خبرنامه تحلیلی پادویش ■ شهریور ماه ۱۳۹۹

امنیت اطلاعات

پادویش®
Padvish®

خبرنامه تحلیلی امنیت اطلاعات،
تهیه شده توسط پادویش

امنیت اطلاعات

فهرست مطالب

مقدمه

در خبرنامه تحلیلی شهریور ماه ۹۹ پادویش، تازه‌ترین اخبار منتشر شده در حوزه امنیت فضای مجازی و رویدادهای بدافزاری را در سه بخش مرور خواهیم کرد.

در ابتدا، هشدارهای امنیتی منتشر شده از سوی پادویش، در ارتباط با معرفی یکی از سایت‌های فیشینگ بورسی را بررسی می‌کنیم. در ادامه، به تازه‌ترین تهدیدهای بدافزاری تحلیل شده از سوی آزمایشگاه تحلیل پادویش در شهریور ماه می‌پردازیم. برای مطالعه تحلیل‌های فنی و تخصصی درباره هر یک از بدافزارهای ارائه شده، می‌توانید به بانک اطلاعات تهدیدات بدافزاری پادویش که آدرس آن در انتهای گزارش آمده است، مراجعه کنید. در انتها نیز، اخبار امن پرداز که در ارتباط با تازه‌ترین نسخه‌های منتشر شده از محصولات امن پرداز هستند، ارائه شده است.

انتشار خبرنامه تحلیلی پادویش در انتهای هر ماه به منظور ارائه خلاصه‌ای از اخبار منتشر شده توسط پادویش انجام می‌شود. شما می‌توانید برای دریافت اخبار به‌روز از آخرین حملات سایبری و تحلیل‌های منتشر شده از سوی کارشناسان پادویش، به اتاق خبر امن پرداز و صفحه پادویش در شبکه‌های اجتماعی مراجعه نمایید.

هشدارهای امنیتی پادویش

کاربران بورس مراقب سایت سجام تقلبی باشند

خبر اختصاصی پادویش؛ سایت sejam[.]press توسط افزونه آنتی فیشینگ پادویش به عنوان سایتی جعلی شناسایی شده است. سیستم سجام که برای تسهیل امور سرمایه‌گذاران در بورس و به عنوان منبعی معتبر برای پیگیری اخبار بورس شناخته می‌شود، تنها از طریق آدرس اینترنتی sejam.ir قابل دسترس است. با توجه به شیوع بالای کلاهبرداری‌های فیشینگ در کشور، لازم است کاربران معیارهای لازم برای معتبر بودن یک سایت اینترنتی را شناخته و در این زمینه دقت کافی داشته باشند. این موضوع به ویژه در ارتباط با درگاه‌های پرداخت بانکی و یا سایت‌هایی مثل سجام که اطلاعات حساب کاربری مهمی را درخواست می‌کنند، حائز اهمیت است. با توجه به پیچیده شدن روش‌های فیشینگ در سال‌های اخیر، در بسیاری از موارد تشخیص سایت جعلی از اصلی برای کاربران عادی امکان‌پذیر نیست. بنابراین، توصیه می‌شود از ابزارهای آنتی فیشینگ معتبر مانند افزونه آنتی‌فیشینگ پادویش برای امنیت هر چه بیشتر استفاده نمایید.

با توجه به پیچیده شدن روش‌های فیشینگ در سال‌های اخیر، در بسیاری از موارد تشخیص سایت جعلی از اصلی برای کاربران عادی امکان‌پذیر نیست.

تهدیدها

کلاهبردارانی که برای شارژ سیم کارت شما "نقشه" می کشند

بدافزار اندرویدی Agent.Smsa از خانواده تروجان‌ها و یکی از ده‌ها بدافزاری است که با استفاده از سرویس‌های ارزش افزوده از کاربران کلاهبرداری می‌کنند. این برنامه که با عنوان "نقشه" در بازارهای اندرویدی منتشر شده است، هیچ اطلاعات مفید و کاربردی به کاربر ارائه نمی‌دهد. با این حال، با فعال کردن سرویس ارزش افزوده بر روی گوشی و کسر روزانه مبلغی مشخص از شارژ سیم کارت، سود زیادی عاید سازندگان بدافزار می‌شود.

پس از عضویت در این سرویس ارزش افزوده، کاربر با محتوایی جعلی و بی‌ارزش که به رایگان در بستر اینترنت در دسترس بوده است، روبرو می‌شود. در نهایت، علاوه بر دریافت هزینه برای عضویت در سرویس ارزش افزوده، با دانلود دو برنامه مخرب دیگر بدون اجازه و اطلاع کاربر، به عنوان یک دانلودر زمینه حضور سایر بدافزارها را نیز فراهم می‌کند. دیگر بدافزارهایی که با همین روش از کاربران کلاهبرداری می‌کنند با نام‌هایی چون برنامه‌های مستهجن، برنامه‌های معروف و کاربردی مانند نقشه، اینستاگرام، تلگرام طلایی، ایرانسل من و ... منتشر می‌شوند.

> **پس از عضویت در این سرویس ارزش افزوده، کاربر با محتوایی جعلی و بی‌ارزش که به رایگان در بستر اینترنت در دسترس بوده است، روبرو می‌شود.**

برای پیشگیری از آلوده شدن گوشی، از دانلود و نصب برنامه از منابع و مارکت‌های موبایلی نامعتبر خودداری کنید و به هنگام نصب آنها، به مجوزهای درخواستی دقت کنید. آنتی ویروس پادویش، این بدافزار را شناسایی و از سیستم شما محافظت می‌کند.

به دنبال ردیابی لپ تاپ سرقت شده خود هستید؟ (مراقب این روت کیت خطرناک باشید)

روت‌کیت‌ها یکی دیگر از گونه‌های بدافزاری هستند و به شکلی طراحی شده‌اند تا عملکرد خود را در سیستم پنهان نگه دارند. بنابراین، در زمانی که مشغول فعالیت مخرب خود هستند، کاربر متوجه اتفاق مشکوکی در سیستم نخواهد شد. قابلیت دیگر این گونه بدافزاری، در اختیار گذاشتن کنترل از راه دور سیستم به سازندگان بدافزار و مجرمان سایبری است و از آنجایی که روت‌کیت‌ها توانایی غیرفعال کردن ابزارهای محافظتی سیستم و یا پنهان شدن از آنها را دارند، می‌توانند تا مدت طولانی فعال بمانند و خسارات زیادی به بار بیاورند. روت‌کیت‌ها انواع مختلفی دارند که در اینجا به معرفی یکی از روت‌کیت‌های سفت افزار (firmware) می‌پردازیم.

> **از آنجایی که روت‌کیت‌ها توانایی غیرفعال کردن ابزارهای محافظتی سیستم و یا پنهان شدن از آنها را دارند، می‌توانند تا مدت طولانی فعال بمانند و خسارات زیادی به بار بیاورند.**

بدافزار روت‌کیتی Lojax، ساخته یکی از گروه‌های نفوذگر با نام fancy bear یا APT۲۸ است. کار اصلی این بدافزار ایجاد یک درب پشتی و دانلودر (جهت دانلود سایر بدافزارها) با بقای بسیار بالا در سیستم قربانی خواهد بود. این بدافزار از راه نرم‌افزار ضدسرقت Computrace LoJack، که خود نوعی نرم‌افزار با عملکرد مشابه روت‌کیت‌ها است، به سیستم کاربران نفوذ می‌کند. Computrace LoJack به این منظور استفاده می‌شود تا در صورت سرقت و حتی پاک‌سازی کامل حافظه رایانه، صاحب اصلی قادر به رصد، شناسایی و کنترل سیستم خود باشد. بدافزار Lojax هم با سوءاستفاده از این ابزار و آسیب‌پذیری ذاتی نسخه‌های پیشین آن، عاملی بدافزاری را جایگزین عامل اصلی برنامه سالم Computrace LoJack کرده و با توجه به چشم پوشی برنامه‌های ویروس‌یاب از این برنامه سالم، Lojax نیز از شناسایی می‌گریزد.

علائم آلودگی

از آنجایی که کلیه عملیات بدافزار هنگام بوت (Boot) رخ می‌دهند، در سیستم‌عامل به جز علائم ثانویه چیزی مشاهده نمی‌شود. درواقع هنگام بالا آمدن سیستم‌عامل، بدافزار رد پای خود را می‌پوشاند. آنتی ویروس پادویش، این بدافزار را شناسایی و از سیستم شما محافظت می‌کند.

اخبار امن پرداز

انتشار نسخه جدید آنتی ویروس پادویش

نسخه ۲.۸ ضدبدافزار خانگی پادویش (نسخه کاندیدای پایدار) منتشر شد.

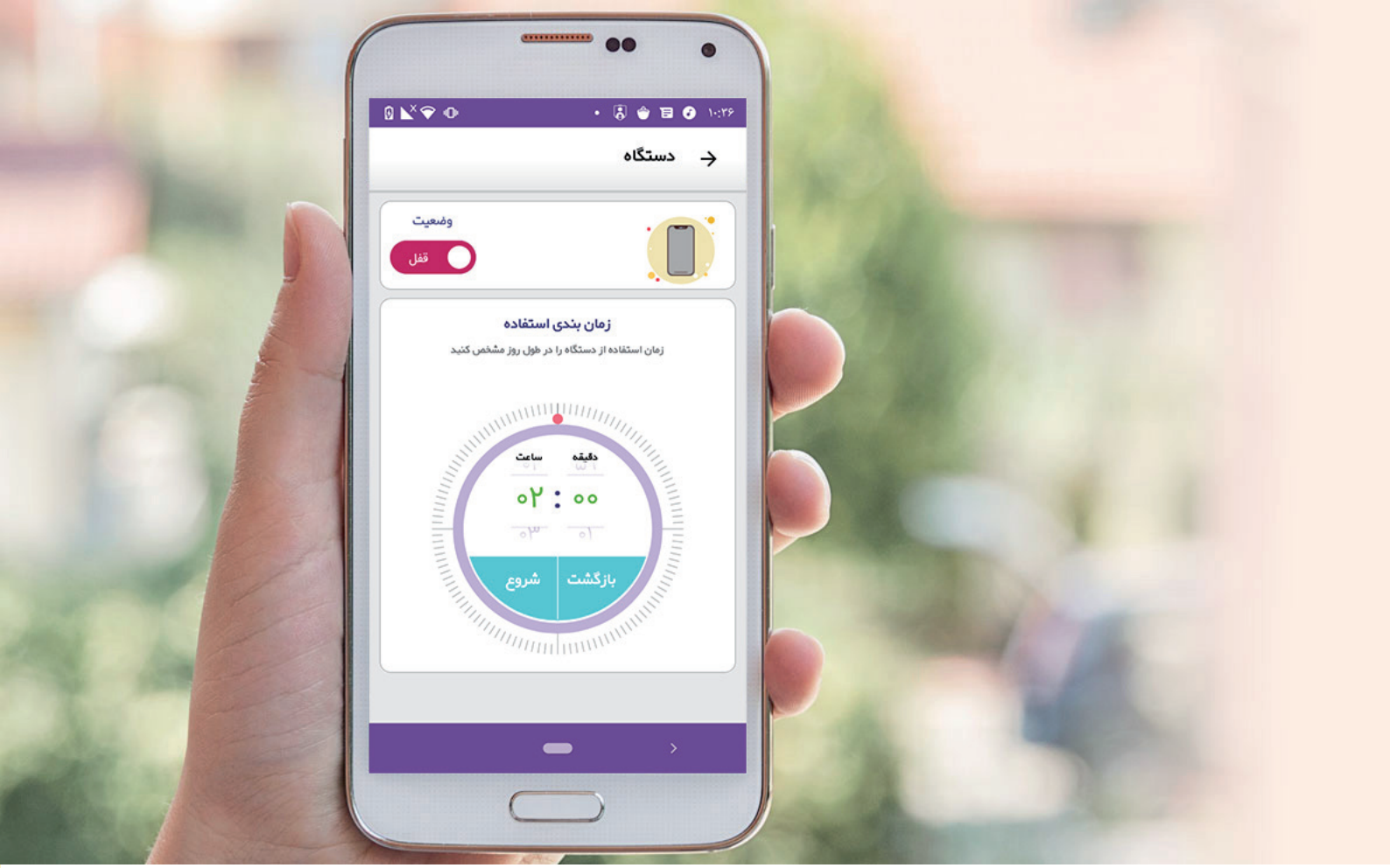
آخرین نسخه ضدبدافزار پادویش ۲٫۸٫۶۷۹٫۶۳۰۲ شامل تغییراتی در موارد زیر است:

• محافظت از شبکه: با مسدودسازی خودکار آدرس‌های مبدا حملات شبکه‌ای، محافظت از شبکه به شکل چشم‌گیری بهبود یافته است (پشتیبانی از رنج آدرس و Subnet در قواعد دیوار آتش به قابلیت‌های قبلی اضافه شده است).

• پویشگر ضدبدافزار: پاکسازی بدافزارهای چندلایه پیچیده به صورت همزمان و به‌کارگیری نسخه جدید امولاتور ویروس، سبب تشخیص قوی‌تر ویروس‌های چندریختی و محافظت حداکثری از سیستم کاربران می‌شود. علاوه بر این، امکان تشخیص بدافزار در فایل‌های اسناد به کمک موتور هوشمند نسخه جدید میسر شده است. در نهایت، با قدرتمندتر شدن ضد باج‌گیر پادویش و بهبود پاکسازی خودکار، باج‌افزارهای جدید با دقت بالایی شناسایی می‌شوند.

• کنترل ابزار: در نسخه جدید پادویش خانگی، برای سهولت بیشتر کاربران، امکان تعریف قواعد جداگانه برای ابزارهای اسکنر (مجزا از ابزارهای پرتابل) فراهم شده است. همچنین، از تبدیل CD/DVD Writer به CD/DVD ROM (حالت فقط خواندنی برای دیسک نوری) و حالت ReadOnly برای درایوهای با فایل‌سیستم NTFS پشتیبانی می‌شود.

به تمامی کاربران توصیه می‌شود از آخرین نسخه آنتی‌ویروس پادویش، که از سایت پادویش قابل دانلود است، برای محافظت سیستم خود استفاده کنند. همچنین به‌روزرسانی خودکار پادویش نیز به مرور سیستم‌های کاربران را به نسخه آخر ارتقا خواهد داد.



انتشار نسخه جدید پادویش پرنتال کنترل

نسخه ۱٫۱۵٫۱۱۱٫۲۲۸ پادویش پرنتال کنترل برای اندروید (نسخه کاندیدای پایدار) منتشر شد.

امروزه حفاظت و مراقبت از فرزندان در استفاده از دستگاه‌های اندرویدی، به یک دغدغه بزرگ برای بسیاری از خانواده‌ها تبدیل شده است. استفاده از پادویش پرنتال کنترل، راهکاری مناسب برای مدیریت فرزندان در استفاده از این نوع دستگاه‌هاست که آسودگی خاطر والدین و استفاده درست و بهینه فرزندان از گوشی‌ها و تبلت‌های اندرویدی را به همراه دارد.

قابلیت‌های پادویش پرنتال کنترل شامل موارد زیر می‌شوند:

- مدیریت و کنترل دیتا طبق زمانبندی مشخص و مورد نظر والدین
- امکان قفل کردن دستگاه همراه با اعمال زمانبندی استفاده
- مسدودسازی استفاده از دوربین جهت جلوگیری از به خطر افتادن امنیت کاربران
- زمان بندی دلخواه برای استفاده از برنامه‌های مختلف
- مدیریت استفاده از وای فای طبق زمانبندی اعمال شده
- قابلیت عدم حذف نصب جهت جلوگیری از حذف برنامه توسط فرزند
- امکان دریافت آخرین به‌روزرسانی برنامه به صورت خودکار
- امکان مشاهده خلاصه‌ای از برنامه‌های مسدود شده

نسخه جدید پادویش پرنتال کنترل علاوه بر قابلیت‌های پیشین با تغییرات زیر همراه بوده است:

- مکان‌یابی و مسیریابی فرزند که به آسانی و در هر زمان قابل دسترس است.
- بهبود رابط کاربری و رفع اشکالات نرم‌افزاری

کاربران محترمی که از نسخه قبلی استفاده می‌کنند با دریافت نسخه جدید از سایت پادویش و نصب آن روی نسخه قبلی، می‌توانند از امکانات جدید پرنتال کنترل پادویش استفاده نمایند.

مختصری درباره امن‌پرداز

شرکت نرم‌افزاری امن پرداز از سال ۱۳۸۳ فعالیت خود را آغاز نموده و به عنوان اولین آنتی ویروس کاملا ایرانی، در جهت برقراری امنیت در فضای سایبری همواره همراه و پشتیبان کاربران خود بوده است. در تلاشیم تا به عنوان مرجعی قابل اعتماد و قابل رقابت با آنتی ویروس‌های خارجی، محصولی متناسب با نیازهای کاربران مختلف خانگی و سازمانی عرضه کنیم. علاقه‌مندان به دریافت اطلاعات بیشتر و مطالعه تحلیل فنی و اخبار روز بدافزارها می‌توانند به وب‌سایت‌های تخصصی امن‌پرداز مراجعه کنند. همچنین برای دریافت هرگونه مشاوره‌ی تخصصی در زمینه امنیت اطلاعات و توسعه نرم‌افزار، از راه‌های زیر با کارشناسان ما در ارتباط باشید:

threats.amnpardaz.com

news.amnpardaz.com

۰۲۱-۴۳۹۱۲۰۰۰

support@amnpardaz.com

https://t.me/padvishsecurity

https://sapp.ir/padvishsupport

WWW.PADVISH.COM