خبرنامه تحلیلی پادویش ■ مرداد ماه ۱۳۹۹

امنیت اطلاعات

پادویش®
Padvish®

خبرنامه تحلیلی امنیت اطلاعات،
تهیه شده توسط پادویش

امنیت اطلاعات

فهرست مطالب

مقدمه

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

در ابتدا، هشدارهای امنیتی منتشر شده از سوی پادویش را بررسی می‌کنیم. در این شماره به خبر شیوع گسترده بدافزار اموتت و فعال شدن مجدد آن پرداخته شده است؛ جزئیات منتشر شده درباره این بدافزار را در این خبرنامه بخوانید. در ادامه، تازه‌ترین تهدیدهای بدافزاری تحلیل شده از سوی آزمایشگاه پادویش در مرداد ماه را مشاهده می‌کنید. 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.

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

بازگشت مجدد بدافزار اموتت

اموتت، مخرب‌ترین و پرهزینه‌ترین بات نت/تروجان شناخته شده، پس از ۵ ماه وقفه، فعالیت مخرب خود را از سر گرفت. اموتت نوعی بدافزار است که با جاسازی در اسناد ورد و اکسل و از راه ایمیل‌های اسپم یا هرزنامه‌ها منتشر می‌شود. اسناد آلوده با به‌کارگیری ماکروها، بدافزار اموتت را در کامپیوتر قربانی دانلود و اجرا می‌کنند که با حضور اموتت یک درب پشتی فعال می‌شود و سبب نفوذ سایر بدافزارهای مخرب از جمله تروجان‌های بانکی و باج افزارها به سیستم می‌شود. علاوه بر این، از کامپیوتر آلوده برای ارسال ایمیل‌های اسپم به دیگر افراد استفاده می‌شود.

اموتت نوعی بدافزار است که با جاسازی در اسناد ورد و اکسل و از راه ایمیل‌های اسپم یا هرزنامه‌ها منتشر می‌شود.

لازم به ذکر است که کمپین جدید شکل گرفته محدود به منطقه خاصی نیست و همه کاربران را تهدید می‌کند. ایالات متحده امریکا و بریتانیا از اهداف اولیه این تهدید به شمار می‌روند اما نمونه‌هایی از آلودگی در خاورمیانه، امریکای جنوبی و آفریقا نیز مشاهده شده است. در صورتی که از آلودگی سیستم خود به بدافزار اموتت مطلع شدید، حتما شبکه‌ای که به آن متصل هستید و حساب‌های ایمیل خود را چک کنید تا از گسترش آلودگی به سایر سیستم‌ها جلوگیری کنید.

راهکارهایی برای پیشگیری از ورود بدافزار اموتت و سایر بدافزارهای ایمیلی به سیستم:

• به ایمیل‌هایی دریافتی خود حساسیت بیشتری نشان دهید. به طور مثال، ایمیلی که از یک دوست اما با عنوان صورتحساب (یا هر عنوان نامرتبط دیگری) دریافت می‌کنید، مشکوک است و می‌تواند نمونه‌ای از ایمیل‌های آلوده به بدافزار باشد.

• در صورتی که سند ورد دریافتی از ایمیل بدون فعال کردن ماکرو برایتان باز نمی‌شود، به آلوده بودن آن شک کنید و به هیچ عنوان ماکرو را فعال نکنید.

• یکی از بهترین روش‌ها برای اطمینان از سالم بودن فایل ورد دریافتی، باز کردن آن به وسیله Google Docs است، چرا که از نصب هرگونه بدافزار بر روی سیستم کاربر جلوگیری می‌کند.

• از کلیک بر روی لینک‌های مشکوک درون ایمیل خودداری و فایل‌های ضمیمه را قبل از اجرا، حتما توسط آنتی ویروس پویش کنید.

تهدیدها

اپلیکیشن عرضه اینترنت رایگان

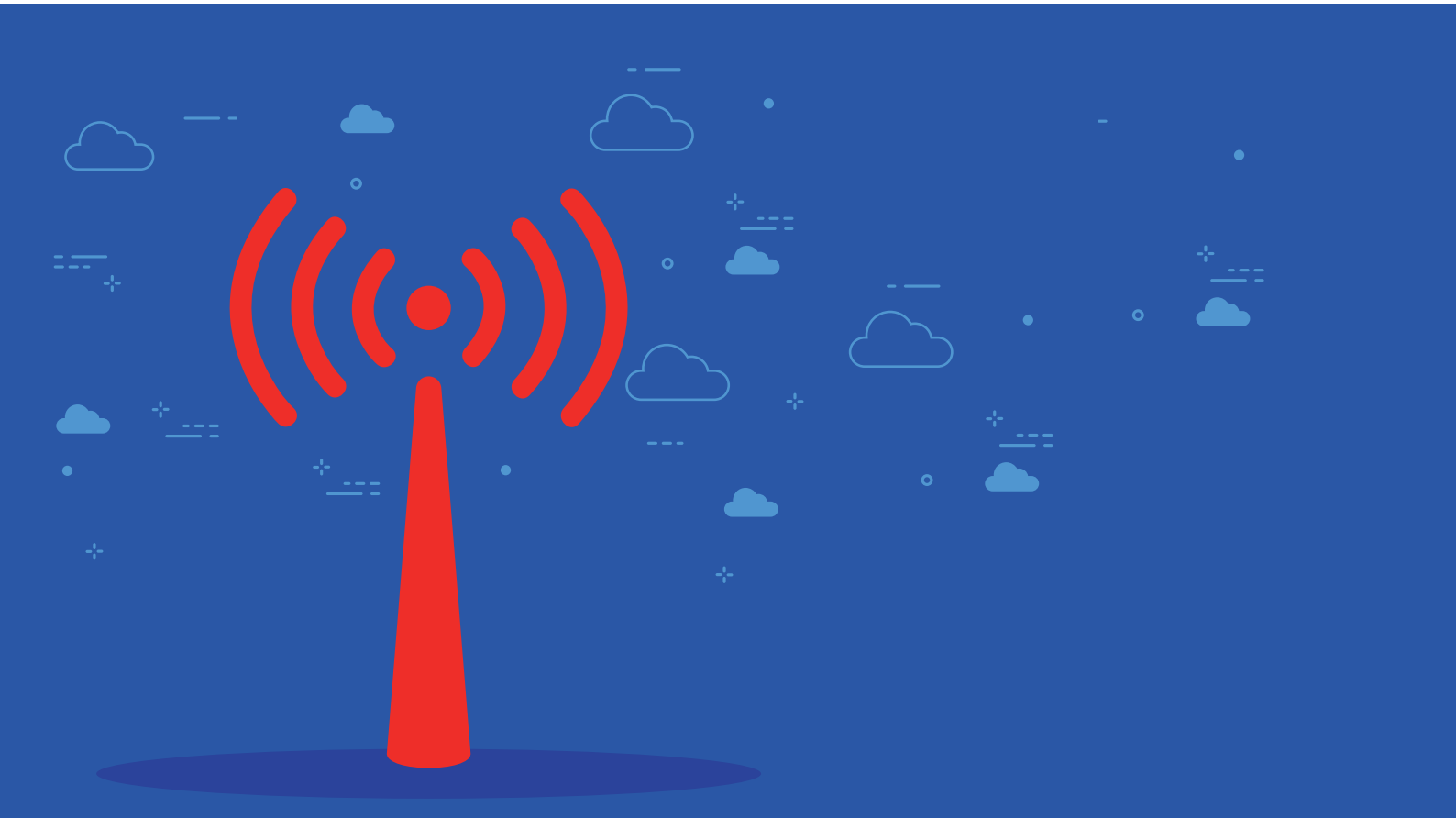
تروجان‌ها از جمله برنامه‌هایی هستند که با ظاهری قانونی وارد سیستم کاربر می‌شوند، اما به هنگام اجرا ماهیت بدافزاری خود را بروز داده و به خرابی سیستم می‌پردازند. یکی از معروف‌ترین انواع این برنامه‌ها، اپلیکیشن‌هایی هستند که با وعده اینترنت رایگان، کاربران بسیاری را فریب می‌دهند و از اطلاعات شخصی آنها سوءاستفاده می‌کنند. تبلیغات این برنامه‌ها در پیام رسان‌ها و شبکه‌های اجتماعی به فراوانی به چشم می‌خورند و با وعده اینترنت و شارژ رایگان، افراد را وسوسه می‌کنند.

> **یکی از معروف‌ترین انواع این برنامه‌ها، اپلیکیشن‌هایی هستند که با وعده اینترنت رایگان، کاربران بسیاری را فریب می‌دهند و از اطلاعات شخصی آنها سوءاستفاده می‌کنند.**

یکی از انواع این بدافزارها، خانواده بدافزاری Anubis است که با عناوین مختلفی مانند 5G Free ،۲۰GBHediye ،۲۰gb_hediye_ internet و ... وجود دارد. نمونه‌ای که توسط آزمایشگاه تحلیل بدافزار پادویش بررسی شده‌است، با عنوان "۲۰ گیگ هدیه اینترنت" تبلیغ می‌شود. با دانلود و نصب این برنامه، بدافزار با نمایش پیام‌هایی به زبان ترکی، دسترسی‌های متعددی را از کاربر درخواست می‌کند تا به راحتی تمامی رفتارهای او را زیر نظر داشته باشد. سپس آیکون خود را مخفی می‌کند و به جمع‌آوری اطلاعات کاربر و ایجاد تغییرات مورد نظر خود می‌پردازد. قسمت‌هایی که تحت کنترل برنامه قرار می‌گیرند، شامل موارد زیر هستند:

- به دست آوردن موقعیت مکانی کاربر، وضعیت اینترنت، خواندن لیست مخاطبین، خواندن پیام‌های ورودی و خروجی، ضبط صدا، ارسال و نوشتن پیام
- امکان ارسال و دریافت پیام کوتاه
- یافتن مختصات جغرافیایی کاربر (GPS)
- دانلود فایل‌های apk دیگر که برای نمایش تبلیغات در گوشی کاربر انجام می‌شود.
- امکان گرفتن Screenshot از صفحه کلید کاربر

آنتی ویروس پادویش، این بدافزار را شناسایی و از سیستم شما محافظت می‌کند.



بدافزار آموزش قانون

به گزارش آزمایشگاه تحلیل بدافزار پادویش، برنامه اندرویدی "قانون به زبان ساده" از سرویس‌های تبلیغاتی برای نمایش اعلان و لینک‌های تبلیغاتی با موضوعات مختلف و به شکلی آزاردهنده استفاده می‌کند. همچنین، از لینک سایت‌های فیلتر شده در این تبلیغات استفاده می‌شود. نکته مهم در عملکرد این برنامه، دسترسی به اطلاعات متعدد و مهمی از کاربر مانند اطلاعات اپراتور سیم کارت، شناسه منحصر به فرد گوشی و موقعیت جغرافیایی کاربر می‌باشد. این برنامه و برنامه‌هایی از این نوع، به عنوان برنامه‌های بالقوه ناخواسته (Potentially Unwanted Application) دسته‌بندی می‌شوند. در اینجا این سوال مطرح می‌شود که آیا برنامه قانون به زبان ساده بدافزار است یا خیر؟ برنامه‌های بالقوه ناخواسته ویژگی‌ها و رفتارهایی از خود بروز می‌دهند که ممکن است از نظر کاربر خوشایند نباشد ولی برای اینکه برنامه‌ای در این گروه قرار بگیرد، لازم است حداقل یکی از موارد زیر درباره آن صدق کند:

> **به طور کلی برنامه‌های بالقوه ناخواسته احتمال آلودگی سیستم به بدافزارهای حقیقی را بالا می‌برند، کشف بدافزار بر روی سیستم را دشوارتر می‌کنند و یا به هزینه‌های پاک‌سازی سیستم اضافه می‌کنند.**

- برنامه حریم خصوصی و یا عملکرد کاربر را محدود کند. برای مثال اطلاعات شخصی کاربر را فاش کند و یا اقداماتی غیر مجاز انجام دهد.
- فشاری بی‌مورد بر منابع سیستم وارد کند. برای مثال بیش از اندازه از حافظه و ذخایر سیستم استفاده شود.
- امنیت دستگاه و یا اطلاعات ذخیره شده بر روی آن را در معرض تهدید قرار دهد. برای مثال محتوا یا برنامه‌های غیر منتظره به کاربر نمایش داده شود.

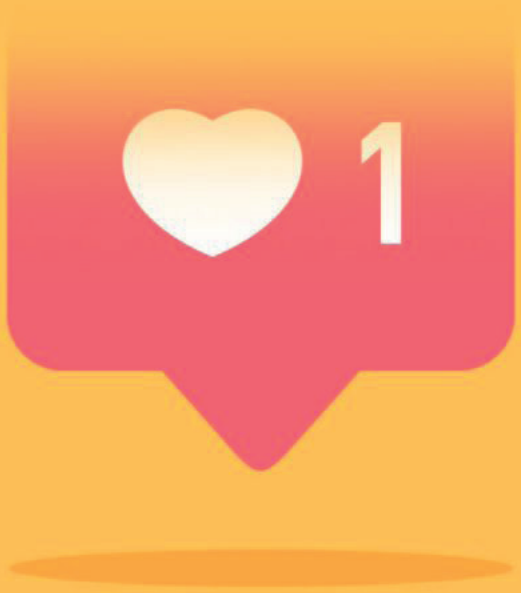
تاثیر این نوع از برنامه‌ها در محدوده گسترده‌ای از متوسط تا شدید قرار می‌گیرد اما معمولا خطر آنها به اندازه‌ای نیست که به عنوان بدافزار تلقی شوند. به طور کلی برنامه‌های بالقوه ناخواسته احتمال آلودگی سیستم به بدافزارهای حقیقی را بالا می‌برند، کشف بدافزار بر روی سیستم را دشوارتر می‌کنند و یا به هزینه‌های پاک‌سازی سیستم اضافه می‌کنند. در نهایت در برخورد با این نوع برنامه‌ها، خود کاربر تعیین می‌کند که با نحوه عملکرد برنامه مشکلی ندارد و یا اینکه نیاز به مسدود کردن دسترسی‌های برنامه و پاک‌سازی آن از سیستم دارد. این برنامه توسط آنتی ویروس پادویش، شناسایی می‌شود.

بدافزار آموزش هک

یکی از ابزارهایی که نقش بسزایی در انتشار آلودگی‌های بدافزاری موبایلی ایفا می‌کنند، ابزارهای RiskTool هستند. اما جالب است بدانید که این ابزارها در دسته بدافزارها قرار نمی‌گیرند و تنها به دلیل سوءاستفاده هکرها و برای تحقق اهداف خرابکارانه آنها به کار گرفته می‌شوند. بنابراین ممکن است در ظاهر، کاربر مشکلی با حضور RiskTool بر روی گوشی خود نداشته باشد اما برنامه در پس زمینه برای انجام اهدافی مخرب در حال فعالیت باشد. در نهایت نتیجه‌ای که معمولا کاربر با آن روبرو می‌شود، کندی سیستم و یا افزایش حجم اینترنت مصرفی خواهد بود. RiskToolها اغلب جزو برنامه‌های تبلیغ افزار هستند که از محبوب‌ترین ابزارهای حمله مهاجمان به تلفن‌های همراه محسوب می‌شوند.

ادامه فعالیت این برنامه وابسته به نصب بودن برنامه کافه بازار بر روی سیستم کاربر دارد و هر زمان که کافه بازار از گوشی حذف شود یا ارتباط بدافزار با برنامه قطع شود، به کاربر پیام هشداری نمایش داده می‌شود تا سیستم را به حالت اولیه برگرداند.

به گزارش آزمایشگاه تحلیل بدافزار پادویش، بدافزار Dnotua که از خانواده RiskToolها است، در قالب بدافزارهای فارسی مشاهده شده است. این برنامه با نام‌های مختلفی از جمله با نام برنامه‌های مستهجن، برنامه‌های معروفی مانند اینستاگرام، تلگرام طلایی، ایرانسل من و ... منتشر شده است. نمونه خاصی که در اینجا بررسی شده، با عنوان آموزش کامل هک و در مارکت‌های اندرودی مشاهده شده است. درآمد این بدافزار از راه تبلیغات درون برنامه‌ای و بدون اطلاع یا اجازه کاربر تامین می‌شود. برنامه برای رسیدن به هدف نمایش تبلیغات، بایستی به اطلاعات سیم کارت و گوشی دسترسی داشته باشد تا تبیلغاتی متناسب با کاربر ارسال و کسب درآمد کند. علاوه بر این، به کاربر پیشنهاد می‌شود تا برای حذف کامل تبلیغات، مبلغی را به برنامه پرداخت کند. ادامه فعالیت این برنامه وابسته به نصب بودن برنامه کافه بازار بر روی سیستم کاربر دارد و هر زمان که کافه بازار از گوشی حذف شود یا ارتباط بدافزار با برنامه قطع شود، به کاربر پیام هشداری نمایش داده می‌شود تا سیستم را به حالت اولیه برگرداند. آنتی ویروس پادویش، این بدافزار را شناسایی و از سیستم شما محافظت می‌کند.



جاسوس افزار اینستاگرامی

کاربران اینستاگرام به دنبال جذب لایک و فالوور بیشتر هستند و در علم روانشناسی ثابت شده است که نیاز به دریافت لایک و فالوور می‌تواند به نوعی اعتیادآور باشد. این نیاز کاربران سبب طراحی اپلیکیشن‌های بسیاری شده است که روشی میان‌بر برای رسیدن به این هدف ارائه می‌دهند. محبوبیت بیشتر و دیده شدن در اینستاگرام، به‌ویژه برای کاربرانی که مدت زمان کوتاهی است که به عضویت این شبکه اجتماعی پیوسته‌اند، مدت زمان زیادی را می‌طلبد. بنابراین، بسیاری از کاربران از طریق مارکت‌های مختلف، چنین برنامه‌هایی را برای دستیابی به نتیجه مطلوب در کوتاه‌ترین زمان ممکن نصب و استفاده می‌کنند. اما برنامه‌هایی که برای افزایش لایک و فالوور نصب می‌شوند، نام کاربری و رمز عبور کاربران را درخواست می‌کنند و معمولا از این اطلاعات برای اهداف شخصی خود بهره می‌برند. در حقیقت، بسیاری از برنامه‌هایی که به عنوان ابزارهای کمکی اینستاگرام معرفی می‌شوند، بدافزار هستند و اطلاعات شخصی کاربران را به سرقت برده و افشا می‌کنند. کشورمان ایران، از اصلی‌ترین مناطق هدف سازندگان بدافزارهای اینستاگرامی به شمار می‌رود.

> **از نسخه‌های غیررسمی برنامه‌ها استفاده نکنید. برنامه‌هایی مانند تلگرام و اینستاگرام نسخه‌های غیررسمی زیادی دارند و بیشتر آنها از طریق کانال‌های تلگرامی انتشار می‌یابند.**

در مطالب قبلی، به تحلیل و بررسی یکی از این برنامه‌ها به نام FakeGram پرداختیم و در این مطلب به تحلیل برنامه اندرویدی FollowerInstagram می‌پردازیم. به گزارش آزمایشگاه تحلیل بدافزار پادویش، این بدافزار با اتصال از راه دور و از طریق سرور مخرب خود، به هر دستگاه اندرویدی که بدافزار بر روی آن نصب است دسترسی پیدا می‌کند. همچنین، قسمت‌های مختلفی از گوشی کاربر را رصد می‌کند که شامل پیام‌ها و لیست مخاطبان، گوش دادن به مکالمات قربانی، ضبط صدا، کنترل دوربین، دریافت دسترسی ادمین و امکان برقراری تماس در گوشی قربانی می‌شوند. این برنامه، با استفاده از مجوزهایی که به هنگام نصب دریافت می‌کند، حذف خود توسط کاربر را عملا غیر ممکن می‌کند. FollowerInstagram از خانواده جاسوس افزارهاست و به بخش‌های مختلف سیستم دسترسی پیدا می‌کند تا تمامی اطلاعات حساس کاربر و مورد نیاز بدافزار را جمع‌آوری کند. آنتی ویروس پادویش، این بدافزار را شناسایی و از سیستم شما محافظت می‌کند.

مراقب بدافزارهای اندرویدی مذهبی در ماه محرم باشید

بدافزارنویسان همواره به دنبال فرصتی هستند تا به فراخور شرایط، محصولات جدیدی منتشر و افراد بیشتری را در دام خود گرفتار کنند. با نزدیک شدن به ماه محرم و اقبال عمومی از برنامه‌های اندرویدی مذهبی با موضاعاتی همچون عزاداری و نوحه سرایی، بدافزارهای متعددی با این موضوع در بازارهای اندرویدی ایرانی مشاهده شده است. با توجه به شیوع ویروس کرونا و لغو شدن اکثر مراسم‌های حضوری امسال، کلیپ‌های عزاداری و برنامه‌های مذهبی به طور گسترده‌ای در کانال‌ها و گروه‌های فضای مجازی بین افراد رد و بدل می‌شوند. از آنجایی که خطر شیوع گسترده فایل‌های بدافزاری در قالب‌های گوناگون کاربران را تهدید می‌کند، هوشیاری و توجه بیشتر افراد به رعایت نکات امنیتی در فضای مجازی مورد نیاز است.

با دانلود و اجرای این بدافزار بر روی گوشی کاربر، تمامی فایل‌هایی که در قسمت‌های مختلف وجود دارند رمزگذاری و صفحه نمایش نیز قفل می‌شود.

به گزارش آزمایشگاه تحلیل بدافزار پادویش، برنامه اندرویدی نوای محرم و مداحی عاشورا یکی از بدافزارهای مذهبی و از خانواده تبلیغ‌افزارهاست که در روزهای گذشته و در بازارهای اندرویدی مشاهده شده است. این بدافزار، عضو خانواده‌ای به نام Notifyer بوده و با استفاده از سرویس‌های ارسال اعلان به کاربران، اعلان‌های تبلیغاتی نمایش می‌دهد. بنابراین، عمده فعالیت این بدافزار، نمایش تبلیغات با موضوعات مختلف و در اکثر مواقع آزاردهنده و مخرب است. اما با دانلود و نصب این برنامه، علاوه بر مواجه شدن با حجم انبوهی از اعلان‌های تبلیغاتی، دسترسی‌های متعددی از بخش‌های مختلف گوشی به بدافزارنویس داده می‌شود که مهم‌ترین آنها عبارت‌اند از:

- لیست کامل تماس‌های گوشی کاربر بر اساس مشخصات آنها (شماره، ID، مدت زمان مکالمه، اسم، روز و...)
- لیست مخاطبین و تمام شماره‌های تلفن مخاطبین
- در صورت وجود، عکس پیوست شده برای هر مخاطب در گوشی کاربر
- آدرس‌های ایمیل مخاطبین کاربر
- لیست ایمیل‌های دریافتی و یا ارسالی کاربر

آنتی ویروس پادویش، این بدافزار را شناسایی و از سیستم شما محافظت می‌کند.

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