بولتن تحلیلی ■ فروردین ماه ۱۳۹۹

امنیت اطلاعات

پادویش®
Padvish®
بولتن تحلیلی امنیت اطلاعات،
تهیه شده توسط پادویش

فهرست مطالب

پیش گفتار

در این شماره از خبرنامه پادویش، به تازه‌ترین اخبار منتشر شده در حوزه امنیت و رویدادهای بدافزاری خواهیم پرداخت. در ابتدا یکی از بدافزارهای اندرویدی را معرفی و برخی ابهامات درباره خدمات ارزش افزوده را برطرف خواهیم کرد. در ادامه به تروجان‌ها، یکی از شایع‌ترین گونه های بدافزاری، می‌پردازیم و بدافزار Adwind را معرفی می‌کنیم. سپس به چند مورد از اصلاحیه‌های امنیتی منتشر شده در دو ماه اخیر و جزئیات هریک اشاره می کنیم. در انتها نیز اخبار امن پرداز در دو ماه گذشته را مرور خواهیم‌کرد.

خدمات ارزش افزوده و یا خدمات محتوایی و جدال بر سر قانونی یا غیر قانونی بودن آن، از بحث‌های داغ سال های اخیر در حوزه فناوری اطلاعات بوده است. این نوع سرویس که باید با اطلاع کاربر فعال شود، با ارائه محتوا به صورت پیامکی و یا از طریق برنامه‌های موبایلی، هزینه‌ای را از آنها دریافت می‌کند. جنبه غیر قانونی و کلاهبرداری خدمات ارزش افزوده زمانی نمایان می‌شود که اپراتور و یا ارائه دهنده خدمات، بدون آگاهی کاربر مبلغی هر چند ناچیز به قبض موبایل آنها اضافه می‌کند. در ادامه به یکی از بدافزارهایی که با سوء استفاده از خدمات ارزش افزوده به سرقت اطلاعات کاربران و دریافت هزینه از کاربران خود می‌پردازد، اشاره می‌کنیم.

بدافزار SMSReg

بدافزار تبلیغاتی SMSReg با هدف انجام تبلیغات حرفه‌ای و مطمئن و با استفاده از سرویس آماروید (Amaroid) که متعلق به شرکت ژوبین است، اطلاعات و علایق کاربران را جمع‌آوری می‌نماید و همچنین آنها را در سرویس‌های ارزش افزوده عضو می‌کند. اخیرا انتشار گروهی از اپلیکیشن‌های آلوده در فضای مجازی مانند کانال‌های مختلف تلگرامی یا صفحات تبلیغ‌های اینستاگرامی مشاهده شده است که به دنبال عضو کردن کاربران در سرویس‌های ارزش افزوده و در نهایت دریافت وجه هستند. انواع مختلفی از این اپلیکیشن‌ها و با نام‌های مختلفی مانند رضوان، جعبه شادی، پرداخت قبض و ... با هدف عضویت افراد در سرویس‌های ارزش افزوده شکل گرفته‌اند.

عملکرد این بدافزارها به این صورت است که به محض نصب و اجرای برنامه، صفحه‌ای با این مضمون به کاربر نمایش داده می‌شود که برای استفاده از برنامه لازم است در یک سرویس ارزش افزوده که از قبل در برنامه مشخص شده است، عضو شود و با راه‌اندازی برنامه از امکانات آن استفاده کند. در این شرایط، حتی پس از حذف برنامه به دلیل عضویت در سرویس مذکور همچنان برروی قبض گوشی کاربر، بدون اینکه دلیل آن را بداند، مبلغی اضافه می‌شود. فعال‌سازی این سرویس‌ها در ازای برداشت مبلغی به صورت روزانه و یا ماهانه است. این برنامه‌ها اغلب اپلیکیشن‌هایی غیرکاربردی هستند که یا محتوایی در برنامه وجود ندارد و یا این محتوا به رایگان در بستر اینترنت در دسترس همگان قرار دارد.

از اهداف دیگر این بدافزار، نمایش تبلیغات با توجه به علاقمندی کاربر و با استفاده از سرویس داده کاوی آماروید است. آماروید پلتفرمی متعلق به شرکت ایده پردازان ژوبین و فعال در زمینه تجزیه و تحلیل دیتا و اطلاعات مربوط به رفتار کاربران در حین استفاده از اپلیکیشن‌هاست و از مجوز "com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE" استفاده می‌کند.

می‌توان نتیجه گرفت که این اپلیکیشن دقت بیشتری برای تبلیغات اینترنتی دارد، چرا که دانستن این نکته که افراد از چه راهی اپلیکیشن را دانلود می‌کنند و یا بعد از نصب آن چه کرده‌اند، اهمیت زیادی دارد. مثلا برای انتخاب زمان نمایش تبلیغات، با در نظر داشتن شلوغ‌ترین زمان مراجعه کاربران به اپلیکیشن، می‌توان برنامه‌های تبلیغاتی را با حداکثر بازده به سمت آنها ارسال کرد. علاوه بر این، اطلاعات مربوط به تاریخچه مرورگرها مانند جستجوهای کاربر در مرورگر تلفن همراه و موقعیت مکانی، بر نوع تبلیغاتی که قرار است برای هر کاربر ارسال شود، اثر گذار است.

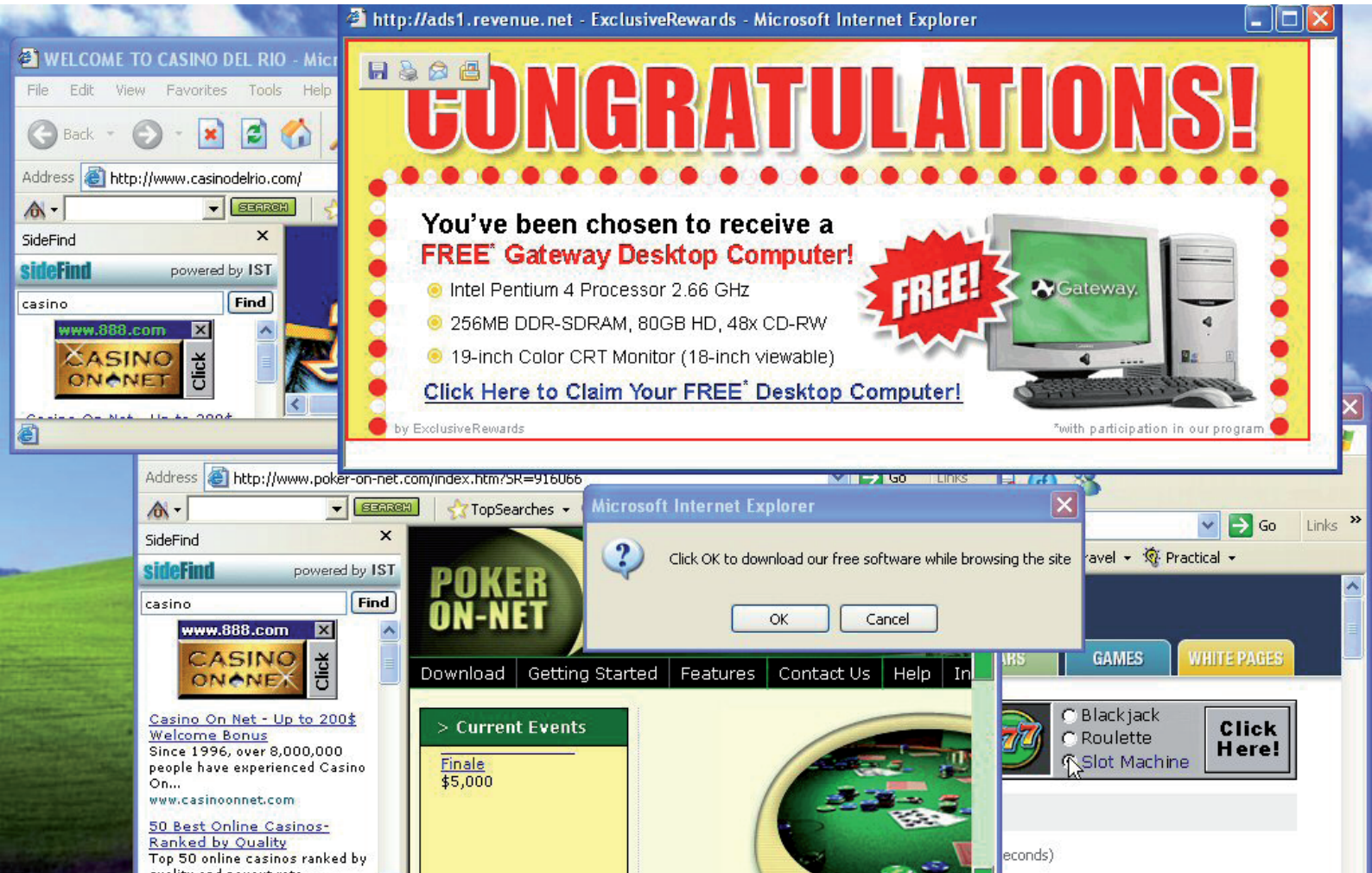
راهکارها:

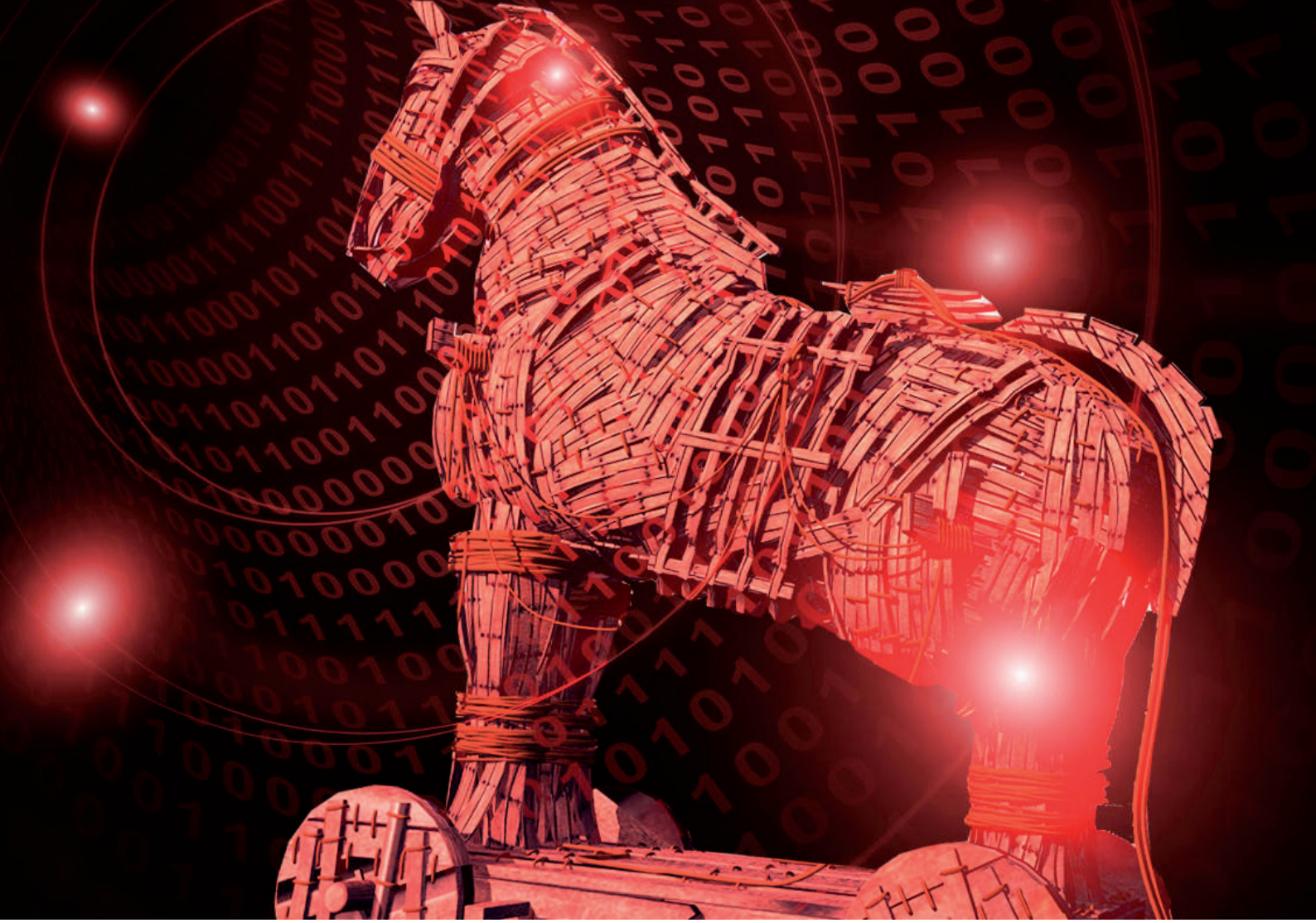
برای پاک‌سازی این بدافزار، ابتدا برنامه را از تلفن همراه خود حذف کنید و برای لغو اشتراک اقدامات زیر را انجام دهید:

ابتدا با شماره گیری #۸۰۰* سرویس‌های فعال را مشاهده و کد دستوری ارسال شده برای لغو سرویس را با توجه به پیام ارسال شده بفرستید.

اگر سیم کارت شما ایرانسل است، بهتر است تمامی سرویس‌های ارزش افزوده را به طور یک‌جا غیرفعال نمایید و یا اینکه به حساب کاربری خود در فروشگاه چارخونه مراجعه و اشتراک خود را لغو کنید.

برای اطمینان خاطر از عدم آلودگی دستگاه، فایل پایگاه داده آنتی‌ویروس پادویش را به‌روز نگه دارید و اسکن آنتی‌ویروس را انجام دهید. این بدافزار توسط آنتی ویروس پادویش، شناسایی می‌شود.





تروجان‌ها خانواده بزرگی از بدافزارها هستند که طیف وسیعی از تغییرات را بر روی سیستم کاربران ایجاد می‌کنند. با شروع فعالیت هر تروجان ممکن است عملیات متفاوتی صورت گیرد که شدت تخریب آن به نوع تروجان بستگی دارد. این تغییرات شامل حذف، مسدود، تغییر و کپی کردن اطلاعات و یا اختلال در عملکرد کامپیوتر و شبکه می‌شود. در متن پیش رو، یکی از تروجان‌هایی که غالبا با هدف جاسوسی از اطلاعات کاربران وارد سیستم می‌شود را معرفی خواهیم کرد.

بدافزار Adwind

سازندگان برنامه‌های مخرب با کمک بدافزار Adwind اطلاعات کاربران را به سرقت می‌برند. این بدافزار که از خانواده تروجان‌هاست و به شکلی کاملا قانونی وارد سیستم قربانی می‌شود، پس از اولین اجرا عملیات جاسوسی خود را آغاز می‌کند. مهاجمان با به‌کارگیری این بدافزار، داده‌های سیستم را جمع‌آوری و استخراج می‌کنند و با دسترسی از راه دور، کنترل اوضاع را به دست می‌گیرند. در نهایت، با مخفی کردن اطلاعات از دید کاربر، دسترسی او را بر برخی از فایل‌ها دچار مشکل می‌کنند. ابزارهای ورودی/خروجی مانند صفحه کلید، ماوس و صفحه نمایش در جمع‌آوری اطلاعات مورد نیاز مهاجمان و رسیدن به اهداف خرابکارانه آنها بسیار مؤثرند.

جهت پیشگیری از آلودگی به Adwind و بدافزارهای مشابه توجه داشته باشید که تروجان‌ها غالبا از راه نرم‌افزارهای فاقد اعتباری که از اینترنت دانلود می‌شوند، جاسازی شدن در متن HTML و یا ضمیمه شدن به یک ایمیل خود را به سیستم قربانی می‌رسانند. خوشبختانه تروجان‌ها توانایی تکثیر خودکار خود را ندارند و با انجام اقدامات پیشگیرانه می‌توان از ورود آنها به سیستم جلوگیری کرد.

اصلاحیه‌های امنیتی منتشر شده در دو ماه اخیر

اصلاحیه‌های امنیتی مایکروسافت

اصلاحیه ماه میلادی مارس: مایکروسافت در ماه مارس برای رفع ۱۱۵ آسیب‌پذیری امنیتی در نسخه‌های مختلف سیستم عامل ویندوز و نرم افزارهای مرتبط، به‌روزرسانی‌هایی منتشر کرد که بزرگترین اصلاحیه‌ی منتشر شده‌ی این شرکت تا به امروز به شمار می‌رود. ۱۱۵ نقص برطرف شده محصولات مختلفی را در بر گرفته است که شامل مایکروسافت ویندوز، مرورگر Edge، اینترنت اکسپلورر، Windows Defender، Azure، office، Exchange server و visual studio می‌شود. از میان اصلاحیه‌های منتشر شده، ۲۶ مورد "بحرانی"، ۸۸ مورد "با اهمیت" و ۱ مورد "متوسط" هستند.

آسیب پذیری بحرانی

مهم‌ترین آسیب‌پذیری این ماه که پس از انتشار اصلاحیه‌ی ماه مارس به صورت جداگانه عرضه شد، مربوط به آسیب‌پذیری خطرناک پروتوکل SMBv۳ است که به مهاجمان اجازه راه‌اندازی بدافزاری کرم‌گونه را می‌دهد تا به صورت خودکار از یک کامپیوتر آسیب‌پذیر به کامپیوتری دیگر منتشر شود. این آسیب‌پذیری با شناسه CVE-۲۰۲۰-۰۷۹۶ مشخص شده است و منجر به اجرای کد از راه دور در ویندوز۱۰ و ویندوز سروری نسخه‌های ۱۹۰۳ و ۱۹۰۹ خواهد شد. Server Message Block یا به اختصار SMB که در پورت TCP ۴۴۵ اجرا می‌شود، یک پروتوکل شبکه‌ای است که برای اشتراک گذاشتن دسترسی به فایل‌ها، چاپگرها و ارتباطات بین پردازش از طریق شبکه طراحی شده است.

سایر اصلاحیه‌های مایکروسافت

آسیب‌پذیری اجرای کد از راه دور LNK که با شناسه CVE-۲۰۲۰-۰۶۸۴ مشخص شده است توسط مهاجمان، فایل‌های میان بر مخرب LNK ایجاد می‌کند و سبب اجرای کد موردنظر آنها می‌شود.

آسیب‌پذیری اجرای کد از راه دور مایکروسافت word با شناسه CVE-۲۰۲۰-۰۸۵۲ مشخص شده است. این نقص به بدافزار اجازه می‌دهد تا با مشاهده یک فایل Word خاص ساخته شده در صفحه پیش نمایش و با همان مجوزهایی که در حال حاضر وارد سیستم شده است، کد موردنظر خود را در سیستم اجرا کند.

چندین مورد آسیب‌پذیری نیز مربوط به اینترنت اکسپلورر با شناسه‌های CVE-۲۰۲۰-۰۸۳۳ و CVE-۲۰۲۰-۰۸۲۴، موتور اسکریپت Chakra با شناسه CVE-۲۰۲۰-۰۸۱۱ و مرورگر Edge با شناسه CVE-۲۰۲۰-۰۸۱۶ است.

اصلاحیه ماه میلادی آوریل: مایکروسافت patchهای مربوط به ۱۱۳ آسیب‌پذیری و ۱۱ محصول خود را منتشر کرده است. حداقل ۳ مورد از این آسیب‌ها مورد بهره‌برداری قرار گرفته‌اند و ۲ مورد دیگری که جزئیات آنها منتشر شده است، در معرض سوءاستفاده هکرها قرار دارند. ۱۹ مورد از ضعف‌های ترمیم شده با درجه بحرانی اعلام شده‌اند؛ به این معنی که مهاجمان می‌توانند کنترل کامل سیستم آسیب‌پذیر را از راه دور و بدون نیاز به کمک کاربر در اختیار بگیرند.

آسیب پذیری‌های مورد بهره برداری مهاجمان

یکی از مهم‌ترین موارد این ماه مربوط به اصلاحیه CVE-۲۰۲۰-۱۰۲۰، نقص موجود در کتابخانه برنامه Adobe Font Manager است که به گفته مایکروسافت مورد سوءاستفاده مهاجمان قرار گرفته‌است. دیگر آسیب‌پذیری روز صفر نیز مربوط به کتابخانه Adobe Font Manager و با شناسه CVE-۲۰۲۰-۰۹۳۸ است.

آسیب‌پذیری روز صفر بعدی مربوط به CVE-۲۰۲۰-۱۰۲۷ است و مربوط به نقص کرنل ویندوز می‌شود. مایکروسافت این مورد را با درجه مهم اعلام کرده است، چرا که از نوع ترفیع امتیاز (elevation of privilege) بوده و بدون اعتبار سنجی مهاجم، سوء استفاده از این آسیب‌پذیری ممکن نیست.

اصلاحیه‌های امنیتی Adobe- آوریل ۲۰۲۰

شرکت نرم افزاری ادوبی در به‌روزرسانی‌های امنیتی ارائه شده در ماه آوریل، به آسیب‌پذیری‌های موجود در سه محصول خود پرداخته‌است. مهاجمان قادرند از برخی از این آسیب‌پذیری‌ها بهره برداری کنند و کنترل سیستم آسیب‌دیده را در دست گیرند. به‌روزرسانی های ارائه شده شامل موارد زیر هستند:

به‌روزرسانی Adobe ColdFusion

به‌روزرسانی Adobe After Effects

به‌روزرسانی Adobe Digital Editions

تازه‌های پادویش

انتشار نسخه رایگان پادویش در اسفند ماه

نسخه کاملا رایگان پادویش اندروید منتشر شد. آنتی‌ویروس پادویش، یک راه حل قدرتمند و سریع برای حفاظت همه جانبه از دستگاه‌های اندرویدی است که به طور پیوسته به‌روزرسانی می‌شود و سیستم شما را از خطر آلودگی به هرگونه ویروس، بدافزار، باج افزار و سایر تهدیدات مخرب، محافظت می‌کند. آنتی‌ویروس بومی پادویش، مجهز به فناوری قدرتمند اسکن درون ابری برای دستگاه‌های اندرویدی است و از جدیدترین صنعت پیشرو در زمینه تشخیص ویروس استفاده می‌کند و مهم‌تر از همه، کندی دستگاه و یا مصرف بی‌اندازه باتری را به همراه نخواهد داشت.

انتشار نسخه جدید آنتی ویروس پادویش در فروردین ماه

نسخه جدید آنتی ویروس پادویش جهت استفاده کاربران سازمانی و خانگی منتشر شد.

نسخه ۲.۶.۸۸۴.۵۵۹۷ امنیت کامل پادویش شامل تغییرات زیر است:

- بهبود عملکرد ضد باج‌گیر
- بهبود عملکرد در ویندوز ۱۰
- رفع باگ‌های جزئی

برای اطلاعات بیشتر و مطالعه تحلیل فنی و اخبار روز بدافزارها می‌توانید به وب‌سایت‌های تخصصی امن‌پرداز مراجعه کنید:

news.amnpardaz.com

threats.amnpardaz.com

همچنین برای دریافت هرگونه مشاوره‌ی تخصصی در زمینه امنیت اطلاعات و توسعه نرم‌افزار، از راه‌های زیر با کارشناسان ما در ارتباط باشید:

۰۲۱-۴۳۹۱۲۰۰۰

support@amnpardaz.com

https://t.me/padvishsecurity

https://sapp.ir/padvishsupport

WWW.PADVISH.COM