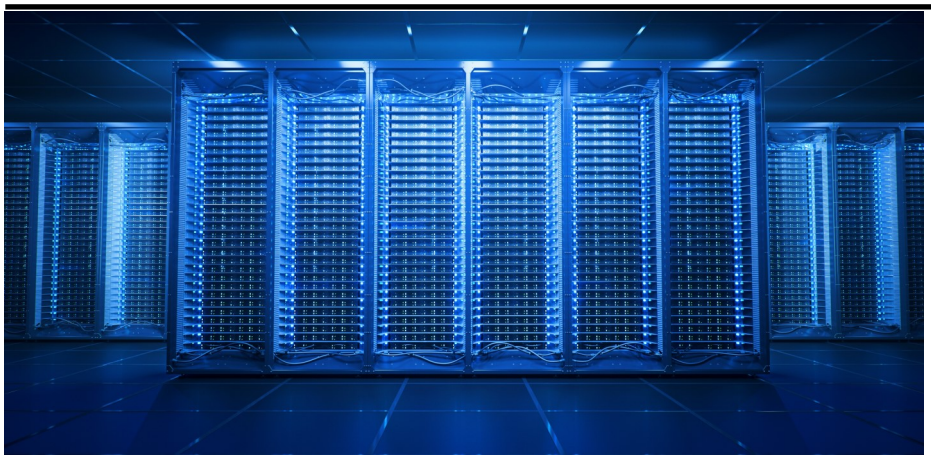
- Nano Cleaner (com.casualplay.leadbro)
- QuickScan (com.zynksoftware.docuscanapp)
- Chrome (com.talkleadihr)
- Play Store (com.girltold85)
- Pocket Screencaster (com.cutthousandjs)
- Chrome (com.biyitunixiko.populolo)
- Chrome (Mobile com.xifoforezuma.kebo)
- BAWAG PSK Security (com.qjlpfydjb.bpycogkzm)

هرساله این تروجان‌ها به جدیدترین متدهای موجود در کلاهبرداری بروزرسانی می‌شوند و قابلیت‌های بسیار بالایی دارند. از جمله این قابلیت‌ها می‌توان به ضبط صفحه‌ی گوشی کابران اشاره کرد.

عموم این اپلیکیشن‌ها از APIهای مختلفی برای اتصال به سرور C&C خود استفاده می‌نمایند.

گردآورنده: محمد مرتضوی

سلطه‌ی رایانش ابری، چالش‌های امنیتی!



واضح است که رایانش ابری به سرعت در حال تبدیل شدن به مدل غالب مشاغل برای میزبانی داده‌ها و برنامه‌ها و توسعه خدمات جدید.

پذیرش رایانش ابری در دهه گذشته به سرعت در حال رشد بوده است و به زودی استفاده از رایانش ابری برای نرم افزارهای کاربردی، نرم افزارهای زیرساختی، خدمات فرآیند کسب و کار و زیرساخت های سیستم، به نقطه عطفی دست خواهد یافت که در دو یا سه سال آینده از سایر گزینه‌های فناوری سنتی پیشی می‌گیرد.

رویدادهای اخیر مانند تغییر اجباری به کارهای ترکیبی، شتاب بیشتری را در توسعه-ی سرویس‌های ابری ایجاد کرده است و با ادامه رشد و تکامل ارائه‌های ابری، این احتمال وجود دارد که پذیرش آن همچنان گسترش یابد.

رایانش ابری مزایای آشکاری دارد. این مزایا شامل مقیاس خدمات تقریباً بی نهایت بر اساس تقاضا بدون نیاز به خرید یا نگهداری سخت افزار گران قیمت و توانایی استفاده از برنامه‌های جدید بدون داشتن تیم هایی از مهندسان در لیست حقوق و دستمزد برای استقرار و مدیریت آن‌ها است.

اما تغییر رویه‌ها به رایانش ابری، چالش‌های جدیدی را نیز به همراه دارد که بزرگترین نگرانی آن مختص به امنیت است.

درست است که یکی از مزیت‌های کلیدی رایانش ابری برای کسب‌وکارها این است که سیستم‌ها و داده‌های خود را می‌توانند به یک شرکت ابری با کارشناسان اختصاصی که برای حفظ امنیت سیستم‌ها کار می‌کنند، بسپارند. مطمئناً این مورد نگرانی ها و سردردهای مربوط به وصله و نگهداری نرم افزار روی سرورها را از بین می برد.

اما این بدان معنا نیست که کسب و کارها می‌توانند پس از انتقال به فضای ابری، شاخص امنیت را فراموش کنند.

بهره‌مندی از مزایای کامل رایانش ابری به معنای استفاده از چندین شرکت ابری است که داده‌ها و بار کاری بین مراکز داده خود شرکت و ابرهای مختلف در آن‌هت جابجا می‌شوند.

در حالی که حرکت به سمت رایانش ابری ممکن است برخی از نگرانی های امنیتی اساسی را برطرف کرده باشد، ظهور ابر ترکیبی مجموعه کاملا جدیدی را معرفی کرده است. این موارد شامل ایمن کردن دسترسی کارکنان به خدمات، اطمینان از اینکه داده‌ها رمزگذاری شده‌اند و به طور تصادفی در معرض دسترسی سایر کاربران ابری قرار نمی گیرند و اطمینان از ایمن ماندن داده‌ها هنگام جابجایی بین برنامه‌ها و سرویس‌های ابری می‌باشد. هیچ دو سرویس ابری دقیقاً یکسان نیستند و با گسترش استفاده از رایانش ابری به مناطق جدید، خطرات آن نیز افزایش می یابند.

گردآورنده: محمد مرتضوی

قوانین جدید دولت هند!

تیم CERT هند، روز پنجشنبه دستورالعمل‌های جدیدی را منتشر کرد که بر اساس آن از ارائه‌دهندگان خدمات، واسطه‌ها، مراکز داده و نهادهای دولتی درخواست کرده تا حوادث امنیت سایبری، از جمله نشت داده‌ها را در عرض شش ساعت گزارش کنند.

طبق این دستورالعمل هر نهادی که در آن نشت اطلاعاتی یا حادثه‌ی سایبری رخ دهد، موظف است ظرف مدت ۶ ساعت این حادثه‌ی سایبری را گزارش نماید.

انواع حوادثی که تحت این محدوده قرار می‌گیرند عبارتند از: به خطر انداختن سیستم‌های حیاتی و حساس، اسکن هدف اسکن قرار گرفتن، دسترسی غیرمجاز به رایانه‌ها و حساب های رسانه‌های اجتماعی، دیفیس وب سایت، استقرار بدافزار، سرقت هویت، حملات DDoS، نقض و نشت داده-ها، اپلیکیشن‌های مخرب همراه، برنامه‌ها و حملات علیه سرورها و ابزارهای شبکه مانند روترها و دستگاه‌های IoT.

دولت اعلام کرده است که این اقدامات را انجام می‌دهند تا اطمینان حاصل کنند که IoCهای مرتبط با رویدادهای امنیتی به راحتی در دسترس هستند و انجام تجزیه و تحلیل، تحقیق و هماهنگی، مطابق با روند قانونی انجام می‌شود.

دستورالعمل‌ها همچنین به سازمان‌های مربوطه اعلام میدارد که ساعت‌های سیستم ICT را با سرور پروتکل زمان شبکه (NTP) مرکز ملی انفورماتیک (NIC) یا آزمایشگاه فیزیکی ملی (NPL) همگام‌سازی کنند، گزارش‌های سیستم‌های ICT را به مدت ۱۸۰ روز حفظ کنند و از ارائه دهندگان خدمات VPN می خواهد که اطلاعاتی مانند نام، آدرس، شماره تلفن، ایمیل و آدرس IP مشترکین را حداقل به مدت پنج سال ذخیره کنند.

علاوه بر این قوانین، که در مدت ۶۰ روز اجرایی می‌شوند، از ارائه دهندگان خدمات دارایی مجازی، صرافی و کیف پول می‌خواهند تا سوابق مشتریان خود (KYC) و تراکنش‌های مالی آنان را به مدت پنج سال نگه داری کنند.

گردآورنده: محمد مرتضوی

۱۰ سال جاسوسی

محققان امنیتی یک کمپینگ جاسوسی کشف کرده‌اند که توسط یک گروه هکری، تحت حمایت چین مدیریت می‌شوند. این کمپینگ از سال ۲۰۱۳ دولت‌ها، سیستم‌های آموزشی و سازمان‌های مخابراتی را هدف قرار می‌دادند.

مهاجمان از طیف وسیعی از تکنیک‌ها برای آلوده کردن اهداف خود به بدافزار استفاده می‌کردند، مانند استفاده از اسناد مخرب Word، دستگاه‌های جعلی قابل حمل و آنتی‌ویروس‌هایی با نماد جعلی که منجر به اجرای فایل‌های مخرب برروی سیستم قربانی می‌شدند.

این گروه بخاطر آشنایی کاربران با آیکون پوشه ویندوز و رابط فایل اکسپلورر آن برای فریب دادن قربانیان به اجرای فایل‌های اجرایی مخرب متکی بود. اهداف اصلی این گروه، سازمان‌هایی در منطقه آسیا و اقیانوسیه (APAC) از جمله استرالیا، کامبوج، هنگ کنگ، سنگاپور و ویتنام بودند.

جوی چن، محقق SentinelLabs معتقد است که Aoqin Dragon یک تیم کوچک چینی زبان است که امروزه به فعالیت خود هنوز ادامه می‌دهد و از دو Backdoor استفاده کرده است که با عملکرد غنی تر و مخفی کاری بیشتر به بهبود آن‌ها همچنان ادامه می‌دهد.

به گفته چن، این گروه بین سال‌های ۲۰۱۲ و ۲۰۱۵ به شدت به نقص‌های آفیس CVE-2012-0158 و CVE-2010-3333 برای به خطر انداختن اهداف خود با یک Backdoor برای دسترسی از راه دور متکی بوده.

این دو آسیب پذیری باعث اجرای کد از راه دور بودند که از پشتیبانی آفیس از فایل‌های Rich Text Format (.rtf) سوء استفاده می‌کردند.

مایکروسافت سال‌ها قبل از اینکه این گروه شروع به استفاده از این آسیب پذیری در اسناد جعلی کنند، برای این آسیب پذیری‌ها وصله‌های امنیتی را منتشر کرد.

از سال ۲۰۱۸، این گروه از دستگاه‌های قابل حمل USB آلوده به عنوان نقطه اولیه انتشار آلودگی استفاده می‌کردند. با کلیک بر روی آیکون میانبر (Shortcut)، لودر مخرب نصب می‌شود که دارای دو مرحله است. اول از همه فایل‌های مخرب را در دستگاه‌های قابل جابجایی برای پخش شدن در شبکه کپی می‌کند، و دوم، یک درب پشتی رمزگذاری شده است که می‌تواند یک دسترسی اجرای کد از راه دور ایجاد کند، فایل‌ها را در دستگاه قربانی بارگذاری کند و همچنین فایل‌های مورد نیاز را از سرورهای فرمان و کنترل مهاجم دانلود کند.

درب پشتی دیگر این گروه نسخه اصلاح شده پروژه منبع باز Heyoka است که از درخواست‌های جعلی DNS برای ایجاد یک تونل دو طرفه استفاده می‌کند.

گردآورنده: محمد مرتضوی

امکان سرقت تسلا با کلیدهای شخصی

سال گذشته، تسلا به‌روزرسانی‌ای را منتشر کرد که راه‌اندازی وسایل نقلیه خود را پس از باز شدن با کارت‌های کلید NFC آسان‌تر کرد. اکنون، یک محقق امنیتی نشان داده است که چگونه می‌توان از این ویژگی برای سرقت خودروها سوء استفاده کرد.

برای سال‌ها، رانندگانی که از کارت کلید NFC تسلا برای باز کردن قفل خودروهای خود استفاده می‌کردند، مجبور بودند برای شروع رانندگی، کارت را روی کنسول مرکزی قرار دهند. پس از به‌روزرسانی، رانندگان می‌توانستند با خودروهای خود بلافاصله پس از باز کردن قفل آن با کارت، کار کنند. کارت NFC یکی از سه وسیله برای باز کردن قفل تسلا است. یک جا کلیدی و یک برنامه تلفن دو مورد دیگر هستند.

مارتین هرفورت، یک محقق امنیتی در اتریش، به سرعت متوجه چیز عجیبی در مورد ویژگی جدید شد: این ویژگی نه تنها به خودرو اجازه می‌دهد تا ظرف ۱۳۰ ثانیه پس از باز شدن قفل با کارت NFC به طور خودکار روشن شود، بلکه خودرو را در وضعیتی قرار می‌دهد که قابل قبول باشد بدون نیاز به احراز هویت.

برنامه رسمی تلفن تسلا اجازه ثبت کلیدها را نمی‌دهد مگر اینکه به حساب مالک متصل باشد، اما علیرغم این، هرفورت دریافت که وسیله نقلیه به راحتی با هر دستگاه بلوتوث کم انرژی یا BLE که در نزدیکی آن است پیام‌ها را مبادله می‌کند. بنابراین این محقق اپلیکیشن خود به نام Teslakee را ساخت که به زبان VCSec صحبت می‌کند، همان زبانی که اپلیکیشن رسمی تسلا برای ارتباط با خودروهای تسلا از آن استفاده می‌کند.

نسخه مخرب Teslakee که هرفورت با هدف اثبات آسیب پذیری طراحی کرده است، نشان می‌دهد که برای سارقان چقدر آسان است که به طور مخفیانه کلید خود را در بازه زمانی ۱۳۰ ثانیه‌ای ثبت کنند. سپس مهاجم از برنامه Teslakee برای تبادل پیام‌های VCSec استفاده می‌کند که کلید جدید را ثبت می‌کند.

تنها چیزی که لازم است این است که در طول پنجره حیاتی ۱۳۰ ثانیه‌ای که قفل آن با کارت NFC باز می شود، در محدوده خودرو باشید. اگر مالک وسیله نقلیه معمولاً از برنامه تلفن برای باز کردن قفل ماشین استفاده می‌کند - تا حد زیادی رایج‌ترین روش باز کردن قفل برای تسلا - مهاجم می‌تواند با استفاده از یک مسدود کننده سیگنال برای مسدود کردن فرکانس BLE مورد استفاده توسط اپلیکیشن تسلا، از کارت NFC استفاده کند.

گردآورنده: محمد مرتضوی

KHARAZMI CERT COORDINATION CENTER

مرکز آپا دانشگاه خوارزمی

رئیس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

جناب آقای دکتر عبادتی

سرکار خانم دکتر یعقوبی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

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.

معاونت پژوهش و فناوری