امنیت اطلاعات

خبرنامه تحلیلی پادویش آبان ماه ۱۳۹۹

پادویش®
Padvish

خبرنامه تحلیلی امنیت اطلاعات،
تهیه شده توسط پادویش

خبرنامه تحلیلی پادویش

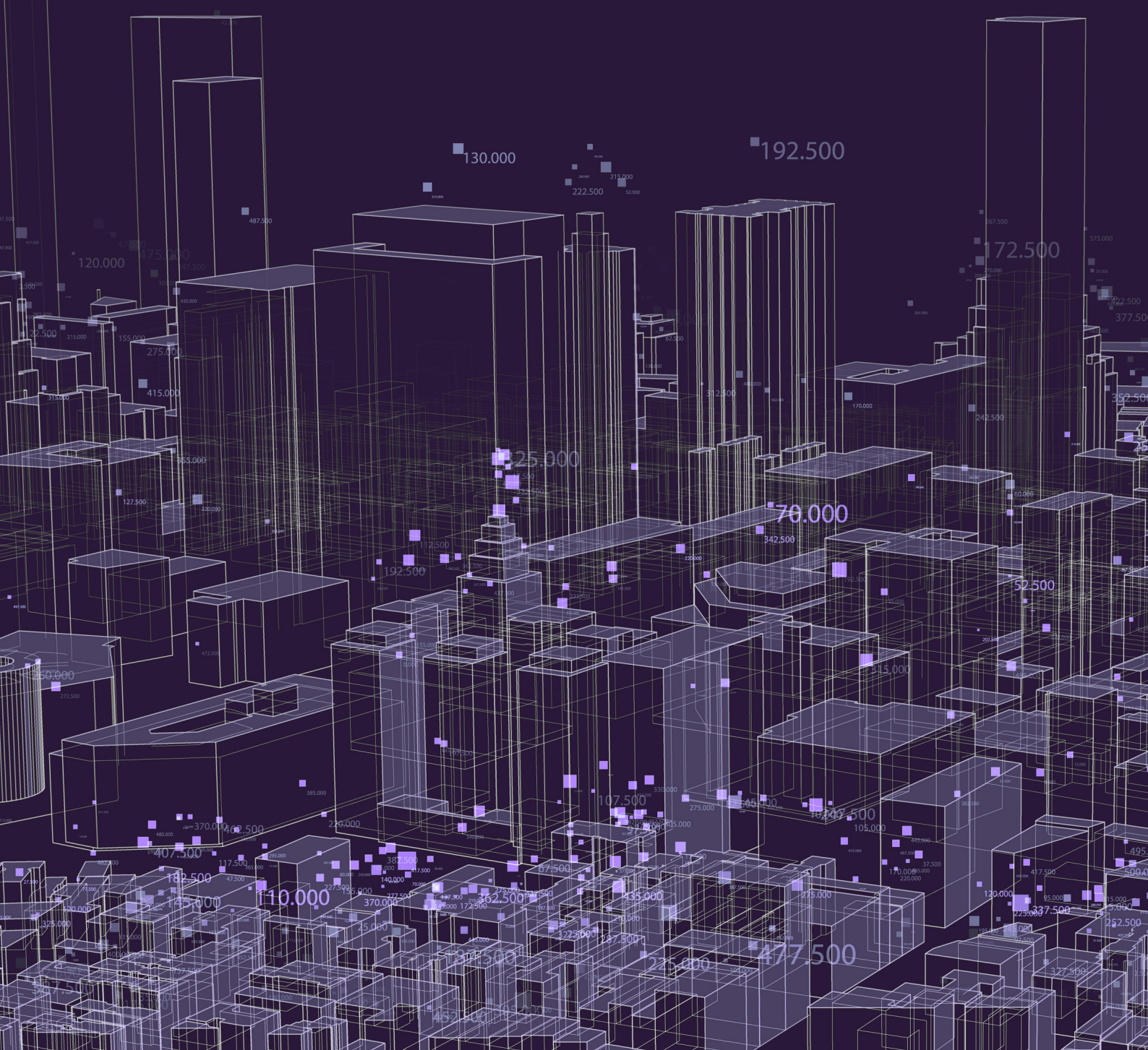
آبان ۹۹

فهرست مطالب

مقدمه

در خبرنامه تحلیلی آبان ماه ۹۹ پادویش، به آخرین اخبار منتشر شده در اتاق خبر امن‌پرداز در حوزه امنیت فضای مجازی و رویدادهای بدافزاری می‌پردازیم.
اخبار این شماره در ۳ بخش تنظیم شده است. در ابتدا تهدیدهای بدافزاری تحلیل شده از سوی آزمایشگاه تحلیل بدافزار پادویش ارائه شده است. پس از آن و در بخش مطالب آموزشی، راهکارهای ساده‌ای برای حفظ امنیت کودکان و نوجوانان در فضای مجازی معرفی شده است. در انتها نیز، با خبری درباره انتشار نسخه امنیت کامل پادویش، خبرنامه آبان ماه را به پایان می‌بریم.

شما می‌توانید برای مطالعه خبرهای منتشر شده از بدافزارهای تحلیل شده از سوی آزمایشگاه تحلیل بدافزار پادویش و اطلاع از جدیدترین هشدارهای امنیتی به سایت اتاق خبر امن پرداز مراجعه نمایید.



تهدیدها

پشت پرده ویدئوهای محبوب TikTok چه می گذرد؟

تیک‌تاک، شبکه اجتماعی چینی محبوب که برای اشتراک‌گذاری موزیک ویدئوهای کوتاه ۳ تا ۶۰ ثانیه‌ای استفاده می‌شود، در ماه‌های اخیر در بسیاری از کشورها از جمله ایران، سر و صدای زیادی به راه انداخته است. تا جایی که بسیاری افراد و دولت‌ها ازجاسوسی بودن برنامه تیک‌تاک خبر می‌دهند، در برخی کشورها از جمله هند و آمریکا فیلتر شده و حتی از لیست برنامه‌های Google Play نیز حذف شده است.

با وجود خبرهای منفی منتشر شده، این برنامه همچنان از محبوبیت بالایی در میان کاربران برخوردار است و همین موضوع سبب ساخت برنامه‌های مشابه بسیاری با عناوین مختلف در Google Play و سایر بازارهای عرضه اپلیکیشن‌های موبایلی شده که البته برخی از آنها برنامه‌های مخرب هستند.
یکی از این برنامه‌ها که توسط آزمایشگاه تحلیل بدافزار پادویش بررسی شده است، برنامه Tiktok v2 و از خانواده بدافزاری GoodNews است. این برنامه که خود را نسخه جدید و رفع فیلتر شده تیک تاک برای کشور هند معرفی می‌کند، پس از اجرا به سراغ دریافت مجوزهای خطرناک زیر می‌رود:

- دسترسی به لیست مخاطبین کاربر
- مجوز ارسال پیام کوتاه
- خواندن وضعیت گوشی
- دریافت موقعیت مکانی کاربر

از آنجایی که هدف اصلی این بدافزار و یا به طور کلی هر بدافزاری، گسترش میان کاربران و قربانی کردن تعداد افراد بیشتری است، این بدافزار پیامکی به مخاطبین قربانی می‌فرستد تا این چرخه مخرب را به شکل زیر ادامه دهد:

۱. دیگر قربانیان، پیامکی که حاوی لینک آلوده دانلود است را دریافت می‌کنند.
۲. به محض کلیک روی لینک آلوده، بدافزار دانلود می‌شود.
۳. قربانیان برنامه آلوده را روی گوشی هوشمند خود نصب می‌کنند.
۴. برنامه آلوده اجرا می‌شود و مجددا روال مخربی که در بالا توضیح داده شد شروع شده و به طور گسترده‌تری ادامه پیدا می‌کند.

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.

بدترین روش برای کاهش مصرف شارژ باتری گوشی

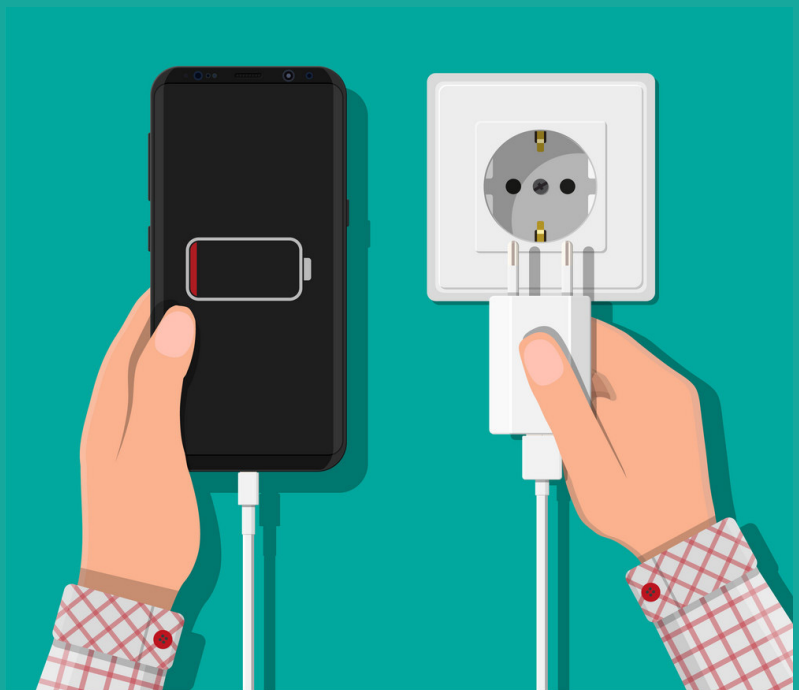
یکی از خانواده‌های بدافزاری شایع و عموماً غیرمخرب که در بازارهای اندرویدی به شکلی گسترده دیده می‌شود، خانواده تبلیغ‌افزارها هستند. سازندگان تبلیغ‌افزارهای اندرویدی، با نمایش بی‌وقفه تبلیغات و تشویق کاربران به استفاده و یا خرید محصولات نشان داده شده، سعی در ترغیب افراد بیشتری به استفاده از برنامه‌های خود و به دنبال آن کسب درآمد بیشتر هستند.

Fictus یکی از تبلیغ افزارهای غیرمخرب است که به طور خودکار تبلیغات را هنگام اجرای برنامه نمایش می‌دهد. بر خلاف بسیاری دیگر از بدافزارها که بدون اطلاع کاربر وارد سیستم شده و به نمایش تبلیغات خود می‌پردازند، Fictus با معرفی خود به عنوان ابزاری کاربردی، توسط کاربر به سیستم وارد می‌شود.

این برنامه که با نام "DU Battery Saver Pro | Power Doctor v3.9.9" در بازارهای اندرویدی مختلف وجود دارد، همان‌گونه که از نامش پیداست برای کاهش مصرف شارژ باتری گوشی افرادی که با مشکل خاموش شدن‌های پی‌درپی مواجه هستند، ارائه شده است.

اما مشکل اصلی برنامه این است که تنها در صورتی امکان استفاده از خدمات واقعی ممکن می‌شود که کاربر بر روی تبلیغات ارسال شده به گوشی خود کلیک کرده و برنامه‌های مورد نظر سازنده را نصب کند. علاوه بر این، برای نمایش تبلیغات متناسب با علایق کاربر، اطلاعات مهم کاربر از گوشی جمع آوری شده و به وب‌سایت‌های تبلیغاتی ارسال 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.



جاسوسی از کاربران به بهانه کرونا همچنان ادامه دارد

از دیگر اپلیکیشن‌هایی که با موضوع ویروس کرونا در بازارهای اندرویدی منتشر شده، برنامه‌ای با عنوان " COVID-19 Test " است. این برنامه که با هدف نمایش اطلاعات مرتبط با بیماری کووید -۱۹ عرضه شده، در حقیقت به دنبال جاسوسی از اطلاعات کاربران است.

برنامه "COVID-19 Test" از خانواده تروجان‌های جاسوسی با دسترسی از راه دور اندرویدی (RAT) است و با نام بدافزاری Ahmyth شناخته می‌شود. این گونه بدافزارها با ورود به گوشی کاربران، دسترسی های متعددی را دریافت می‌کنند.

بدافزار Ahmyth نیز با دسترسی به clipboard و سایر بخش‌های حساس، به اطلاعات مختلفی از جمله موارد زیر دست می‌یابد:

- تمام اطلاعات موجود در گوشی کاربر مانند تمام عکس‌ها، فایل‌ها، cookieها و ...
- دسترسی به تمام پیام‌های ارسالی و دریافتی کاربر به همراه محتویات (تاریخ ارسال یا دریافت پیام، متن پیام، نوع پیام)
- امکان ارسال پیام کوتاه به هر شماره دلخواه
- تهیه لیستی از گزارشات تماس (شماره تلفن، نوع تماس، تماس ورودی یا خروجی، تاریخ برقراری تماس)
- تهیه لیستی از مخاطبین گوشی (نام و شماره تلفن)
- ضبط صدا از طریق میکروفون و ذخیره آن در قالب یک فایل صوتی با نام Sound و نوع mp۳
- به دست آوردن مکان جغرافیایی کاربر (GPS)
- به دست آوردن اطلاعات کاملی در مورد اتصالات شبکه
- بررسی و به دست آوردن لیست تمام مجوزهای دریافت شده توسط برنامه
- به دست آوردن لیست کاملی از اطلاعات تمام برنامه‌های نصب شده

در نهایت این بدافزار پس از انجام عملیات مخرب خود و جمع‌آوری اطلاعات مورد نظرش در مورد قربانی، با سرور خود ارتباط برقرار کرده و اطلاعات جمع‌آوری شده را به آن ارسال می‌کند.

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.

آیا حاضرید برای استفاده از این برنامه هزینه کنید؟

برنامه‌های بالقوه ناخواسته یا PUA برنامه‌هایی هستند که به خودی خود بدافزار نیستند و ماهیت مخربی ندارند اما عموما از نظر کاربران برنامه‌هایی نامناسب و بی‌فایده تلقی می‌شوند.

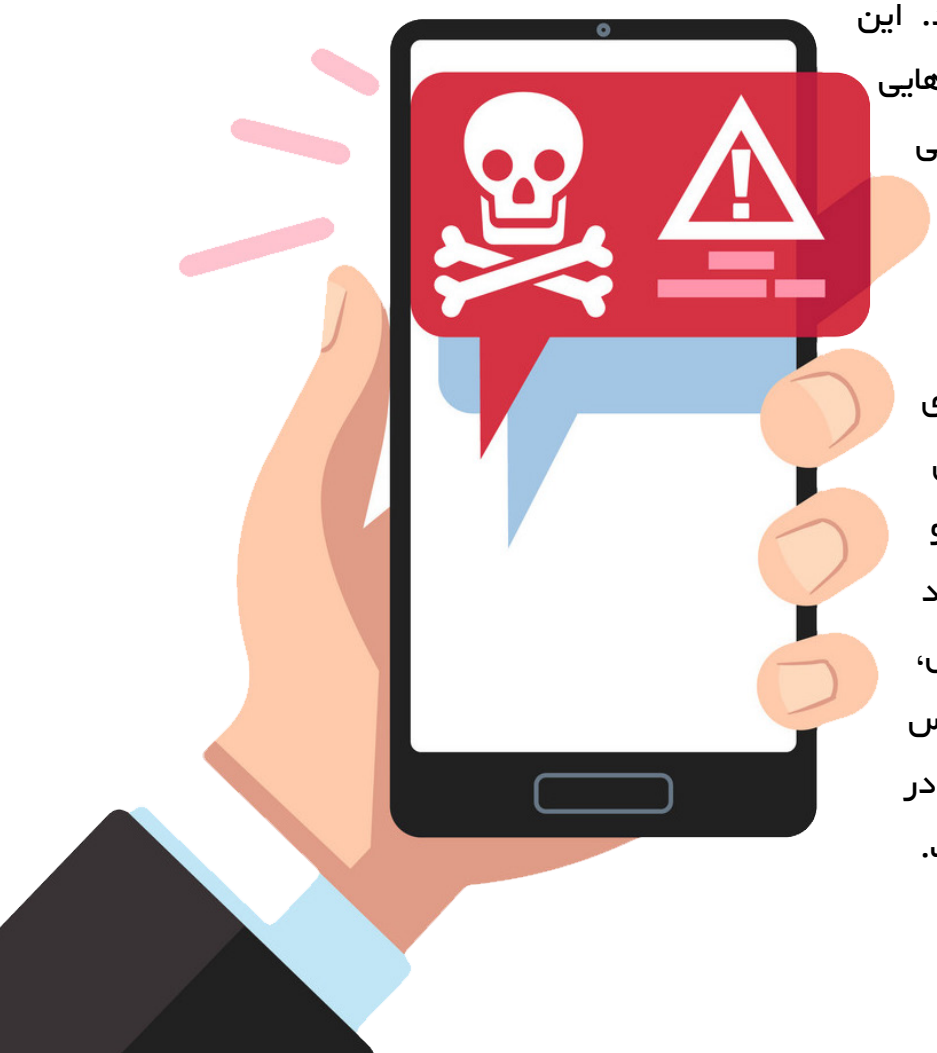
به‌طور مثال، برنامه‌های تبلیغ‌افزاری، ابزارهای کنترل از راه دور و ابزارهای دانلودر از نمونه برنامه‌هایی هستند که PUA به شمار می‌روند اما خطرناک نیستند. با این حال، برخی از این ابزارها ماهیت بدافزاری دارند و به طور مستقیم برای عملیات مخرب به کار می‌روند، مانند ابزارهای اسکن شبکه و یا ابزارهای تست نفوذ.

بررسی بازارهای موبایلی داخل، خبر از حضور گسترده ابزارهایی می‌دهد که از سرویس‌های ارزش افزوده برای کسب درآمد خود استفاده می‌کنند. این برنامه‌ها از سوی بسیاری از کاربران برنامه‌هایی مزاحم با تبلیغات فراوان و هزینه گزاف تلقی می‌شوند و از سوی برخی دیگر، برنامه‌هایی مفید و کاربردی.

یکی از خانواده‌های مشهور از برنامه‌های بالقوه ناخواسته، خانواده بدافزاری Dnotua است که شامل برنامه‌های معروفی مانند تلگرام طلایی، ایرانسل من و یا برنامه‌هایی مربوط به موضوعات پرکاربرد روز مانند آموزش بورس، نوسان‌گیر بورس، تحلیلگران بورس، بورس و بازار سهام، بورس از مبتدی تا پیشرفته و ... می‌شود که در بازارهای اندرویدی مختلف دیده شده است.

نمونه مورد بررسی در این خبر، با نام آموزش بورس منتشر شده است که بنابر شرایط فعلی جامعه و بازار بورس، در گروه برنامه‌هایی است که دانلود و استفاده زیادی دارد. این برنامه که بدون عضویت کاربر در سرویس ارزش افزوده قابل استفاده نیست، برای ارائه خدمات خود روزانه مبلغی از شارژ سیم کارت کسر می‌کند و یا اینکه تبلیغاتی درون برنامه‌ای را بدون اطلاع یا اجازه کاربر فعال می‌کند.

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.



مطالب آموزشی

۵ روش برای حفظ امنیت کودکان در فضای مجازی

از مهم‌ترین دغدغه‌های والدین در عصر حاضر، حفظ امنیت کودکان در فضای آنلاین است. سهولت دسترسی به اینترنت و استفاده گسترده از گوشی‌های هوشمند، راه را برای وقوع جرایم سایبری علیه کودکان همچون آزارهای جنسی در فضای مجازی، هموارتر کرده است.

معمولا، نظارت بر فعالیت کودکان و محافظت از آنان در برابر آسیب‌های فضای مجازی، در کامپیوتر و یا دستگاه‌های اشتراکی که قابل رصد توسط والدین هستند، ساده‌تر از گوشی‌های موبایل است. اما امروزه داشتن گوشی موبایل حتی برای کودکان زیر ۱۲ سال به امری رایج تبدیل شده و همین موضوع اهمیت آگاهی والدین از خطرات موجود در این بستر را دو چندان می‌کند.

نکاتی که در ادامه بیان می‌شود، به بالا بردن امنیت کودکان در اینترنت و شبکه‌های اجتماعی کمک خواهد کرد:

۱ – گوشی آلوده نخرید!

زمانی که برای اولین بار تصمیم به خرید گوشی موبایل و یا تبلت برای فرزندتان می‌گیرید، باید تمام جوانب را سنجیده و از خطرات آن اگاه باشید. بسیاری از خانواده‌ها گوشی کارکرده خود و یا دیگران را در اختیار فرزندانشان می‌گذارند. حتی در صورتی که تمام اطلاعات گوشی کاملا پاک شده باشد، احتمال آلوده بودن سیستم به بدافزار وجود دارد و همین موجب به دردسر افتادن فرزندتان خواهد شد.

بنابراین، بهتر است گوشی که برای فرزندتان تهیه می‌کنید از مرکز معتبری تهیه کرده باشید و در صورت استفاه از گوشی‌های کار کرده، با کمک گرفتن از کارشناسان، از نبود هرگونه آلودگی بدافزاری در سیستم مطمئن شوید.

۲ – کودکان و حملات فیشینگ

حملات فیشینگ یکی از انواع حملات سایبری شایع هستند که از میان کودکان و یا افراد کم اطلاع بیشتر قربانی می‌گیرند. لینک‌ها و سایت‌های فیشینگ معمولا مشخصه‌های شناخته شده‌ای دارند اما کودکان قادر به تشخیص آنها نیستند.

در نتیجه، لازم است که والدین نشانه‌های لینک‌های جعلی را به کودکان و نوجوانان آموزش دهند تا روی هر لینکی کلیک نکنند و یا در صورتی که فرستنده پیامی را نمی‌شناسند، آن را باز نکنند.

۳– از ورود بدافزارها به سیستم جلوگیری کنید

بسیاری اوقات کودکان به دلیل کنجکاوی برای نصب برنامه‌های مختلف و یا علاقه به بازی‌های موبایلی و کامپیوتری، برنامه‌های مختلفی را از منابع غیرمعتبر دانلود و نصب می‌کنند و سبب ورود ناخواسته بدافزارها به سیستم می‌شوند. حتما، درباره بدافزارها و خطرات آلودگی سیستم با کودکان گفتگو کنید. همچنین، نصب آنتی ویروس مطمئن و یا ابزارهای کنترل والدین، به محافظت هر چه بیشتر از گوشی کودک شما کمک خواهد کرد.

۴– سریع از کوره در نروید!

به کودکان نشان دهید که متوجه اهمیت و نقش پر رنگ تکنولوژی و اینترنت در زندگی آنها هستید. مطالعات نشان می‌دهد که در مواقع بحرانی، بسیاری از کودکان و نوجوانان به سراغ پدر و مادرشان نمی‌روند، چرا که از این واهمه دارند که درکشان نکنند و یا آنها را از استفاده از کامپیوتر و موبایلشان منع کنند.

در نتیجه، پیش از هر گونه اتفاقی، با گفتگو درباره امنیت فضای مجازی، اعتماد آنها را جلب کنید و به جای توبیخ و سرزنش در زمان بروز مشکل، با دقت به صحبت‌هایشان گوش دهید و به دنبال راهکار مناسب باشید.

۵- ارتباط با افراد در شبکه‌های اجتماعی را به کودکان آموزش دهید

به کودکان یادآوری کنید که زمانی که مطلب و یا عکسی را در فضای اینترنت به اشتراک گذاشتند، نمی‌توانند آن را به طور کامل حذف کنند. همچنین، اطلاعات شخصی مثل عکس‌های خصوصی و خانوادگی، آدرس، شماره تلفن، وضعیت مالی خانواده و یا کد ملی از اطلاعاتی هستند که باید شخصی بمانند. علاوه بر آموزش به کودکان، می‌توانید با استفاده از ابزارهای کنترل والدین (Parental control) از انتشار اطلاعات و عکس‌های خصوصی خود در اینترنت جلوگیری کنید.

در آخر همیشه به خاطر داشته باشید که محافظت حداکثری از کودکان در فضای مجازی، تنها با پیشگیری و اقدام به موقع والدین امکان‌پذیر خواهد شد.

اخبار امن پرداز

انتشار نسخه جدید آنتی ویروس پادویش

نسخه کاندیدای پایدار ضدبدافزار خانگی پادویش امنیت کامل منتشر شد.

ضدبدافزار پادویش نسخه ۲.۸.۱۱۷۸.۶۸۰۸ شامل بهبودهایی در موارد زیر است:

قدرت پویش: امکان انجام پویش چندلایه در یک مرتبه پویش.

این تغییر، منجر به قدرت تشخیص بالاتر آنتی‌ویروس در برخورد با فایل‌هایی با چندین بدافزار خواهد شد.

کنترل ابزار: در نسخه جدید پادویش خانگی، دستگاه‌های متعددی به لیست کنترل ابزار اضافه شده‌اند که شامل وب‌کم، اسکنر، دستگاه‌های قابل‌حمل، کارت شبکه داخلی، کارت شبکه خارجی، WiFi داخلی، WiFi خارجی می‌شود.

دیوار آتش: قابلیت اضافه کردن کلاینت‌ها به وسیله‌ی گروه IP به دیوار آتش پادویش و همچنین قابلیت اضافه کردن کلاینت‌ها توسط Subnet به قواعد دیوار آتش پادویش

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

مختصری درباره امن‌پرداز

شرکت نرم‌افزاری امن پرداز از سال ۱۳۸۳ فعالیت خود را آغاز نموده و به عنوان تنها 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:

سایت اتاق خبر: news.amnpardaz.com
این سایت شامل ۶ بخش و به شرح زیر است:
تهدیدها، هشدارهای امنیتی، مطالب آموزشی، اصلاحیه‌ها و آسیب‌پذیری‌ها، اخبار امن پرداز و مجله‌ها
در سایت اتاق خبر امن پرداز، آخرین اخبار مربوط به امنیت سایبری و بدافزارهای تحلیل شده توسط کارشناسان

امن پرداز را به زبانی ساده و غیر تخصصی بخوانید.

سایت تهدیدات: threats.amnpardaz.com
بانک اطلاعات تهدیدات بدافزاری پادویش حاوی اطلاعات تخصصی در خصوص بدافزارهای کشف شده و روش‌های مورد استفاده توسط این بدافزارهاست. شما می‌توانید با مراجعه به این سایت، اطلاعات لازم برای شناخت فنی از بدافزارهای کشف شده توسط پادویش را مشاهده نموده و از ابعاد فنی آنها مطلع گردید. ضمنا

سایر تولیدکنندگان محصولات امنیت اطلاعات نیز می‌توانند از این اطلاعات در جهت استفاده در محصولات یا

خدمات خود استفاده نمایند.

فروم امن پرداز: forum.amnpardaz.com
شما می‌توانید سوالات متداول مربوط به آنتی ویروس پادویش را در تالار پشتیبانی شرکت امن پرداز بیابید.

همچنین، سوالات و مشکلات خود را در اینجا مطرح کنید تا کارشناسان ما در کمترین زمان پاسخ‌گوی آنها باشند.

پایگاه دانش امن پرداز : kb.amnpardaz.com

پایگاه دانش پشتیبانی امن پرداز شامل مقالاتی تخصصی در ۵ زمینه زیر است:
ضدویروس پادویش، ضدباجگیر پادویش، ضدویروس پادویش اندروید، کنسول مدیریتی پادویش (سازمانی) و مطالب عمومی

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

تلفن: ۰۲۱-۴۳۹۱۲۰۰۰

فکس: ۰۲۱-۴۳۹۱۲۸۰۰

پیام‌رسان تلگرام: @padvishsupport

پیام‌رسان سروش: @padvishnetsupport

ایمیل پشتیبانی: support@amnpardaz.com